

**ANALISA DAN PERBANDINGAN BUKTI FORENSIK APLIKASI
MEDIA SOSIAL FACEBOOK DAN TWITTER PADA SMARTPHONE
ANDROID**

SKRIPSI



Oleh :

WISNU ARI MUKTI

1112091000029

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SYARIF HIDAYATULLAH
JAKARTA**

2017

**ANALISA DAN PERBANDINGAN BUKTI FORENSIK APLIKASI
MEDIA SOSIAL FACEBOOK DAN TWITTER PADA SMARTPHONE
ANDROID**

SKRIPSI

Sebagai Salah Satu Syarat untuk
Memperoleh Gelar Sarjana Komputer (S.Kom)



Oleh :

WISNU ARI MUKTI

1112091000029

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SYARIF HIDAYATULLAH
JAKARTA
2017**

LEMBAR PERSETUJUAN

ANALISA DAN PERBANDINGAN BUKTI FORENSIK APLIKASI
MEDIA SOSIAL FACEBOOK DAN TWITTER PADA SMARTPHONE
ANDROID

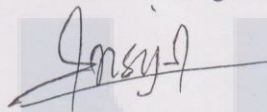
Skripsi
Sebagai Salah Satu Syarat Untuk Memperoleh Gelar
Sarjana Komputer
Fakultas Sains dan Teknologi
Universitas Islam Negeri Syarif Hidayatullah Jakarta

Oleh :
WISNU ARI MUKTI

1112091000029

Menyetujui,

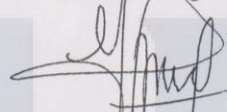
Pembimbing I



Siti Ummi Masruroh, M.Sc

NIP. 19820823 201101 2 013

Pembimbing II

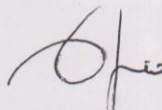


Dewi Khairani, M.Sc

NIP. 19820522 201101 2 009

Mengetahui,

Ketua Prodi Teknik Informatika,



Arini, MT

NIP. 19760131 200901 2 001

LEMBAR PENGESAHAN

Skripsi yang berjudul “ANALISA DAN PERBANDINGAN BUKTI FORENSIK APLIKASI MEDIA SOSIAL FACEBOOK DAN TWITTER PADA SMARTPHONE ANDROID” telah diujikan dalam sidang munaqasyah Fakultas Sains dan Teknologi UIN Syarif Hidayatullah Jakarta pada Desember 2016, skripsi ini telah diterima sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer (S.Kom) pada Program Studi Teknik Informatika.

Jakarta, 18 Januari 2017

Tim Penguji,

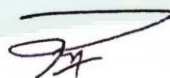
Penguji I



Victor Amrizal, M.Kom

NIP. 19740624 200710 1 001

Penguji II

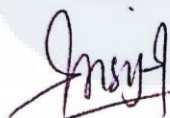


Rizal Bahaweres, M.Kom

NIP. 19710806 201411 1 001

Tim Pembimbing,

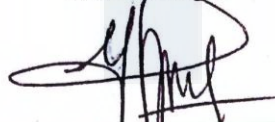
Pembimbing I



Siti Umami Masruroh, M.Sc

NIP. 19820823 201101 2 013

Pembimbing II



Dewi Khairani, M.Sc

NIP. 19820522 201101 2 009

Mengetahui,

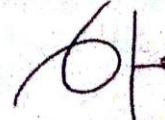
Dekan Fakultas Sains dan Teknologi,



Dr. Agus Salim, M.Si

NIP. 19720816 199903 1 003

Ketua Prodi Teknik Informatika,



Arini, MT

NIP. 19760131 200901 2 001

PERNYATAAN ORISINILITAS

Dengan ini saya menyatakan bahwa :

1. Skripsi ini merupakan hasil karya asli saya yang diajukan untuk memenuhi salah satu persyaratan memperoleh gelar Strata 1 di UIN Syarif Hidayatullah Jakarta
2. Semua sumber yang saya gunakan dalam penulisan ini telah saya cantumkan sesuai dengan ketentuan yang berlaku di UIN Syarif Hidayatullah Jakarta
3. Apabila di kemudian hari terbukti karya ini bukan hasil karya asli saya atau merupakan hasil jiplakan karya orang lain, maka saya bersedia menerima sanksi yang berlaku di UIN Syarif Hidayatullah Jakarta

Jakarta, 18 Januari 2017

Wisnu Ari Mukti

PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI

Sebagai civitas akademik UIN Syarif Hidayatullah Jakarta, saya yang bertanda tangan di bawah ini :

Nama : Wisnu Ari Mukti

NIM : 1112091000029

Program Studi : Teknik Informatika

Fakultas : Sains dan Teknologi

Jenis Karya : Skripsi

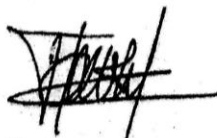
demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Islam Negeri Syarif Hidayatullah Jakarta Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul :

Analisa dan Perbandingan Bukti Forensik Aplikasi Media Sosial Facebook dan Twitter pada Smartphone Android

beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Islam Negeri Syarif Hidayatullah Jakarta berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta. Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 18 Januari 2017

Wisnu Ari Mukti



Wisnu

(.....)

Wisnu Ari Mukti 1112091000029, Analisa dan Perbandingan Bukti Forensik Aplikasi Media Sosial Facebook dan Twitter pada *Smartphone* Android. Skripsi. Jakarta: Fakultas Sains dan Teknologi, Universitas Islam Negeri Syarif Hidayatullah, 2017.

ABSTRAK

Perkembangan teknologi internet dan *smartphone* yang semakin pesat diikuti pula oleh meningkatnya pengguna media sosial yang mengakses menggunakan *smartphone* khususnya Android. Salah satu permasalahan yang tak luput dari media sosial adalah tindak kejahatan dunia maya yang memanfaatkan media sosial. Berdasarkan data statistik dari Instant Checkmate pada tahun 2013, 81% kejahatan internet (*cyber crime*) melibatkan media sosial. 39% pengguna media sosial telah menjadi korban penipuan, *hacking* dan *fake link*. Dan 33% semua kejahatan seks pada dunia maya dipicu melalui situs jejaring sosial. Sehingga diperlukan digital forensik untuk mencari bukti-bukti kejahatan tersebut. karena pada dasarnya tidak ada kejahatan yang tidak meninggalkan jejak. Penelitian ini dilakukan untuk menemukan dan membandingkan bukti-bukti forensik tersebut pada aplikasi media sosial Facebook dan Twitter yang diakses pada *smartphone* Android. Facebook dan Twitter dipilih karena memiliki beberapa fitur yang mirip. Pada penelitian ini, metode simulasi digunakan dalam penelitian dengan menjalankan 11 skenario diantaranya adalah pengembalian file yang dihapus, pencarian bukti forensik berupa nama akun, lokasi, nomor telpon, tanggal lahir, *photo profile*, *cover photo*, *posting* berupa teks, *posting* berupa gambar, isi *private message* berupa teks dan isi *private message* berupa gambar. Hasil dari penelitian ini menunjukkan bahwa semua bukti forensik pada aplikasi media sosial Facebook berhasil ditemukan semua. Sedangkan pada aplikasi media sosial Twitter hanya berhasil ditemukan berupa nama akun, data lokasi, *photo profile*, *cover photo*, *posting* berupa teks dan *posting* berupa gambar.

Kata Kunci : Digital Forensik, Bukti Forensik, *Smartphone*, Facebook, Twitter.

Jumlah Pustaka : 23 (Tahun 2007-2016)

Jumlah Halaman : VI BAB + xviii Halaman + 94 Halaman + 51 Gambar + 26 Tabel + 23 Daftar Pustaka

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Allah SWT atas segala rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan penelitian hingga akhir penulisan skripsi. Penulis mengucapkan terima kasih kepada:

1. Bapak Dr. Agus Salim, M.Si., selaku Dekan Fakultas Sains dan Teknologi;
2. Ibu Arini, ST. MT., selaku ketua Program Studi Teknik Informatika, serta Bapak Feri Fahrianto, M.Sc. selaku sekretaris Program Studi Teknik Informatika;
3. Siti Ummi Masruroh, M.Sc., selaku Dosen Pembimbing I dan Dewi Khairani, M.Sc., selaku Dosen Pembimbing II, penulis ucapkan terima kasih tak terhingga atas kesediaan waktu dan pikiran dalam membimbing, memberikan saran dan selalu memberikan dorongan semangat kepada penulis dari awal hingga akhir penelitian dan penulisan skripsi;
4. Rizal Broer Bahaweres, M.Kom., selaku penasihat akademis, terima kasih atas bimbingan dan arahan selama masa perkuliahan;
5. Seluruh Dosen, Staf Karyawan Fakultas Sains dan Teknologi, khususnya Program Studi Teknik Informatika, terima kasih atas ilmu, pengalaman, dan bantuan yang telah diberikan kepada penulis selama masa perkuliahan;
6. Orang tua penulis, yaitu Ayah Yatino dan Ibu Tarmi, serta kedua adik penulis, Febriyanti Puspa Rini dan Tribuana Puspa Dewi, penulis ucapkan terima kasih yang tak terbatas atas kasih sayang, doa, pengertian, bimbingan, semangat, dan dorongan yang diberikan baik moril maupun materiil selama ini, sehingga penulis dapat menyelesaikan skripsi;
7. Sahabat penulis, khususnya sahabat Core iC : Ahmad Akmaludin, Mohamad Rizal, Rahmat Fajar Alfarizky, Muhammad Irsal Yudanto, Aulia Rahman Andaf, Perdana Priatna, Muhammad Fachri Fadly, Rangga Arif Rahman, Alvin Fauzi Murod, Fachrudin Arrahji, Untung Tri Pamungkas dan Nurul Fikri, Serta sahabat Relawan : Khalid Faruqi, Didik

Pratama Saputra, Muhammad Ashari dan Putra Hadi Kamil. Terimakasih atas kesediaannya menciptakan momen-momen berharga bersama, saling menemani, menyemangati, dan saling mengingatkan baik dalam urusan akademik maupun non akademik; Teman-teman seangkatan dan seperjuangan TI UIN 2012, terima kasih atas semua kenangan yang telah diciptakan bersama selama perkuliahan dan tetap semangat.

8. Seluruh pihak HIMTI UIN Jakarta, baik adik-adik angkatan dan senior-senior angkatan terima kasih atas dorongan semangat dan do'a yang diberikan, serta ilmu-ilmu baik akademik maupun non-akademik yang disalurkan;

Penulis mohon maaf atas segala kekurangan dan salah kata bagi semua pihak. Skripsi ini masih jauh dari sempurna, namun penulis berharap skripsi ini dapat bermanfaat bagi penulis, pembaca, dan perkembangan ilmu pengetahuan.

Jakarta, 2017

Penulis

DAFTAR ISI

| | |
|---|--------------|
| LEMBAR PERSETUJUAN | iii |
| LEMBAR PENGESAHAN | iv |
| PERNYATAAN ORISINILITAS | v |
| PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI | vi |
| ABSTRAK | vii |
| KATA PENGANTAR..... | viii |
| DAFTAR ISI..... | x |
| DAFTAR GAMBAR..... | xv |
| DAFTAR TABEL | xviii |
| 1. BAB I PENDAHULUAN | 1 |
| 1.1 Latar Belakang | 1 |
| 1.2 Rumusan Masalah..... | 5 |
| 1.3 Batasan Masalah | 5 |
| 1.4 Tujuan | 6 |
| 1.5 Manfaat | 6 |
| 1.6 Metodologi Penelitian | 7 |
| 1.7 Sistematika Penulisan | 8 |
| 2. BAB II LANDASAN TEORI..... | 10 |
| 2.1 Forensik Digital | 10 |
| 2.1.1 Penjelasan | 10 |
| 2.1.2 Data Forensik | 10 |
| 2.1.3 Objek Forensik..... | 11 |
| 2.1.4 Kejahatan Komputer | 11 |
| 2.2 Mobile Forensic | 12 |
| 2.2.1 Collection | 13 |
| 2.2.2 Identification | 13 |
| 2.2.3 Acquisition | 14 |

| | | |
|-------------|---|----|
| 2.3 | File | 14 |
| 2.4 | Recovery | 14 |
| 2.5 | Android | 14 |
| 2.5.1 | <i>File System</i> pada Android | 15 |
| 2.5.2 | Struktur <i>File System</i> Android..... | 15 |
| 2.5.3 | <i>Rooting</i> pada Perangkat Android | 15 |
| 2.6 | Smartphone | 15 |
| 2.7 | Media Sosial | 16 |
| 2.8 | Facebook | 16 |
| 2.9 | Twitter | 17 |
| 2.10 | SQLite | 18 |
| 2.10.1 | Penjelasan umum | 18 |
| 2.10.2 | Fitur..... | 18 |
| 2.11 | SQLite Manager | 19 |
| 2.12 | Metode Simulasi | 20 |
| 2.12.1 | Problem Formulation | 20 |
| 2.12.2 | Conceptual Model..... | 20 |
| 2.12.3 | Input / Output Data | 21 |
| 2.12.4 | Modeling | 21 |
| 2.12.5 | Simulation | 22 |
| 2.12.6 | Verification and Validation..... | 22 |
| 2.12.7 | Experimentation | 22 |
| 2.12.8 | Output Analysis | 23 |
| 2.13 | Kelebihan Metode Simulasi | 23 |
| 3. | BAB III METODOLOGI PENELITIAN | 24 |
| 3.1 | Metode Pengumpulan Data | 24 |
| 3.1.1 | Data Primer | 24 |
| 3.1.2 | Data Sekunder | 24 |

| | | |
|------------|--|-----------|
| 3.2 | Metode Simulasi | 27 |
| 3.2.1 | Problem Formulation | 28 |
| 3.2.2 | Conceptual Model | 28 |
| 3.2.3 | Input and Output Data..... | 28 |
| 3.2.4 | Modeling | 28 |
| 3.2.5 | Simulation | 28 |
| 3.2.6 | Verification and Validation..... | 29 |
| 3.2.7 | Experimentation | 29 |
| 3.2.8 | Output Analysis | 29 |
| 3.3 | Kerangka Berpikir | 29 |
| 4. | BAB IV IMPLEMENTASI SIMULASI DAN EKSPERIMEN | 31 |
| 4.1 | <i>Problem Formulation</i> | 31 |
| 4.2 | <i>Conceptual Model</i>..... | 33 |
| 4.2.1 | <i>Smartphone</i> | 34 |
| 4.2.2 | Aplikasi media sosial | 35 |
| 4.2.3 | Aplikasi <i>recovery file</i> | 35 |
| 4.2.4 | Aplikasi <i>Database Browser</i> | 35 |
| 4.2.5 | Akun Palsu Media Sosial | 35 |
| 4.2.6 | <i>Output/Bukti forensik yang ditemukan</i> | 36 |
| 4.3 | <i>Input Output Data</i> | 36 |
| 4.3.1 | <i>Input</i> | 36 |
| 4.3.2 | <i>Output</i> | 37 |
| 4.4 | <i>Modeling</i> | 37 |
| 4.4.1 | Skenario 1 | 37 |
| 4.4.2 | Skenario 2 | 38 |
| 4.4.3 | Skenario 3 | 38 |
| 4.4.4 | Skenario 4 | 38 |
| 4.4.5 | Skenario 5 | 39 |

| | | |
|------------|---|-----------|
| 4.4.6 | Skenario 6 | 39 |
| 4.4.7 | Skenario 7 | 39 |
| 4.4.8 | Skenario 8 | 39 |
| 4.4.9 | Skenario 9 | 40 |
| 4.4.10 | Skenario 10 | 40 |
| 4.4.11 | Skenario 11 | 40 |
| 4.5 | <i>Simulation</i> | 41 |
| 4.5.1 | <i>Rooting</i> pada Perangkat Android | 41 |
| 4.5.2 | Pembuatan Akun Palsu pada Media Sosial | 41 |
| 4.5.3 | Pemasangan Aplikasi <i>Recovery File</i> | 42 |
| 4.5.4 | Pemasangan Aplikasi SQLite Manager | 43 |
| 4.5.5 | <i>Flowchart</i> Simulasi | 43 |
| 4.6 | <i>Verification and Validation</i> | 45 |
| 4.7 | <i>Experimentation</i> | 45 |
| 4.8 | <i>Output Analisis</i> | 45 |
| 5. | BAB V HASIL DAN PEMBAHASAN | 46 |
| 5.1 | <i>Verification & Validation</i> | 46 |
| 5.2 | <i>Experimentation</i> | 46 |
| 5.3 | <i>Output Analysis</i> | 47 |
| 5.3.1 | Hasil Simulasi Skenario 1 | 47 |
| 5.3.2 | Hasil Simulasi Skenario 2 | 48 |
| 5.3.3 | Hasil Simulasi Skenario 3 | 50 |
| 5.3.4 | Hasil Simulasi Skenario 4 | 53 |
| 5.3.5 | Hasil Simulasi Skenario 5 | 56 |
| 5.3.6 | Hasil Simulasi Skenario 6 | 57 |
| 5.3.7 | Hasil Simulasi Skenario 7 | 61 |
| 5.3.8 | Hasil Simulasi Skenario 8 | 64 |
| 5.3.9 | Hasil Simulasi Skenario 9 | 67 |

| | | |
|-----------------------|--|-----------|
| 5.3.10 | Hasil Simulasi Skenario 10 | 71 |
| 5.3.11 | Hasil Simulasi Skenario 11 | 73 |
| 5.4 | <i>Output Analisis Hasil Pencarian Bukti Forensik</i> | 76 |
| 5.4.1 | <i>Output Analisis Skenario 1</i> | 76 |
| 5.4.2 | <i>Output Analisis Skenario 2</i> | 77 |
| 5.4.3 | <i>Output Analisis Skenario 3</i> | 78 |
| 5.4.4 | <i>Output Analisis Skenario 4</i> | 79 |
| 5.4.5 | <i>Output Analisis Skenario 5</i> | 80 |
| 5.4.6 | <i>Output Analisis Skenario 6</i> | 80 |
| 5.4.7 | <i>Output Analisis Skenario 7</i> | 82 |
| 5.4.8 | <i>Output Analisis Skenario 8</i> | 83 |
| 5.4.9 | <i>Output Analisis Skenario 9</i> | 84 |
| 5.4.10 | <i>Output Analisis Skenario 10</i> | 86 |
| 5.4.11 | <i>Output Analisis Skenario 11</i> | 87 |
| BAB VI | PENUTUP | 90 |
| 6.1 | Kesimpulan | 90 |
| 6.2 | Saran | 91 |
| DAFTAR PUSTAKA | | 92 |
| LAMPIRAN | | 94 |

DAFTAR GAMBAR

| | |
|--|----|
| Gambar 1.1 Statistik perbandingan pengakses internet berdasarkan <i>platform</i> | 1 |
| Gambar 1.2 Statistik pengguna media sosial | 2 |
| Gambar 1.3 Statistik pengguna media sosial dan instant message | 3 |
| Gambar 3.1 Perbandingan penelitian penulis dengan penelitian sebelumnya | 27 |
| Gambar 3.2 Kerangka Berpikir | 30 |
| Gambar 4.1 Arsitektur simulasi pencarian dan analisa bukti forensik | 33 |
| Gambar 4.2 Arsitektur komunikasi data pada akun media sosial | 33 |
| Gambar 4.3 Proses recovery data | 34 |
| Gambar 4.4 Flowchart Simulasi | 44 |
| Gambar 5.1 Proses <i>recovery</i> data aplikasi Facebook dan Twitter | 47 |
| Gambar 5.2 Data pada aplikasi Facebook yang berhasil dikembalikan | 47 |
| Gambar 5.3 Data pada aplikasi Twitter yang berhasil dikembalikan. | 48 |
| Gambar 5.4 Nama akun pengguna aplikasi media sosial Facebook aplikasi SQLite Manager | 48 |
| Gambar 5.5 Nama akun pengguna aplikasi media sosial Facebook aplikasi DB Browser fo SQLite | 49 |
| Gambar 5.6 Nama akun pengguna media sosial Twitter aplikasi SQLite Manager | 50 |
| Gambar 5.7 Nama akun pengguna media sosial Twitter aplikasi DB Browser for SQLite | 50 |
| Gambar 5.8 Bukti forensik berupa lokasi pada Facebook menggunakan SQLite Manager | 51 |
| Gambar 5.9 Bukti forensik berupa lokasi pada Facebook menggunakan DB Browser for SQLite | 52 |
| Gambar 5.10 Bukti forensik berupa lokasi pada Twitter dengan SQLite Manager | 52 |
| Gambar 5.11 Bukti forensik berupa lokasi pada Twitter dengan DB Browser for SQLite | 53 |
| Gambar 5.12 Bukti forensik berupa nomor telepon dengan SQLite Manager | 54 |

| | |
|--|----|
| Gambar 5.13 Bukti forensik berupa nomor telepon dengan DB Browser for SQLite | 55 |
| Gambar 5.14 Bukti forensik berupa tanggal lahir pada Facebook dengan SQLite Manager | 56 |
| Gambar 5.15 Bukti forensik berupa tanggal lahir pada Facebook dengan DB Browser for SQLite | 56 |
| Gambar 5.16 Bukti forensik berupa url dari <i>profile picture</i> Facebook dengan SQLite Manager | 58 |
| Gambar 5.17 Bukti forensik berupa url dari <i>profile picture</i> Facebook dengan DB Browser for SQLite | 58 |
| Gambar 5.18 Ketika <i>url</i> dibuka menggunakan <i>browser</i> | 59 |
| Gambar 5.19 Bukti forensik berupa url dari <i>profile picture</i> dengan SQLite Manager | 59 |
| Gambar 5.20 Bukti forensik berupa url dari <i>profile picture</i> dengan DB Browser for SQLite | 60 |
| Gambar 5.21 Ketika <i>url</i> dibuka menggunakan <i>browser</i> | 61 |
| Gambar 5.22 Bukti forensik berupa <i>cover photo</i> Facebook dengan SQLite Manager | 61 |
| Gambar 5.23 Bukti forensik berupa <i>cover photo</i> Facebook dengan DB Browser for SQLite | 62 |
| Gambar 5.24 Bukti forensik berupa <i>url</i> dari <i>cover photo</i> pada Twitter dengan SQLite Manager | 63 |
| Gambar 5.25 Bukti forensik berupa <i>url</i> dari <i>cover photo</i> pada Twitter dengan DB Browser for SQLite | 64 |
| Gambar 5.26 Ketika <i>url</i> dibuka menggunakan <i>browser</i> | 64 |
| Gambar 5.27 Bukti forensik <i>posting</i> berupa teks dengan menggunakan SQLite Manager | 65 |
| Gambar 5.28 Bukti forensik <i>posting</i> berupa teks menggunakan DB Browser for SQLite | 66 |
| Gambar 5.29 Bukti forensik <i>posting(tweet)</i> berupa teks dengan SQLite Manager | 66 |
| Gambar 5.30 Bukti forensik <i>posting(tweet)</i> berupa teks menggunakan DB Browser for SQLite | 67 |

| | |
|--|----|
| Gambar 5.31 Bukti forensik <i>posting</i> berupa gambar dengan SQLite Manager.... | 68 |
| Gambar 5.32 Bukti forensik <i>posting</i> berupa gambar dengan DB Browser fo SQLite | 69 |
| Gambar 5.33 Bukti forensik <i>posting(tweet)</i> berupa gambar dengan SQLite Manager | 69 |
| Gambar 5.34 Bukti forensik <i>posting(tweet)</i> berupa gambar dengan DB Browser for SQLite | 70 |
| Gambar 5.35 Ketika <i>url</i> dibuka dengan menggunakan <i>browser</i> | 71 |
| Gambar 5.36 Bukti forensik percakapan pada <i>private message</i> pada Facebook dengan SQLite Manager | 72 |
| Gambar 5.37 Bukti forensik percakapan pada <i>private message</i> pada Facebook dengan SQLite Manager | 73 |
| Gambar 5.38 Bukti forensik <i>private message</i> berupa gambar menggunakan SQLite Manager..... | 74 |
| Gambar 5.39 Bukti forensik <i>private message</i> berupa gambar menggunakan SQLite Manager..... | 75 |
| Gambar 5.40 Ketika <i>url</i> dibuka menggunakan <i>browser</i> | 75 |
| Gambar 5.41 Hasil perbandingan pencarian bukti forensik menggunakan SQLite Manager | 89 |
| Gambar 5.42 Hasil perbandingan pencarian bukti forensik menggunakan DB Browser for SQLite..... | 89 |

DAFTAR TABEL

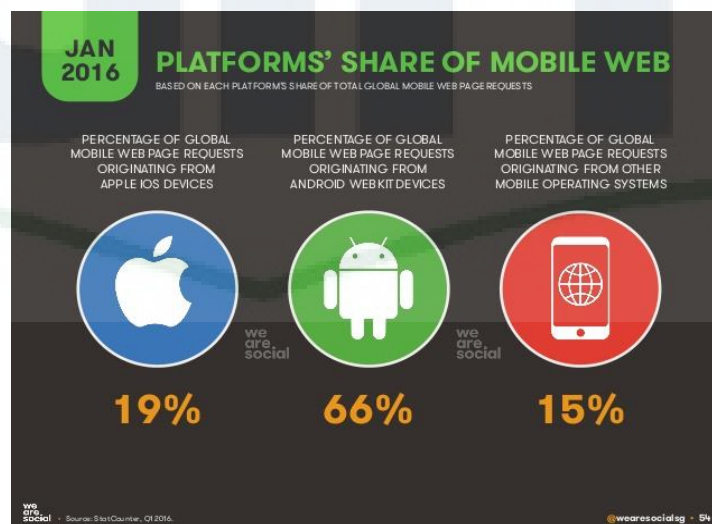
| | |
|---|----|
| Table 3.1 Perbandingan Studi Literatur | 25 |
| Table 4.1 Bukti forensik yang akan dicari | 36 |
| Table 4.2 Skenario 1 | 37 |
| Table 4.3 Skenario 2 | 38 |
| Table 4.4 Skenario 3 | 38 |
| Table 4.5 Skenario 4 | 38 |
| Table 4.6 Skenario 5 | 39 |
| Table 4.7 Skenario 6 | 39 |
| Table 4.8 Skenario 7 | 39 |
| Table 4.9 Skenario 8 | 39 |
| Table 4.10 Skenario 9 | 40 |
| Table 4.11 Skenario 10 | 40 |
| Table 4.12 Skenario 11 | 40 |
| Table 4.13 Akun Gmail palsu | 41 |
| Table 4.14 Akun Media Sosial Palsu | 42 |
| Table 5.1 Hasil perbandingan skenario 1 | 76 |
| Table 5.2 Hasil perbandingan skenario 2 | 77 |
| Table 5.3 Hasil perbandingan skenario 3 | 78 |
| Table 5.4 Hasil perbandingan skenario 4 | 79 |
| Table 5.5 Hasil perbandingan skenario 5 | 80 |
| Table 5.6 Hasil perbandingan skenario 6 | 81 |
| Table 5.7 Hasil perbandingan skenario 7 | 82 |
| Table 5.8 Hasil perbandingan skenario 8 | 83 |
| Table 5.9 Hasil perbandingan skenario 9 | 85 |
| Table 5.10 Hasil perbandingan skenario 10 | 86 |
| Table 5.11 Hasil perbandingan skenario 11 | 87 |

BAB I

PENDAHULUAN

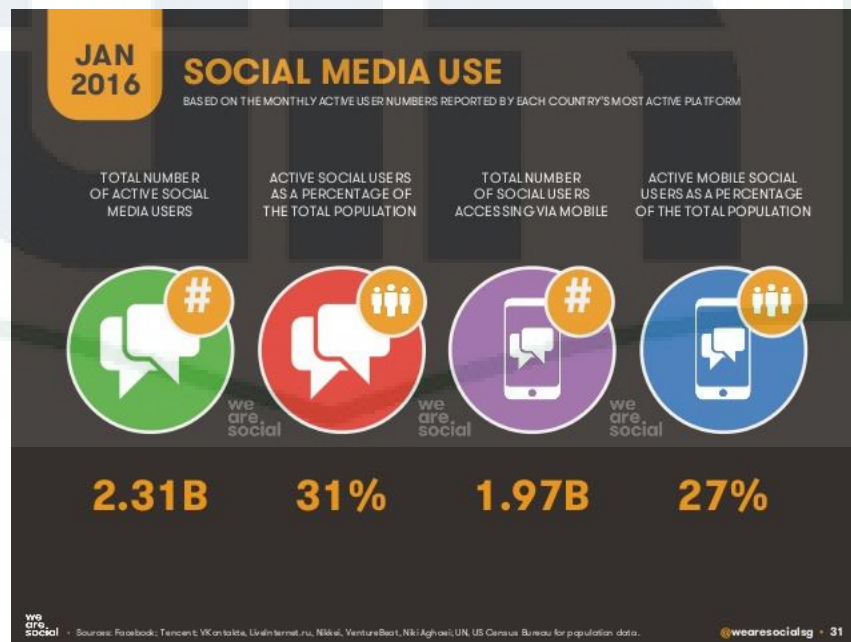
1.1 Latar Belakang

Pada saat ini, perkembangan teknologi semakin berkembang dengan pesat dan salah satunya adalah *smartphone*. Telepon genggam pada masa kini sudah tidak sekedar digunakan untuk melakukan panggilan atau berkirim pesan singkat. Telepon genggam pada masa kini telah dilengkapi dengan sistem operasi sehingga dapat melakukan beberapa fungsi layaknya *personal computer*, salah satunya adalah mengakses internet. Dengan adanya *smartphone* saat ini orang-orang dapat mengakses internet kapanpun dan dimanapun. Salah satu sistem operasi yang paling banyak digunakan pada *smartphone* saat ini adalah Android. Berdasarkan data yang didapatkan oleh penulis dari wearesocial.com pada Januari 2016 pengguna *smartphone* mengakses internet dengan *platform* berbasis Android sebanyak 66%, Apple iOS 19% dan platform lainnya sebanyak 15%. Seperti tercantum pada gambar 1.1 (wearesocial.com).



Gambar 1.1 Statistik perbandingan pengakses internet berdasarkan *platform*

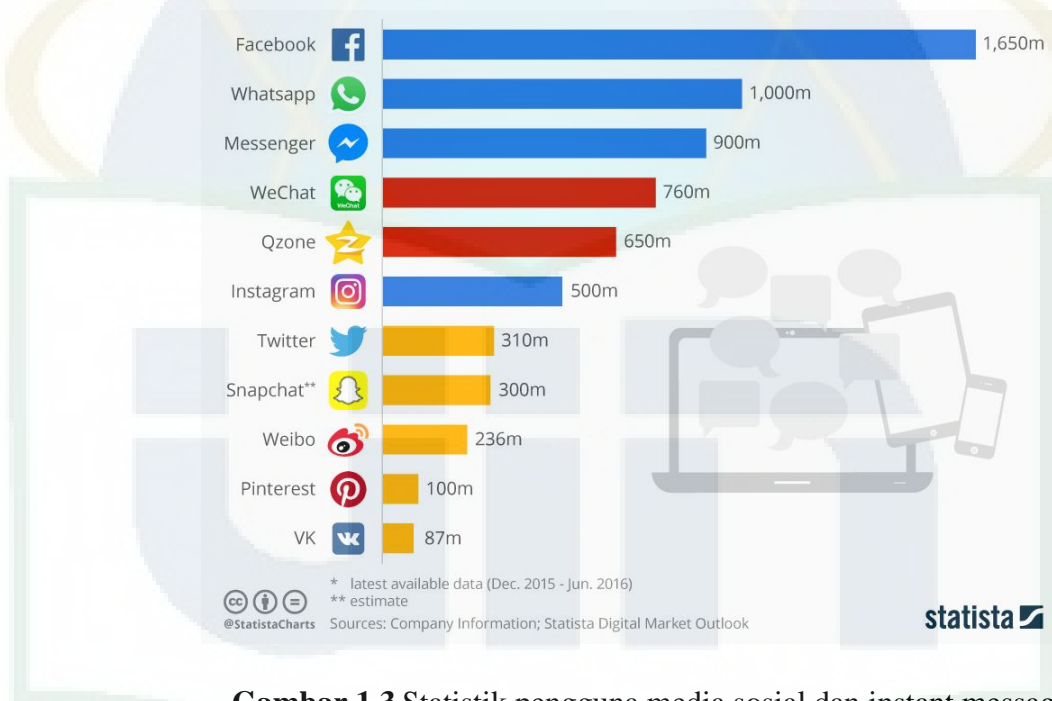
Perkembangan teknologi *smartphone* yang memudahkan orang-orang dalam mengakses internet diiringi juga dengan banyaknya penggunaan media sosial. Banyak orang keliru membedakan sosial media dan *instant messaging*. Berdasarkan pada data yang penulis dapatkan pada website wearesocial.com pada Januari 2016 (gambar 1.2), jumlah pengguna aktif media sosial diseluruh dunia mencapai 2,31 Triliun, yang artinya setara dengan 31% dari total populasi penduduk dunia. Pada awalnya media sosial hanya terbatas diakses dengan menggunakan *personal computer* (PC). Kemudian semakin berkembangnya teknologi, para pengguna media sosial mulai menggunakan *smartphone* untuk mengakses media sosial. Berdasarkan data dari website wearesocial.com pada Januari 2016 pengguna media sosial yang mengakses media sosial dengan menggunakan *smartphone* sebanyak 1,97 Triliun atau setara dengan 27% dari total populasi penduduk bumi.



Gambar 1.2 Statistik pengguna media sosial

Pada media sosial ini pengguna dapat mencari teman, saling berinteraksi, bertukar pendapat, berbagi komentar, mengirim file,

berbagi informasi dan lain sebagainya. (Devita & Amal, 2014). Berdasarkan data yang penulis dapat dari website statista.com (Gambar 1.3) pada Juni 2016 media sosial dengan pengguna paling banyak adalah Facebook 1,65 Milyar pengguna, WhatsApp 1 Milyar pengguna (*instant messaging*), Messenger 900 Juta pengguna (*instant messaging*), WeChat 760 Juta pengguna (*instant messaging*), Qzone 650 Juta pengguna, Instagram 500 Juta pengguna, Twitter 310 Juta pengguna dan seterusnya.



Gambar 1.3 Statistik pengguna media sosial dan instant message

Namun perkembangan media sosial dimanfaatkan oleh sebagian orang untuk melakukan tindak kejahatan. Tidak sedikit tindak kejahatan dilakukan menggunakan media sosial yang diakses melalui smartphone. Kejahatan yang bisa disebabkan oleh media sosial diantaranya penculikan, penipuan, pemerasan, *cyberbully* dan lainnya. Berdasarkan data pada website www.theguardian.com kejahatan pada media sosial Facebook dan Twitter meningkat sebanyak 780% selama 4 tahun dari tahun 2008 (556 kasus) sampai tahun 2012 (4908) kasus. Dengan semakin meningkatnya tindak kejahatan pada media sosial dan

meningkatnya pengguna aplikasi media sosial pada *smartphone* membuat perangkat ini menjadi tambang emas bagi penyidik forensik karena sifat personalias dari kepemilikan *smartphone* tersebut. Bukti potensial bisa didapatkan pada perangkat ini dengan menggunakan *tool* yang tepat dan metode pemeriksaan. (Mutawa, Baggili, & Marrington, 2012).

Beberapa penelitian yang telah dilakukan mengenai *mobile forensic* diantaranya adalah penelitian yang dilakukan oleh Ilman Zuhri Yadi dalam jurnalnya pada tahun 2014 yang berjudul Analisis Forensik Pada Platform Android. Penelitiannya berfokus pada identifikasi bukti forensik berupa SMS, *Call log*, kontak, file gambar yang disimpan dan lainnya, serta mengevaluasi kinerja *tool* ekstraksi dari ponsel Android. Penelitian tentang *mobile forensic* dilakukan pula oleh Noora Al Mutawa dalam jurnalnya pada tahun 2012 yang berjudul *Forensic Analysis of Social Networking Application on Mobile*. Penelitiannya berfokus pada pencarian dan analisa forensik terhadap berbagai jenis sistem operasi pada *smartphone* dan juga 3 jenis media sosial. Selain itu terdapat pula penelitian yang dilakukan oleh Walnycky tahun 2015 yang berjudul *Network and Device Forensic Analysis of Android Social-messaging Application*. Penelitian tersebut berfokus melakukan analisa forensik terhadap aplikasi *instant-messaging* pada *smartphone* berbasis Android. Beliau mencoba melakukan observasi terhadap *Network Traffic* dan pengambilan data aplikasi *instant-messaging* yang tersimpan pada *smartphone* tersebut.

Penelitian yang dilakukan oleh para peneliti diatas berfokus pada pencarian dan pengembalian bukti forensik yang terdapat pada *smartphone*. Data yang diambil dari perangkat *smartphone* dengan sendirinya dapat dijadikan bukti. Bukti-bukti ini dapat menjadi landasan ketika menyelidiki suatu perkara oleh lembaga penegak hukum. (Yadi & Kunang, 2014). Namun masih terdapat beberapa

kekurangan dalam mencari bukti forensik tersebut pada penelitian sebelumnya, dimana pencarian bukti forensik masih sangat terbatas.

Berdasarkan pernyataan diatas, penulis akan melakukan penelitian dengan judul “Analisa dan Pencarian Bukti Forensik pada Aplikasi Media Sosial Facebook dan Twitter pada *Smartphone* Android”.

1.2 Rumusan Masalah

Adapun yang menjadi rumusan masalah berdasarkan latar belakang penulisan adalah Bagaimana hasil analisa dan pencarian bukti forensik pada aplikasi media sosial Facebook dan Twitter pada *smartphone* berbasis Android?

1.3 Batasan Masalah

Berdasarkan latar belakang dan rumusan masalah yang ada, maka penulis memberikan batasan masalah sebagai berikut:

- Metodologi
 1. Metode yang digunakan yaitu metode simulasi.
 2. Simulasi dilakukan dengan asumsi perangkat digital digunakan sebagai alat bantu untuk melakukan tindak kriminal.
- Proses
 1. *Smartphone* yang digunakan sudah melalui proses *root*.
 2. Data aplikasi media sosial pada *smartphone* dihapus, kemudian dilakukan proses *recovery* sebelum dilakukan pencarian bukti forensik.
 3. Penelitian difokuskan mencari bukti forensik pada kedua aplikasi tersebut.
 4. Data yang diinput pada aplikasi media sosial adalah sama, baik berupa teks atau gambar.
- Tools

1. Penelitian dilakukan pada aplikasi Facebook versi 77.0.0.20.66, Facebook Messenger versi 70.0.0.12.68 dan Twitter versi 5.109.0 pada *smartphone* Android Redmi 2.
2. Device yang digunakan hanya pada device yang sudah di root dengan versi OS Android 4.4.4.
3. Akun yang digunakan adalah akun palsu yang sengaja dibuat untuk penelitian.
4. Proses recovery menggunakan aplikasi Wondershare Dr. Fone for Android.
5. Analisa *database* menggunakan aplikasi SQLite Manager yang merupakan *add-ons* pada *browser* Mozilla Firefox.

1.4 Tujuan

Tujuan dari penelitian ini adalah menemukan data dan bukti-bukti forensik pada aplikasi sosial media Facebook dan Twitter yang diakses melalui *smartphone* berbasis Android.

1.5 Manfaat

Penelitian yang dilakukan oleh penulis diharapkan dapat memberikan manfaat kepada berbagai pihak, diantaranya :

1. Penulis

- Menambah pengetahuan penulis dalam melakukan analisa forensik terhadap media sosial.
- Sebagai portofolio penulis di masa yang akan datang.

2. Universitas

- Menambah referensi literatur kepustakaan untuk Universitas Islam Negeri Syarif Hidayatullah Jakarta.
- Mengetahui kemampuan mahasiswa dalam menerapkan ilmunya dan sebagai bahan evaluasi.

- Sebagai referensi untuk mahasiswa lain dalam mengembangkan penulisan atau penelitian yang berhubungan dengan topik penelitian sejenis.

3. Masyarakat

- Dapat membantu pihak berwenang untuk melakukan investigasi terhadap pelaku kejahatan yang memanfaatkan media sosial dan menemukan bukti kejahatannya.

1.6 Metodologi Penelitian

1.6.1. Metode Pengumpulan Data

Metode pengumpulan data yang digunakan penulis dalam melakukan penelitian yaitu :

1. Studi Pustaka

Penulis melakukan pengumpulan data dengan cara mencari informasi dari buku, jurnal, *ebook* atau literatur terkait dengan topik penelitian. Hal ini ditujukan untuk penulisan pada landasan teori, penulis juga mencari pembelajaran dan mencari perbandingan dengan literatur sejenis.

1.6.2. Metode Simulasi

Dalam penelitian ini, penulis melakukan pembahasan dengan metode penelitian simulasi, dimana penulis melakukan simulasi terhadap model yang ditentukan untuk mendapatkan data-data forensik yang disimpan pada aplikasi media sosial. Pada metode simulasi ini terdapat beberapa langkah yang akan dilakukan yaitu :

- 1. Problem Formulation*
- 2. Conceptual Model*

3. *Input/Output data*
4. *Modelling*
5. *Simulation*
6. *Verification and Validation*
7. *Experimentation*
8. *Output Analysis*

1.7 Sistematika Penulisan

Dalam penelitian ini pembahasan terbagi menjadi lima bab yang secara singkat diuraikan sebagai berikut :

I. BAB 1 PENDAHULUAN

Pada bab ini dijelaskan tentang latar belakang penelitian, perumusan masalah, batasan masalah, tujuan dan manfaat penelitian, metode penelitian dan sistematika penulisan

II. BAB 2 LANDASAN TEORI

Pada bab ini dibahas mengenai teori yang mendasari analisis permasalahan yang berkaitan dengan topik yang dibahas. Literatur yang digunakan dapat berupa buku ataupun penelitian sejenis yang mendukung.

III. BAB 3 METODOLOGI PENELITIAN

Bab ini menjelaskan metode penelitian yang digunakan diantaranya metode pengumpulan data, metode implementasi dan metode pengujian.

IV. BAB 4 IMPLEMENTASI

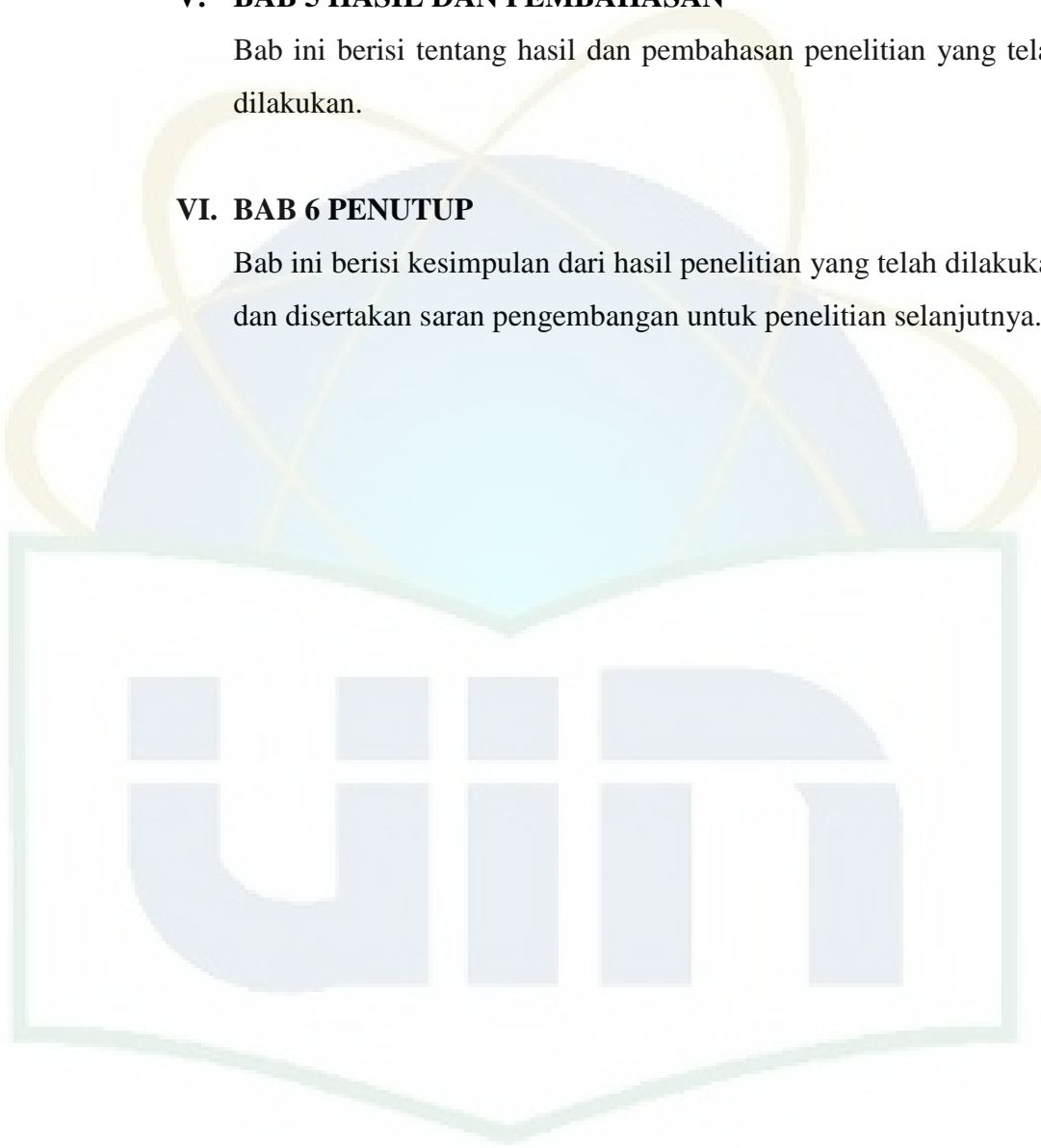
Bab ini memaparkan penjelasan tentang simulasi dan implementasi untuk menyelesaikan masalah yang ada berdasarkan landasan teori yang telah dipaparkan sebelumnya.

V. BAB 5 HASIL DAN PEMBAHASAN

Bab ini berisi tentang hasil dan pembahasan penelitian yang telah dilakukan.

VI. BAB 6 PENUTUP

Bab ini berisi kesimpulan dari hasil penelitian yang telah dilakukan dan disertakan saran pengembangan untuk penelitian selanjutnya.



BAB II

LANDASAN TEORI

2.1 Forensik Digital

2.1.1 Penjelasan

Forensik merupakan kegiatan untuk melakukan investigasi dan menetapkan fakta yang berhubungan dengan kejadian criminal dan permasalahan hukum lainnya. Sedangkan forensik digital merupakan bagianagain ilmu forensik yang melingkupi penemuan dan investigasi materi (data) yang ditemukan pada perangkat digital (computer, *handphone*, tablet, PDA, *networking devices*, storage dan sejenisnya). (Raharjo, 2013).

2.1.2 Data Forensik

Menurut (Indrajit, 2012), fokus data yang dikumpulkan dapat dikategorikan menjadi 3, diantaranya :

2.1.2.1 Active Data

Informasi terbuka yang dapat dilihat oleh siapa saja, terutama data, program, maupun file yang dikendalikan oleh sistem operasi.

2.1.2.2 Archival Data

Informasi yang telah menjadi arsip sehingga telah disimpan sebagai backup dalam berbagai bentuk alat penyimpanan seperti *external harddisk*, CD-ROM, *backup tape*, DVD, dan lain-lain.

2.1.2.3 Latent Data

Informasi yang membutuhkan alat khusus untuk mendapatkannya karena sifatnya yang khusus,

misalnya: telah dihapus, ditimpa data lain, rusak (*corrupted file*), dan lain sebagainya.

2.1.3 Objek Forensik

Apa saja yang bisa dipergunakan sebagai obyek forensik, terutama dalam kaitannya dengan jenis kejahatan yang telah dikemukakan tersebut? Dalam dunia kriminal dikenal istilah “tidak ada kejahatan yang tidak meninggalkan jejak”. Ada banyak sekali hal yang bisa menjadi petunjuk atau jejak dalam setiap tindakan kriminal yang dilakukan dengan menggunakan teknologi seperti komputer. Contohnya adalah sebagai berikut: (Indrajit, 2012)

- Log file atau catatan aktivitas penggunaan komputer yang tersimpan secara rapi dan detail di dalam sistem.
- File yang sekilas telah terhapus secara sistem, namun secara teknis masih bisa diambil dengan cara-cara tertentu.
- *Harddisk* yang berisi data/informasi backup dari sistem utama;
- Rekaman *email*, *mailing list*, *blog*, *chat*, dan mode interaksi dan komunikasi lainnya.
- Beraneka ragam jenis berkas file yang dibuat oleh sistem maupun aplikasi untuk membantu melakukan manajemen file (misalnya: *.tmp*, *.dat*, *.txt*, dan lain-lain).
- Rekam jejak interaksi dan trafik via internet dari satu tempat ke tempat yang lain (dengan berbasis IP address misalnya).

2.1.4 Kejahatan Komputer

Menurut (Indrajit, 2012), berbeda dengan di dunia nyata, kejahatan di dunia komputer dan internet variasinya begitu banyak, dan cenderung dipandang dari segi jenis dan

kompleksitasnya, meningkat secara eksponensial. Agar tidak salah pengertian, perlu diperhatikan bahwa istilah “komputer” mengandung makna yang luas, yaitu piranti digital yang dapat digunakan untuk mengolah data dan melakukan perhitungan secara elektronik. Secara prinsip, kejahatan di dunia computer dibagi menjadi tiga, yaitu:

- Aktivitas dimana komputer atau piranti digital dipergunakan sebagai alat bantu untuk melakukan tindakan kriminal.
- Aktivitas dimana komputer atau piranti digital dijadikan target dari kejahatan itu sendiri.
- Aktivitas dimana pada saat yang bersamaan computer atau piranti digital dijadikan alat untuk melakukan kejahatan terhadap target yang merupakan komputer atau piranti digital juga.

2.2 *Mobile Forensic*

Menurut (Yadi & Kunang, 2014), *Mobile phone* forensik merupakan ilmu yang melakukan proses rekoveri bukti digital dari perangkat *mobile* menggunakan cara yang sesuai dengan kondisi forensik. Forensik sendiri bisa dilakukan pada berbagai ponsel, tidak hanya terpaku pada *smartphone*. Dengan meningkatnya jumlah ponsel yang kaya fitur membuat sulitnya membuat satu tool forensik atau standar khusus untuk satu platform. Bukti digital dalam perangkat *mobile* mudah rentan tertimpa dengan data baru atau terhapus. Perangkat *mobile* sendiri menggunakan *flash memory* untuk menyimpan data. Keuntungan menggunakan *flash memory* adalah ketahanannya terhadap suhu dan tekanan yang tinggi sehingga lebih sulit untuk dihancurkan. Dari sudut pandang forensik hal ini menguntungkan karena flash memory bisa saja berisi informasi yang

sudah dihapus bahkan setelah seseorang berusaha untuk menghancurkan barang bukti.

Perangkat mobile merupakan sumber berharga sebagai bukti digital dan berisi informasi penting yang tidak tersedia pada perangkat lain. Selain itu sifat personaliti dari perangkat tersebut membuatnya mudah untuk membuktikan jejak yang mengaitkan perangkat ke individu. Dalam forensik perangkat *mobile* data yang diambil dari ponsel dengan sendirinya bisa dijadikan sebagai bukti. Bukti-bukti ini bisa menjadi landasan ketika menyelidiki suatu perkara oleh lembaga penegak hukum. Artefak ini bisa diekstrak dengan metode *logic* maupun fisik. Secara *logic* adalah mengekstrak data dari *file system* dengan langsung berinteraksi dengan perangkat menggunakan beberapa *tool* khusus. *Software* atau *tool* yang bisa mengekstrak artefak (bukti forensik) ini sangat terbatas.

Forensik *mobile* juga menggunakan metode yang sama dengan investigasi forensik secara umum. Ada beberapa teknik yang perlu diikuti, meskipun belum ada format standar penyelidikan pada forensik *mobile*. Metode penyelidikan yang digunakan kurang lebih sama dengan investigasi digital. Tahapan proses penyelidikan yang diikuti adalah :

2.2.1 Collection

Merupakan langkah awal dan paling penting dalam penyelidikan. Tujuan utamanya adalah untuk mengumpulkan sumber-sumber bukti potensial pada perangkat *mobile*.

2.2.2 Identification

Tahap ini difokuskan pada pengenalan sumber barang bukti dengan pelabelan.

2.2.3 Acquisition

Tahapan ini berkaitan dengan proses ekstraksi data atau bukti dari berbagai sumber yang telah dikumpulkan.

2.3 File

Menurut (Merola, 2008) *file* adalah sebuah istilah yang digunakan di dunia komputer untuk mengindikasikan sebuah blok dari informasi yang disimpan (*binary digits*) seperti sebuah dokumen dalam *file doc*, dan sebuah foto dalam *file jpg* atau sebuah program dalam *file exe*. Selanjutnya tergantung dari aplikasi yang bersangkutan untuk memahami blok dari *binary digits* dengan tujuan untuk menampilkan atau mengeksekusi konten yang ada dengan benar. *Files* dapat dibuat, dipindah, dimodifikasi, diduplikasi, dan dihapus.

2.4 Recovery

Recovery merupakan teknik pengembalian file yang menggunakan informasi file system yang tersisa setelah penghapusan file. Informasi tersebut dapat digunakan untuk mengembalikan file dengan syarat jenis file system dari data yang ingin dikembalikan harus diketahui. (Beek, 2011).

2.5 Android

Android adalah sebuah sistem operasi untuk perangkat mobile berbasis linux yang mencakup sistem operasi, middleware dan aplikasi. Android menyediakan platform terbuka bagi para pengembang untuk menciptakan aplikasi mereka (Safaat, 2012).

Menurut (Safaat, 2012) Android dipuji sebagai “platform mobile pertama yang lengkap, terbuka dan bebas”:

2.5.1 *File System* pada Android

File System pada Android tidak didefinisikan secara tunggal. Android dikembangkan pada kernel Linux dan Linux mendukung banyak *file system*. Setiap *file system* adalah implementasi VFS (*Virtual File System*). VFS adalah lapisan abstrak Kernel yang mengalirkan file dan direktori operasi aplikasi. Setiap sistem berkas memiliki modul Kernel terpisah yang mendukung operasi. (Wilson, 2015)

2.5.2 Struktur *File System* Android

Android menggunakan lebih dari satu *file system* dan beberapa partisi untuk mengatur *file* dan *folder* dalam perangkat. Dalam partisi *file system* diwakili oleh direktori. Ada enam partisi utama yang digunakan oleh perangkat android yaitu boot, system, recovery, data, cache dan misc. (Wilson, 2015)

2.5.3 *Rooting* pada Perangkat Android

Rooting adalah proses mencapai kontrol istimewa dari perangkat Android. Proses ini memberi izin *root* pada perangkat Android. *Rooting* perangkat Android membantu untuk mengatasi keterbatasan perangkat yang diberikan oleh produsen. Dengan proses *rooting* kita bisa menjalankan aplikasi yang membutuhkan akses sistem tertentu seperti mengakses *file system* dan *file database*. (Wilson, 2015)

2.6 Smartphone

Menurut (Williams & Sawyer, 2011), *smartphone* adalah telepon selular dengan mikroprosesor, memori, layar dan modem bawaan. Smartphone merupakan ponsel multimedia yang menggabungkan fungsionalitas PC dan *handset* sehingga menghasilkan gadget yang

mewah, di mana terdapat pesan teks, kamera, pemutar musik, video, game, akses *email*, tv digital, *search engine*, pengelola informasi pribadi, fitur GPS, jasa telepon internet dan bahkan terdapat telepon yang juga berfungsi sebagai kartu kredit.

2.7 Media Sosial

Media sosial adalah sebuah media online dimana para penggunanya dapat dengan mudah berpartisipasi. Berpartisipasi dalam arti seseorang akan dengan mudah berbagi informasi, menciptakan konten atau isi yang ingin disampaikan kepada orang lain, memberi komentar terhadap masukan yang diterimanya dan seterusnya. Semua dapat dilakukan dengan cepat dan tak terbatas. (Devita & Amal, 2014).

Pada dasarnya media sosial merupakan perkembangan mutakhir dari teknologi-teknologi *web* baru berbasis internet, yang memudahkan semua orang untuk dapat berkomunikasi, berpartisipasi, saling berbagi dan membentuk sebuah jaringan secara *online*, sehingga dapat menyebarluaskan konten mereka sendiri. Post di blog, tweet, atau video YouTube dapat diproduksi dan dapat dilihat secara langsung oleh jutaan orang secara gratis. (Setyani & Ika, 2013).

2.8 Facebook

Facebook adalah suatu situs jejaring sosial yang dapat dijadikan sebagai tempat untuk menjalin hubungan pertemanan dengan seluruh orang yang ada di belahan dunia untuk dapat berkomunikasi satu dengan yang lainnya. Facebook merupakan situs pertemanan yang dapat digunakan oleh manusia untuk bertukar informasi, berbagi video, dan lainnya. (Setyani & Ika, 2013).

Pada aplikasi Facebook Android, direktori *file* untuk menyimpan data-data aplikasi tersebut berada pada folder *com.facebook.katana*.

(Möller, Kranz, Schmid, Roalter, & Diewald, 2013), secara lengkap, direktori tersebut berada pada `root/data/data/com.facebook.katana`. Sedangkan untuk Facebook Messenger berada pada folder `com.facebook.orca`, secara lengkap direktori tersebut berada pada `root/data/data/com.facebook.orca`. Untuk dapat menemukan direktori tersebut maka harus masuk kedalam direktori `root`, dimana untuk mengakses direktori tersebut perangkat Android diharuskan sudah melewati proses *rooting*.

2.9 Twitter

Twitter adalah suatu situs web yang merupakan layanan dari microblog, yaitu suatu bentuk blog yang membatasi ukuran tiap postnya, yang memberikan fasilitas bagi pengguna untuk dapat menuliskan pesan dalam twitter *update* hanya berisi 140 karakter. Twitter merupakan salah satu jejaring sosial yang paling mudah digunakan, karena hanya memerlukan waktu yang singkat tetapi informasi yang disampaikan dapat langsung menyebar secara luas.

Ciri-ciri sebuah microblogging atau twitter, yaitu memiliki *update status* yang biasa disebut dengan *tweet* berjumlah 140 karakter lebih singkat daripada media lainnya. Dapat mengomentari *tweet* yang dibuat oleh *following* dengan menggunakan *reply*, selanjutnya dapat menulis dengan menggunakan fungsi *RT@username*. Memiliki cara tersendiri untuk berbagi foto dan video yang biasa disebut *tweetpic*. (Setyani & Ika, 2013).

Pada aplikasi Twitter Android, direktori *file* untuk menyimpan data-data aplikasi tersebut berada pada folder `com.twitter.android`. (Mathur, Schlotfeldt, & Chetty, 2015), secara lengkap, direktori tersebut berada pada `root/data/data/com.twitter.android`. Untuk dapat menemukan direktori tersebut maka harus masuk kedalam direktori

root, dimana untuk mengakses direktori tersebut perangkat Android diharuskan sudah melewati proses *rooting*.

2.10 SQLite

2.10.1 Penjelasan umum

SQLite merupakan sebuah system manajemen basis data relasional yang bersifat *ACID - compliant* dan memiliki ukuran pustaka kode yang relatif kecil, ditulis dalam bahasa C. SQLite merupakan proyek yang bersifat public domain yang dikerjakan oleh D. Richard Hipp. Tidak seperti pada paradigma *client-server* umumnya, Inti SQLite bukanlah sebuah sistem yang mandiri yang berkomunikasi dengan sebuah program, melainkan sebagai bagian integral dari sebuah program secara keseluruhan. Sehingga protokol komunikasi utama yang digunakan adalah melalui pemanggilan API secara langsung melalui bahasa pemrograman. Mekanisme seperti ini tentunya membawa keuntungan karena dapat mereduksi overhead, latency times, dan secara keseluruhan lebih sederhana. Seluruh elemen basisdata (definisi data, tabel, indeks, dan data) disimpan sebagai sebuah file. Kesederhanaan dari sisi disain tersebut bisa diraih dengan cara mengunci keseluruhan file basis data pada saat sebuah transaksi dimulai. SQLite adalah *database* yang digunakan pada aplikasi yang berjalan pada perangkat Android. Setiap aplikasi yang dipasang pada perangkat Android akan menggunakan *database* ini. (Nugroho, Suadi, & Pratomo, 2010).

2.10.2 Fitur

SQLite mengimplementasikan hampir seluruh elemen-elemen standar yang berlaku pada SQL-92, termasuk transaksi yang bersifat atomic, konsistensi basisdata, isolasi, dan

durabilitas (dalam bahasa Inggris lebih sering disebut ACID), trigger, dan kueri-kueri yang kompleks. Tidak ada pengecekan tipe sehingga data bisa dientrikan dalam bentuk string untuk sebuah kolom bertipe integer. Beberapa kalangan melihat hal ini sebagai sebuah inovasi yang menambah nilai guna dari sebuah basis data, utamanya ketika digunakan dalam bahasa pemrograman berbasis script (PHP, Perl), sementara kalangan lain melihat hal tersebut sebagai sebuah kekurangan. Beberapa proses ataupun thread dapat berjalan secara bersamaan dan mengakses basisdata yang sama tanpa mengalami masalah. Hal ini disebabkan karena akses baca data dilakukan secara paralel. Sementara itu akses tulis data hanya bisa dilakukan jika tidak ada proses tulis lain yang sedang dilakukan; jika tidak, proses tulis tersebut akan gagal dan mengembalikan kode kesalahan (atau bisa juga secara otomatis akan mencobanya kembali sampai sejumlah nilai waktu yang ditentukan habis). Hanya saja ketika sebuah tabel temporer dibuat, mekanisme penguncian pada proses multithread akan menyebabkan masalah. Update yang terkini (versi 3.3.4) dikatakan telah memperbaiki masalah ini. Sebuah program yang mandiri dinamakan *sqlite* disediakan dan bisa digunakan untuk mengeksekusi kueri dan manajemen file-file basisdata *SQLite*. Program tersebut juga merupakan contoh implementasi penulisan aplikasi yang menggunakan pustaka *SQLite*. (Nugroho, Suadi, & Pratomo, 2010).

2.11 SQLite Manager

SQLite Manager adalah Add-ons pada browser Mozilla Firefox. *SQLite Manager* adalah aplikasi yang berguna untuk melihat dan manajemen *database SQLite*. Fitur yang dimiliki oleh *SQLite Manager* antara lain (Iazierthanhou, 2016) :

1. Dapat melakukan manajemen *database* SQLite.
2. Dapat melakukan eksekusi terhadap segala jenis SQL query.
3. Dapat melihat dan mencari table yang terdapat pada *database*.

2.12 Metode Simulasi

Metode Simulasi merupakan metode untuk melakukan simulasi dan pemodelan yang diadaptasi dari penelitian yang dilakukan oleh Sajjad A. Madani, Jawad Kazmi dan Stefan Mahlkecht pada tahun 2010 dengan karya publikasi yang berjudul *Wireless sensor network: Modeling and Simulation*. Dalam penelitian tersebut metode simulasi digunakan untuk melakukan pemodelan dan simulasi terhadap *Wireless Sensor Network (WSN)*. (Madani, Jawad, & Mahlkecht, 2010).

Menurut (Madani, Jawad, & Mahlkecht, 2010) terdiri dari beberapa tahapan yang terdiri dari :

2.12.1 Problem Formulation

Proses simulasi dimulai dengan masalah praktis yang memerlukan pemecahan atau pemahaman. Sebagai contoh sebuah perusahaan kargo ingin mencoba untuk mengembangkan strategi baru untuk pengiriman truk, contoh lain yaitu astronom mencoba memahami bagaimana sebuah nebula terbentuk. Pada tahap ini kita harus memahami perilaku dari sistem, mengatur operasi sistem sebagai objek untuk percobaan. Maka kita perlu menganalisa berbagai solusi dengan menyelidiki hasil sebelumnya dengan masalah yang sama. Solusi yang paling diterima yang harus dipilih.

2.12.2 Conceptual Model

Langkah ini terdiri dari deskripsi tingkat tinggi dari struktur dan perilaku sebuah sistem dan mengidentifikasi semua benda dengan atribut dan *interface* mereka. Kita juga harus menentukan variable statenya, bagaimana cara mereka

berhubungan, dan mana yang penting untuk penelitian. Pada tahap ini dinyatakan aspek-aspek kunci dari *requirement*. Selama definisi model konseptual, kita perlu mengungkapkan fitur yang penting. Kita juga harus mendokumentasikan informasi non-fungsional, misalnya seperti perubahan pada masa yang akan datang, perilaku non-*intuitive* atau non-formal, dan hubungan dengan lingkungan.

2.12.3 Input / Output Data

Pada tahap ini kita mempelajari sistem untuk mendapatkan data *input* dan *output*. Untuk melakukannya kita harus mengumpulkan dan mengamati atribut yang telah ditentukan pada tahap sebelumnya. Ketika entitas sistem yang dipelajari, maka dicoba mengaitkannya dengan waktu. Isu penting lainnya pada tahap ini adalah pemilihan ukuran sampel yang valid secara statistik dan format data yang dapat diproses dengan komputer. Kita harus memutuskan atribut mana yang stokastik dan deterministik. Dalam beberapa kasus, tidak ada sumber data yang dapat dikumpulkan (misalnya pada sistem yang belum ada). Dalam kasus tersebut kita perlu mencoba untuk mendapatkan set data dari sistem yang ada (jika tersedia). Pilihan lain yaitu dengan menggunakan pendekatan stokastik untuk menyediakan data yang diperlukan melalui generasi nomor acak.

2.12.4 Modeling

Pada tahap pemodelan, kita harus membangun representasi yang rinci dari sistem berdasarkan model konseptual dan *input/output* data yang dikumpulkan. Model ini dibangun dengan mendefinisikan objek, atribut, dan metode

menggunakan paradigma yang dipilih. Pada tahap ini spesifikasi model dibuat, termasuk set persamaan yang mendefinisikan perilaku dan struktur. Setelah menyelesaikan definisi ini, kita harus membangun struktur awal model (mungkin berkaitan sistem dan metrik kerja).

2.12.5 Simulation

Pada tahap simulasi, kita harus memilih mekanisme untuk menerapkan model (dalam banyak kasus menggunakan komputer dan bahasa pemrograman dan alat-alat yang memadai), dan model simulasi yang dibangun. Selama langkah ini, mungkin perlu untuk mendefinisikan algoritma simulasi dan menerjemahkannya ke dalam program komputer.

2.12.6 Verification and Validation

Pada tahap sebelumnya, tiga model yang berbeda yang dibangun yaitu model konseptual (spesifikasi), sistem model (desain), dan model simulasi (*executable program*). Kita perlu memverifikasi dan memvalidasi model ini. Verifikasi terkait dengan konsistensi internal antara tiga model. Validasi difokuskan pada korespondensi antara model dan realitas yaitu hasil simulasi yang konsisten dengan sistem yang dianalisis.

2.12.7 Experimentation

Kita harus menjalankan model simulasi, menyusul tujuan yang dinyatakan pada model konseptual. Selama fase ini kita harus mengevaluasi *output* dari simulator menggunakan korelasi statistik untuk menentukan tingkat presisi untuk metrik kerja. Fase ini dimulai dengan desain eksperimen, menggunakan teknik yang berbeda. Beberapa teknik ini meliputi analisis sensitivitas, optimasi, dan seleksi (dibandingkan dengan sistem alternatif).

2.12.8 Output Analysis

Pada tahap analisis output, output simulasi dianalisis untuk memahami perilaku sistem. Output ini digunakan untuk mendapatkan tanggapan tentang perilaku sistem yang asli. Pada tahap ini, alat visualisasi dapat digunakan untuk membantu proses tersebut.

2.13 Kelebihan Metode Simulasi

Selain digunakan untuk melakukan permodelan dan simulasi terhadap Wireless Sensor Network (WSN), metode simulasi dapat digunakan sebagai metode perbandingan algoritma karena beberapa kelebihan, yaitu:

Pada tahapan simulasi, metode ini juga dapat menggunakan algoritma untuk dapat melakukan simulasi dan menerjemahkan dalam bentuk perangkat lunak (program). (Madani, Jawad, & Mahlke, 2010).

Selain itu pada tahapan ke-2 sampai tahapan ke-8 dari metode simulasi ini dapat digunakan model pengembangan perangkat lunak secara bertahap (incremental development) yaitu model spiral yang dapat dilakukan revisi (perbaikan dan penambahan fitur) pada setiap iterasi fase pengembangannya. (Madani, Jawad, & Mahlke, 2010).

BAB III

METODOLOGI PENELITIAN

3.1 Metode Pengumpulan Data

Dalam penelitian ini, diperlukan data-data serta informasi sebagai bahan yang dapat mendukung kebenaran materi uraian dan pembahasan. Data yang dikumpulkan penulis adalah sebagai berikut.

3.1.1 Data Primer

Untuk mendapatkan data primer, penulis mengumpulkan data-data dan informasi yang diperoleh dengan mencari data-data survey dan melakukan analisis melalui kegiatan simulasi yang dilakukan, seperti dijelaskan dibawah ini :

3.1.1.1 Data Simulasi

Penulis mengumpulkan data-data simulasi dengan melakukan simulasi mencari dan membandingkan data forensik menggunakan *smartphone* berbasis Android dengan versi 4.4.4 (Kitkat) yang telah terpasang aplikasi Facebook dan Twitter dan menggunakan akun palsu, dimana data hasil simulasi ini akan dijadikan penulis sebagai hasil penelitian penulis.

3.1.2 Data Sekunder

Penulis mendapatkan data-data sekunder dengan melakukan studi pustaka dan studi literatur, seperti dijabarkan dibawah ini :

3.1.1.2 Studi Pustaka

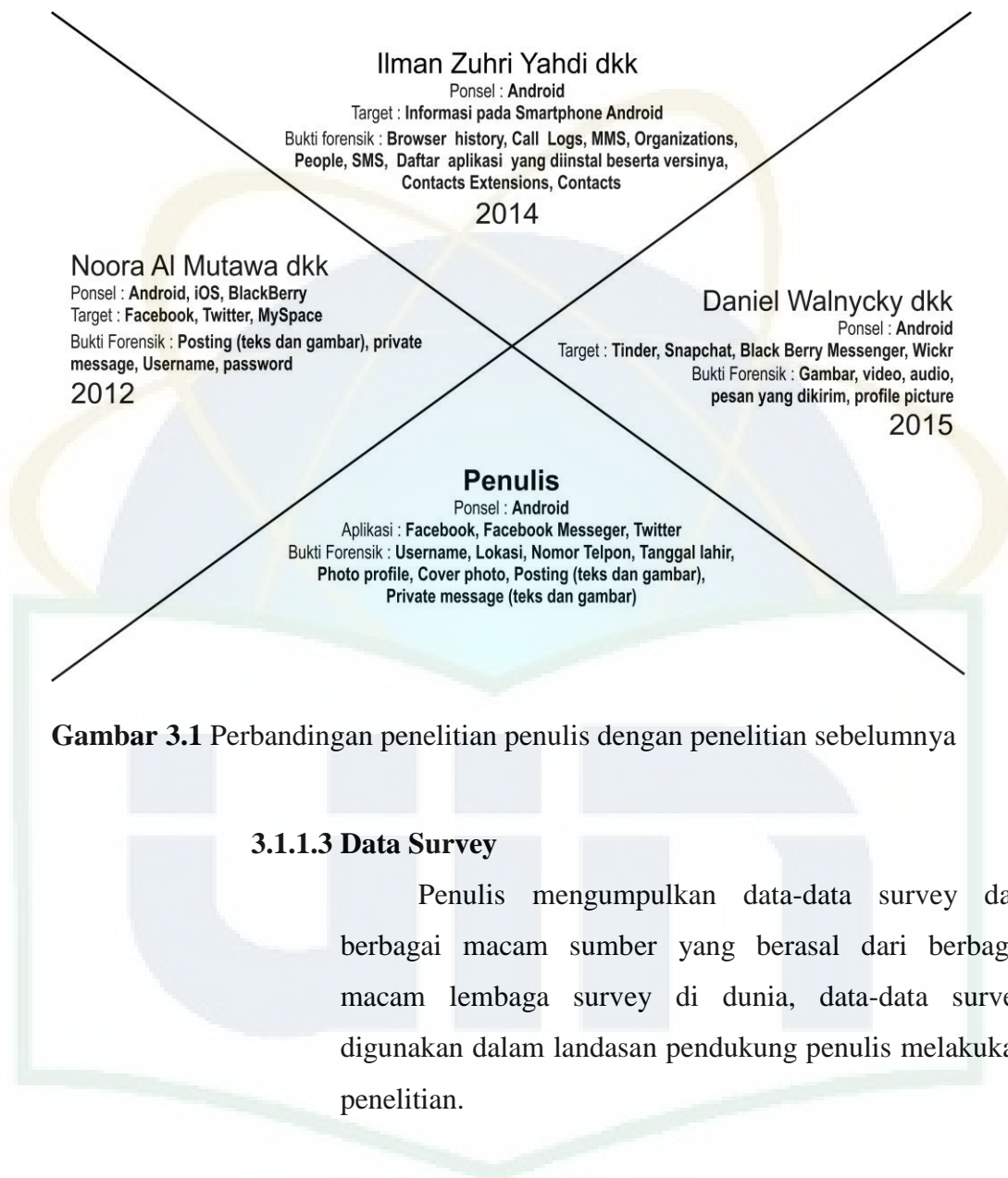
Pada tahapan pengumpulan data dengan cara studi pustaka, penulis mencari referensi-referensi yang relevan dengan objek yang akan diteliti. Pencarian referensi dilakukan di perpustakaan, took buku, maupun secara online dengan menggunakan internet. Informasi yang didapatkan dapat digunakan dalam menyusun landasan teori, metodologi penelitian, menentukan apliaksi untuk melakukan simulasi dan cara melakukan simulasi.

Salah satu pengumpulan data dengan cara studi pustaka adalah dengan melakukan studi literatur. Berikut studi literatur yang dilakukan peneliti dengan membandingkan penelitian ini dengan penelitian sejenis:

Table 3.1 Perbandingan Studi Literatur

| No | Judul | Penulis | Tujuan | Perbedaan |
|----|---|---------------------|--|--|
| 1 | Forensic Analisis of Social Networking Applications on Mobile Devices | Noora Al Mutawa dkk | Analisa forensik pada berbagai macam <i>smartphone</i> dan berbagai macam aplikasi media sosial pada <i>smartphone</i> | Melakukan analisis forensik aplikasi media sosial (Facebook (hanya aplikasi Facebook tanpa adisertakan aplikasi Facebook Messenger), Twitter, dan MySpace) pada berbagai jenis System Operation pada <i>smartphone</i> (Android, iOS dan BlackBerry) |
| 2 | Network and Device | Daniel Walnycky dkk | Melakukan analisa | Melakukan analisa |

| | | | | |
|---|--|---|---|--|
| | Forensic Analysis of Android Social-messaging Applications | | forensik terhadap <i>network</i> dan <i>device</i> pada aplikasi <i>social-messaging</i> pada <i>smartphone</i> berbasis Android dan menemukan bukti forensik berupa gambar, <i>video</i> , <i>audio</i> , pesan yang dikirim, <i>profile picture</i> dan lainnya | forensik terhadap <i>network</i> dan <i>device</i> pada aplikasi <i>social-messaging</i> pada <i>smartphone</i> berbasis Android |
| 3 | Analisis Forensik pada Platform Android | Ilman Zuhri Yahdi, Yesi Novaria Kunang | Melakukan evaluasi kinerja <i>tool</i> ekstraksi yang mendukung <i>smartphone</i> berbasis Android | Membandingkan dan menganalisa <i>tool</i> ekstraksi dalam menemukan bukti forensik pada <i>smartphone</i> berbasis Android |



Gambar 3.1 Perbandingan penelitian penulis dengan penelitian sebelumnya

3.1.1.3 Data Survey

Penulis mengumpulkan data-data survey dari berbagai macam sumber yang berasal dari berbagai macam lembaga survey di dunia, data-data survey digunakan dalam landasan pendukung penulis melakukan penelitian.

3.2 Metode Simulasi

Dalam penemelitain ini, penulis menggunakan metode simulasi sebagai metode untuk mencari dan membandingkan bukti forensik dengan cara melakukan ujicoba simulasi terhadap aplikasi media sosial Facebook dan Twitter yang terpasang pada smartphone berbasis Android versi 4.4.4 (Kitkat). Metode simulasi ini terdiri dari beberapa tahapan yang terdiri dari:

3.2.1 Problem Formulation

Setelah melakukan pengumpulan data maka didapatkan permasalahan utama dalam pencarian bukti forensik yaitu dapatkah bukti forensik ditemukan pada aplikasi media sosial Facebook dan Twitter versi saat ini yang diakses pada smartphone berbasis Android versi 4.4.4 (Kitkat) dan aplikasi manakah yang paling banyak menghasilkan bukti forensik.

3.2.2 Conceptual Model

Setelah memformulasikan permasalahan, dilakukan perancangan dan penggambaran konsep model untuk simulasi yang akan dilakukan.

3.2.3 Input and Output Data

Pada tahap ini kita harus membuat *input* dan *output* apa yang akan diproses pada simulasi. *Input* berupa atribut yang diperlukan dalam simulasi yaitu data dari akun palsu yang telah dibuat ketika mengakses media sosial pada *smartphone* berbasis Android. Sementara output berdasarkan permasalahan yang diformulasikan yaitu ditemukan atau tidaknya bukti forensik dan perbandingan bukti forensik yang didapatkan dari aplikasi media sosial tersebut.

3.2.4 Modeling

Langkah awal pada tahapan ini adalah menentukan parameter yang digunakan selama simulasi, pada tahapan ini dilakukan pembuatan scenario-skenario yang akan digunakan untuk simulasi.

3.2.5 Simulation

Pada tahapan ini dilakukan implementasi model yang dihasilkan dalam tahapan sebelumnya. Selain itu dilakukan pula

proses root pada *smartphone* Android, pemasangan aplikasi *database browser* (SQLite Manager) dan aplikasi *recovery* (Wondershare Dr. Fone for Android) dan pembuatan akun palsu yang akan digunakan pada aplikasi media sosial.

3.2.6 Verification and Validation

Pada tahapan ini dilakukan verifikasi dan validasi untuk mengecek kebenaran dari tahap sebelumnya, sehingga simulasi siap untuk dilaksanakan. Verifikasi dan validasi akan dilakukan terhadap tahap *conceptual model*, *modeling* dan *simulation*.

3.2.7 Experimentation

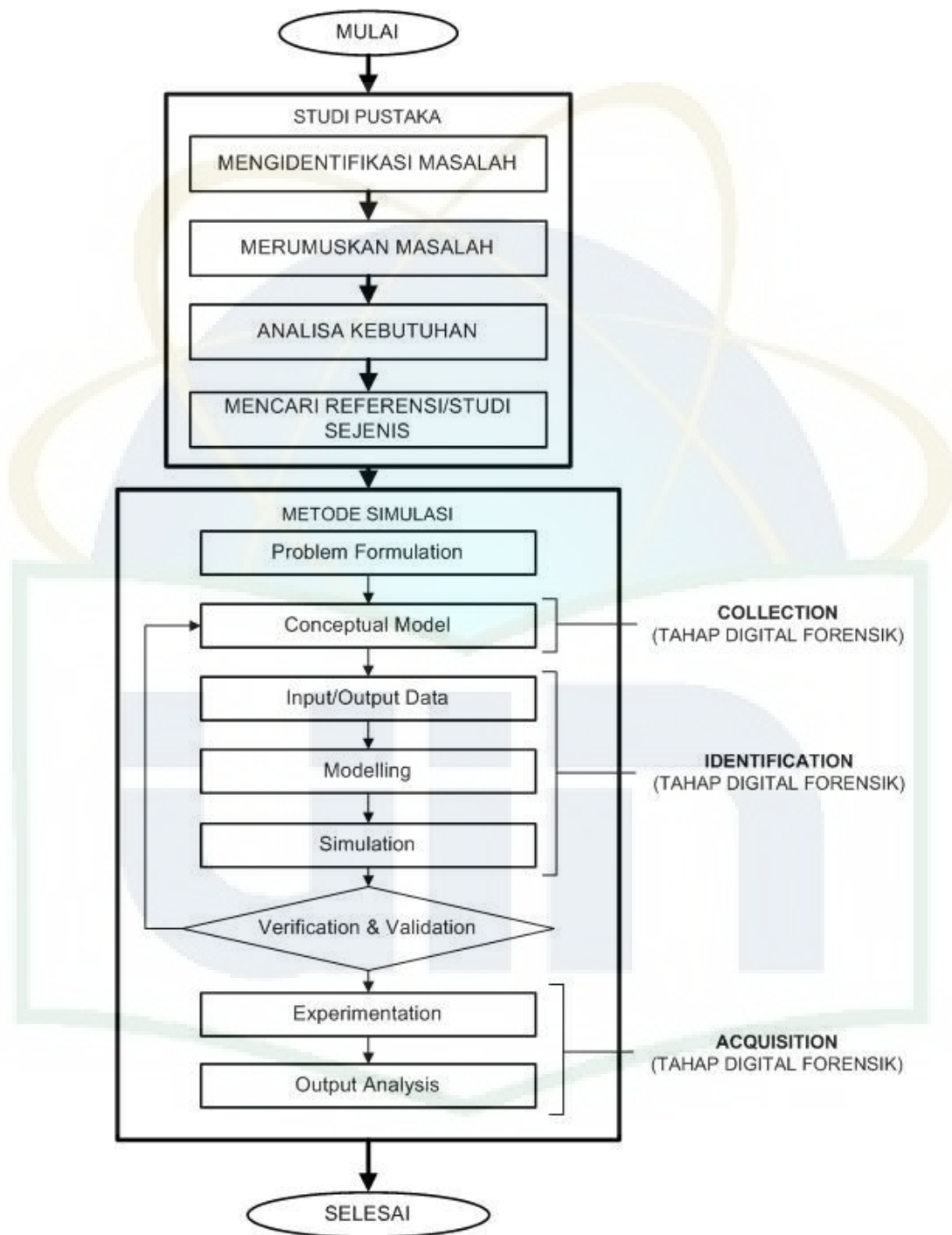
Tahap experimentation merupakan tahap paling penting dalam penelitian. Proses simulasi dari skenario yang telah ditentukan sebelumnya akan dijalankan pada tahap ini. Hasil yang didapat kemudian dianalisa untuk dilakukan perbandingan bukti forensik.

3.2.8 Output Analysis

Pada tahap ini dilakukan analisis *output* dari simulasi yang dilakukan pada tahap sebelumnya. Hasil penelitian dianalisa untuk mengetahui apakah bukti forensik berhasil ditemukan atau tidak dan untuk dilakukan perbandingan terhadap bukti forensik tersebut.

3.3 Kerangka Berpikir

Berikut ini kerangka berpikir yang penulis gunakan dalam penelitian ini:



Gambar 3.2 Kerangka Berpikir

BAB IV

IMPLEMENTASI SIMULASI DAN EKSPERIMEN

4.1 *Problem Formulation*

Perkembangan *smartphone* sudah sangat pesat terutama *smartphone* berbasis Android. Dan hal ini berbanding lurus dengan meningkatnya akses media sosial melalui *smartphone* berbasis Android. Berdasarkan data dari situs wearesocial.com tahun 2016 jumlah pengguna yang mengakses media sosial menggunakan *smartphone* sebanyak 1,97 Triliun.

Permasalahan utama dengan meningkatnya akses media sosial dengan menggunakan *smartphone* adalah maraknya tindak kejahatan yang dilakukan oleh pihak yang tidak bertanggung jawab dengan memanfaatkan media sosial yang diakses melalui *smartphone*. Berdasarkan data statistik dari Instant Checkmate pada tahun 2013, 81% kejahatan internet (*cyber crime*) melibatkan media sosial. 39% pengguna media sosial telah menjadi korban penipuan, *hacking* dan *fake link*. Dan 33% semua kejahatan seks pada dunia maya dipicu melalui situs jejaring sosial.

Beberapa penelitian yang telah dilakukan mengenai *mobile forensic* diantaranya adalah penelitian yang dilakukan oleh Ilman Zuhri Yadi dalam jurnalnya pada tahun 2014 yang berjudul Analisis Forensik Pada Platform Android. Penelitiannya berfokus pada identifikasi bukti forensik berupa SMS, *Call log*, kontak, file gambar yang disimpan dan lainnya, serta mengevaluasi kinerja *tool* ekstraksi dari ponsel Android. Penelitian tentang *mobile forensic* dilakukan pula oleh Noora Al Mutawa dalam jurnalnya pada tahun 2012 yang berjudul *Forensic Analysis of Social Networking Application on Mobile*. Penelitiannya berfokus pada pencarian dan analisa forensik terhadap berbagai jenis sistem operasi pada *smartphone* dan juga 3 jenis media sosial

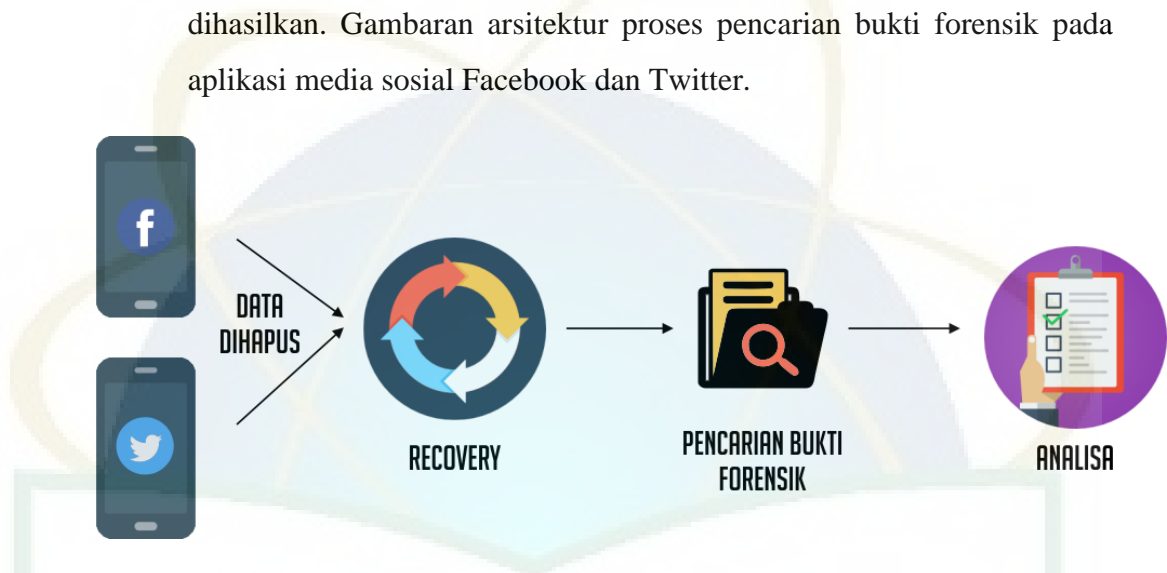
(Facebook tanpa aplikasi Facebook Messenger, Twitter dan MySpace), namun penelitian tersebut tidak terlalu spesifik dalam pencarian bukti forensik. Selain itu terdapat pula penelitian yang dilakukan oleh Walnycky tahun 2015 yang berjudul *Network and Device Forensic Analysis of Android Social-messaging Application*. Penelitian tersebut berfokus melakukan analisa forensik terhadap aplikasi *instant-messaging* pada *smartphone* berbasis Android. Beliau mencoba melakukan observasi terhadap *Network Traffic* dan pengambilan data aplikasi *instant-messaging* yang tersimpan pada *smartphone* tersebut.

Dengan tingginya jumlah pengguna yang mengakses media sosial dengan menggunakan *smartphone* dan tingginya angka kriminalitas pada media sosial, diperlukan upaya pencarian bukti forensik dan analisa untuk membantu pihak berwenang dalam menyelidiki kasus kejahatan yang melibatkan media sosial dan *smartphone*, karena pada dasarnya dalam dunia kriminal dikenal istilah “tidak ada kejahatan yang tidak meninggalkan jejak” (Indrajit, 2012). Menurut (Mutawa, Baggili, & Marrington, 2012) bukti forensik pada *smartphone* menjadi tambang emas bagi penyidik forensik karena sifat personalias dari kepemilikan *smartphone* tersebut. Dan menurut (Yadi & Kunang, 2014) Data yang diambil dari perangkat *smartphone* dengan sendirinya dapat dijadikan bukti. Bukti-bukti ini dapat menjadi landasan ketika menyelidiki suatu perkara oleh lembaga penegak hukum.

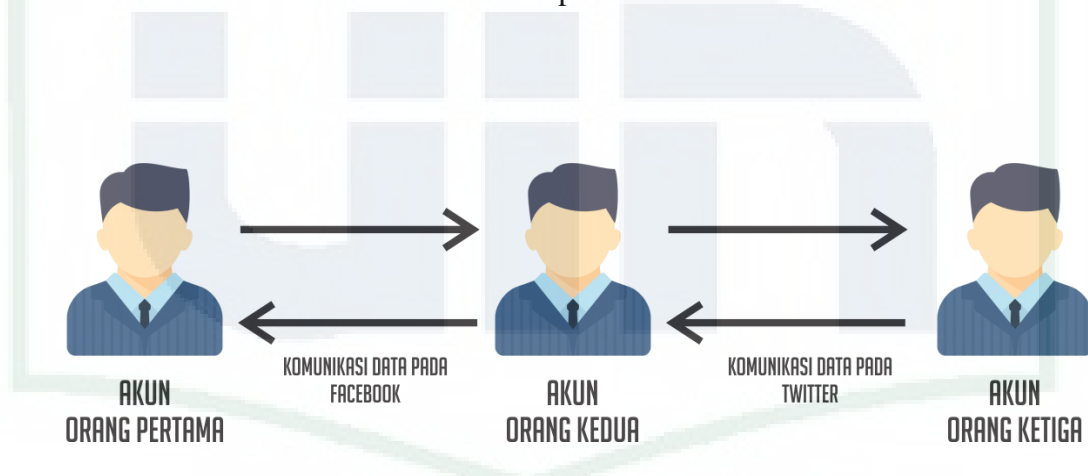
Berdasarkan pemaparan di atas, penulis akan melakukan analisis dan pencarian bukti forensik terhadap aplikasi media sosial Facebook dan Twitter yang diakses pada *smartphone* Android. Penelitian tersebut bertujuan untuk menemukan dan membandingkan bukti forensik yang ditemukan pada *smartphone* yang digunakan untuk mengakses media sosial.

4.2 Conceptual Model

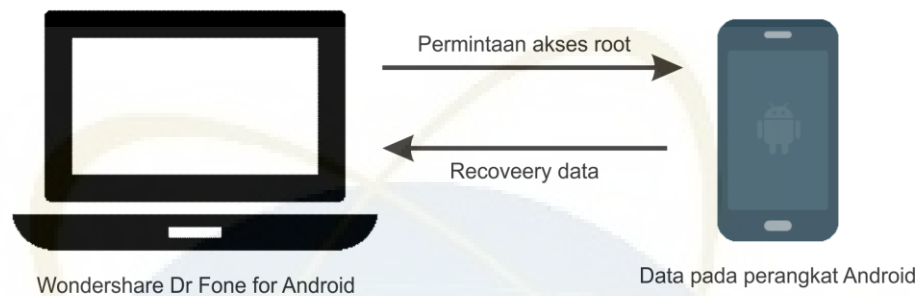
Dalam penelitian ini, tahap membuat konsep model merupakan tahap dilakukannya penggambaran dari *input*, proses dan *output* yang dihasilkan. Gambaran arsitektur proses pencarian bukti forensik pada aplikasi media sosial Facebook dan Twitter.



Gambar 4.1 Arsitektur simulasi pencarian dan analisa bukti forensik



Gambar 4.2 Arsitektur komunikasi data pada akun media sosial



Gambar 4.3 Proses recovery data

Gambar 4.1 menggambarkan arsitektur dalam pencarian dan analisa bukti forensik pada penelitian kali ini. Perbedaan hanya terdapat pada aplikasi media sosial yang digunakan. Sedangkan pada gambar 4.2 menggambarkan komunikasi data pada akun media sosial sebelum dilakukan pencarian bukti forensik pada aplikasi media sosial tersebut. Selain itu penulis melakukan penghapusan data pada aplikasi media sosial dengan asumsi bahwa data tersebut dihapus oleh pelaku tindak kriminal untuk menghilangkan jejak kejahatan. Pada gambar 4.3 menggambarkan proses *recovery data* menggunakan aplikasi Wondershare Dr Fone for Android. Aplikasi tersebut meminta akses root pada perangkat Android dan data hasil *recovery* akan disimpan pada perangkat komputer. Komponen pada tiap-tiap arsitektur adalah sebagai berikut:

4.2.1 *Smartphone*

Smartphone digunakan sebagai *platform* untuk mengakses media sosial Facebook dan Twitter. *Smartphone* yang digunakan oleh penulis adalah *smartphone* bermerek Xiaomi Redmi 2 berbasis Android Versi 4.4.4 (Kitkat) yang telah mendapat akses *root*.

4.2.2 Aplikasi media sosial

Aplikasi media sosial yang diinstall pada smartphone adalah Facebook Apps versi 77.0.0.20.66, Facebook Messenger versi 70.0.0.12.68 dan Twitter Apps versi 5.109.0.

4.2.3 Aplikasi *recovery file*

Aplikasi *recovery* digunakan untuk mengembalikan data yang sebelumnya telah dihapus untuk menghilangkan bukti forensik. Aplikasi yang penulis gunakan adalah Wondershare Dr. Fone for Android. Aplikasi ini akan meminta akses *root* untuk dapat melakukan *recovery* pada *smartphone*.

4.2.4 Aplikasi *Database Browser*

Database Tool digunakan untuk melakukan analisa dan pencarian terhadap bukti forensik yang tersimpan pada *database* yang sebelumnya berhasil dikembalikan dengan menggunakan aplikasi *recovery*. Aplikasi *database* yang digunakan adalah SQLite Manager dan DB Browser for SQLite.

4.2.5 Akun Palsu Media Sosial

Akun palsu digunakan dalam pencarian bukti forensik. Sebelum dilakukan pencarian bukti forensik terlebih dahulu dilakukan komunikasi data antara akun media sosial tersebut. Berdasarkan gambar 4.2 akun orang pertama akan melakukan komunikasi data dengan akun orang kedua melalui Facebook dimana posisi orang pertama adalah pelaku kejahatan dan orang kedua adalah korban. Sedangkan akun orang ketiga akan melakukan komunikasi data dengan akun orang kedua melalui Twitter dimana posisi orang ketiga adalah pelaku kejahatan dan orang kedua adalah korban.

4.2.6 Output/Bukti forensik yang ditemukan

Setelah pencarian bukti forensik pada *database* telah selesai, maka bukti forensik pada aplikasi media sosial Facebook dan Twitter akan saling dibandingkan sesuai dengan skenario yang dilakukan.

4.3 Input Output Data

4.3.1 Input

Pada tahap ini merupakan proses penentuan *input* yang akan digunakan dalam penelitian. Input pada penelitian yang akan digunakan pada aplikasi media sosial Facebook dan Twitter adalah sama yang berupa teks dan gambar diantaranya adalah :

Table 4.1 Bukti forensik yang akan dicari

| No. | Data yang di-input & bukti forensik yang dicari | Bentuk data | Isi teks dan file gambar |
|-----|---|-------------|--------------------------|
| 1. | Nama akun | Teks | Pratama Pertama |
| 2. | Lokasi | Teks | Semarang, Indonesia |
| 3. | Nomor telepon | Teks | +6285776267290 |
| 4. | Tanggal lahir | Teks | 1 Januari 1991 |
| 5. | <i>Photo profile</i> | Gambar | Profile.jpg |
| 6. | <i>Cover Photo</i> | Gambar | Siput.jpg |
| 7. | <i>Posting</i> berupa teks | Teks | Test 1 2 3 |
| 8. | <i>Posting</i> berupa gambar | Gambar | 3310.jpg |

| | | | |
|-----|-----------------------------------|--------|---|
| 9. | Isi private message berupa teks | Teks | Percakapan 2 pihak terkait jual beli <i>handphone</i> |
| 10. | Isi private message berupa gambar | Gambar | Nokia3310.jpg |

4.3.2 Output

Output pada penelitian ini adalah data aplikasi media sosial yang telah dihapus dan bukti forensik yang didapatkan pada aplikasi media Facebook dan Twitter yang diakses pada *smartphone* berbasis Android.

4.4 Modeling

Pada simulasi pencarian bukti forensik pada aplikasi media sosial Facebook dan Twitter ini dilakukan beberapa kali pengujian dengan beberapa skenario yang berbeda. Pada jurnal (Mutawa, Baggili, & Marrington, 2012), bukti forensik yang dicari adalah berupa *photo profile*, *posting*, *username* dan *private message*. Untuk itu penulis menambahkan beberapa skenario pencarian bukti forensik. Skenario yang akan dijalankan pada simulasi ini adalah sebagai berikut:

4.4.1 Skenario 1

Table 4.2 Skenario 1

| No. | Aplikasi Media Sosial | Data yang hapus | Data yang diharapkan berhasil dikembalikan |
|-----|-----------------------|--|--|
| 1. | Facebook | Apliaksi dan seluruh data pada aplikasi tersebut | <i>File database</i> |
| 2. | Twitter | Apliaksi dan seluruh data pada aplikasi tersebut | <i>File database</i> |

Pada skenario 1 dilakukan *uninstall* dan penghapusan seluruh data aplikasi media sosial Facebook dan Twitter. Hal ini bertujuan untuk mengasumsikan bahwa data dihapus oleh pelaku kriminal. Setelah itu dilakukan pengembalian data yang telah terhapus tersebut dengan menggunakan aplikasi *recovery file*.

4.4.2 Skenario 2

Table 4.3 Skenario 2

| No. | Aplikasi Media Sosial | Bukti Forensik | Bentuk data |
|-----|-----------------------|----------------|-------------|
| 1. | Facebook | Nama akun | Teks |
| 2. | Twitter | Nama akun | Teks |

Pada skenario 2 hingga 11 adalah skenario dalam pencarian bukti forensik pada aplikasi media sosial Facebook dan Twitter. Skenario tersebut dilakukan secara manual dengan melakukan pencarian bukti forensik pada *file database* dengan bantuan aplikasi SQLite Manager.

4.4.3 Skenario 3

Table 4.4 Skenario 3

| No. | Aplikasi Media Sosial | Bukti Forensik | Bentuk data |
|-----|-----------------------|----------------------|-------------|
| 1. | Facebook | Email yang digunakan | Teks |
| 2. | Twitter | Email yang digunakan | Teks |

4.4.4 Skenario 4

Table 4.5 Skenario 4

| No. | Aplikasi Media Sosial | Bukti Forensik | Bentuk data |
|-----|-----------------------|----------------|-------------|
|-----|-----------------------|----------------|-------------|

| | | | |
|----|----------|--------------|------|
| 1. | Facebook | Nomor telpon | Teks |
| 2. | Twitter | Nomor telpon | Teks |

4.4.5 Skenario 5

Table 4.6 Skenario 5

| No. | Aplikasi Media Sosial | Bukti Forensik | Bentuk data |
|-----|-----------------------|----------------|-------------|
| 1. | Facebook | Tanggal lahir | Teks |
| 2. | Twitter | Tanggal lahir | Teks |

4.4.6 Skenario 6

Table 4.7 Skenario 6

| No. | Aplikasi Media Sosial | Bukti Forensik | Bentuk data |
|-----|-----------------------|----------------------|-------------|
| 1. | Facebook | <i>Photo profile</i> | Gambar |
| 2. | Twitter | <i>Photo profile</i> | Gambar |

4.4.7 Skenario 7

Table 4.8 Skenario 7

| No. | Aplikasi Media Sosial | Bukti Forensik | Bentuk data |
|-----|-----------------------|--------------------|-------------|
| 1. | Facebook | <i>Cover photo</i> | Gambar |
| 2. | Twitter | <i>Cover photo</i> | Gambar |

4.4.8 Skenario 8

Table 4.9 Skenario 8

| No. | Aplikasi Media Sosial | Bukti Forensik | Bentuk data |
|-----|-----------------------|----------------|-------------|
|-----|-----------------------|----------------|-------------|

| | | | |
|----|----------|------------------|------|
| 1. | Facebook | <i>Posting 1</i> | Teks |
| 2. | Twitter | <i>Tweet 1</i> | Teks |

4.4.9 Skenario 9

Table 4.10 Skenario 9

| No. | Aplikasi Media Sosial | Bukti Forensik | Bentuk data |
|-----|-----------------------|------------------|-------------|
| 1. | Facebook | <i>Posting 2</i> | Gambar |
| 2. | Twitter | <i>Tweet 2</i> | Gambar |

4.4.10 Skenario 10

Table 4.11 Skenario 10

| No. | Aplikasi Media Sosial | Bukti Forensik | Bentuk data |
|-----|-----------------------|-----------------------------------|-------------|
| 1. | Facebook | Kirim <i>private message</i> 1 | Teks |
| 2. | Twitter | Kirim <i>direct message</i> 1 | Teks |

4.4.11 Skenario 11

Table 4.12 Skenario 11

| No. | Aplikasi Media Sosial | Bukti Forensik | Bentuk data |
|-----|-----------------------|-----------------------------------|-------------|
| 1. | Facebook | Kirim <i>private message</i> 2 | Gambar |
| 2. | Twitter | Kirim <i>direct message</i> 2 | Gambar |

4.5 Simulation

Proses simulasi akan dijalankan menggunakan skenario yang telah ditentukan pada tahap sebelumnya pada tahap ini. Selain itu, pengujian dilakukan sesuai dengan parameter yang telah ditentukan juga pada tahap sebelumnya.

4.5.1 Rooting pada Perangkat Android

Proses *rooting* pada perangkat Android merk Xiaomi Redmi 2 dilakukan dengan cara sebagai berikut:

1. Mengunduh file Root.zip pada internet. File ini akan dipasang pada perangkat Android.
2. Buka aplikasi Updater, kemudian pilih opsi “Choose Update Package”, kemudian navigasikan pada file Root.zip yang telah diunduh sebelumnya. Setelah itu perangkat akan melakukan *reboot* otomatis dan melakukan *flashing* untuk memasang file Root.zip.
3. Setelah proses *flashing* telah selesai maka akan muncul aplikasi SuperSu. Buka aplikasi tersebut lalu lakukan *update*. Kemudian pilih “Normal” saat aplikasi SuperSu menanyakan metode *recovery* mana yang akan digunakan. Maka proses *rooting* telah selesai.

4.5.2 Pembuatan Akun Palsu pada Media Sosial

Pembuatan akun palsu dilakukan untuk melakukan simulasi pada pencarian bukti forensik pada aplikasi media sosial Facebook dan Twitter. Akun palsu yang dibuat diantaranya:

4.5.2.1 Dataset

Table 4.13 Akun Gmail palsu

| No. | Alamat Email | Kata Sandi |
|-----|----------------------------|---------------|
| 1 | orangpertama1111@gmail.com | orangpertama1 |

| | | |
|---|---------------------------|--------------|
| 2 | orangkedua2222@gmail.com | orangkedua2 |
| 3 | orangketiga3333@gmail.com | orangketiga3 |

4.5.2.2 Akun Media Sosial Palsu

Table 4.14 Akun Media Sosial Palsu

| No. | Alamat Email | Media Sosial | Perangkat yang digunakan | Status |
|-----|----------------------------|--------------|--------------------------|--|
| 1 | orangpertama1111@gmail.com | Facebook | <i>Smartphone</i> | Tersangka (yang akan dicari bukti forensiknya) |
| 2 | orangkedua2222@gmail.com | Facebook | Komputer | Korban |
| | | Twitter | | |
| 3 | orangketiga3333@gmail.com | Twitter | <i>Smartphone</i> | Tersangka (yang akan dicari bukti forensiknya) |

4.5.3 Pemasangan Aplikasi *Recovery File*

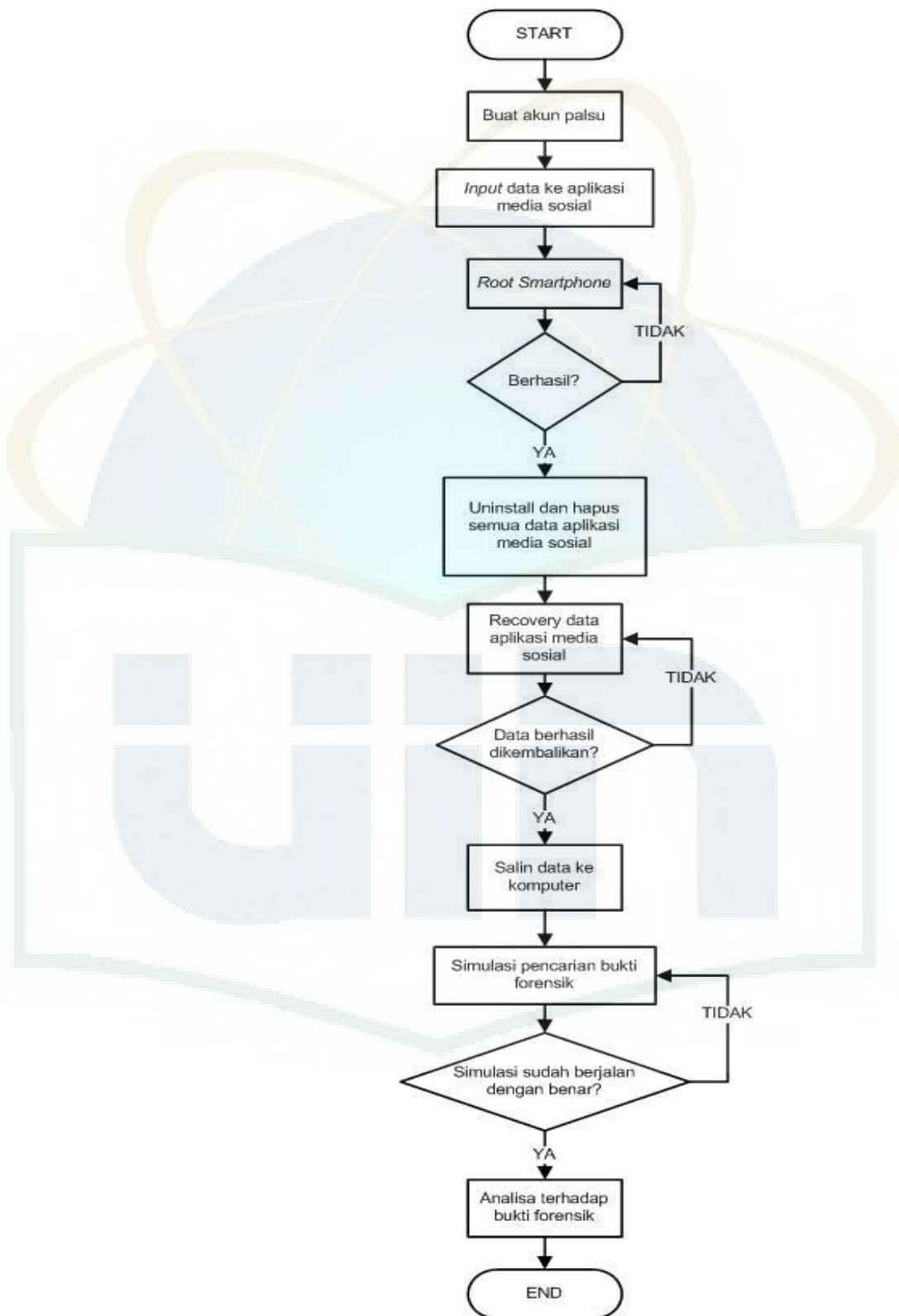
1. Melakukan instalasi Wondershare Dr. Fone for Android (dengan klik 2 kali pada *installer* aplikasi tersebut) pada komputer untuk mengembalikan data yang dihapus pada Android dan menyimpan hasil pengembalian data tersebut.
2. Untuk melakukan recovery data pada *smartphone*, hubungkan *smartphone* dengan komputer maka aplikasi Wondershare Dr. Fone for Android akan mendeteksi jenis *smartphone* dan meminta persetujuan untuk melakukan proses *recovery*.
3. Aplikasi Wondershare Dr. Fone for Android dapat berjalan bila *smartphone* telah dilakukan proses *root* sebelumnya.

4.5.4 Pemasangan Aplikasi SQLite Manager

1. Melakukan instalasi aplikasi SQLite Manager dengan cara membuka aplikasi Mozilla Firefox terlebih dahulu setelah itu melakukan instalasi pada aplikasi DB Browser for SQLite.
2. Setelah itu pilih menu Tools, kemudian pilih Add-ons. Setelah itu cari add-ons SQLite Manager kemudian install.
3. Untuk melihat isi database yang ada, pilih menu open kemudian navigasikan pada *file database* yang akan dianalisa.

4.5.5 Flowchart Simulasi

Berikut ini flowchart simulasi pencarian dan analisa bukti forensik pada aplikasi media sosial Facebook dan Twitter pada *smartphone* Android. Simulasi yang dilakukan diasumsikan pada kejadian nyata.



Gambar 4.4 Flowchart Simulasi

4.6 *Verification and Validation*

Penjelasan dan pemaparan mengenai verifikasi dan validasi dijelaskan pada BAB V penelitian ini tentang hasil dan pembahasan.

4.7 *Experimentation*

Penjelasan dan pemaparan mengenai verifikasi dan validasi dijelaskan pada BAB V penelitian ini tentang hasil dan pembahasan.

4.8 *Output Analisis*

Penjelasan dan pemaparan mengenai verifikasi dan validasi dijelaskan pada BAB V penelitian ini tentang hasil dan pembahasan.

BAB V

HASIL DAN PEMBAHASAN

5.1 Verification & Validation

Verifikasi dan validasi dari tahap-tahap sebelumnya dilakukan pada tahap ini. Jika terjadi kesalahan pada masing-masing tahap metode simulasi maka akan dilakukan koreksi atau perbaikan pada tahap tersebut. Verifikasi dilakukan dengan menguji apakah proses *root* pada *smartphone* berhasil dilakukan atau tidak dan menguji apakah aplikasi *recovery file* (Wondershare Dr. Fone for Android) dan *database browser* (SQLite Manager dan DB Browser for SQLite) dapat berjalan. Sedangkan validasi dilakukan dengan cara mengecek kembali apakah akses *root* pada *smartphone* berjalan lancar tanpa terdapat kesalahan dan mengecek kembali aplikasi *recovery file* (Wondershare Dr. Fone for Android) dan *database browser* (SQLite Manager dan DB Browser for SQLite) telah sesuai dengan ketentuan pada *conceptual model*, *input output data*, dan *modelling*.

5.2 Experimentation

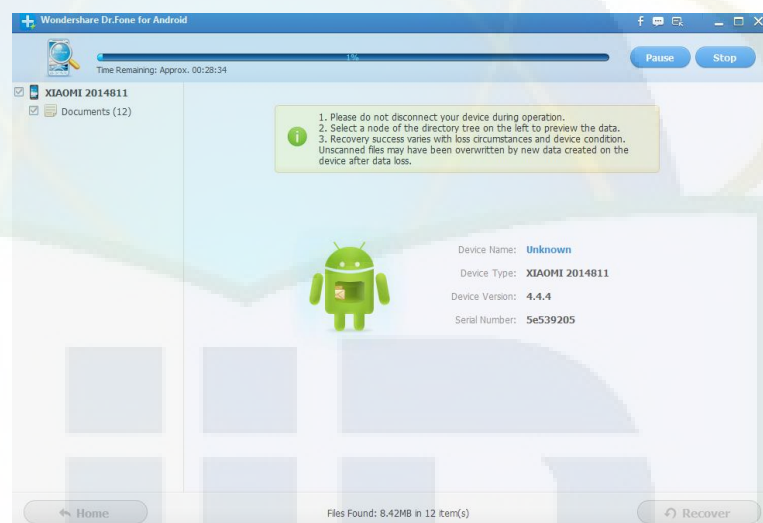
Setelah proses *root* pada *smartphone* berhasil dilakukan tanpa ada kesalahan dan aplikasi *recovery file* (Wondershare Dr. Fone for Android) dan *database browser* (SQLite Manager dan DB Browser for SQLite) telah terpasang, maka akan dilakukan proses simulasi pencarian bukti forensik pada aplikasi media sosial yang diakses menggunakan *smartphone* berbasis Android sesuai dengan konsep, model dan flowchart simulasi yang telah dijelaskan sebelumnya. Setelah proses pencarian bukti forensik selesai, maka akan dilakukan analisa terhadap bukti-bukti forensik tersebut.

5.3 Output Analysis

5.3.1 Hasil Simulasi Skenario 1

5.3.1.1 Percobaan 1

Percobaan pertama skenario 1 dilakukan untuk mengembalikan data-data yang dihapus pada aplikasi media sosial Facebook dengan menggunakan aplikasi Wondershare Dr. Fone for Android.



Gambar 55.1 Proses *recovery* data aplikasi Facebook dan Twitter

Pada percobaan ini berhasil ditemukan file aplikasi media sosial Facebook yang sebelumnya telah dihapus.

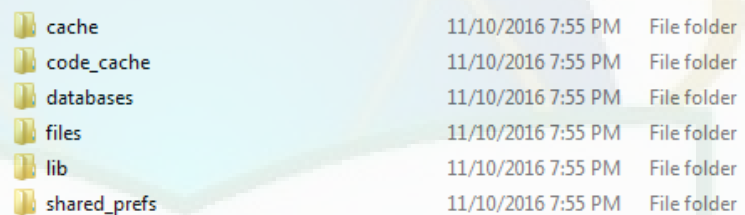
| | | | | | |
|-----------------------------|--------------------|-------------|-----------------------------|--------------------|-------------|
| app_acra-reports | 9/26/2016 12:28 PM | File folder | app_acra-reports | 9/26/2016 12:28 PM | File folder |
| app_analytics | 9/26/2016 12:28 PM | File folder | app_gatekeepers | 9/26/2016 12:28 PM | File folder |
| app_analytics_beacon | 9/26/2016 12:28 PM | File folder | app_light_prefs | 9/26/2016 12:28 PM | File folder |
| app_funnel_beacon | 9/26/2016 12:28 PM | File folder | app_omnistore | 9/26/2016 12:28 PM | File folder |
| app_gatekeepers | 9/26/2016 12:28 PM | File folder | app_qe_sessioned | 9/26/2016 12:28 PM | File folder |
| app_light_prefs | 9/26/2016 12:28 PM | File folder | app_qe_sessionless | 9/26/2016 12:28 PM | File folder |
| app_omnistore | 9/26/2016 12:28 PM | File folder | app_sessionless_gatekeepers | 9/26/2016 12:28 PM | File folder |
| app_permissions | 9/26/2016 12:28 PM | File folder | app_state_logs | 9/26/2016 12:28 PM | File folder |
| app_qe_sessioned | 9/26/2016 12:28 PM | File folder | app_webview | 9/26/2016 12:28 PM | File folder |
| app_qe_sessionless | 9/26/2016 12:28 PM | File folder | cache | 9/26/2016 12:28 PM | File folder |
| app_sessionless_gatekeepers | 9/26/2016 12:28 PM | File folder | databases | 9/26/2016 12:28 PM | File folder |
| app_state_logs | 9/26/2016 12:28 PM | File folder | dex | 9/26/2016 12:28 PM | File folder |
| app_webview | 9/26/2016 12:28 PM | File folder | files | 9/26/2016 12:28 PM | File folder |
| cache | 9/26/2016 12:28 PM | File folder | lib | 9/26/2016 12:28 PM | File folder |
| databases | 9/27/2016 1:52 AM | File folder | lib-assets | 9/26/2016 12:28 PM | File folder |
| dex | 9/26/2016 12:29 PM | File folder | lib-main | 9/26/2016 12:28 PM | File folder |
| files | 9/26/2016 12:29 PM | File folder | lib-zxs | 9/26/2016 12:28 PM | File folder |
| lib | 9/26/2016 12:29 PM | File folder | shared_prefs | 9/26/2016 12:28 PM | File folder |
| lib-assets | 9/26/2016 12:29 PM | File folder | crash_lock | 9/26/2016 12:26 PM | File |
| lib-main | 9/26/2016 12:29 PM | File folder | crash_log | 9/26/2016 12:26 PM | File |
| lib-zxs | 9/26/2016 12:29 PM | File folder | | | |
| shared_prefs | 9/26/2016 12:25 PM | File | | | |
| crash_lock | 9/26/2016 12:25 PM | File | | | |
| crash_log | 9/26/2016 12:25 PM | File | | | |

Gambar 5.2 Data pada aplikasi Facebook yang berhasil dikembalikan

5.3.1.2 Percobaan 2

Percobaan kedua skenario 1 dilakukan untuk mengembalikan data-data yang dihapus pada aplikasi media sosial Twitter dengan menggunakan aplikasi Wondershare Dr. Fone for Android. Proses *recovery file* sama dengan Gambar 5.1 diatas.

Pada percobaan ini berhasil ditemukan file aplikasi media sosial Twitter yang sebelumnya telah dihapus.



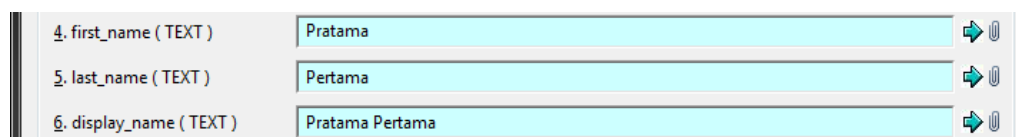
| | | |
|--------------|--------------------|-------------|
| cache | 11/10/2016 7:55 PM | File folder |
| code_cache | 11/10/2016 7:55 PM | File folder |
| databases | 11/10/2016 7:55 PM | File folder |
| files | 11/10/2016 7:55 PM | File folder |
| lib | 11/10/2016 7:55 PM | File folder |
| shared_prefs | 11/10/2016 7:55 PM | File folder |

Gambar 5.3 Data pada aplikasi Twitter yang berhasil dikembalikan.

5.3.2 Hasil Simulasi Skenario 2

5.3.2.1 Percobaan 1

Percobaan pertama skenario 2 dilakukan untuk mencari bukti forensik berupa nama akun pengguna aplikasi media sosial Facebook pada *smartphone* Android menggunakan aplikasi SQLite Manager. Akun palsu yang digunakan adalah **Orang Pertama**.



| | | |
|--------------------------|-----------------|-----|
| 4. first_name (TEXT) | Pratama | ➡ 🔒 |
| 5. last_name (TEXT) | Pertama | ➡ 🔒 |
| 6. display_name (TEXT) | Pratama Pertama | ➡ 🔒 |

Gambar 5.4 Nama akun pengguna aplikasi media sosial Facebook aplikasi SQLite Manager

Pada percobaan dengan aplikasi SQLite Browser, berhasil ditemukan nama akun dari pengguna aplikasi media sosial Facebook. Bukti forensik ditemukan pada *file database* **contact_db2**, pada tabel **contacts**. Pada gambar 5.4 dapat diketahui bahwa pengguna bernama **Pratama Pertama**.

Setelah itu dilakukan percobaan dengan menggunakan aplikasi DB Browser for SQLite.

| first_name | last_name | display_name |
|------------|-----------|-----------------|
| Filter | Filter | Filter |
| Pratama | Pertama | Pratama Pertama |

Gambar 5.5 Nama akun pengguna aplikasi media sosial Facebook aplikasi DB Browser fo SQLite

Pada percobaan dengan aplikasi DB Browser for SQLite, berhasil ditemukan nama akun dari pengguna aplikasi media sosial Facebook. Bukti forensik ditemukan pada *file database* **contact_db2**, pada tabel **contacts**. Pada gambar 5.5 dapat diketahui bahwa pengguna bernama **Pratama Pertama**.

5.3.2.2 Percobaan 2


Percobaan kedua skenario 2 dilakukan untuk mencari bukti forensik berupa nama akun pengguna aplikasi media sosial Twitter pada *smartphone* Android menggunakan aplikasi SQLite Manager. Akun palsu yang digunakan adalah **Orang Ketiga**.

| | |
|----------------------|-----------------|
| 3. username (TEXT) | Pratama1_satu |
| 4. name (TEXT) | Pratama Pertama |

Gambar 5.6 Nama akun pengguna media sosial Twitter aplikasi SQLite Manager

Pada percobaan ini berhasil ditemukan nama akun dari pengguna aplikasi media sosial Facebook. Bukti forensik ditemukan pada *file database 732798704059621380-43*, pada tabel **users**. Pada gambar 5.6 dapat diketahui bahwa pengguna bernama **Pratama Pertama** dengan *username* **Pratama1_satu**.

Setelah itu dilakukan percobaan dengan menggunakan aplikasi DB Browser for SQLite.

| _id | user_id | username | name |
|--------|--------------------|---|-----------------|
| Filter | Filter | Prata  | Filter |
| 1 | 732798704059621380 | Pratama1_satu | Pratama Pertama |

Gambar 5.7 Nama akun pengguna media sosial Twitter aplikasi DB Browser for SQLite

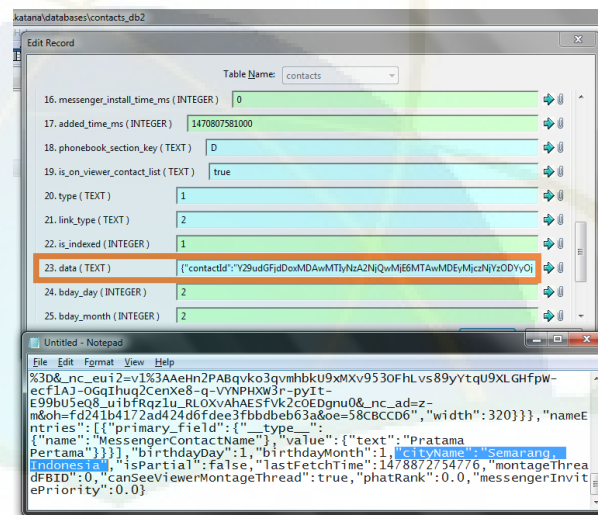
Pada percobaan ini berhasil ditemukan nama akun dari pengguna aplikasi media sosial Facebook. Bukti forensik ditemukan pada *file database 732798704059621380-43*, pada tabel **users**. Pada gambar 5.7 dapat diketahui bahwa pengguna bernama **Pratama Pertama** dengan *username* **Pratama1_satu**.

5.3.3 Hasil Simulasi Skenario 3

5.3.3.1 Percobaan 1

Percobaan pertama skenario 3 dilakukan untuk mencari bukti forensik berupa lokasi pengguna aplikasi

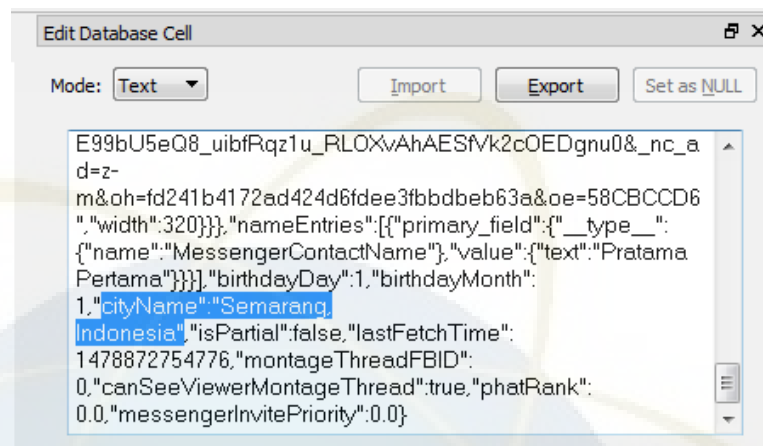
media sosial Facebook pada *smartphone* Android menggunakan SQLite Manager. Akun palsu yang digunakan adalah **Orang Pertama**.



Gambar 5.8 Bukti forensik berupa lokasi pada Facebook menggunakan SQLite Manager

Pada percobaan ini berhasil ditemukan lokasi dari pengguna aplikasi media sosial Facebook. Bukti forensik ditemukan pada *file database contact_db2*, pada tabel **contacts**, dan pada kolom **data**. Pada gambar 5.8 diatas, isi dari kolom data sangat panjang sehingga isi dari kolom tersebut disalin pada aplikasi notepad untuk memudahkan pencarian bukti forensik. dapat diketahui bahwa lokasi pengguna adalah **Semarang, Indonesia**.

Setelah itu dilakukan percobaan dengan menggunakan aplikasi DB Browser for SQLite.



Gambar 5.9 Bukti forensik berupa lokasi pada Facebook menggunakan DB Browser for SQLite

Pada percobaan ini berhasil ditemukan lokasi dari pengguna aplikasi media sosial Facebook. Bukti forensik ditemukan pada *file database contact_db2*, pada tabel **contacts**, dan pada kolom **data**. Pada gambar 5.9 diatas dapat diketahui bahwa lokasi pengguna adalah **Semarang, Indonesia**.

5.3.3.2 Percobaan 2

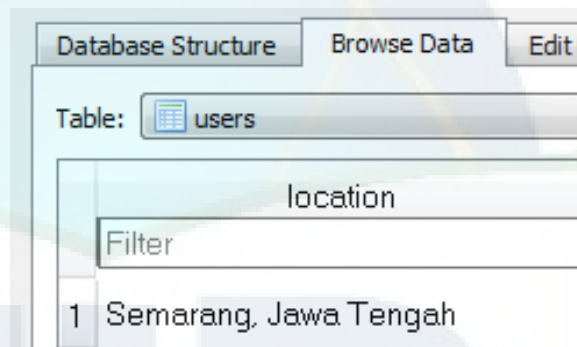
Percobaan kedua skenario 3 dilakukan untuk mencari bukti forensik berupa lokasi pengguna aplikasi media sosial Twitter pada *smartphone* Android dengan menggunakan SQLite Manager. Akun palsu yang digunakan adalah **Orang Ketiga**.

| | |
|--------------------------------------|---|
| 13. extended_profile_fields (BLOB) | X'491D0A2B6C89EF572004120112011307C11D00000158D1830C66496A065055424C494358' |
| 14. location (TEXT) | Semarang, Jawa Tengah |
| 15. structured_location (BLOB) | X'493858' |

Gambar 5.10 Bukti forensik berupa lokasi pada Twitter dengan SQLite Manager

Pada percobaan ini berhasil ditemukan lokasi dari pengguna aplikasi media sosial Twitter. Bukti forensik ditemukan pada *file database* **732798704059621380-43**, pada tabel **users**. Pada gambar 5.10 diatas dapat diketahui bahwa lokasi pengguna adalah **Semarang, Indonesia**.

Setelah itu dilakukan percobaan dengan menggunakan aplikasi DB Browser for SQLite.



Gambar 5.11 Bukti forensik berupa lokasi pada Twitter dengan DB Browser for SQLite

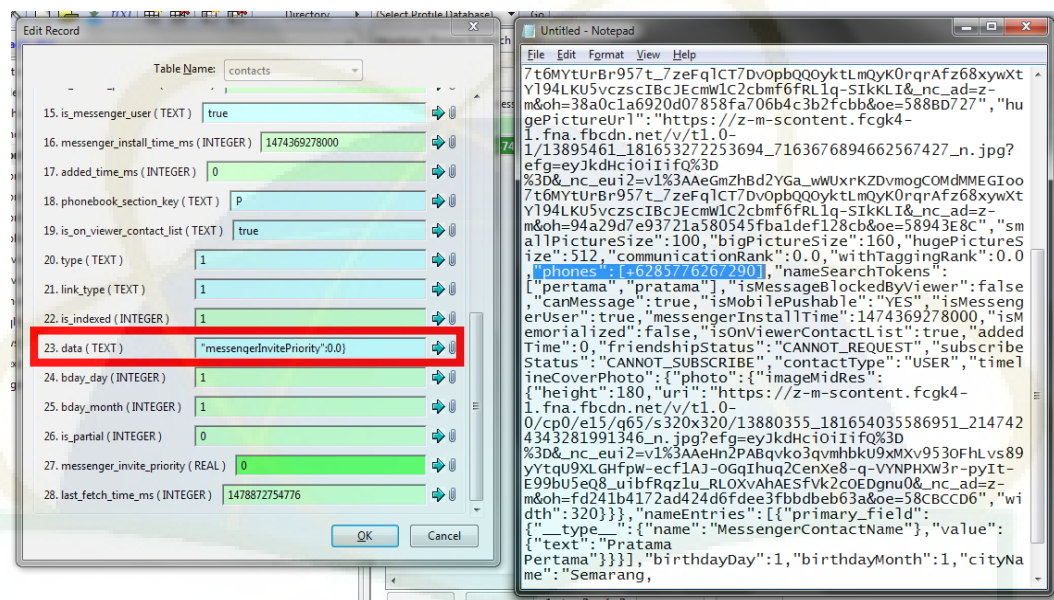
Pada percobaan ini berhasil ditemukan lokasi dari pengguna aplikasi media sosial Twitter. Bukti forensik ditemukan pada *file database* **732798704059621380-43**, pada tabel **users**. Pada gambar 5.11 diatas dapat diketahui bahwa lokasi pengguna adalah **Semarang, Indonesia**.

5.3.4 Hasil Simulasi Skenario 4

5.3.4.1 Percobaan 1

Percobaan pertama skenario 4 dilakukan untuk mencari bukti forensik berupa nomor telepon pengguna aplikasi media sosial Facebook pada *smartphone*

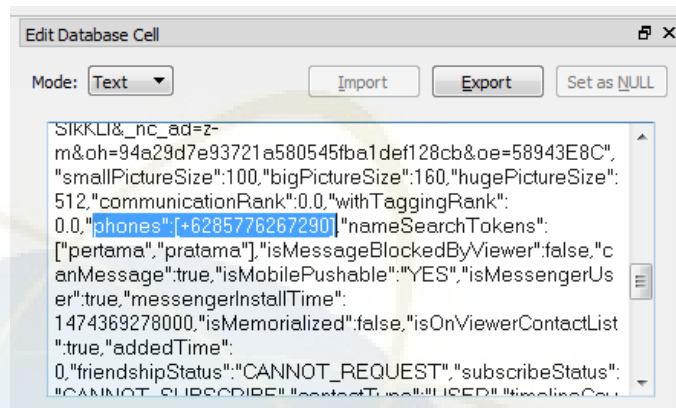
Android menggunakan SQLite Manager. Akun palsu yang digunakan adalah **Orang Pertama**.



Gambar 5.12 Bukti forensik berupa nomor telepon dengan SQLite Manager

Pada percobaan ini berhasil ditemukan nomor telepon dari pengguna aplikasi media sosial Facebook. Bukti forensik ditemukan pada *file database contact_db2*, pada tabel **contacts**, dan pada kolom **data**. Pada gambar 5.8 diatas, isi dari kolom data sangat panjang sehingga isi dari kolom tersebut disalin pada aplikasi notepad untuk memudahkan pencarian bukti forensik. dapat diketahui bahwa nomor telepon pengguna adalah **+6285776267290**.

Setelah itu dilakukan percobaan dengan menggunakan aplikasi DB Browser for SQLite.



Gambar 5.13 Bukti forensik berupa nomor telepon dengan DB Browser for SQLite

Pada percobaan ini berhasil ditemukan nomor telepon dari pengguna aplikasi media sosial Facebook. Bukti forensik ditemukan pada *file database contact_db2*, pada tabel **contacts**, dan pada kolom **data**. Pada gambar 5.13 diatas dapat diketahui bahwa nomor telepon pengguna adalah **+6285776267290**.

5.3.4.2 Percobaan 2

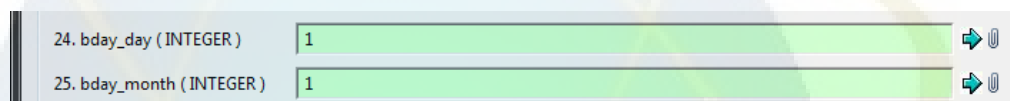
Percobaan kedua skenario 4 dilakukan untuk mencari bukti forensik berupa nomor telepon pengguna aplikasi media sosial Twitter pada *smartphone* Android menggunakan SQLite Manager. Akun palsu yang digunakan adalah **Orang Ketiga**.

Pada pencarian bukti forensik berupa nomor telepon pada aplikasi media sosial Twitter tidak berhasil ditemukan bahkan pada aplikasi DB Browser for SQLite.

5.3.5 Hasil Simulasi Skenario 5

5.3.5.1 Percobaan 1

Percobaan pertama skenario 5 dilakukan untuk mencari bukti forensik berupa tanggal lahir pengguna aplikasi media sosial Facebook pada *smartphone* Android. Akun palsu yang digunakan adalah **Orang Pertama**.

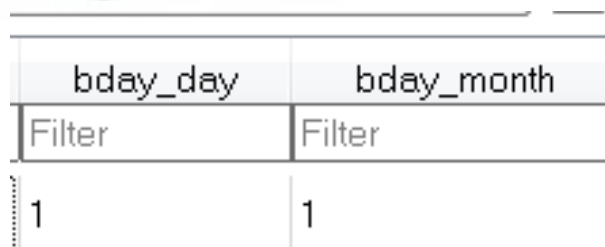


| | | | |
|--------------------------|---|---|---|
| 24. bday_day (INTEGER) | 1 | ➡ | 📄 |
| 25. bday_month (INTEGER) | 1 | ➡ | 📄 |

Gambar 5.14 Bukti forensik berupa tanggal lahir pada Facebook dengan SQLite Manager

Pada percobaan ini berhasil ditemukan tanggal lahir dari pengguna aplikasi media sosial Facebook. Bukti forensik ditemukan pada *file database* **contact_db2**, pada tabel **contacts**. Pada gambar 5.14 diatas dapat diketahui bahwa pengguna lahir pada tanggal **1 Januari**. Namun sayangnya tahun kelahiran pengguna tidak ditemukan pada *database*.

Setelah itu dilakukan percobaan dengan menggunakan aplikasi DB Browser for SQLite.



| bday_day | bday_month |
|----------|------------|
| Filter | Filter |
| 1 | 1 |

Gambar 5.15 Bukti forensik berupa tanggal lahir pada Facebook dengan DB Browser for SQLite

Pada percobaan ini juga berhasil ditemukan tanggal lahir dari pengguna aplikasi media sosial Facebook. Bukti forensik ditemukan pada *file database contact_db2*, pada tabel **contacts**. Pada gambar 5.15 diatas dapat diketahui bahwa pengguna lahir pada tanggal **1 Januari**. Namun sayangnya tahun kelahiran pengguna tidak ditemukan pada *database*.

5.3.5.2 Percobaan 2

Percobaan kedua skenario 5 dilakukan untuk mencari bukti forensik berupa tanggal lahir pengguna aplikasi media sosial Twitter pada *smartphone* Android. Akun palsu yang digunakan adalah **Orang Ketiga**.

Pada pencarian bukti forensik berupa tanggal lahir pada aplikasi media sosial Twitter tidak berhasil ditemukan bahkan pada aplikasi DB Browser for SQLite.

5.3.6 Hasil Simulasi Skenario 6

5.3.6.1 Percobaan 1

Percobaan pertama skenario 6 dilakukan untuk mencari bukti forensik berupa *profile picture* pengguna aplikasi media sosial Facebook pada *smartphone* Android menggunakan SQLite Manager. Akun palsu yang digunakan adalah **Orang Pertama**.

| | |
|------------------------------------|--|
| 7. small_picture_url (TEXT) | https://scontent-sit4-1.xx.fbcdn.net/v/t1.0-1/p100x100 |
| 8. big_picture_url (TEXT) | m&oh=f06ecf4a770d703d9d9874fb09f59be2&oe=58F4BA26 |
| 9. huge_picture_url (TEXT) | m&oh=5bdcd04e43cc09260a810c4d1044df39&oe=58B0096C |
| 10. small_picture_size (INTEGER) | 100 |
| 11. big_picture_size (INTEGER) | 160 |
| 12. huge_picture_size (INTEGER) | 720 |

Gambar 5.16 Bukti forensik berupa url dari *profile picture* Facebook dengan SQLite Manager

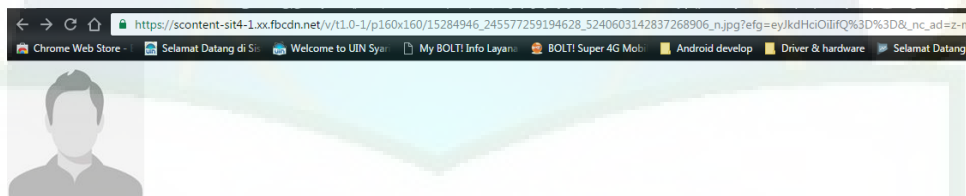
Pada percobaan ini berhasil ditemukan bukti forensik *profile pictures* dari akun pengguna aplikasi media sosial Facebook. Bukti forensik ditemukan pada *file database contact_db2*, pada tabel **contacts**. Pada gambar 5.16 diatas, bukti forensik ditemukan dalam bentuk *url* yang disimpan pada *database*. *url* tersebut adalah https://scontent-sit4-1.xx.fbcdn.net/v/t1.0-1/p720x720/15284946_245577259194628_5240603142837268906_n.jpg?efg=eyJkdHciOiIifQ%3D%3D&nc_ad=z-m&oh=5bdcd04e43cc09260a810c4d1044df39&oe=58B0096C. Bila *url* tersebut disalin dan dibuka dengan menggunakan *browser* maka akan ditampilkan gambar dari *profile picture* akun tersebut.

Setelah itu dilakukan percobaan dengan menggunakan aplikasi DB Browser for SQLite.

| small_picture_url | big_picture_url | huge_picture_url |
|---|---|---|
| Filter | Filter | Filter |
| https://z-m-scontent.fcgk4-1.fna.fbcdn.net/v/t1.0-1/p100x100 | https://z-m-scontent.fcgk4-1.fna.fbcdn.net/v/t1.0-1/p160x160 | https://z-m-scontent.fcgk4-1.fna.fbcdn.net/v/t1.0-1/p720x720 |

Gambar 5.17 Bukti forensik berupa url dari *profile picture* Facebook dengan DB Browser for SQLite

Pada percobaan ini berhasil ditemukan bukti forensik *profile pictures* dari akun pengguna aplikasi media sosial Facebook. Bukti forensik ditemukan pada *file database contact_db2*, pada tabel **contacts**. Pada gambar 5.16 diatas, bukti forensik ditemukan dalam bentuk *url* yang disimpan pada *database*. Bila *url* tersebut disalin dan dibuka dengan menggunakan *browser* maka akan ditampilkan gambar dari *profile picture* akun tersebut yang dapat dilihat pada gambar 5.18.



Gambar 5.18 Ketika *url* dibuka menggunakan *browser*

5.3.6.2 Percobaan 2

Percobaan kedua skenario 6 dilakukan untuk mencari bukti forensik berupa *profile picture* pengguna aplikasi media sosial Twitter pada *smartphone* Android menggunakan SQLite Manager. Akun palsu yang digunakan adalah **Orang Ketiga**.

| | |
|----------------------------|---|
| 9. bg_color (INTEGER) | -657158 |
| 10. link_color (INTEGER) | -14835214 |
| 11. image_url (TEXT) | /796687130806235141/RpdUQBRE_normal.jpg |

Gambar 5.19 Bukti forensik berupa *url* dari *profile picture* dengan SQLite Manager

Pada percobaan ini berhasil ditemukan bukti forensik *profile pictures* dari akun pengguna aplikasi media sosial Twitter. Bukti forensik ditemukan pada *file database 732798704059621380-43*, pada tabel **users**. Pada gambar 5.12 diatas, bukti forensik ditemukan dalam bentuk *url* yang disimpan pada *database*. *url* tersebut,

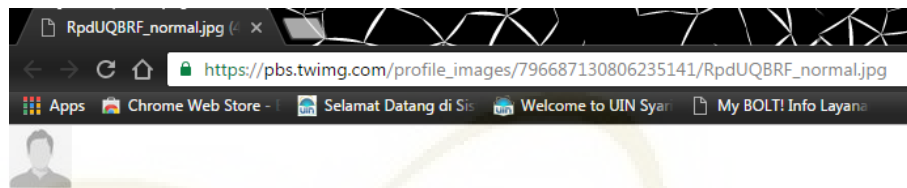
https://pbs.twimg.com/profile_images/796687130806235141/RpdUQBRF_normal.jpg bila disalin dan dibuka dengan menggunakan *browser* maka akan ditampilkan gambar dari *profile picture* akun terkait.

Setelah itu dilakukan percobaan dengan menggunakan aplikasi DB Browser for SQLite.

| image_url | |
|---|--|
| Filter | |
| https://pbs.twimg.com/profile_images/796687130806235141/RpdUQBRF_normal.jpg | |

Gambar 5.20 Bukti forensik berupa url dari *profile picture* dengan DB Browser for SQLite

Pada percobaan ini berhasil ditemukan bukti forensik *profile pictures* dari akun pengguna aplikasi media sosial Twitter. Bukti forensik ditemukan pada *file database 732798704059621380-43*, pada tabel **users**. Pada gambar 5.12 diatas, bukti forensik ditemukan dalam bentuk *url* yang disimpan pada *database*. bila disalin dan dibuka dengan menggunakan *browser* maka akan ditampilkan gambar dari *profile picture* akun terkait yang dapat dilihat pada gambar 5.21.

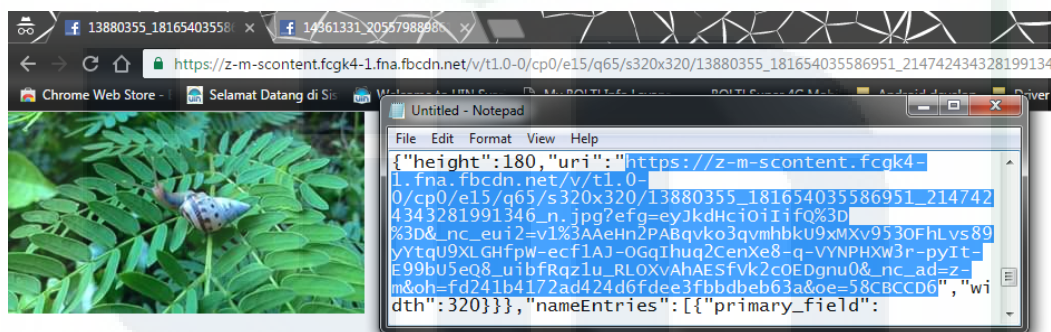


Gambar 5.21 Ketika *url* dibuka menggunakan *browser*

5.3.7 Hasil Simulasi Skenario 7

5.3.7.1 Percobaan 1

Percobaan pertama skenario 7 dilakukan untuk mencari bukti forensik berupa *cover photo* pengguna aplikasi media sosial Facebook pada *smartphone* Android menggunakan SQLite Manager. Akun palsu yang digunakan adalah **Orang Pertama**.



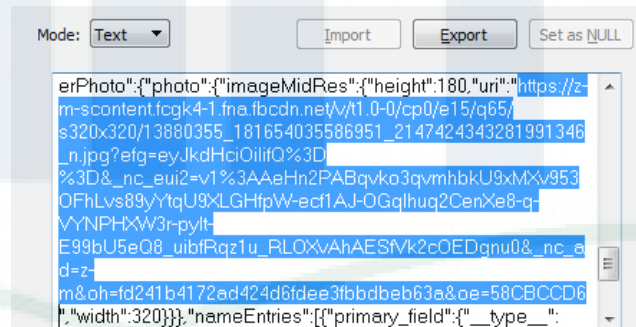
Gambar 5.22 Bukti forensik berupa *cover photo* Facebook dengan SQLite Manager

Pada percobaan ini berhasil ditemukan bukti forensik *cover photo* dari akun pengguna aplikasi media sosial Facebook. Bukti forensik ditemukan pada *file database contact_db2*, pada tabel **contacts**, dan pada kolom **data**. Pada gambar 5.22 diatas, isi dari kolom data sangat panjang sehingga isi dari kolom tersebut disalin pada aplikasi Notepad untuk memudahkan pencarian bukti forensik. Bukti forensik ditemukan

dalam bentuk *url* yang disimpan pada *database*. *Url* tersebut,

https://z-m-scontent.fcgk4-1.fna.fbcdn.net/v/t1.0-0/cp0/e15/q65/s320x320/13880355_181654035586951_2147424343281991346_n.jpg?efg=eyJkdHciOiIifQ%3D%3D&_nc_eui2=v1%3AAeHn2PABqvko3qvmhbkU9xMXv953OFhLvs89yYtqU9XLGHfpW-ecf1AJ-OGqIhuq2CenXe8-q-VYNPHXW3r-pyIt-E99bU5eQ8_uibfRqz1u_RLOXvAhAESfVk2cOEDgnu0&_nc_ad=z-m&oh=fd241b4172ad424d6fdee3fbdb63a&oe=58CBCCD6 Bila disalin dan dibuka dengan menggunakan *browser* maka akan ditampilkan gambar dari *cover photo* akun terkait.

Setelah itu dilakukan percobaan dengan menggunakan aplikasi DB Browser for SQLite.



Gambar 5.23 Bukti forensik berupa *cover photo* Facebook dengan DB Browser for SQLite

Pada percobaan ini berhasil ditemukan bukti forensik *cover photo* dari akun pengguna aplikasi media sosial Facebook. Bukti forensik ditemukan pada *file database contact_db2*, pada tabel **contacts**, dan pada kolom **data**. Bukti forensik ditemukan dalam bentuk *url*

yang disimpan pada *database*. Bila disalin dan dibuka dengan menggunakan *browser* maka akan ditampilkan gambar dari *cover photo* akun terkait.

5.3.7.2 Percobaan 2

Percobaan kedua skenario 7 dilakukan untuk mencari bukti forensik berupa *cover photo* pengguna aplikasi media sosial Twitter pada *smartphone* Android menggunakan SQLite Manager. Akun palsu yang digunakan adalah **Orang Ketiga**.

| | |
|--------------------------------------|---|
| 12. header_url (TEXT) | https://pbs.twimg.com/profile_banners/732798704059621380/1480930200 |
| 13. extended_profile_fields (BLOB) | X'491D0A2B6C89EF572004120112011307C11D00000158D1830C66496A0 |

Gambar 5.24 Bukti forensik berupa *url* dari *cover photo* pada Twitter dengan SQLite Manager

Pada percobaan ini berhasil ditemukan bukti forensik *cover photo* dari akun pengguna aplikasi media sosial Twitter. Bukti forensik ditemukan pada *file database* **732798704059621380-43**, pada tabel **users**. Pada gambar 5.24 diatas, bukti forensik ditemukan dalam bentuk *url* yang disimpan pada *database*. *Url* tersebut,

https://pbs.twimg.com/profile_banners/732798704059621380/1480930200 bila disalin dan dibuka dengan menggunakan *browser* maka akan ditampilkan gambar dari *cover photo* akun terkait.

Setelah itu dilakukan percobaan dengan menggunakan aplikasi DB Browser for SQLite.

| header_url |
|---|
| Filter |
| https://pbs.twimg.com/profile_banners/732798704059621380/1480930200 |

Gambar 5.25 Bukti forensik berupa *url* dari *cover photo* pada Twitter dengan DB Browser for SQLite

Pada percobaan ini berhasil ditemukan bukti forensik *cover photo* dari akun pengguna aplikasi media sosial Twitter. Bukti forensik ditemukan pada *file database 732798704059621380-43*, pada tabel **users**. Pada gambar 5.24 diatas, bukti forensik ditemukan dalam bentuk *url* yang disimpan pada *database*. Bila *url* tersebut disalin dan dibuka dengan menggunakan *browser* maka akan ditampilkan gambar dari *cover photo* akun terkait yang dapat dilihat pada gambar 5.26.



Gambar 5.26 Ketika *url* dibuka menggunakan *browser*

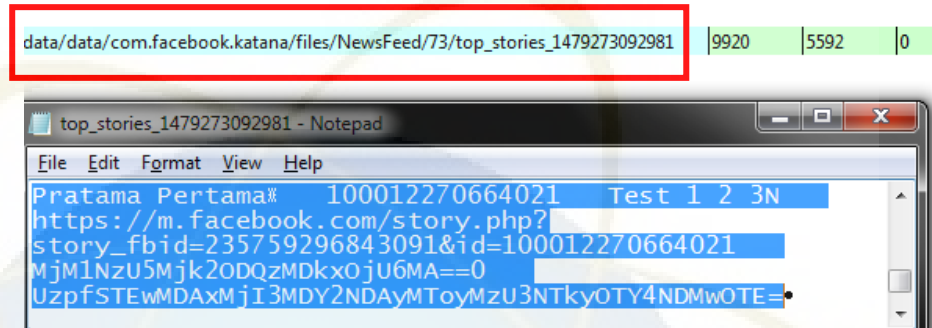
5.3.8 Hasil Simulasi Skenario 8

5.3.8.1 Percobaan 1

Percobaan pertama skenario 8 dilakukan untuk mencari bukti forensik berupa *posting* berupa teks pengguna aplikasi media sosial Facebook pada

smartphone Android menggunakan SQLite Manager.

Akun palsu yang digunakan adalah **Orang Pertama**.



Gambar 5.27 Bukti forensik *posting* berupa teks dengan menggunakan SQLite Manager

Pada percobaan ini berhasil ditemukan bukti forensik berupa *posting* dari akun pengguna aplikasi media sosial Facebook. Bukti forensik ditemukan pada file **top_stories_1479273092981**. Bukti tersebut ditemukan setelah melakukan pencarian pada *database newsfeed_db*. Pada database tersebut ditemukan tabel berisi alamat tempat file disimpan. Setelah file **top_stories_1479273092981** dibuka dengan menggunakan aplikasi Notepad, ditemukan isi *posting* beserta *url posting* tersebut, sayangnya url tersebut tidak dapat dibuka. Pada gambar 5.27 diatas dapat diketahui bahwa isi *posting* tersebut adalah “**Test 1 2 3**”.

Setelah itu dilakukan percobaan dengan menggunakan aplikasi DB Browser for SQLite.

| cache_file_path |
|--|
| Filter |
| /data/data/com.facebook.katana/files/NewsFeed/73/top_stories_1479273092981 |

Gambar 5.28 Bukti forensik *posting* berupa teks menggunakan DB Browser for SQLite

Pada percobaan ini berhasil ditemukan bukti forensik berupa *posting* dari akun pengguna aplikasi media sosial Facebook. Bukti forensik ditemukan pada file **top_stories_1479273092981**. Bukti tersebut ditemukan setelah melakukan pencarian pada *database newsfeed_db*. Setelah file **top_stories_1479273092981** dibuka dengan menggunakan aplikasi Notepad, ditemukan isi *posting* beserta *url posting* tersebut, sayangnya url tersebut tidak dapat dibuka. Pada gambar 5.27 diatas dapat diketahui bahwa isi *posting* tersebut adalah “**Test 1 2 3**”.

5.3.8.2 Percobaan 2

Percobaan kedua skenario 8 dilakukan untuk mencari bukti forensik berupa *posting (tweet)* berupa teks pengguna aplikasi media sosial Twitter pada *smartphone* Android menggunakan SQLite Manager. Akun palsu yang digunakan adalah **Orang Ketiga**.

| | |
|----------------------------|------------|
| 3. full_content (TEXT) | Test 1 2 3 |
| 4. r_full_content (TEXT) | Test 1 2 3 |

Gambar 5.29 Bukti forensik *posting(tweet)* berupa teks dengan SQLite Manager

Pada percobaan ini berhasil ditemukan bukti forensik berupa *posting(tweet)* dari akun pengguna

aplikasi media sosial Twitter. Bukti forensik ditemukan pada *file database* **732798704059621380-43**, pada tabel **full_content**. Pada gambar 5.29 diatas dapat diketahui bahwa isi *tweet (posting)* tersebut adalah “**Test 1 2 3**”.

Setelah itu dilakukan percobaan dengan menggunakan aplikasi DB Browser for SQLite.

| status_id | full_content | r_full_content |
|------------|--------------|----------------|
| Filter | test 1 | Filter |
| 2954391684 | Test 1 2 3 | Test 1 2 3 |

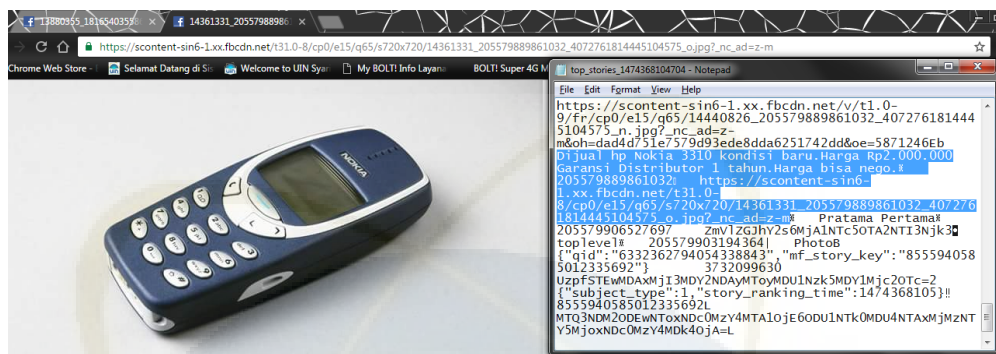
Gambar 5.30 Bukti forensik *posting(tweet)* berupa teks menggunakan DB Browser for SQLite

Pada percobaan ini berhasil ditemukan bukti forensik berupa *posting(tweet)* dari akun pengguna aplikasi media sosial Twitter. Bukti forensik ditemukan pada *file database* **732798704059621380-43**, pada tabel **full_content**. Pada gambar 5.18 diatas dapat diketahui bahwa isi *tweet (posting)* tersebut adalah “**Test 1 2 3**”.

5.3.9 Hasil Simulasi Skenario 9

5.3.9.1 Percobaan 1

Percobaan pertama skenario 9 dilakukan untuk mencari bukti forensik berupa *posting* berupa gambar pengguna aplikasi media sosial Facebook pada *smartphone* Android menggunakan SQLite Manager. Akun palsu yang digunakan adalah **Orang Pertama**.



Gambar 5.31 Bukti forensik *posting* berupa gambar dengan SQLite Manager

Pada percobaan ini berhasil ditemukan bukti forensik berupa *posting* dari akun pengguna aplikasi media sosial Facebook. Bukti forensik ditemukan pada file **top_stories_1474368104704**. Bukti tersebut ditemukan setelah melakukan pencarian pada *database newsfeed_db*. Pada database tersebut ditemukan tabel berisi alamat tempat file disimpan. Setelah file **top_stories_1474368104704** dibuka dengan menggunakan aplikasi Notepad, pada gambar 5.31 ditemukan posting bertuliskan “**Dijual hp Nokia 3310 kondisi baru. Harga Rp2.000.000 Garansi Distributor 1 tahun. Harga bisa nego**” dan *url* yang mengarahkan pada gambar tersebut. *Url* tersebut, ***https://scontent-sin6-1.xx.fbcdn.net/t31.0-8/cp0/e15/q65/s720x720/14361331_205579889861032_4072761814445104575_o.jpg?_nc_ad=z-m*** bila disalin dan dibuka dengan menggunakan *browser* maka akan ditampilkan gambar dari *cover photo* akun terkait.

Setelah itu dilakukan percobaan dengan menggunakan aplikasi DB Browser for SQLite.

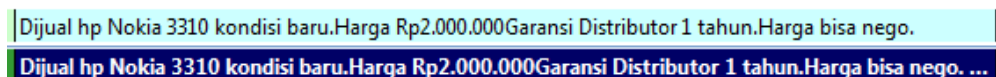


Gambar 5.32 Bukti forensik *posting* berupa gambar dengan DB Browser fo SQLite

Pada percobaan ini berhasil ditemukan bukti forensik berupa *posting* dari akun pengguna aplikasi media sosial Facebook. Bukti forensik ditemukan pada file **top_stories_1474368104704**. Bukti tersebut ditemukan setelah melakukan pencarian pada *database newsfeed_db*. Pada database tersebut ditemukan tabel berisi alamat tempat file disimpan. Setelah file **top_stories_1474368104704** dibuka dengan menggunakan aplikasi Notepad, pada gambar 5.31 ditemukan posting bertuliskan “**Dijual hp Nokia 3310 kondisi baru. Harga Rp2.000.000 Garansi Distributor 1 tahun. Harga bisa nego**” dan *url* yang mengarahkan pada gambar tersebut.

5.3.9.2 Percobaan 2

Percobaan kedua skenario 9 dilakukan untuk mencari bukti forensik berupa *posting (tweet)* berupa teks pengguna aplikasi media sosial Twitter pada *smartphone* Android menggunakan SQLite Manager. Akun palsu yang digunakan adalah **Orang Ketiga**.

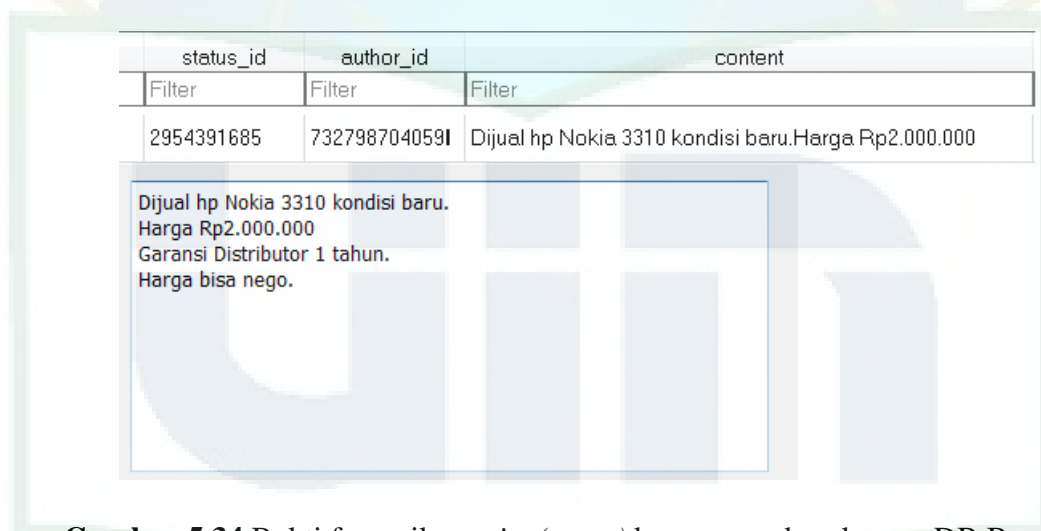


Gambar 5.33 Bukti forensik *posting(tweet)* berupa gambar dengan SQLite Manager

Pada percobaan ini berhasil ditemukan bukti forensik *posting(tweet)* berupa gambar dari akun

pengguna aplikasi media sosial Twitter. Bukti forensik ditemukan pada *file database 732798704059621380-43*, pada tabel **statuses**. Pada gambar 5.33 terlihat bukti yang ditemukan berupa isi *tweet (posting)* bertuliskan **“Dijual hp Nokia 3310 kondisi baru. Harga Rp2.000.000 Garansi Distributor 1 tahun. Harga bisa nego.”** dan *url pic.twitter.com/mf0fdePyDE*. Bila *url* tersebut dibuka dengan menggunakan *browser* maka akan menampilkan gambar yang dimaksud.

Setelah itu dilakukan percobaan dengan menggunakan aplikasi DB Browser for SQLite.



| status_id | author_id | content |
|------------|-----------------------|--|
| Filter | Filter | Filter |
| 2954391685 | 732798704059621380-43 | Dijual hp Nokia 3310 kondisi baru. Harga Rp2.000.000 Garansi Distributor 1 tahun. Harga bisa nego. |

Gambar 5.34 Bukti forensik *posting(tweet)* berupa gambar dengan DB Browser for SQLite

Pada percobaan ini berhasil ditemukan bukti forensik *posting(tweet)* berupa gambar dari akun pengguna aplikasi media sosial Twitter. Bukti forensik ditemukan pada *file database 732798704059621380-43*, pada tabel **statuses**. Pada gambar 5.34 terlihat bukti yang ditemukan berupa isi *tweet (posting)* bertuliskan **“Dijual hp Nokia 3310 kondisi baru. Harga Rp2.000.000 Garansi Distributor 1 tahun. Harga bisa nego.”**

bisa nego.” dan *url* pic.twitter.com/mf0fdePyDE. Bila *url* tersebut dibuka dengan menggunakan *browser* maka akan menampilkan gambar yang dimaksud yaitu pada gambar 5.35.



Gambar 5.35 Ketika *url* dibuka dengan menggunakan *browser*

5.3.10 Hasil Simulasi Skenario 10

5.3.10.1 Percobaan 1

Percobaan pertama skenario 10 dilakukan untuk mencari bukti forensik berupa isi dari *private message* (berbentuk teks) pengguna aplikasi media sosial Facebook pada *smartphone* Android menggunakan SQLite Manager. Akun palsu yang digunakan adalah **Orang Pertama**.

| text | sender |
|--|---------------------------------|
| Terima kasih, saya akan segera kirim barangnya | {"email":null,"user_ke... |
| saya sudah kirim bukti bayar dan sudah saya transfer sesuai kesepakatan | {"email":null,"user_k... |
| | {"email":null,"user_ke... |
| Ke rekening bang ABC.Nomor rekening 987654321 | {"email":null,"user_ke... |
| baik kalau begitu, kemana saya bisa kirim uang? | {"email":null,"user_ke... |
| Tentu bisa.. :) | {"email":null,"user_ke... |
| Apa harga hp tersebut bisa kurang lagi jadi 1,8jt? | {"email":null,"user_ke... |
| Ya? | {"email":null,"user_ke... |
| Halo pak pratama, | {"email":null,"user_ke... |
| You're now friends with Duo Kedua. Send a message to say hello! | {"email":null,"user_ke... |
| | |
| | {"email":null,"user_ke... |
| Barang sudah saya paketkan. Tunggu beberapa hari sampai barangnya tiba | {"email":null,"user_ke... |
| terima kasih | {"email":null,"user_ke... |
| Sama-sama :) | {"email":null,"user_ke... |
| test | {"email":null,"user_ke... |
| Test | {"email":null,"user_ke... |

Gambar 5.36 Bukti forensik percakapan pada *private message* pada Facebook dengan SQLite Manager

Pada percobaan ini berhasil ditemukan bukti forensik percakapan pada *private message*. Bukti forensik ditemukan pada *file database threads_db2*, pada tabel **messages**. Seluruh isi percakapan terdapat pada kolom **text**. Salah satu percakaannya bertuliskan sebagai berikut :

Duo kedua : Halo pak pratama

Pratama pertama : ya?

Duo kedua : Apa harga hp tersebut bisa kurang lagi jadi 1,8jt?

Pratama pertama : Tentu bisa ☺.

Setelah itu dilakukan percobaan dengan menggunakan aplikasi DB Browser for SQLite.

| | text |
|---|---|
| | Filter |
| 1 | Terima kasih, saya akan segera kirim barangnya |
| 2 | saya sudah kirim bukti bayar dan sudah saya transfer sesuai kesepakatan |
| 3 | |
| 4 | Ke rekening bang ABC.Nomor rekening 987654321 |
| 5 | baik kalau begitu, kemana saya bisa kirim uang? |
| 6 | Tentu bisa.. :) |
| 7 | Apa harga hp tersebut bisa kurang lagi jadi 1,8jt? |
| 8 | Ya? |
| 9 | Halo pak pratama, |

Gambar 5.37 Bukti forensik percakapan pada *private message* pada Facebook dengan SQLite Manager

Pada percobaan ini berhasil ditemukan bukti forensik percakapan pada *private message*. Bukti forensik ditemukan pada *file database threads_db2*, pada tabel **messages**. Seluruh isi percakapan terdapat pada kolom **text**.

5.3.10.2 Percobaan 2

Percobaan kedua skenario 10 dilakukan untuk mencari bukti forensik berupa isi dari *private message* (berbentuk teks) pengguna aplikasi media sosial Twitter pada *smartphone* Android menggunakan SQLite Manager. Akun palsu yang digunakan adalah **Orang Ketiga**.

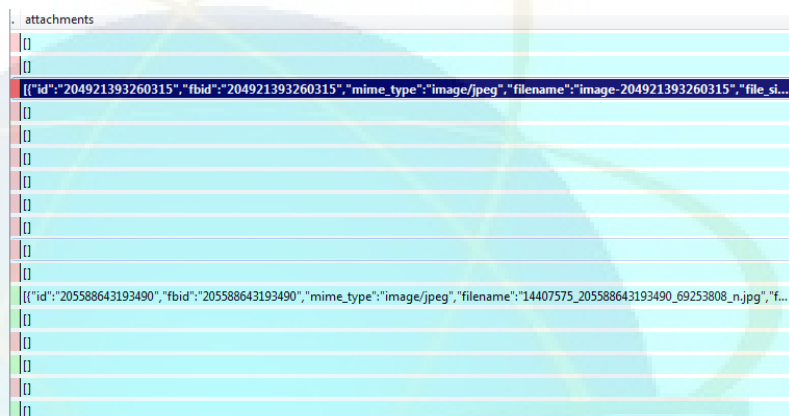
Pada pencarian bukti forensik berupa tanggal lahir pada aplikasi media sosial Twitter tidak berhasil ditemukan bahkan dengan menggunakan DB Browser for SQLite.

5.3.11 Hasil Simulasi Skenario 11

5.3.11.1 Percobaan 1

Percobaan pertama skenario 11 dilakukan untuk mencari bukti forensik berupa isi dari *private message*

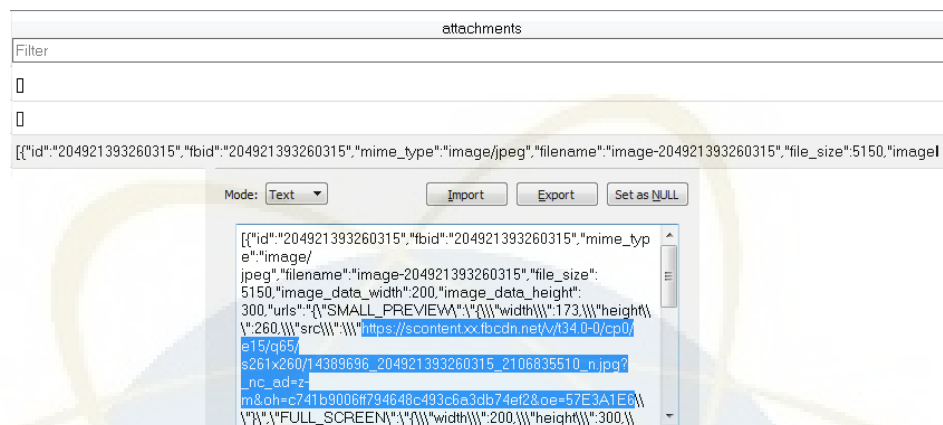
(berbentuk gambar) pengguna aplikasi media sosial Facebook pada *smartphone* Android menggunakan SQLite Manager. Akun palsu yang digunakan adalah **Orang Pertama**.



Gambar 5.38 Bukti forensik *private message* berupa gambar menggunakan SQLite Manager

Pada percobaan ini berhasil ditemukan bukti forensik isi *private message* berupa gambar. Bukti forensik ditemukan pada *file database* **threads_db2**, pada tabel **attachments**. Bukti forensik yang ditemukan berupa *url*. *Url* tersebut adalah https://scontent.xx.fbcdn.net/v/t34.0-12/fr/cp0/e15/q65/14389696_204921393260315_2106835510_n.jpg?_nc_ad=z-m&oh=15da0ba1bc784b6dce926b988db10e73&oe=57E3C350, bila disalin dan dibuka pada *browser* maka akan menampilkan gambar terkait.

Setelah itu dilakukan percobaan dengan menggunakan aplikasi DB Browser for SQLite.



Gambar 5.39 Bukti forensik *private message* berupa gambar menggunakan SQLite Manager

Pada percobaan ini berhasil ditemukan bukti forensik isi *private message* berupa gambar. Bukti forensik ditemukan pada *file database threads_db2*, pada tabel **attachments**. Bukti forensik yang ditemukan berupa *url*. Bila disalin dan dibuka pada *browser* maka akan menampilkan gambar terkait pada gambar 5.40.



Gambar 5.40 Ketika *url* dibuka menggunakan *browser*

5.3.11.2 Percobaan 2

Percobaan kedua skenario 11 dilakukan untuk mencari bukti forensik berupa isi dari *private message*

(berbentuk gambar) pengguna aplikasi media sosial Twitter pada *smartphone* Android menggunakan SQLite Manager. Akun palsu yang digunakan adalah **Orang Ketiga**.

Pada pencarian bukti forensik berupa tanggal lahir pada aplikasi media sosial Twitter tidak berhasil ditemukan bahkan dengan menggunakan DB Browser for SQLite.

5.4 Output Analisis Hasil Pencarian Bukti Forensik

Setelah data-data hasil setiap percobaan skenario didapatkan, maka *output* tersebut akan dianalisa dan dibandingkan untuk menentukan banyaknya bukti forensik yang ditemukan.

Output akan dijabarkan dalam bentuk tabel dari setiap skenario yang dilakukan sebanyak 11 skenario.

5.4.1 Output Analisis Skenario 1

Pada skenario 1 simulasi dilakukan untuk mengembalikan *file* dan data-data aplikasi media sosial yang sebelumnya telah dihapus pada *smartphone*. Berikut adalah hasil simulasi skenario :

Table 5.1 Hasil perbandingan skenario 1

| Skenario 1 | Facebook | Twitter |
|--|--|---|
| Mengembalikan <i>file</i> dan data-data yang dihapus | <i>File</i> dan data-data berhasil dikembalikan | <i>File</i> dan data-data berhasil dikembalikan |
| Data dan <i>file</i> yang dikembalikan | com.facebook.katana (<i>file</i> dan data-data Facebook Apps) | com.twitter.android (<i>file</i> dan data-data Twitter Apps) |

| | | |
|--|--|--|
| | com.facebook.orca (file dan data-data Facebook Messenger) | |
|--|--|--|

Pada tabel 5.1 dapat dilihat hasil skenario 1, data-data pada aplikasi media sosial Facebook dan Twitter yang sebelumnya telah dihapus telah berhasil dikembalikan. Pada aplikasi media sosial Facebook, data yang berhasil dikembalikan adalah file **com.facebook.katana** (file dan data-data Facebook Apps) dan file **com.facebook.orca** (file dan data-data Facebook Messenger).

Sedangkan pada aplikasi media sosial Twitter, data yang berhasil dikembalikan adalah file **com.twitter.android** (file dan data-data Twitter Apps).

5.4.2 Output Analisis Skenario 2

Pada skenario 2 simulasi dilakukan untuk menemukan bukti forensik berupa nama akun dari pengguna aplikasi media sosial Facebook dan Twitter pada *smartphone* Android. Berikut adalah hasil simulasi skenario :

Table 5.2 Hasil perbandingan skenario 2

| Skenario 2 | Facebook | Twitter |
|---|---------------------------------------|--|
| Menemukan bukti forensik berupa nama akun | Nama akun berhasil ditemukan | Nama akun berhasil ditemukan |
| Bukti forensik yang ditemukan | Nama akun : Pratama Pertama | Nama akun : Pratama Pertama (@Pratama1_satu) |

Pada tabel 5.2 dapat dilihat hasil skenario 2, pada aplikasi media sosial Facebook, bukti forensik berupa nama akun berhasil ditemukan. Bukti forensik ditemukan pada *file database contact_db2*, pada tabel **contacts**.

Kemudian pada aplikasi media sosial Twitter, bukti forensik berupa nama akun juga berhasil ditemukan. Bukti forensik ditemukan pada *file database 732798704059621380-43*, pada tabel **users**.

5.4.3 Output Analisis Skenario 3

Pada skenario 3 simulasi dilakukan untuk menemukan bukti forensik berupa data lokasi dari pengguna aplikasi media sosial Facebook dan Twitter pada *smartphone* Android. Berikut adalah hasil simulasi skenario :

Table 5.3 Hasil perbandingan skenario 3

| Skenario 3 | Facebook | Twitter |
|--|---|---|
| Menemukan bukti forensik berupa lokasi | Data lokasi berhasil ditemukan | Data lokasi tidak berhasil ditemukan |
| Bukti forensik yang ditemukan | Data lokasi : Semarang, Indonesia | Data lokasi : Semarang, Indonesia |

Pada tabel 5.3 dapat dilihat hasil skenario 3, pada aplikasi media sosial Facebook, bukti forensik berupa data lokasi berhasil ditemukan. Bukti forensik ditemukan pada *file database contact_db2*, pada tabel **contacts**, dan pada kolom **data**.

Kemudian pada aplikasi media sosial Twitter, bukti forensik berupa data lokasi akun juga berhasil ditemukan.

Bukti forensik ditemukan pada *file database* **732798704059621380-43**, pada tabel **users**.

5.4.4 Output Analisis Skenario 4

Pada skenario 4 simulasi dilakukan untuk menemukan bukti forensik berupa data nomor telepon dari pengguna aplikasi media sosial Facebook dan Twitter pada *smartphone* Android. Berikut adalah hasil simulasi skenario :

Table 5.4 Hasil perbandingan skenario 4

| Skenario 4 | Facebook | Twitter |
|---|--|---|
| Menemukan bukti forensik berupa nomor telepon | Nomor Telepon berhasil ditemukan | Nomor Telepon tidak berhasil ditemukan |
| Bukti forensik yang ditemukan | Nomor telepon : +6285776267290 | Tidak ada Asumsi data tidak ditemukan : data tidak tersimpan pada <i>database</i> melainkan pada <i>server</i> . |

Pada tabel 5.4 dapat dilihat hasil skenario 4, pada aplikasi media sosial Facebook, bukti forensik berupa nomor telepon pada berhasil ditemukan. Bukti forensik ditemukan pada *file database* **contact_db2**, pada tabel **contacts**, dan pada kolom **data**.

Sedangkan pada aplikasi media sosial Twitter, bukti forensik berupa nomor telepon pada akun tidak berhasil ditemukan. Penulis berasumsi bahwa bukti forensik yang tidak berhasil ditemukan tersebut disebabkan karena data tersebut tidak disimpan pada *database* melainkan pada *server*.

5.4.5 Output Analisis Skenario 5

Pada skenario 5 simulasi dilakukan untuk menemukan bukti forensik berupa data tanggal lahir dari pengguna aplikasi media sosial Facebook dan Twitter pada *smartphone* Android. Berikut adalah hasil simulasi skenario :

Table 5.5 Hasil perbandingan skenario 5

| Skenario 5 | Facebook | Twitter |
|---|----------------------------------|---|
| Menemukan bukti forensik berupa tanggal lahir | Tanggal lahir berhasil ditemukan | Tanggal lahir tidak berhasil ditemukan |
| Bukti forensik yang ditemukan | Tanggal lahir : 1 Januari | Tidak ada Asumsi data tidak ditemukan : data tidak tersimpan pada <i>database</i> melainkan pada <i>server</i> |

Pada tabel 5.5 dapat dilihat hasil skenario 5, pada aplikasi media sosial Facebook, bukti forensik berupa data tanggal lahir akun berhasil ditemukan. Bukti forensik ditemukan pada *file database contact_db2*, pada tabel **contacts**.

Sedangkan, pada aplikasi media sosial Twitter, bukti forensik berupa tanggal lahir akun tidak berhasil ditemukan. Penulis berasumsi bahwa bukti forensik yang tidak berhasil ditemukan tersebut disebabkan karena data tersebut tidak disimpan pada *database* melainkan pada *server*.

5.4.6 Output Analisis Skenario 6

Pada skenario 6 simulasi dilakukan untuk menemukan bukti forensik berupa *profile picture* dari pengguna aplikasi

media sosial Facebook dan Twitter pada *smartphone* Android. Berikut adalah hasil simulasi skenario :

Table 5.6 Hasil perbandingan skenario 6

| Skenario 6 | Facebook | Twitter |
|--|---|---|
| Menemukan bukti forensik berupa <i>Profile Picture</i> | <i>Profile Picture</i> berhasil ditemukan | <i>Profile Picture</i> berhasil ditemukan |
| Bukti forensik yang ditemukan | <p><i>url</i> yang mengarahkan pada <i>Profile Picture</i> akun tersebut :</p> <p><i>https://scontent-sit4-1.xx.fbcdn.net/v/t1.0-1/p160x160/15284946_245577259194628_5240603142837268906_n.jpg?efg=eyJkdHciOiIifQ%3D%3D&_nc_ad=z-mm&oh=f06ecf4a770d703d9d9874fb09f59be2&oe=58F4BA26</i></p> | <p><i>url</i> yang mengarahkan pada <i>Profile Picture</i> akun tersebut :</p> <p><i>https://pbs.twimg.com/profile_images/796687130806235141/RpdUQBRF_normal.jpg</i></p> |

Pada tabel 5.6 dapat dilihat hasil skenario 6, pada aplikasi media sosial Facebook, bukti forensik berupa *profil picture* akun berhasil ditemukan. Bukti forensik ditemukan pada *file database contact_db2*, pada tabel **contacts**.

Kemudian pada aplikasi media sosial Twitter, bukti forensik berupa *profil picture* akun juga berhasil ditemukan. Bukti forensik ditemukan pada *file database 732798704059621380-43*, pada tabel **users**.

5.4.7 Output Analisis Skenario 7

Pada skenario 7 simulasi dilakukan untuk menemukan bukti forensik berupa *cover photo* dari pengguna aplikasi media sosial Facebook dan Twitter pada *smartphone* Android. Berikut adalah hasil simulasi skenario :

Table 5.7 Hasil perbandingan skenario 7

| Skenario 7 | Facebook | Twitter |
|--|--|---|
| Menemukan bukti forensik berupa <i>Cover Photo</i> | <i>Cover Photo</i> berhasil ditemukan | <i>Cover Photo</i> berhasil ditemukan |
| Bukti forensik yang ditemukan | <p><i>url</i> yang mengarahkan pada <i>cover photo</i> akun tersebut :</p> <p><i>https://z-m-scontent.fcgk4-1.fna.fbcdn.net/v/t1.0-0/cp0/e15/q65/s320x320/13880355_181654035586951_2147424343281991346_n.jpg?efg=eyJkdHciOilifQ%3D%3D&_nc_eui2=v1%3AAeHn2PABqvko3qvmhbkU9xMXv953OFhLvs89yYtqU9XLGHfpW-ecf1AJ-OGqIhuq2CenXe8-q-VYNPHXW3r-pyIt-E99bU5eQ8_uibfRqz1u_RLOXvAhAESfVk2cOEDgnu0&_nc_ad=z-</i></p> | <p><i>url</i> yang mengarahkan pada <i>cover photo</i> akun tersebut :</p> <p><i>https://pbs.twimg.com/profile_banners/732798704059621380/1480930200</i></p> |

| | | |
|--|---|--|
| | <i>m&oh=fd241b4172ad424d6fdee3fbdbeb63a&oe=58CBCCD6</i> | |
|--|---|--|

Pada tabel 5.7 dapat dilihat hasil skenario 7, pada aplikasi media sosial Facebook, bukti forensik berupa *cover photo* berhasil ditemukan. Bukti forensik ditemukan pada *file database contact_db2*, pada tabel **contacts**, dan pada kolom **data**.

Kemudian pada aplikasi media sosial Twitter, bukti forensik berupa *cover photo* pada akun juga berhasil ditemukan. Bukti forensik ditemukan pada *file database 732798704059621380-43*, pada tabel **users**.

5.4.8 Output Analisis Skenario 8

Pada skenario 8 simulasi dilakukan untuk menemukan bukti forensik berupa *posting* atau *tweet* (bentuk teks) dari pengguna aplikasi media sosial Facebook dan Twitter pada *smartphone* Android. Berikut adalah hasil simulasi skenario :

Table 5.8 Hasil perbandingan skenario 8

| Skenario 8 | Facebook | Twitter |
|--|--|--|
| Menemukan bukti forensik berupa <i>posting</i> atau <i>tweet</i> (bentuk teks) | <i>Posting</i> berhasil ditemukan | <i>Twitter</i> berhasil ditemukan |
| Bukti forensik yang ditemukan | Isi <i>posting</i> bertuliskan : Test 1 2 3 dan <i>url</i> yang mengarahkan kepada <i>posting</i> terkait : | Isi <i>posting</i> bertuliskan : Test 1 2 3 |

| | | |
|--|---|--|
| | https://m.facebook.com/story.php?story_fbid=235759296843091&id=100012270664021MjM1NzU5Mjk2ODQzMdkxOjU6MA==0UzpfSTewMDAxMjI3MDY2NDYyMToyMzU3NTkyOTY4NDMwOTE= | |
|--|---|--|

Pada tabel 5.8 dapat dilihat hasil skenario 8, pada aplikasi media sosial Facebook, bukti forensik berupa *posting* (bentuk teks) pada akun berhasil ditemukan. Bukti forensik ditemukan pada file **top_stories_1479273092981**. Bukti tersebut ditemukan setelah melakukan pencarian pada *database newsfeed_db*. Pada database tersebut ditemukan tabel berisi alamat tempat file disimpan. Setelah file **top_stories_1479273092981** dibuka dengan menggunakan aplikasi Notepad, ditemukan isi *posting* beserta *url posting* tersebut.

Kemudian pada aplikasi media sosial Twitter, bukti forensik berupa *tweet* (bentuk teks) pada akun juga berhasil ditemukan. Bukti forensik ditemukan pada *file database 732798704059621380-43*, pada tabel **full_content**.

5.4.9 Output Analisis Skenario 9

Pada skenario 9 simulasi dilakukan untuk menemukan bukti forensik berupa *posting* atau *tweet* (bentuk gambar) dari

pengguna aplikasi media sosial Facebook dan Twitter pada *smartphone* Android. Berikut adalah hasil simulasi skenario :

Table 5.9 Hasil perbandingan skenario 9

| Skenario 9 | Facebook | Twitter |
|--|---|--|
| Menemukan bukti forensik berupa <i>posting</i> atau <i>tweet</i> (bentuk gambar) | <i>Posting</i> berhasil ditemukan | <i>Tweet</i> berhasil ditemukan |
| Bukti forensik yang ditemukan | <p>Isi <i>posting</i> bertuliskan :</p> <p>Dijual hp Nokia 3310 kondisi baru.</p> <p>Harga Rp2.000.000</p> <p>Garansi Distributor 1 tahun.</p> <p>Harga bisa nego. dan <i>url</i> yang mengarahkan kepada gambar terkait</p> <p>: <i>https://scontent-sin6-1.xx.fbcdn.net/t31.0-8/cp0/e15/q65/s720x720/14361331_205579889861032_4072761814445104575_o.jpg?_nc_ad=z-m</i></p> | <p>Isi <i>posting</i> bertuliskan :</p> <p>Dijual hp Nokia 3310 kondisi baru.</p> <p>Harga Rp2.000.000</p> <p>Garansi Distributor 1 tahun.</p> <p>Harga bisa nego. dan <i>url</i> yang mengarahkan kepada gambar terkait :</p> <p><i>pic.twitter.com/mf0fdePyDE</i></p> |

Pada tabel 5.9 dapat dilihat hasil skenario 9, pada aplikasi media sosial Facebook, bukti forensik berupa *posting* (berupa gambar) pada akun berhasil ditemukan. Bukti forensik ditemukan pada file **top_stories_1474368104704**. Bukti

tersebut ditemukan setelah melakukan pencarian pada *database newsfeed_db*. Pada database tersebut ditemukan tabel berisi alamat tempat file disimpan. Setelah file **top_stories_1474368104704** dibuka dengan menggunakan aplikasi Notepad, ditemukan *url* yang mengarahkan pada gambar tersebut. Bila *url* tersebut dibuka dengan menggunakan *browser* maka akan menampilkan gambar yang dimaksud.

Kemudian pada aplikasi media sosial Twitter, bukti forensik berupa *tweet* (berupa gambar) pada akun juga berhasil ditemukan. Bukti forensik ditemukan pada *file database 732798704059621380-43*, pada tabel **statuses**. Pada gambar terlihat bukti yang ditemukan berupa *url*. Bila *url* tersebut dibuka dengan menggunakan *browser* maka akan menampilkan gambar yang dimaksud.

5.4.10 Output Analisis Skenario 10

Pada skenario 10 simulasi dilakukan untuk menemukan bukti forensik berupa *private message* atau *direct message* (bentuk teks) dari pengguna aplikasi media sosial Facebook dan Twitter pada *smartphone* Android. Berikut adalah hasil simulasi skenario :

Table 5.10 Hasil perbandingan skenario 10

| Skenario 10 | Facebook | Twitter |
|---|---|--|
| Menemukan bukti forensik berupa <i>private message</i> atau <i>direct message</i> (bentuk teks) | <i>Private message</i> (bentuk teks) berhasil ditemukan | <i>Direct message</i> (bentuk teks) tidak berhasil ditemukan |
| Bukti forensik yang ditemukan | Isi percakapan Duo kedua : Halo | Tidak ditemukan Asumsi data tidak |

| | | |
|--|--|---|
| | <p>pak pratama</p> <p>Pratama pertama : ya?</p> <p>Duo kedua : Apa harga hp tersebut bisa kurang lagi jadi 1,8jt?</p> <p>Pratama pertama : Tentu bisa 😊</p> <p>Dan seterusnya</p> | <p>ditemukan : data tidak tersimpan pada <i>database</i> melainkan pada <i>server</i></p> |
|--|--|---|

Pada tabel 5.10 dapat dilihat hasil skenario 10, pada aplikasi media sosial Facebook, bukti forensik berupa *private message* (bentuk teks) pada akun berhasil ditemukan. Bukti forensik ditemukan pada *file database threads_db2*, pada tabel **messages**. Seluruh isi percakapan terdapat pada kolom **text**.

Sedangkan pada aplikasi media sosial Twitter, bukti forensik berupa *direct message* (bentuk teks) pada akun tidak berhasil ditemukan. Penulis berasumsi bahwa bukti forensik yang tidak berhasil ditemukan tersebut disebabkan karena data tersebut tidak disimpan pada *database* melainkan pada *server*.

5.4.11 Output Analisis Skenario 11

Pada skenario 11 simulasi dilakukan untuk menemukan bukti forensik berupa *private message* atau *direct message* (bentuk gambar) dari pengguna aplikasi media sosial Facebook dan Twitter pada *smartphone* Android. Berikut adalah hasil simulasi skenario :

Table 5.11 Hasil perbandingan skenario 11

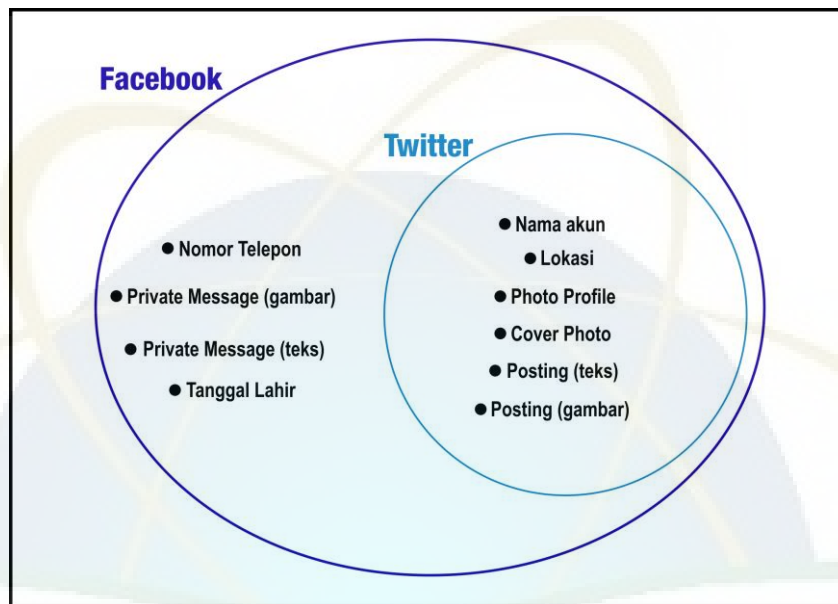
| Skenario 11 | Facebook | Twitter |
|-------------|----------|---------|
|-------------|----------|---------|

| | | |
|---|---|---|
| Menemukan bukti forensik berupa <i>private message</i> atau <i>direct message</i> (bentuk gambar) | <i>Private message</i> (bentuk gambar) berhasil ditemukan | <i>Direct message</i> (bentuk gambar) tidak berhasil ditemukan |
| Bukti forensik yang ditemukan | <i>url</i> yang mengarahkan kepada gambar terkait : <i>https://scontent.xx.fbcdn.net/v/t34.0-12/fr/cp0/e15/q65/14389696_204921393260315_2106835510_n.jpg?_nc_ad=z-m&oh=15da0ba1bc784b6dce926b988db10e73&oe=57E3C350</i> | Tidak ditemukan Asumsi data tidak ditemukan : data tidak tersimpan pada <i>database</i> melainkan pada <i>server</i> |

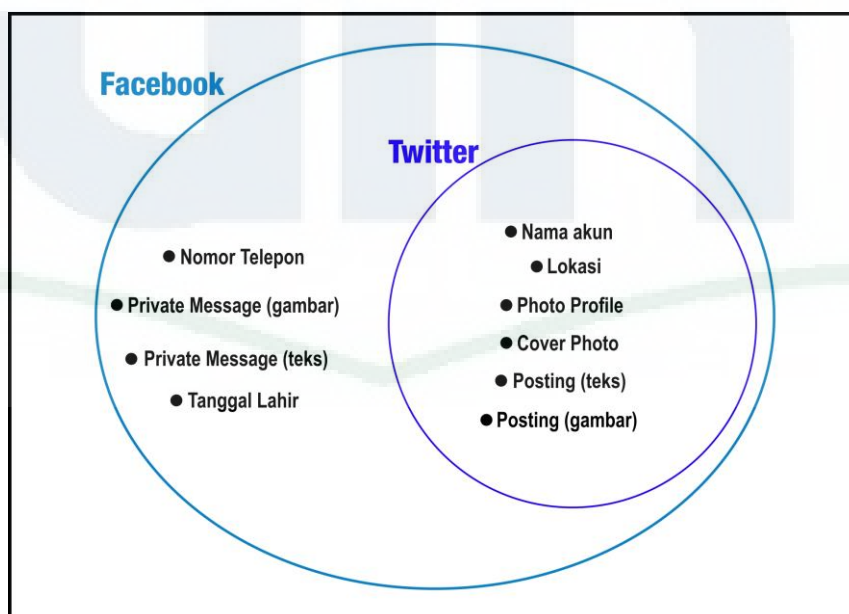
Pada tabel 5.11 dapat dilihat hasil skenario 11, pada aplikasi media sosial Facebook, bukti forensik berupa *private message* (bentuk gambar) pada akun berhasil ditemukan. Bukti forensik ditemukan pada *file database threads_db2*, pada tabel **messages**. Bukti forensik yang ditemukan berupa *url*. Bila *url* tersebut disalin dan dibuka pada *browser* maka akan menampilkan gambar tersebut.

Sedangkan pada aplikasi media sosial Twitter, bukti forensik berupa *direct message* (bentuk gambar) pada akun tidak berhasil ditemukan. Penulis berasumsi bahwa bukti forensik yang tidak berhasil ditemukan tersebut disebabkan karena data tersebut tidak disimpan pada *database* melainkan pada *server*.

5.4.12 Hasil Keseluruhan Analisis



Gambar 5.41 Hasil perbandingan pencarian bukti forensik menggunakan SQLite Manager



Gambar 5.42 Hasil perbandingan pencarian bukti forensik menggunakan DB Browser for SQLite

BAB VI

PENUTUP

6.1 Kesimpulan

Berdasarkan hasil dari tahapan-tahapan metode simulasi yang telah dilakukan, proses pencarian dan analisa bukti forensik pada aplikasi media sosial Facebook dan Twitter yang diakses pada *smartphone* Android dapat disimpulkan bahwa data-data pada media sosial Facebook dan Twitter tidak sepenuhnya disimpan pada *server*. Data tersebut juga tersimpan pada memori internal perangkat Android yang hanya dapat diakses setelah perangkat Android melalui proses *root*.

Berdasarkan tabel hasil semua skenario pencarian bukti forensik yang telah ditentukan sebelumnya, pada aplikasi media sosial Facebook semua bukti forensik dapat ditemukan. Bukti forensik yang ditemukan adalah nama akun, data lokasi, nomor telepon, tanggal lahir, *photo profile*, *cover photo*, *posting* berupa teks, *posting* berupa gambar, *private message* berupa teks dan *private message* berupa gambar. Kemudian pada aplikasi media sosial Twitter bukti forensik yang ditemukan hanya nama akun, data lokasi, *photo profile*, *cover photo*, *tweet (posting)* berupa teks dan *tweet (posting)* berupa gambar. Sedangkan bukti forensik berupa nomor telepon, tanggal lahir, *direct message* berupa teks dan *direct message* berupa gambar tidak ditemukan.

Berdasarkan gambar pada 5.41 dan 5.42 menunjukkan bahwa tidak ada perbedaan hasil pencarian bukti forensik dengan menggunakan aplikasi SQLite Manager maupun DB Browser for SQLite.

6.2 Saran

Penulis menyarankan untuk melakukan pengembangan penelitian selanjutnya agar menjadi lebih baik karena penelitian ini masih memiliki banyak kekurangan dan keterbatasan. Berikut saran untuk penelitian selanjutnya, diantaranya :

1. Melakukan penelitian pencarian bukti forensik lebih lanjut pada aplikasi media sosial Facebook dan Twitter untuk menemukan bukti forensik yang tidak berhasil ditemukan oleh penulis seperti tanggal lahir, nomor telepon, *direct message* berupa teks maupun gambar pada aplikasi media sosial Twitter.
2. Menggunakan aplikasi media sosial dan perangkat *smartphone* dengan sistem operasi lainnya untuk melakukan analisa dan pencarian bukti forensik.

DAFTAR PUSTAKA

- Beek, C. (2011). Introduction to File Carving. *McAfee*.
- Devita, & Amal, N. N. (2014). Media Sosial dan Perkembangan Fashion Hijab. *Jurnal Komunikasi*.
- Guardian, T. (2012, Desember 27). *Social media related crime reports up 780% in four years*. Retrieved from The Guardian:
<https://www.theguardian.com/media/2012/dec/27/social-media-crime-facebook-twitter>
- Indrajit, R. E. (2012). Forensik Komputer. *Forensik Komputer*.
- Jansen, W., & Ayers, R. (2007). *Guidelines on Cell Phone Forensics*. Gaithersburg: National Institute of Standards and Technology.
- Kemp, S. (2016, Januari 27). *Digital in 2016*. Retrieved from We Are Social Website: <http://wearesocial.com/uk/special-reports/digital-in-2016>
- lazierthanthou. (2016, 10 1). *Mozilla Foundation*. Retrieved from Mozilla Foundation Website: <https://addons.mozilla.org/id/firefox/addon/sqlite-manager/>
- Madani, S. A., J. K., & Mahlknecht, S. (2010). Wireless sensor networks : modeling and simulation.
- Mathur, A., Schlotfeldt, B., & Chetty, M. (2015). A mixed-methods study of mobile users' data usage practices in South Africa. *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, 1209-1220.
- Merola, A. (2008). Data Carving Concept. *Data Carving*.
- Möller, A., Kranz, M., Schmid, B., Roalter, L., & Diewald, S. (2013). Investigating self-reporting behavior in long-term studies. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2931-2940.
- Mutawa, N. A., Baggili, & Marrington. (2012). Forensic analysis of social networking applications on mobile devices. *Digital Investigation*.
- Nugroho, D. R., Suadi, W., & Pratomo, B. A. (2010). Implementasi Sistem Manajemen Database untuk SQLite di Sistem Android. *Android Database SQLite*.
- Raharjo, B. (2013). Sekilas Mengenai Forensik Digital.

- Safaat, N. (2012). *Pemrograman Aplikasi Mobile Smartphone*. Bandung: Informatika.
- Setyani, & Ika, N. (2013). Penggunaan Media Sosial Sebagai Sarana Bagi Komunitas. *Jurnal Komunikasi*.
- Smith, E. (2013, Agustus 21). *Crime Wire : Social Media and Crime*. Retrieved from Instant Checkmate:
<https://www.instantcheckmate.com/crimewire/2013/08/21/social-media-and-crime-2/>
- staff, A. (2012, Juli 18). *Social Media's Role In Law Enforcement Growing*. Retrieved from Breaking Gov Website:
<http://breakinggov.com/2012/07/18/social-medias-role-in-law-enforcement-growing/>
- Walniycky, D., Baggili, I., Marrington, A., Moore, J., & Breitingner, F. (2015). Network and device forensic analysis of Android. *Digital Investigation*.
- Williams, B. K., & Sawyer, S. C. (2011). *Using Information Technology: A Practical Introduction to Computers & Communications*. (9th edition). New York: McGraw-Hill.
- Wilson, C. (2015, September 15). *Android Phone Forensic Analysis*. Retrieved from Data Forensic: <http://www.dataforensics.org/android-phone-forensics-analysis/>
- Yadi, I. Z., & Kunang, Y. N. (2014). Analisis Forensik pada Platform Android. *Konferensi Nasional Ilmu Komputer (KONIK) 2014*.
- Yusoff, M., Dehghantanha, A., & Mahmud, R. (2016). Forensic Investigation of Social Media and Instant Messaging Services in Firefox OS: Facebook, Twitter, Google+, Telegram, OpenWapp and Line as Case Studies. *Forensic*.

LAMPIRAN

SURAT KETERANGAN BIMBINGAN SKRIPSI

| | | | | | | | | | | | |
|---|--|--|-------|-------------------------------|--------------------------|-----------------|---------------|----------------------|---------------|---|--|
|  | KEMENTERIAN AGAMA UNIVERSITAS ISLAM NEGERI (UIN) SYARIF HIDAYATULLAH JAKARTA FAKULTAS SAINS DAN TEKNOLOGI | <small>Email : fst@uinjkt.ac.id Website : fst.uinjkt.ac.id</small> | | | | | | | | | |
| <small>Jl. Ir. H. Juanda No. 95 Ciputat 15412 Indonesia Telp.: (62-21) 7493606, 7493547, 7401925 Fax.: (62-21) 7493315</small> | | | | | | | | | | | |
| <table border="0" style="width: 100%;"> <tr> <td style="width: 30%;">Nomor</td> <td style="width: 40%;">: Un.01/F9/PP.00.9/11192/2016</td> <td style="width: 30%; text-align: right;">Jakarta, 26 Oktober 2016</td> </tr> <tr> <td>Lampiran</td> <td>: -</td> <td></td> </tr> <tr> <td>Perihal</td> <td>: Bimbingan Skripsi</td> <td></td> </tr> </table> | | | Nomor | : Un.01/F9/PP.00.9/11192/2016 | Jakarta, 26 Oktober 2016 | Lampiran | : - | | Perihal | : Bimbingan Skripsi | |
| Nomor | : Un.01/F9/PP.00.9/11192/2016 | Jakarta, 26 Oktober 2016 | | | | | | | | | |
| Lampiran | : - | | | | | | | | | | |
| Perihal | : Bimbingan Skripsi | | | | | | | | | | |
| <p>Kepada Yth.</p> <ol style="list-style-type: none"> 1. Siti Umami Masruroh, M.Sc 2. Dewi Khairani M.Sc <p>Dosen Pembimbing Skripsi</p> | | | | | | | | | | | |
| <p><i>Assalamu 'alaikum Wr.Wb.</i></p> <p>Dengan ini diharapkan kesediaan Saudara untuk menjadi pembimbing I/II/ (Materi/Teknis)* penulisan skripsi mahasiswa:</p> <table border="0" style="width: 100%; margin-top: 10px;"> <tr> <td style="width: 30%;">Nama</td> <td>: Wisnu Arimukti</td> </tr> <tr> <td>NIM</td> <td>: 1112091000029</td> </tr> <tr> <td>Program Studi</td> <td>: Teknik Informatika</td> </tr> <tr> <td>Judul Skripsi</td> <td>: "Analisa Dan Perbandingan Bukti Forensik Aplikasi Media Sosial Facebook Dan Twitter Pada Smartphone Android"</td> </tr> </table> <p>Judul tersebut telah disetujui oleh Program Studi bersangkutan pada tanggal 26 Oktober 2016 dengan outline, abstraksi dan daftar pustaka terlampir. Bimbingan skripsi ini diharapkan selesai dalam waktu 6 (enam) bulan setelah ditandatanganinya surat penunjukan pembimbing skripsi.</p> <p>Apabila terjadi perubahan terkait dengan skripsi tersebut selama proses pembimbingan, harap segera melaporkan kepada Program Studi bersangkutan.</p> <p>Demikian atas kesediaan Saudara, kami ucapkan terima kasih.</p> <p><i>Wassalamu 'alaikum Wr.Wb.</i></p> <div style="text-align: right; margin-top: 20px;"> <p>a.n Dekan Kabag. TU</p>  <p>Ahmad Zaidi, S.Sos., M. Si NIP. 19590406 198003 1 003</p> </div> | | | Nama | : Wisnu Arimukti | NIM | : 1112091000029 | Program Studi | : Teknik Informatika | Judul Skripsi | : "Analisa Dan Perbandingan Bukti Forensik Aplikasi Media Sosial Facebook Dan Twitter Pada Smartphone Android" | |
| Nama | : Wisnu Arimukti | | | | | | | | | | |
| NIM | : 1112091000029 | | | | | | | | | | |
| Program Studi | : Teknik Informatika | | | | | | | | | | |
| Judul Skripsi | : "Analisa Dan Perbandingan Bukti Forensik Aplikasi Media Sosial Facebook Dan Twitter Pada Smartphone Android" | | | | | | | | | | |
| <p><small>Tembusan: Dekan (sebagai laporan)</small></p> | | | | | | | | | | | |