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

Wisnu Ari Mukti, Siti Ummi Masruroh, Dewi Khairani

Jurusan Teknik Informatika UIN Syarif Hidayatullah Jakarta
Jl.Ir. H. Juanda No.95 Ciputat 15412 Jakarta-Indonesia
wisnuarimukti@gmail.com

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. 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*

ABSTRACT

The development of internet technology and smartphones are increasing rapidly followed by increasing social media users who access using a smartphone, especially Android. One of the problems that did not escape from social media is cyber crime acts that utilize social media. Because basically no crime does not leave a trace. This study was conducted to find and compare the forensic evidence on social media applications Facebook and Twitter are accessed on Android smartphones. Facebook and Twitter are selected for having some similar features. In this study, the simulation method used in the research by running 11 scenarios such as the return of deleted files, the search for forensic evidence in the form of account name, location, phone number, birth date, photo profile, photo cover, text posts, Private message in the form of text and private message content in the form of picture. The results of this study indicate that all forensic evidence on Facebook social media applications found all. While in the social media application Twitter only managed to be found in the form of account name, location data, photo profile, photo cover, text posts and post images.

Keywords: *Digital Forensics, Forensic Evidence, Smartphone, Facebook, Twitter*

I. PENDAHULUAN

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. Pada Januari 2016 pengguna *smartphone* mengakses internet dengan *platform* berbasis Android sebanyak 66%, Apple iOS 19% dan platform lainnya sebanyak 15%[6].

Perkembangan teknologi *smartphone* yang memudahkan orang-orang dalam mengakses internet diiringi juga dengan banyaknya penggunaan media sosial. 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). 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[6]. Pada Juni 2016 media sosial dengan pengguna paling banyak adalah Facebook 1,65 Milyar pengguna,, Qzone 650 Juta pengguna, Instagram 500 Juta pengguna, Twitter 310 Juta [24].

Namun perkembangan media sosial dimanfaatkan oleh sebagian orang untuk melakukan tindak kejahatan. Tidak sedikit tindak kejahatan dilakukan menggunakan media sosial yang diakses melalui *smartphone*. Kejatahan yang bisa disebabkan oleh media sosial diantaranya penculikan, penipuan, pemerasan, *cyberbully* dan lainnya. Kejahatan pada media sosial Facebook dan Twitter meningkat sebanyak 780% selama 4 tahun dari tahun 2008 (556 kasus) sampai tahun 2012 (4908) kasus[3].

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

II. METODOLOGI PENELITIAN

Penelitian ini menggunakan metode simulasi, metode simulasi terdiri dari beberapa tahap-tahap seperti berikut:

A. *Problem Simulation*

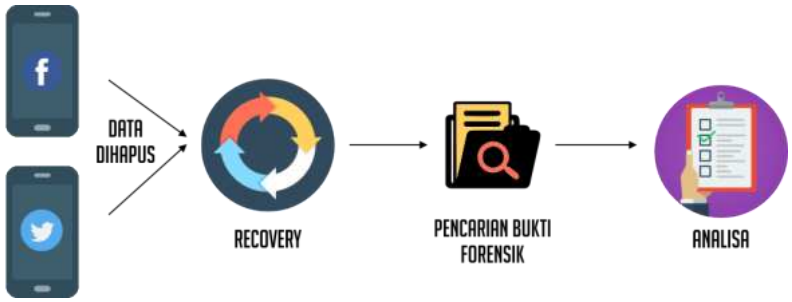
Permasalahan utama dengan meningkatnya akses media sosial dengan menggunakan *smartphone* adalah maraknya tindak kejahatan yang dilakukan oleh pihak yang tidak bertanggung jawab dengan memanfaatkan media sosial yang diakses melalui *smartphone*. Pada tahun 2013, 81% kejahatan internet (*cyber crime*) 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[17].

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"[4]. Bukti forensik pada *smartphone* menjadi tambang emas bagi penyidik forensik karena sifat personalias dari kepemilikan *smartphone* tersebut [12]. Data yang diambil dari perangkat *smartphone* dengan sendirinya dapat dijadikan bukti. Bukti-bukti ini dapat menjadi landasan ketika menyelediki suatu perkara oleh lembaga penegak hukum [22].

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.

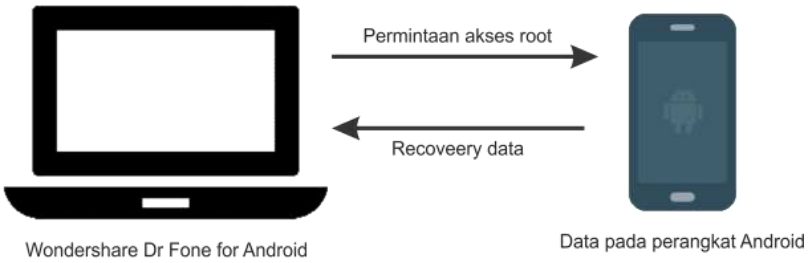
B. *Conceptual Model*

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 2.1 Arsitektur simulasi pencarian dan analisa bukti forensik

Gambar 2.2 Arsitektur komunikasi data pada akun media sosial



Gambar 2.3 Proses recovery data

Gambar 1 menggambarkan asrsitektur dalam pencarian dan analisa bukti forensik pada penelitian kali ini. Perbedaan hanya terdapat pada aplikasi media sosial yang digunakan. Sedangkan pada gambar 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 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:

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.
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.
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. 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.
5. Validasi
   Akun palsu digunakan dalam pencarian bukti forensik. Sebelum dilakukan pencarian bukti forensik terlebih dahulu dilakukan komunikasi data antara akun media sosial tersebut. Berdasarkan gambar 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.
6. 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.

C. *Input/Output Data*

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: Nama akun, Lokasi, Nomor telepon, Tanggal lahir, *Photo profile*, Cover photo, posting berupa teks, posting berupa gambar, isi *private message* berupa teks, isi *private message* berupa gambar. Semua data yang di-*input* adalah sama.

Tabel 2.1 Bukti forensik yang akan dicari

Data yang di-input	Bentuk data	Isi teks dan file gambar
Nama akun	Teks	Pratama Pertama
Lokasi	Teks	Semarang, Indonesia
Nomor telepon	Teks	+6285776267290
Tanggal lahir	Teks	1 Januari 1991
Photo profile	Gambar	Profile.jpg
Cover Photo	Gambar	Siput.jpg
Posting berupa teks	Teks	Test 1 2 3
Posting berupa gambar	Gambar	3310.jpg
Isi private message berupa teks	Teks	Percakapan 2 pihak terkait jual beli *handphone*
Isi private message berupa gambar	Gambar	Nokia3310.jpg

D. *Modelling*

Pembuatan skenario-skenario yang akan digunakan untuk proses simulasi. Pada penelitian ini terdapat 11 skenario, masing-masing skenario dilakukan 2 kali percobaan. Skenario tersebut adalah sebagai berikut:

Skenario 1 adalah melakukan *recovery data* pada aplikasi Facebook dan Twitter yang sebelumnya telah dihapus pada *smartphone*. Selanjutnya skenario 2-11 adalah tahap pencarian bukti forensik terhadap aplikasi Facebook dan Twitter. Bukti forensik yang dicari adalah sebagai berikut: Nama akun, Lokasi, Nomor telepon, Tanggal lahir, *Photo profile*, Cover photo, posting berupa teks, posting berupa gambar, isi *private message* berupa teks, isi *private message* berupa gambar.

E. *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.

Sebelum simulasi dijalankan dilakukan beberapa persiapan seperti *rooting* perangkat Android, pembuatan akun palsu, pemasangan

aplikasi *recovery file* dan pemasangan aplikasi *database browser*.

F. *Verification and 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 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.

G. *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.

H. *Output Analysis*

Analisa hasil yang didapat setelah selesai menjalankan semua skenario yang akan dibahas pada bab selanjutnya.

III. HASIL DAN PEMBAHASAN

A. *Simulasi 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:

Tabel 3.1 Hasil Perbandingan Skenario 1

Skenario 1	Facebook	Twitter
Mengembalikan *file* dan data-data yang dihapus	*File* dan data-data berhasil dikembalikan	*File* dan data-data berhasil dikembalikan
Data dan *file* yang dikembalikan	com.facebook.katana (*file* dan data-data Facebook Apps) com.facebook.orca (file dan data-data Facebook Messenger)	com.twitter.android (*file* dan data-data Twitter Apps)

Pada tabel 3.1 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).

B. *Simulasi 2*

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

Tabel 3.2 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 3.2 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.

C. *Simulasi 3*

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

Tabel 3.3 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 3.3 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.

D. *Simulasi 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 menggunakan SQLite Manager dan DB Browser for SQLite. Berikut adalah hasil simulasi skenario:

Tabel 3.4 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 *database* melainkan pada *server*.

Pada tabel 3.4 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*.

E. *Simulasi 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 menggunakan SQLite Manager dan DB Browser for SQLite. Berikut adalah hasil simulasi skenario:

Tabel 3.5 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 *database* melainkan pada *server*

Pada tabel 3.5 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*.

F. *Simulasi 6*

Pada skenario 6 simulasi dilakukan untuk menemukan bukti forensik berupa *profile picture* dari pengguna aplikasi media sosial Facebook dan Twitter pada *smartphone* Android menggunakan SQLite Manager dan DB Browser for SQLite. Berikut adalah hasil simulasi skenario:

Tabel 3.6 Hasil Perbandingan Skenario 6

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

Pada tabel 3.6 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 pada *file database* 732798704059621380-43, pada tabel users.

G. *Simulasi 7*

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

Tabel 3.7 Hasil Perbandingan Skenario 7

Skenario 7	Facebook	Twitter
Menemukan bukti forensik berupa *Cover Photo*	*Cover Photo* berhasil ditemukan	*Cover Photo* berhasil ditemukan
Bukti forensik yang ditemukan	*url* yang mengarahkan pada *cover photo* akun tersebut: *https://z-m-scontent.fcgk4-1.fna.fbcdn.net/v/t1.0-0/cp0/e15/q65/s320x320/13880355_1818165403558695 1_2147424343281991346_n.jpg?efg=eyJkdHciOiIifQ%3D%3D&_nc_eui2=v1%3AAeHn2PABqvko3qvmhbkU9xMXv953OFhLvs89yYtqU9XLGHfpW-ecf1AJ-OGqIhuq2CenXe8-q-VYNPHXW3r-pyIt-E99bU5eQ8_uibfRqz1u_RLOXvAhAESfVk2cOEDgnu0&_nc_ad=z-m&oh=fd241b4172ad424d6fdee3fbbdbeb63a&oe=58CBCCD6*	*url* yang mengarahkan pada *cover photo* akun tersebut: *https://pbs.twimg.com/profile_banners/732798704059621380/1480930200*

Pada tabel 3.7 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.

H. *Simulasi 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 menggunakan SQLite Manager dan DB Browser for SQLite. Berikut adalah hasil simulasi skenario:

Tabel 3.8 Hasil Perbandingan Skenario 8

Skenario 8	Facebook	Twitter
Menemukan bukti forensik berupa *posting* atau *tweet* (bentuk teks)	*Posting* berhasil ditemukan	*Twitter* berhasil ditemukan
Bukti forensik yang ditemukan	Isi *posting* bertuliskan: Test 1 2 3 dan *url* yang mengarahkan kepada *posting* terkait: *https://m.facebook.com/story.php?story_fbid=235759296843091&id=100012270664021MjM1NzU5Mjk2ODQzMDkxOjU6MA==0UzpfSTEwMDAxMjI3MDY2NDAyMToyMzU3NTkyOTY4NDMwOTE=*	Isi *posting* bertuliskan : Test 1 2 3

Pada tabel IX 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 pada *file database* 732798704059621380-43, pada tabel full_content.

I. *Simulasi 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 menggunakan SQLite Manager dan DB Browser for SQLite. Berikut adalah hasil simulasi skenario:

Tabel 3.9 Hasil Perbandingan Skenario 9

Skenario 9	Facebook	Twitter
Menemukan bukti forensik berupa *posting* atau *tweet* (bentuk gambar)	*Posting* berhasil ditemukan	*Tweet* berhasil ditemukan
Bukti forensik yang ditemukan	Isi *posting* bertuliskan: Dijual hp Nokia 3310 kondisi baru. Harga Rp2.000.000 Garansi Distributor 1 tahun. Harga bisa nego. dan *url* yang mengarahkan kepada gambar terkait: *https://scontent-sin6-1.xx.fbcdn.net/t31.0-8/cp0/e15/q65/s720x720/14361331_2055 79889861032_4072 761814445104575_ o.jpg?_nc_ad=z-m*	Isi *posting* bertuliskan: Dijual hp Nokia 3310 kondisi baru. Harga Rp2.000 .000 Garansi Distributor 1 tahun. Harga bisa nego. dan *url* yang mengarahkan kepada gambar terkait: *pic.twitter.com/ mf0fdeP yDE*

Pada tabel 3.9 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.

J. *Simulasi 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 menggunakan SQLite Manager dan DB Browser for SQLite. Berikut adalah hasil simulasi skenario:

Tabel 3.10 Hasil Perbandingan Skenario 10

Skenario 10	Facebook	Twitter
Menemukan bukti forensik berupa *private message* atau *direct message* (bentuk teks)	*Private message* (bentuk teks) berhasil ditemukan	*Direct message* (bentuk teks) tidak berhasil ditemukan
Bukti forensik yang ditemukan	Isi percakaan Duo kedua: Halo pak pratama Pratama pertama: ya? Duo kedua: Apa harga hp tersebut bisa kurang lagi jadi 1,8jt?	Tidak ditemukan Asumsi data tidak ditemukan: data tidak tersimpan pada *database* melainkan pada *server*

	Pratama pertama: Tentu bisa ☺ Dan seterusnya	

Pada tabel 3.10 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*.

K. *Simulasi 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 menggunakan SQLite Manager dan DB Browser for SQLite. Berikut adalah hasil simulasi skenario:

Tabel 3.11 Hasil Perbandingan Skenario 11

Skenario 11	Facebook	Twitter
Menemukan bukti forensik berupa *private message* atau *direct message* (bentuk gambar)	*Private message* (bentuk gambar) berhasil ditemukan	*Direct message* (bentuk gambar) tidak berhasil ditemukan
Bukti forensik yang ditemukan	*url* yang mengarahkan kepada gambar terkait: *https://scontent.xx.fbcdn.net/v/t34.0-12/fr/cp0/e15/q65/14389696_20492139260315_2106835510_n.jpg?_nc_ad=z-m&oh=15da0ba1bc784b6dce926b988db10e73&oe=57E3C350*	Tidak ditemukan Asumsi data tidak ditemukan: data tidak tersimpan pada *database* melainkan pada *server*

Pada tabel 3.11 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*.

IV. PENUTUP

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.

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. Tidak ada

perbedaan hasil pencarian bukti forensik dengan menggunakan aplikasi SQLite Manager maupun DB Browser for SQLite.

Berdasarkan pemaparan tersebut dapat disimpulkan bahwa bukti forensik lebih banyak ditemukan pada media sosial Facebook dan tidak ada perbedaan hasil pencarian bukti forensik dengan menggunakan aplikasi SQLite Manager maupun DB Browser for SQLite.

DAFTAR PUSTAKA

[1] Beek, C. (2011). Introduction to File Carving. *McAfee*.

[2] Devita, & Amal, N. N. (2014). Media Sosial dan Perkembangan Fashion Hijab. *Jurnal Komunikasi*.

[3] 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

[4] Indrajit, R. E. (2012). Forensik Komputer. *Forensik Komputer*.

[5] Jansen, W., & Ayers, R. (2007). *Guidelines on Cell Phone Forensics.* Gaithersburg: National Institute of Standards and Technology.

[6] Kemp, S. (2016, Januari 27). *Digital in 2016*. Retrieved from We Are Social Website: http://wearesocial.com/uk/special-reports/digital-in-2016

[7] Lazierthanthou. (2016, 10 1). *Mozilla Foundation*. Retrieved from Mozilla Foundation Website: https://addons.mozilla.org/id/firefox/addon/sqlite-manager/

[8] Madani, S. A., J. K., & Mahlknecht, S. (2010). Wireless sensor networks: modeling and simulation.

[9] 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.

[10] Merola, A. (2008). Data Carving Concept. *Data Carving*.

[11] 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.

[12] Mutawa, N. A., Baggili, & Marrington. (2012). Forensic analysis of social networking applications on mobile devices. *Digital Investigation*.

[13] Nugroho, D. R., Suadi, W., & Pratomo, B. A. (2010). Implementasi Sistem Manajemen Database untuk SQLite di Sistem Android. *Android Database SQLite*.

[14] Raharjo, B. (2013). Sekilas Mengenai Forensik Digital.

[15] Safaat, N. (2012). *Pemrograman Aplikasi Mobile Smartphone*. Bandung: Informatika.

[16] Setyani, & Ika, N. (2013). Penggunaan Media Sosial Sebagai Sarana Bagi Komunitas. *Jurnal Komunikasi*.

[17] 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/

[18] 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/

[19] Walniyccky, D., Baggili, I., Marrington, A., Moore, J., & Breitinger, F. (2015). Network and device forensic analysis of Android. *Digital Investigation*.

[20] Wiliams, B. K., & Sawyer, S. C. (2011). Using Information Technology: A Practical Introduction to Computers & Communications. (9th edition). New York: McGraw-Hill.

[21] Wilson, C. (2015, September 15). *Android Phone Forensic Analysis*. Retrieved from Data Forensic: http://www.dataforensics.org/android-phone-forensics-analysis/

[22] Yadi, I. Z., & Kunang, Y. N. (2014). Analisis Forensik pada Platform Android. *Konferensi Nasional Ilmu Komputer (KONIK) 2014*.

[23] Yusoff, M., Dehghantanha, A., & Mahmod, 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*.

[24] Felix Richter (2016). Facebook Inc. Dominates the Social Media Landscape: https://www.statista.com/chart/5194/active-users-of-social-networks-and-messaging-services/