

ANALISIS KONTEN DUGAAN TINDAK KEJAHATAN DENGAN BARANG BUKTI DIGITAL BLACKBERRY MESSENGER

Dedy Hariyadi¹, Wing Wahyu Winarno², Ahmad Luthfi³

Magister Informatika Fakultas Teknologi Industri
Universitas Islam Indonesia

¹13917112@students.uui.ac.id, ²maswing@gmail.com, ³ahmad.luthfi@uui.ac.id

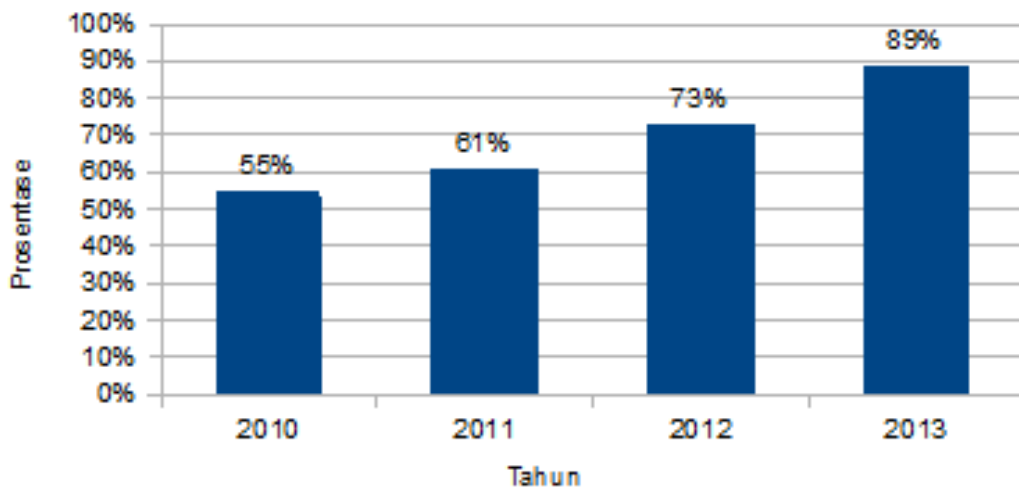
Abstrak

Barang bukti ponsel yang ditangani Pusat Laboratorium Forensik Kepolisian Republik Indonesia linier dengan pertumbuhan ponsel cerdas secara global. Hal ini menggambarkan tindak kejahatan menggunakan perangkat digital semakin banyak. Dalam penelitian ini mencoba melakukan analisis terhadap barang bukti digital berupa ponsel yang fokus pada percakapan antara pemilik ponsel dengan rekan-rekannya. Tidak hanya jumlah kontak dan komunikasi yang dianalisis namun percakapan teks menjadi petunjuk penting dalam analisis tindak kejahatan. Hasil analisis teks percakapan dengan visualisasi wordcloud diharapkan dapat dijadikan petunjuk pihak Kepolisian dalam menentukan keterkaitan pihak lain dalam dugaan tindak kejahatan yang memanfaatkan ponsel.

Kata Kunci: term frequency, wordcloud, SNI 27037:2014, forensik digital, blackberry messenger, BBMPork, R.

1. Pendahuluan

Pusat Laboratorium Forensik Kepolisian Republik Indonesia melalui *Digital Analysis Forensics Team* (DFAT) mencatat jumlah kejahatan melalui ponsel dari tahun 2010 sampai dengan 2013 mengalami pertumbuhan tiap tahunnya. Pertumbuhan ini diperoleh dari barang bukti berupa ponsel yang ditangani oleh DFAT. Gambar 1 menunjuk pertumbuhan jumlah barang bukti berupa ponsel yang ditangani oleh DFAT.



Gambar 2: Pertumbuhan barang bukti ponsel (observasi)

Informasi yang didapat dari situs web Humas Kepolisian Republik Indonesia bahwa kejahatan menggunakan aplikasi Blackberry Messenger (BBM) juga cukup banyak. Hal ini seiring dengan pertumbuhan barang bukti berupa ponsel yang selalu meningkat dari tahun ke tahun. Tabel 1 menunjukkan tindak kejahatan yang memanfaatkan aplikasi BBM.

Table 1: Kejahatan yang Memanfaatkan BBM (Observasi)

No	Tahun Kejadian	Kasus
1.	2014	Prostitusi daring di Surabaya yang mengatasnamakan jasa penginapan
2.	2015	Status BBM yang menyebabkan penangkapan dan penyiksaan seorang siswi di Yogyakarta
3.	2015	Mengendalikan bisnis prostitusi dari Lembaga Masyarakat Kerobokan
4	2015	Prostitusi daring di Jakarta yang melibatkan artis

Meningkatnya tingkat kejahatan menggunakan ponsel cerdas dengan memanfaatkan aplikasi pengiriman pesan seperti BBM menuntut aparat penegak hukum untuk lebih teliti dalam melakukan analisis tindak kejahatan. Prosedur penanganan barang bukti digital yang dapat digunakan sebagai acuan aparat penegak hukum ada beberapa tahap. Ada pun tahapan diantaranya *preservation, acquisition, examination and analysis*, dan *reporting* (Jansen & Ayers 2007).

Berdasarkan hasil laporan dari uji forensik ponsel cerdas yang menggunakan Cellebrite UFED masih memerlukan analisis lebih lanjut seperti membaca pesan satu per satu. Hasil observasi pada aplikasi Oxygen Forensics hanya memiliki fitur *Link and Stats*² dan *Social Graph*³ yang berfungsi untuk menganalisis jumlah komunikasi antara pemilik ponsel dengan rekan-rekannya yang tersimpan pada daftar kontak. Dengan berbagai keterbatasan tersebut, maka diperlukan sebuah alat bantu. Alat bantu tersebut tidak sekedar berfungsi untuk menghitung jumlah komunikasi, namun juga membantu proses analisis dari konten percakapan/komunikasi.

Pada setiap ponsel cerdas yang menggunakan sistem operasi seperti iOS, Android, Windows Phone, dan Blackberry 10 memiliki basis data SQLite

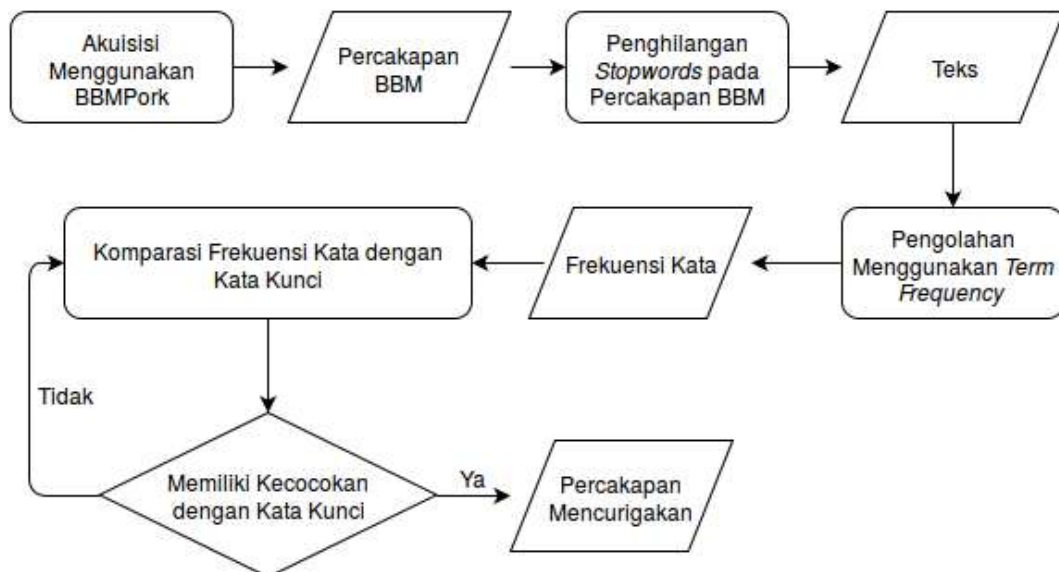
2 <http://www.oxygen-forensic.com/en/products/oxygen-forensic-detective/analyst/links-and-stats>

3. <http://www.oxygen-forensic.com/en/products/oxygen-forensic-detective/analyst/social-graph>

sebagai sumber utama untuk pengelolaan data. Menganalisis berkas basis data SQLite menjadi penting karena dimungkinkan terdapat data yang bersifat kritis sedangkan pada perangkat analisis forensik digital belum tentu menyediakan analisis secara mendalam (Reiber 2016). Berkas SQLite yang merupakan barang bukti digital dapat dianalisis dengan menggunakan perangkat analisis basis data atau dikombinasi dengan perangkat lunak analisis pengolah data lainnya.

2. Metode Penelitian

Tahapan-tahapan dalam penelitian ini terilustrasi pada gambar 2 yang merupakan alur proses penelitian. Untuk mendapatkan barang bukti digital teks terlebih dahulu melakukan akuisisi secara *logical* menggunakan *tools* BBMPork. Aplikasi Blackberry Messenger memiliki barang bukti digital berupa berkas basis data SQLite, *master.db*. Berkas tersebut dapat diperoleh di direktori */data/data/com.bbm5.rr_mod5/files/bbmcore*. Dalam penelitian ini digunakan aplikasi Blackberry Messenger yang telah dimodifikasi oleh pihak lain namun masih dapat berkomunikasi antar pengguna BBM lainnya.

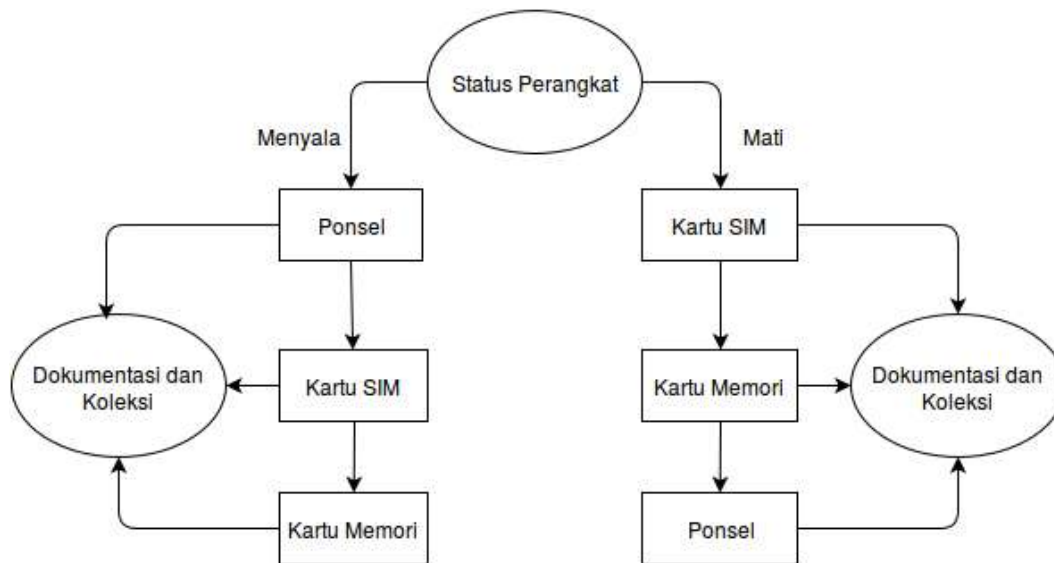


Gambar 2: Alur proses penelitian

Berkas *master.db* yang menyimpan data percakapan diolah menggunakan BBMPork untuk menampilkan percakapan antar pemilik ponsel dengan rekan-rekannya. Melalui BBMPork percakapan dikonversi menjadi berkas teks yang mudah dianalisis yaitu dalam bentuk berkas CSV (*Comma Separated Value*).

2.1 Akuisisi Barang Bukti Digital

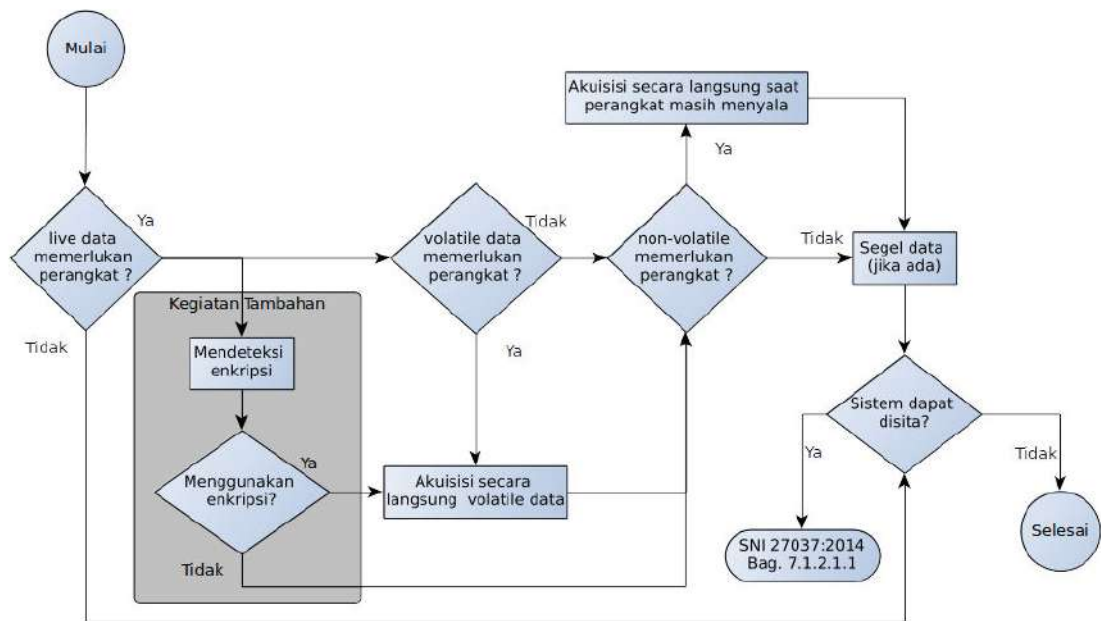
Penanganan barang bukti elektronik berupa ponsel dan barang bukti digital yang terdapat dalam ponsel caranya beragam. Prinsipnya ponsel tersebut dalam kondisi menyala atau mati. Menurut Lee Reiber dalam buku *Mobile Forensics Investigation: A Guide to Evidence Collection, Analysis, and Presentation* proses mengakuisi barang bukti digital berupa ponsel terilustrasi pada Gambar 3.



Gambar 3: Prinsip akuisisi ponsel

Menurut Standar Nasional Indonesia (SNI) 27037:2014 juga telah mengatur prosedur akuisisi barang bukti elektronik dan barang bukti digital. Khusus untuk perangkat dalam kondisi menyala SNI 27037:2014 telah mengaturnya pada bagian 7.1.3.1.1. Adapun ilustrasi proses akuisisi bukti digital pada perangkat dalam kondisi menyala dapat dilihat pada Gambar 4.

BBMPork telah dirancang menyesuaikan dengan SNI 27037:2014 bagian 7.1.3.1.1 dengan status ponsel dalam kondisi menyala. BBMPork merupakan aplikasi logical forensics berlisensi MIT yang dikembangkan menggunakan IGN-SDK dengan fungsi utama untuk melakukan analisis percakapan Blackberry Messenger yang berjalan di ponsel bersistem operasi Android (Hariyadi & Irawan 2014)□. Barang bukti digital yang didapatkan berupa berkas SQLite *master.db* dapat dikonversi ke berkas teks untuk analisis lebih lanjut.



Gambar 4: Akuisisi barang bukti digital dengan kondisi menyala (BSN, 2014)

2.2 Analisis Teks

Barang bukti digital berupa berkas SQLite *master.db* yang didalamnya terdapat percakapan antara pemilik ponsel dengan rekan-rekannya dapat dikonversi ke berkas CSV menggunakan BBMPork. Sehingga berkas CSV tersebut dapat dianalisis lebih lanjut menggunakan perangkat lunak analisis t seperti R yang dikembangkan oleh John Chambers. R memiliki berbagai fitur statistik (linear dan pemodelan non-linier, uji statistik klasik, analisis *time-series*, klasifikasi, dan sebagainya) dan teknik grafis serta ekstensibel (The R Foundation 2014)□. Menggunakan R juga dapat mengolah data kejahatan dalam bentuk visualisasi jejaring kejahatan (G 2015)□.

R melalui pustaka *tm* dapat menganalisis kemunculan kata dalam sebuah teks. Pustaka *tm* merupakan implementasi dari analisis *Term Frequency*. Namun teks yang akan dianalisis harus dibersihkan melalui tahap pra proses. Langkah awal dalam melakukan analisis teks adalah melakukan pra proses pada data yang ada di dalam berkas CSV. Tahapan pra proses meliputi penghapusan spasi, konversi huruf kapital ke huruf kecil, penghapusan tanda baca dan *wildchar*, penghapusan angka, dan penghapusan *stopword* bahasa Inggris dan Indonesia

2.2.1 Penghapusan Spasi

Beberapa penulisan terkadang terdapat jeda antar kata yang lebih dari satu spasi. Pada proses ini berfungsi untuk menghapus jeda antar kata yang lebih dari satu spasi dari menjadi jeda satu spasi dari sumber data teks. Contoh perintah dalam R untuk memproses penghapusan jeda antar kata yang berlebih adalah `corpus <- tm_map(corpus, stripWhitespace)`.

2.2.2 Konversi Huruf Kecil

Teks terdapat kata-kata yang beragam, ada yang diawali dengan huruf kapital, ada yang semua kata adalah huruf kapital atau kata yang terdiri huruf kecil semua. Proses ini berfungsi untuk menyamaratakan karakter huruf yaitu mengkonversi huruf kapital atau huruf besar menjadi huruf kecil. Contoh perintah dalam R untuk mengkonversi huruf kapital ke huruf kecil adalah `corpus <- tm_map(corpus, tolower)`.

2.2.3 Penghapusan Angka

Proses ini berfungsi untuk menghapus karakter angka pada teks yang tidak akan digunakan dalam analisis. Contoh perintah dalam R untuk memproses penghapusan karakter angka adalah `corpus <- tm_map(corpus, removeNumbers)`.

2.2.4 Penghapusan Tanda Baca

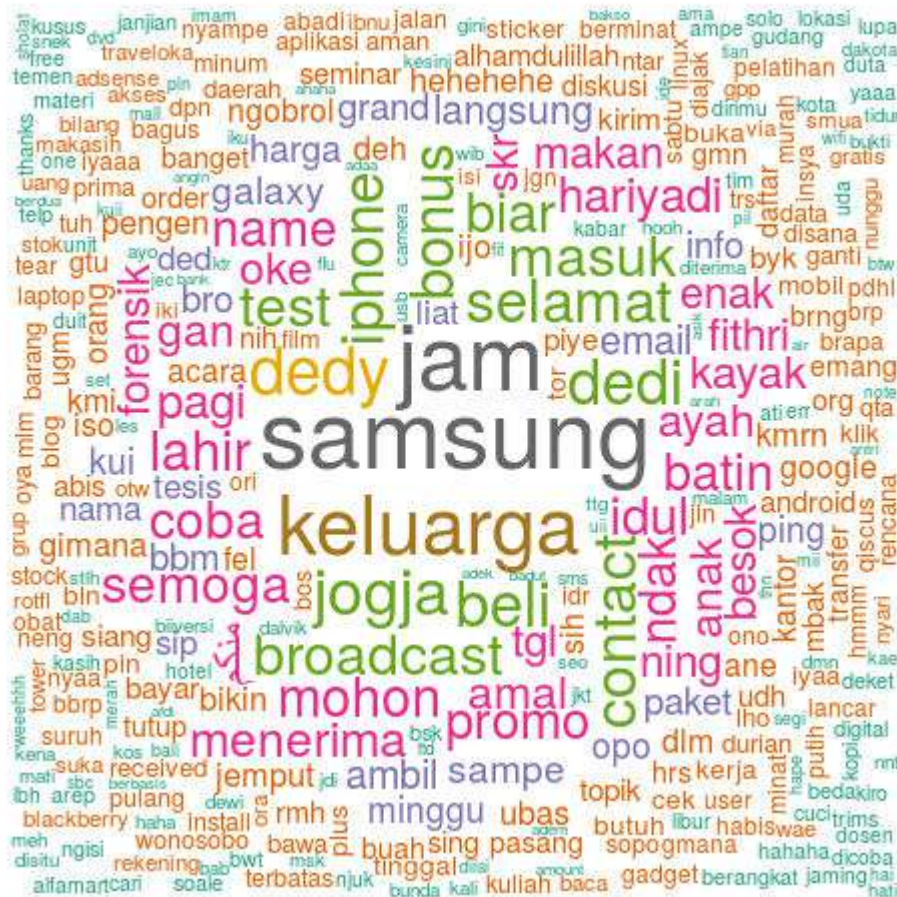
Proses ini berfungsi untuk menghapus tanda-tanda baca dan *wildchar* pada teks yang tidak akan digunakan dalam analisis. Contoh perintah dalam R untuk memproses penghapusan tanda baca adalah `corpus <- tm_map(corpus, removePunctuation)`.

2.2.5 Penghapusan Stopword

Kata penghubung dalam analisis teks tidak diperlukan oleh sebab itu perlu dihapus. Pada proses ini kata-kata yang tidak digunakan dalam analisis dihapus. Tidak hanya kata penghubung, kata-kata yang yang tidak perlu dianalisis dapat dihapus. Penelitian ini menggunakan *stopwords* dari penelitian berjudul "A Study of Stemming Effects on Information Retrieval in Bahasa Indonesia" (Tala 2003)□. Contoh perintah dalam R untuk memproses penghapusan tanda baca adalah `corpus <- tm_map(corpus, removeWords, c(stopwords("english"), stopwords_id))`.

3. Hasil Penelitian

Berkas hasil analisis yang masih tersimpan dalam korpus kemudaian dianalisis menjadi sebuah dokumen matrik untuk mempermudah analisis kemunculan kata. Kemunculan kata tersebut divisualisasikan dalam bentuk *wordcloud* seperti tampak pada Gambar 5.



Gambar 5: Visualisasi *word cloud*

Visualisasi *wordcloud* pada gambar 5 masih belum terlihat indikasi sebuah percakapan yang terkait dengan tindak kejahatan. Untuk mendapatkan visualisasi *wordcloud* yang memiliki indikasi tindak kejahatan hasil analisis kemunculan kata dilakukan komparasi dengan kata kunci atau kata-kata unik yang didapatkan dari kepolisian dengan menggunakan teknik *term frequency* yang terdapat pada pustaka *tm tools* analisis R.

Dalam proses komparasi jika terdapat kata yang sering muncul yang bukan kategori kata kunci dapat dikonsultasikan kembali dengan Kepolisian. Hasil analisis *term frequency* dengan mengkomparasi kata kunci dari kepolisian dibedakan dengan warna abu-abu dan hitam yang tervisualisasi pada *wordcloud*.

Warna abu-abu merupakan kata-kata umum yang digunakan dalam percakapan antara pemilik ponsel dengan rekan-rekannya. Kata-kata yang berwarna hitam pada visualisasi *wordcloud* seperti kata paket, ubas, ijo, putih, dan pil merupakan kosakata yang diduga digunakan dalam tindak kejahatan. Gambar 6 menunjukkan visualisasi *wordcloud* yang memiliki indikasi percakapan terkait tindak kejahatan.



Gambar 3: Visualisasi *wordcloud* dugaan kejahatan

4. Penutup

Suatu percakapan dapat dianalisis kemunculan kata menggunakan *term frequency* yang tervisualisasi dalam bentuk *wordcloud*. Namun banyaknya percakapan belum bisa teranalisis berdasarkan topik percakapan dalam hal ini dugaan tindak kejahatan. Melalui kerjasama dengan pihak Kepolisian analisis percakapan menggunakan *term frequency* akan lebih mudah menemukan indikasi sebuah percakapan terkait dugaan kejahatan. Pihak kepolisian juga lebih cepat dan mudah melakukan analisis keterkaitan pihak lain dalam dugaan tindak kejahatan yang tervisualisasi dalam bentuk *wordcloud*. Penelitian selanjutnya diharapkan dapat dikembangkan menggunakan metode analisis *term frequency* yang dikombinasikan dengan metode lainnya untuk meningkatkan akurasi dalam menentukan dugaan tindak kejahatan disebuah percakapan.

Daftar Pustaka

- Badan Standardisasi Nasional, 2014. *Pedoman Identifikasi, Pengumpulan, Akuisisi dan Preservasi Bukti Digital (ISO/IEC 27037:2012, IDT)*, Jakarta.
- G, S., 2015. Crime Data Investigation and Visualization using R. *International Journal of Emerging Technology and Innovative Engineering*, I(5), hal.128–131.
- Hariyadi, D. & Irawan, E.T., 2014. Purwarupa Forensik BBM di Telepon Seluler Android Menggunakan IGN-SDK. *Indonesia Security Conference 2014*, hal.2–8.
- Jansen, W. & Ayers, R., 2007. Guidelines on Cell Phone Forensics. *NIST Special Publication 800-101*, hal.1–104. Available at: <http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf>.
- Reiber, L., 2016. *Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation*, Mc Graw Hill Education.
- Tala, F.Z., 2003. *A Study of Stemming Effects on Information Retrieval in Bahasa Indonesia*. Universiteti van Amsterdam The Netherlands. Available at: <https://www.illc.uva.nl/Research/Publications/Reports/MoL-2003-02.text.pdf>.
- The R Foundation, 2014. R: What is R? Available at: <http://www.r-project.org/about.html> [Diakses Mei 7, 2015].