SINERGI Vol.20, No.3, Oktober 2016: 207-212
DOAJ: http://doaj.org/toc/2460-1217
DOI: http://doi.org/10.22441/sinergi.2016.3.006

WHATSAPP FORENSICS PADA ANDROID *SMARTPHONE: A SURVEY*

Zulkarnaen Akbar, Beny Nugraha, Mudrik Alaydrus
Jurusan Magister Teknik Elektro, Pascasarjana Universitas Mercu Buana,
Jln. Meruya Selatan, Kembangan, Jakarta 11650
Email: zoel.akbar.id@gmail.com; benynugraha@mercubuana.ac.id;
mudrikalaydrus@mercubuana.ac.id

Abstrak *-- Salah satu applikasi jejaring sosial yang sangat populer saat ini adalah WhatsApp. Hampir seluruh pengguna smartphone menggunakan applikasi ini sebagai media komunikasi. Berbagai macam perkembangan atau fitur baru telah banyak ditambahkan pengembang sebagai fasilitas yang dapat memanjakan para pengguna. Peranan sistem keamanan tentunya sangat penting untuk menunjang keamanan privasi para pengguna agar kerahasiaan tetap terjaga. Beberapa peneliti telah banyak melakukan experimen mobile forensics untuk mendapatkan berbagai informasi dari para pengguna WhatsApp. Pada paper ini membahas survey berbagai metoda dari berbagai para peneliti WhatsApp forensics. Dalam sebuah proses mobile metoda yang digunakan dalam proses forensics antara lain menggunakan internet protocol dan live memory. Untuk proses mobile forensics khususnya pada applikasi WhatsApp dapat dilakukan dengan menggunakan metoda tersebut untuk memperoleh data informasi yang dibutuhkan.*

Kata kunci: *Android Device, WhatsApp, Digital Forensics, Mobile Forensics, Live Memory.*

Abstract *– WhatsApp is one of the social networking application that are very popular today as almost all smartphone users use this application as a communication media. Security system is certainly a very important feature to ensure the privacy and confidentiality of the users. Several researchers have done many experiments in mobile forensics to get any information from WhatsApp users, thus, in this paper the various methods of WhatsApp forensics is discussed. Forensic methods that are discussed in this papers use internet protocol and live memory. These two methods are proven to be able to obtain information of WhatsApp users, however, each method needs different prerequisite to be fulfilled. The use of Internet Protocol requires the communication to be still ongoing, while the use of live memory requires the communication to be finished.*

Keywords: *Android Device, WhatsApp, Digital Forensics, Mobile Forensics, Live Memory.*

PENDAHULUAN

Dengan lebih dari 700 juta pengguna aktif, WhatsApp kini menjadi salah satu aplikasi pesan instan paling populer. Namun, basis pengguna yang luas juga membuat aplikasi ini rentan terhadap serangan *hacker* serta sejumlah risiko keamanan lainnya. WhatsApp kembali menghadirkan fitur terbaru. Mulai dari fitur bisa mengirim video, dokumen, bahkan *voice* yang memungkinkan seorang *user* dapat berbicara dengan melalui menggunakan jaringan internet.

Pernah WhatsApp muncul dalam media surat kabar *online* yaitu WhatsApp adalah salah satu aplikasi jejaring sosial paling poluler yang bisa dikatakan mendominasi dari semua kompetitornya. Tetapi dalam segi kemanan jaringan menjadi salah satu applikasi yang rentan dengan pembajakan dan penyadapan oleh para *hacker* oleh karena itu kali ini WhatsApp menghadirkan fitur yang mengubah sistem keamanan menjadi *End-to-End Encryption*. Mode keamanan tersebut sama seperti yang digunakan iMessage aplikasi milik Apple. Setiap pesan yang dikirim langsung dienkripsi secara aman dan hanya bisa dibuka oleh pengirim dan penerima pesan saja.

Fitur tersebut akan otomatis aktif ketika berkirim pesan asalkan kedua *device* yang berhubungan sudah menggunakan versi terbaru aplikasi WhatsApp. Tidak ada pengaturan apapun, semua chat akan menggunakan mode *End-to-End Encryption* sebagai fitur keamanan bawaan.

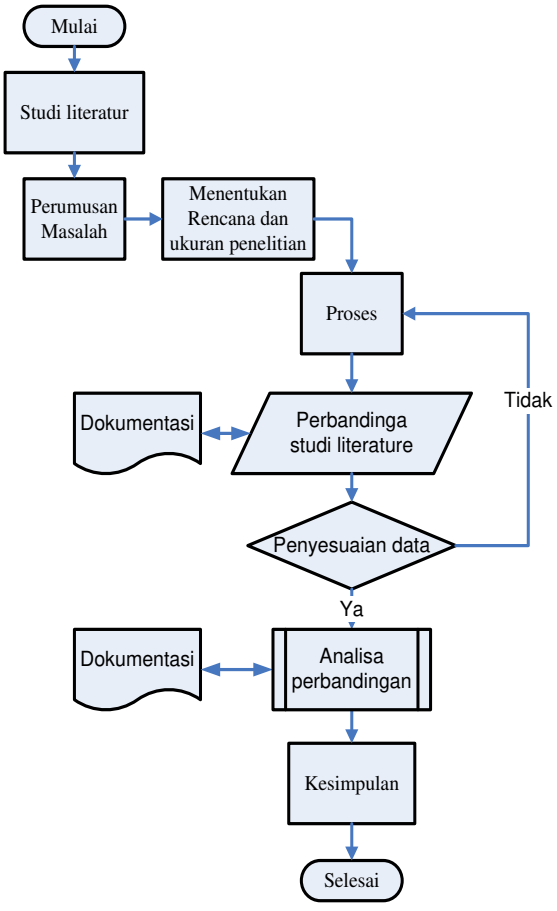
Dalam dunia *digital forensic* banyak menggunakan *tools* untuk memudahkan dalam melakukan infestigasi. Salah satu *tools* yang dapat digunakan dalam dunia *forensics* yaitu Kalilinux dengan dengan beberapa *tools* yang ada didalamnya akan memudahkan dalam melakukan infestigasi.

Dalam paper ini akan disajikan beberapa metode WhatsApp *forensics* yang nantinya akan berguna sebagai acuan para peneliti selanjutnya. Untuk menentukan metode-metode yang bisa digunakan dalam melakukan WhatsApp *forensics*.

Struktur selanjutnya dari paper ini adalah sebagai berikut: bagian kedua tulisan ini membahas metodologi penelitian pada paper ini. Kemudian, teori terkait mengenai *mobile forensics* dibahas pada bagian ketiga. Deskripsi lengkap mengenai teknik-teknik *digital forensic* pada WhatsApp dijabarkan pada bagian keempat. Analisa dari hasil survey akan terdapat pada bagian kelima. Kesimpulan dari paper ini terdapat pada bagian keenam.

METODOLOGI PENELITIAN

Metodologi penelitian yang digunakan adalah dengan membandingkan jurnal-jurnal terkait yang melakukan penelitian *forensics* pada WhatsApp. Pada penulisan paper ini kami akan membahas tentang beberapa metoda dalam *mobile forensics* pada aplikasi WhatsApp. *Flowchart* dari metodologi penelitian dapat dilihat pada Gambar 1.



Gambar 1. *Flowchart* Metodologi Penelitian

Seperti terlihat pada Gambar 1 bahwa metodologi penelitian yang digunakan adalah metode kualitatif, di mana studi literatur dari berbagai metode WhatsApp *forensic* pada smartphone android akan dianalisis dan dibandingkan.

MOBILE FORENSICS

Maraknya tindakan kejahatan dalam dunia komputer, membutuhkan proses pembuktian yang tidaklah mudah, oleh karena itu, kajian bidang komputer forensik ini masih tergolong baru dan masih terus dikembangkan, sehingga nantinya, semua kasus-kasus kejahatan komputer mampu dibuktikan secara sah di pengadilan (Casey, 2010).

Digital forensic mempunyai banyak cabang salah salah satunya adalah *mobile forensics*. *Mobile forensics* merupakan cabang dari forensik digital yang berkaitan dengan pemulihan bukti digital atau data dari perangkat mobile di bawah forensik kondisi suara. Perangkat selular frase biasanya merujuk ke ponsel, namun juga dapat berhubungan dengan perangkat digital yang memiliki memori internal dan kemampuan komunikasi (Karpisek, 2015).

Dalam kegiatan *forensics* mempunyai tujuan yaitu salah satunya untuk membantu memulihkan, menganalisa, dan mempresentasikan materi/entitas berbasis digital atau elektronik sedemikian rupa sehingga dapat dipergunakan sebagai alat bukti yang sah di pengadilan. Misalnya, melalui Internet Forensik, bisa dilacak siapa yang mengirim email, kapan dikirim dan sang pengirim berada dimana, ataupun misalnya, dapat melacak siapa saja pengunjung suatu website lengkap dengan informasi IP Address, komputer yang dipakai serta berada di daerah/negara mana dan apa saja aktifitas yang dilakukan pada website tersebut. Dapat juga mempunyai tujuan untuk mendukung proses identifikasi alat bukti dalam waktu yang relatif cepat, agar dapat diperhitungkan perkiraan potensi dampak yang ditimbulkan akibat perilaku jahat yang dilakukan oleh kriminal terhadap korbannya, sekaligus mengungkapkan alasan dan motivitasi tindakan tersebut sambil mencari pihak-pihak terkait yang terlibat secara langsung maupun tidak langsung dengan perbuatan tidak menyenangkan dimaksud.

TEKNIK - TEKNIK *FORENSIC* WHATSAPP

Peneliti *mobile forensics* banyak menggunakan percobaan dengan berbagai metoda dalam mengumpulkan informasi *forensics* khususnya WhatsApp *forensics*, berukut adalah berbagai macam teknik–teknik dalam melakukan kegiantan mobile forensics yang telah dilakukan oleh para ahli *mobile forensics* di aplikasi WhatsApp. Terdapat lima buah teknik *forensic* WhatsApp yang dianalisia pada paper ini, namun dibagi berdasarkan cara kerjanya, yaitu menggunakan *Internet Protocol* dan *Live Memory*.

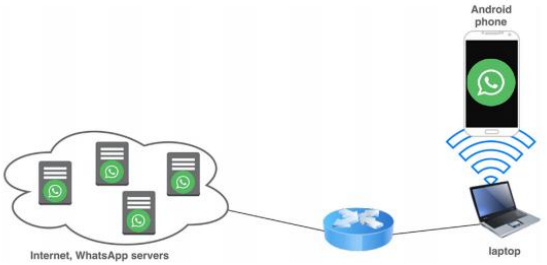
Menggunakan *Internet Protocol*

Dalam dunia *forensics* perlu diperhatikan beberapa hal penting agar kegiatan *forensics* dapat berberjalan dengan lancar tanpa adanya kendala dan dapat menghasilkan hasil yang diinginkan. Salah satu cara untuk mendapatkan suatu informasi dalam dunia *digital forensic* adalah menggunkan *internet protocol*.

Dengan menggukan *internet protocol* tentu saja bertujuan untuk mendapatkan informasi ketika para pengguna sedang melakukan komunikasi, bisa dikatakan suatu mobil smartpone disadap.

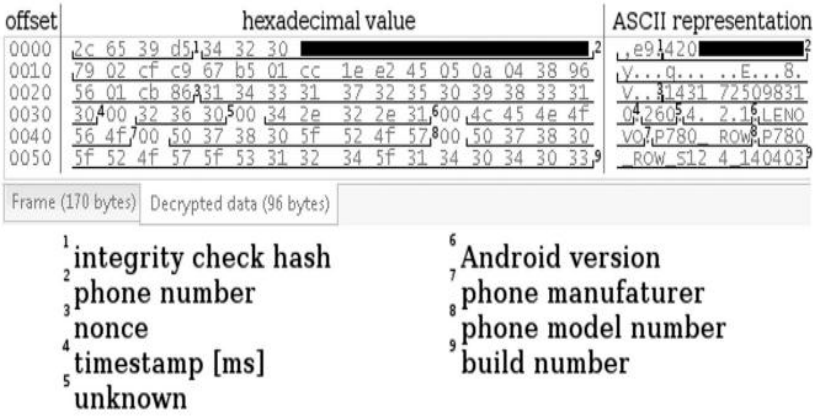
Gambar 2 menggambarkan skema yang telah dilakukan peneliti untuk mendapatkan informasi dari WhatsApp dengan menggunakan *internet protocol*.

Cara untuk mendapatkan informasi dari sebuah device adalah salah satunya dengen menggunakan internet protokol.



Gambar 2. Metodologi WhatsApp *Forensic* Dengan *Internet Protocol* (Marshall, 2008)

Pada penelitian yang dilakukan oleh Karpisek (2015) peneliti melakukan sebuah percobaan dengan mengambil informasi dari dua buah ponsel yang terinstal aplikasi WhatsApp, dan mengujinya dengan menggunakan IP protokol didapatkan beberapa informasi seperti, pesan yang dikirim, log panggilan, *timestamp*, dan sebagainya.

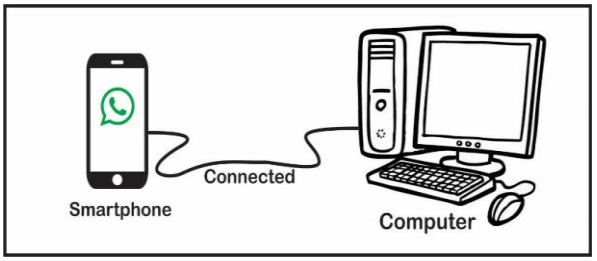


Gambar 3. Hasil dari WhatsApp *forensics* dengan menggunakan *tools* wireshark (Marshall, 2008)

Seperti yang terlihat pada Gambar 3, penggunaan *tools* Wireshark dapat menghasilkan berbagai informasi seperti nomor telepon WhatsApp, IP WhatsApp Server, WhatsApp codec audio (Opus) durasi WhatsApp panggilan, terminasi WhatsApp panggilan. Hanya dengan menggunakan sebuah *tool* yang telah dimodifikasi agar bisa dapat menangkap sebuah lalu lintas jaringan dari WhatsApp.

Menggunakan *memory* / *live memory*

Berbeda dengan metoda *forensics* menggunakan *internet protocol* dengan menggunakan *memory* / *live memory* tentu saja mempunyai tujuan dan kebutuhan yang berbeda ketika sedang melakukan kegiatan *forensics*. Dengan menggunakan metoda ini seorang ahli *forensics* dapat mendapatkan informasi *forensics* ketika suatu kejadian telah berakhir atau bisa dikatakan kita mencari informasi dengan bantuan *log* / *history data base* dari applikasi WhatsApp yang telah tersimpan dalam *smartphone*. Metoda ini banyak digunakan oleh berbagai peneliti karena metode ini sangat mudah dan hanya membutuhkan *log* / *history data base* yang tertulis didalam smartphone dengan mengekstrak *log* / *history data base* tersebut dengan bantuan *tools* yang telah tersedia. Gambar 4 menggambarkan metodologi WhatsApp *forensic* dengan menggunakan *live memory.*



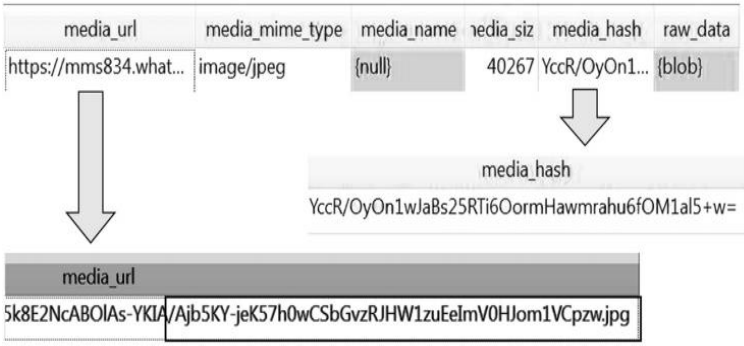
Gambar 4. Metodologi WhatsApp *Forensics* Menggunakan *Live Memory*

Pada penelitian yang dilakukan oleh Anglano (2014), diberikan deskripsi lengkap dari semua artefak yang dihasilkan oleh WhatsApp Messenger. Penelitian tersebut membahas decoding dan interpretasi masing-masing dari aplikasi WhatsApp. Tulisan ini menunjukkan bagaimana mereka dapat dikorelasikan bersama-sama untuk menyimpulkan berbagai jenis informasi yang tidak dapat diperoleh dengan mempertimbangkan masing-masing dari mereka dalam isolasi. Penelitian tersebut berhasil menganalisis daftar kontak dan kronologi pesan yang telah ditukar oleh pengguna layanan. Selainitu, penelitian ini menyimpulan informasi seperti kontak tertentu yang telah ditambahkan, untuk memulihkan kontak yang telah terhapus dan waktu ketika menghapus, untuk menentukan pesan yang telah terhapus, dan lain sebagainya (Anglano, 2014).

	key_id	key_remote_jid	key_from_me	timestamp	received_timestamp	data
1	1329115800-1	39348 @s.whatsapp.net	0	1329116347000	1329116349643	Message 1
2	1329116349-1	39348 @s.whatsapp.net	1	1329116423505	1329116423532	Reply 1
3	1329115800-2	39348 @s.whatsapp.net	0	1329116791000	1329116793357	Message 2
4	1329116349-2	39348 @s.whatsapp.net	1	1329116941607	1329116941626	Reply 2

Gambar 5. *Log / history database*, nomor telepon yang berwarna abu-abu untuk memastikan privasi pemilik (Anglano, 2014)

Gambar 6. *Multimedia file exchange: sender side* (Anglano, 2014)



Gambar 7. *Multimedia file exchange: recipient side* (Anglano, 2014)

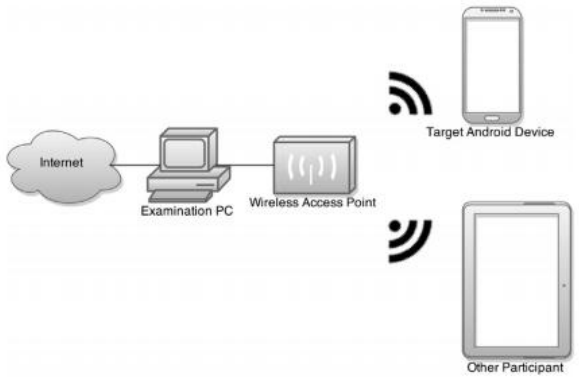
Log dari proses WhatsApp *forensic* dengan *live memory* dapat dilihat pada Gambar 5, Gambar 6, dan Gambar 7. Gambar 5 menggambarkan *history database*, Gambar 6 menggambarkan *history* pertukaran file dari sisi pengirim, dan Gambar 7 menggambarkan *history* pertukaran file dari sisi penerima.

Dapat dihasilkan dari file data base yang diekstrak mendapatkan berbagai informasi seperti chat log waktu, media url yang dikirim dan diterima. Dalam proses yang telah dilakukan ternyata hasil forensics dapat menghasilkan informasi pesan yang telah dihapus dari tampilan aplikasi WhatsApp di smartphone (Anglano, 2014)(Sahu, 2014).

Berbeda dengan para peneliti di atas yang telah dipaparkan dalam penelitian yang dilakukan oleh (Walnycky, 2015) adalah menerapkan

kedua metoda dalam penelitiannya. Pada penelitian tersebut dilakukan percobaan dengan berbagai macam media sosial massaging yang populer untuk android untuk saat ini dan lalulintas jaringan dari 20 aplikasi tersebut. Penulis mampu merekontruksi beberapa atau seluruh isi 16 pesan dari 20 aplikasi yang diiuji yang berdampaik buruk pada langkah langkah keamanan dan privasi yang diterapkan oleh aplikasi sehingga dapat ditafsirkan secara positif untuk tujuan pengumpulan bukti oleh praktisi *digital forensic* (Walnycky, 2015).

Gambar 8 menggambarkan *setup* perangkat untuk pengujian *menggunakan live memory*.



Gambar 8. Topologi Jaringan *untuk Analysis Experimental Setup* (Walnycky, 2015)

Kebanyakan dari hasil yang telah diperoleh dari kebanyakan kasus penulis mampu merekontruksi atau data inpect seperti *password*, screenshot diambil oleh aplikasi, gambar, video, audio dikirim, pesan yang dikirim, sketsa, gambar profil dan banyak lagi (Shortall, 2015).

ANALISA HASIL

Perkembangan *digital mobile* semakin lama semakin berkembang. Perkembangan aplikasi juga semakin lama semakin berkembang dengan penambahan fitur-fitur yang baru yang berguna untuk mempermudah user untuk berkomunikasi dan perkembangan tersebut juga meluputi perkembangan dari sistem keamanan untuk menjaga kerahasiaan atau privasi user. Dengan berkembangnya sistem keamanan yang semakin lama semakin berkembang maka semakin susah pula dalam melakukan kegiatan *forensics*. Oleh karena itu perlu adanya metode-metode yang berguna dalam melakukan kegiatan *forensics*.

Dalam kegiatan *survey* telah dikelompokkan motode-metode yang telah digunakan beberapa ahli *forensics* dalam *mobile* WhatsApp yaitu dengan metode *internet protocol* dan metode *live memory.* Adapun dalam metode tersebut cara menggunakannya akan berbeda tergantung dalam tujuan kegiatan *forensics* yang akan digunakan.

Tabel 1 berikut adalah hasil perbandingan dari berbagai peneliti *forensics* yang telah melakukan WhatsApp forensics.

Tabel 1. Perbandingan Teknik *WhatsApp Forensic*

Peneliti	Metoda	OS
F.Karpisek, I. Baggli, F. Breitinger.	*Internet protocol forensic*	*Android device*
Cosimo Anglano	*Hardisk / live Memory Smartphone*	*Android device*
Daniel Walnycky, Ibrahim Baggili, Andrew Marrington, Jason Moore, Frank Breitinger.	*Hardisk / live Memory Smartphone*	*Android device*
Shortall, A., & Azhar, M. A. H. Bin.	*Hardisk / Live Memory Smartphone*	*Android device, iOS device, dan Windows Phone device*
Sgaras, C., & Kechadi, M.	*Internet protocol forensic*	*iOS device*

KESIMPULAN

Kesimpulan yang dapat ditarik dari penelitian ini adalah sebagai berikut. Dalam kegatan *forensics* perlu adanya metode – motode yang digunakan untuk mendapatkan hasil yang dibutuhkan. Dari beberapa survey yang telah dilakukan mendapatkan berbagai macam hasil yang diperolah. untuk memperoleh data yang dibuthkan ketika dalam pengumpulan informasi ketika dalam keadaan sedang terjadinya sebuah komunikasi maka akan tejadi suatu lalulintas jaringan metoda yang sangat tepat adalah menggunakan metoda *internet protocols* karena sangat memungkinlkan mendapatkan informasi yang dibutuhkan menggunakan tools yang telah tersedia. Sebaliknya ketika komunikasi sudah selesai dan adanya barang bukti berupa *smartphone* maka metode yang tepat adalah menggunakan metoda live memory smartphone dengan mengambil dari histori yang telah tercatat di database *smartphone* kemudian dapat mengekstraknya menjadi sebuah atau beberapa informasi yang dibutuhkan.

Metoda yang dipakai oleh peneliti memang dapat menghasilkan data yang dibutuhkan seperti log timestamps, foto yang dikirim, log panggilan, pesan yang dikirim dan diterima. Tetapi dalam memperoleh suatu informasi para peneliti belum dapat medefinisikan metode enkripsi yang digunakan dalam pesan WhatsApp tersebut.

DAFTAR PUSTAKA

Anglano, C. Forensic analysis of WhatsApp Messenger on Android smartphones. *Digital Investigation Journal*. 2014; 11 (3): 1–13. http://doi.org/10.1016 /j.diin.2014.04.003

Casey, E. *Handbook of Digital Forensics and Investigation*. Acedemic Press Pubblication. USA. 2010.

Marshall, A. M. Digital Forensics : Digital Evidence in Criminal Investigation. John Wiley and Sons, Ltd., USA. 2008.

Karpisek, F., Baggili, I., & Breitinger, F. WhatsApp network forensics : Decryption and understanding the WhatsApp call signaling messages. *Digital Investigation*. 2015; 15: 110-118. http://doi.org/10.1016/j.diin.2015.09.002

Sahu, S. An Analysis of WhatsApp Forensics in Android Smartphones. *International Journal of Engineering Research*. 2014; 3 (5): 349–350.

Sgaras, C., & Kechadi, M. Forensic Acquisition and Analysis of Tango VoIP. *International Journal of Innovations in Engineering and Management.* 2014; 4 (2): ISSN: 2319-3344

Shortall, A., & Azhar, M. A. H. Bin. Forensic Acquisitions of WhatsApp Data on Popular Mobile Platforms. *International Conference on Emerging Security Technologies (EST)*, 2015: 13–17. http://doi.org/10.1109/EST.2015.16

Walnycky, D., Baggili, I., Marrington, A., Moore, J., & Breitinger, F. Network and device forensic analysis of Android social-messaging applications. Digital *Investigation*. 2015; 14: S77–S84. http://doi.org/10.1016/j.diin.2015.05.009