ANALISIS FORENSIK DIGITAL APLIKASI *BEETALK* UNTUK PENANGANAN *CYBERCRIME* MENGGUNAKAN METODE NIST

Muhammad Irwan Syahib [(1)], Imam Riadi [(2)], Rusydi Umar [(3)]
[(1)(3)] Program Studi Teknik Informatika, Universitas Ahmad Dahlan
[(2)] Program Studi Sistem Informasi, Universitas Ahmad Dahlan
Jl. Prof. Soepono SH,Warungboto, Umbulharjo, Yogyakarta, Indonesia
e-mail : muhammadirwansyahib13@gmail.com [(1)], imam.riadi@is.uad.ac.id [(2)], rusydi@mti.uad.ac.id [(3)]

Abstrak
Perkembangan teknologi smartphone tumbuh semakin pesat, kemajuan teknologi ini menghasilkan berbagai aplikasi instant messenger di smartphone yang berdampak pada banyaknya pengguna media sosial yang dapat memudahkan untuk berinteraksi antar pengguna. Salah satu aplikasi instan messanger tersebut adalah aplikasi Beetalk. Semakin banyaknya fitur yang diberikan Beetalk maka dapat disalahgunakan oleh oknum-oknum tertentu untuk tujuan melakukan tindakan kriminal, banyak tindak kriminal seperti pembunuhan berencana, pornografi, penipuan, perjudian, perdagangan narkoba, dan bahkan kejahatan terorisme. Jika smartphone digunakan sebagai barang bukti dalam kasus pidana, maka sebuah tindakan analisis mobile forensik dapat dilakukan sehingga mendapatkan barang bukti digital seperti riwayat percakapan, gambar, dokumen, dan video. Bukti digital tersebut diharapkan dapat membantu pihak berwajib dalam proses penegakan hukum untuk mengungkap kejahatan digital dan bertanggung jawab untuk proses hukum di pengadilan.

***Kata Kunci** : Teknologi, Smartphone, Forensic, Messenger, Beetalk.*

1. PENDAHULUAN

Perkembangan teknologi dari waktu ke waktu sangat pesat, salah satunya perkembangan smartphone yang selalu mengalami perkembangan dari segi sistem operasi, fitur, spesifikasi, dan aplikasi. Teknologi yang semakin canggih menjadi bagian yang tidak bisa lepas dari kehidupan masyarakat, tidak hanya melakukan kegiatan-kegiatan positif namun kegiatan-kegiatan negatif.

Perkembangan teknologi smartphone ini juga diiringi dengan banyaknya pengguna media sosial yang dapat memudahkan untuk berinteraksi antar pengguna. Jumlah pengguna aktif media sosial diseluruh dunia mencapai 2,31 Triliun, yang artinya setara dengan 31% dari total populasi penduduk dunia. Pada Januari 2016 pengguna media sosial yang mengakses smartphone sebanyak 1,97 Triliun atau setara dengan 27% populasi penduduk dunia (Wisnu Ari Mukti:2017).

Perkembangan smartphone dan media sosial saat ini banyak disalahgunakan untuk melakukan tindak kejahatan (cybercrime) seperti perdagangan manusia, cyberbully, penipuan, pemerasan, penyebaran hoax dan lainya. Pada 2016 kejahatan siber yang ditangani Polri sebanyak 4.931 kasus, sementara pada 2017 meningkat menjadi 5.061 kasus. Pada tahun 2016 penyelesaian kasus kejahatan siber sebanyak 1.119 kasus, dan tahun 2017 hanya 1.369 kasus yang diselesaikan. Kasus kejahatan siber yang menonjol adalah ujaran kebencian yaitu sebanyak 1.829 kasus, tetapi pada 2017 meningkat drastis menjadi 3.325 kasus. Kasus kejahatan pada digital forensik sangat rentan pada aplikasi apa saja, selama aplikasi tersebut menyediakan menyediakan fitur untuk mengirim pesan taks, gambar, dan video (Ambaranie Nadia:2017).

Beetalk memiliki syarat untuk dikatakan aplikasi yang rentan kejahatan siber, dimana beetalk memiliki berbagai macam fitur seperti, mengirim pesan taks, gambar, dan pesan suara. Untuk saat ini, sudah 50 juta kali aplikasi beetalk di unduh melalui playstore. Kasus-kasus kejahatan menggunakan beetalk sangat banyak di beritakan melalui media nasional maupun swasta, media cetak maupun online. Seperti kasus cybercrime penguna beetalk di Apartemen Kalibata City. dalam pengakuanya tersangka menggunakan aplikasi Beetalk untuk menawarkan perempuan dengan menulis OPEN BO/Booking Out atau menerima pesanan yang dapat memuaskan seksual (Clara Mari : 2018), Pada kasus Prostitusi Online di Manado, Pelaku menawarkan perempuan melalui Aplikasi BeeTalk. dalam pengakuanya tersangka juga menggunakan aplikasi Beetalk untuk menawarkan prostitusi online (Seruni Cyber : 2018).

Penelitian ini akan menganalisis pencarian bukti digital pada aplikasi Beetalk. Penelitian ini diharapkan dapat membantu pihak yang berwajib menemukan bukti forensik untuk menyelesaikan kasus cybercrime yang terjadi pada media sosial.

2. TINJAUAN PUSTAKA

Penelitian terdahulu yang relevan dengan penelitian ini dilakukan oleh Wisnu Ari Mukti, dkk (2017) yang berjudul Analisa dan Perbandingan Bukti Forensik Aplikasi Media Sosial Facebook dan Twitter Pada Smartphone Android. Penelitian ini menggunakan metode simulasi untuk mendapatkan bukti digital pada facebook dan twitter, tahapan metode simulasi yang digunakan adalah Problem Simulation, Conceptual Model, Input/Output Data, Modelling, Simulation, Verification and Validation, Experimentation, dan Output Analysis. Penelitian ini menggunakan tools Recovery file untuk mengembalikan data yang sebelumnya telah dihapus untuk menghilangkan bukti forensik. Bukti forensik yang ditemukan pada penelitian ini 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.

Ikhwan Anshori, dkk (2018) yang berjudul Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist. Metode yang digunakan untuk melakukan analisis terhadap bukti digital atau tahapan untuk mendapatkan informasi dari bukti digital pada penelitian ini adalah metode NIST (National Institute of Standards Technology). Sedangkan tools yang digunakan adalah Oxygen Forensic.

Muhamad Caesar Febriansyah Putra, dkk (2018) yang berjudul Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute Of Justice (NIJ). Proses akuisisi data dalam penelitian ini menggunakan metode National Institute Of Justice (NIJ) yang merekomendasikan beberapa macam tahapan seperti persiapan, koleksi, pemeriksaan, analisis dan pelaporan. Proses akuisisi yang dilakukan menggunakan tolls OXYGEN forensik supaya mendapatkan hasil sesuai dengan yang diinginkan yakni barang bukti digital berupa gambar/foto dan percakapan/chatting dari sosial media Instagram yang terpasang pada smartphone tersebut.

Imam Mahfudl Nasrulloh, dkk (2018) yang berjudul Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute Of Justice (NIJ). penelitian ini mengadaptasi dan mengimplementasikan metode analisa forensik dari National Institute of Justice (NIJ). Metode ini untuk menjelaskan bagaimana tahapan penelitian yang akan dilakukan sehingga dapat diketahui alur dan langkah-langkah penelitian secara sistematis sehingga dapat dijadikan pedoman dalam menyelesaikan permasalahan yang ada. Berdasarkan hasil dari penelitian yang telah dilakukan pada implementasi salah satu software pembeku drive yaitu Shadow Defender yang dapat membekukan suatu drive SSD (frozen solid state drive) dan terbukti berpengaruh terhadap praktik eksaminasi dan analisa forensik terhadap didapatkannya buktibukti digital. Tidak semua file dapat direstorasi dengan baik karena struktur file dan data sudah rusak, serta catatan pengguna komputer (recent activity) dan sejarah internet (history internet) tercatat ketika fitur pembeku drive diaktifkan.

Roni Anggara Putra, dkk (2017) yang berjudul Forensik Digital Pada Smartwatch Berbasis Android, penelitian ini menggunakan 2 tools yaitu tool mobiledit forensik pada windows dan tool forensik metasploit pada kali linux. Dari hasil akusisi berdasarkan 2 tools tersebut,maka didapat keberhasilan hampir 100% dalam megumpulkan data-data yang ada berupa sms, data kontak, dan data panggilan yang ada di smartwatch.

Ruuhwan, dkk (2016) yang berjudul Penerapan Integrated Digital Forensic Investigation Framework v2 (IDFIF) pada Proses Investigasi Smartphone, tools yang digunakan dalam penelitian ini adalah Mobileedit Forensic. metode penelitian yang digunakan terdapat beberapa langkah diantaranya *Research problem* merupakan langkah awal yang dilakukan untuk memperoleh dan menentukan topik penelitian yang akan diteliti lebih lanjut. *Literature review* diharapkan mampu menggali seluruh informasi yang terkait dengan permasalahan yang akan diteliti. Dan yang terakhir *Case Study*, merupakan proses penerapan IDFIF v2 terhadap proses investigasi smartphone. Hasil yang diharapkan dalam penelitian ini dapat menjadi standar dalam proses investigasi barang bukti digital di Indonesia sehingga nantinya tidak akan ada perbedaan hasil investigasi dalam proses penanganan barang bukti yang telah didapatkan karena framework tersebut memiliki fleksibilitas dalam menangani barang bukti digital yang ditemukan TKP.

Zulkarnaen Akbar, dkk (2016) yang berjudul Whatsapp Forensics Pada Android Smartphone: A Survey, Metodologi penelitian yang digunakan adalah dengan membandingkan jurnal-jurnal terkait yang melakukan penelitian forensics pada WhatsApp. Teknik akusisi yang dilakukan menggunakan Teknik–teknik 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. Kesimpuln yang didapat adalah 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.

Hafid Wijaya, dkk (2017) yang berjudul Analisis Forensik Digital Aplikasi Telegram Pada Smartphone Berbasis Android. dalam penelitiannya, pada penelitian ini, proses pengangkatan barang bukti digital dari aplikasi Telegram dengan menggunakan MOBILedit Forensic Tool 7.0 dan menggunakan metode Mobile Forensic yang dibuat oleh National Institute of Standard and Technology (NIST).

Ammar Fauzan, dkk (2016) yang berjudul Analisis Forensik Digital Pada Line Messenger Untuk Penanganan Cybercrime. dalam penelitiannya Amar Fauzan melakukan penelitian dengan beberapa langkah, yakni preservation, collection, examination, dan pada akhirnya adalah analysis. Analisis yang dihasilkan merupakan gambaran dari semua proses investigasi. Proses investigasi dilakukan pada perangkat pelaku. Proses collection atau pengumpulan data diawali dengan rooting menggunakan tool Zenfone RootKit untuk mempermudah pengangkatan data-data yang ada di dalam perangkat Android. Kemudian perangkat Android yang telah di-root, direcovery menggunakan tool Kamas Lite atau AFLogical. Diharapkan data-data yang direcovery dapat menunjukan file percakapan pada aplikasi Line yang berupa teks maupun gambar.

Rauhulloh Ayatulloh Khomeini Noor Bintang, dkk (2018) yang berjudul Perancangan Perbandingan Live Forensics Pada Keamanan Media Sosial Instagram, Facebook Dan Twitter Di Windows 10. Penelitian ini menggunakan The U.S National Institute of Justice (NIJ) sebagai metode, metode ini memiliki beberapa tahapan (Collection, Examinition, Analysis dan Reporting) berikut dijalankan menggunakan perangkat lunak (tools FTK Imager) sebagai bahan pendukung untuk mengetahui keamanan masing-masing pada media sosial (facebook, twitter, dan instagram). Untuk meyakinkan bahwa akun media sosial (facebook, twitter dan instagram) menjadi nilai yang merepresentasikan string asli atau akun asli lakukan dengan cloning data dan Hashing data fungsi. Berdasarkan hasil dari tahapan-tahapan metode yang dilakukan, proses analisis mengenai data pada media sosial (facebook, twitter, dan facebook) berupa barang bukti data yang valid (asli atau palsu).

Mustafa, dkk (2018) yang berjudul Rancangan Investigasi Forensik Email Dengan Metode National Institute Of Standards And Technology (Nist). Tools yang digunakan dalam penelitian ini adalah Aid4Mail Forensic. Penelitian ini menggunakan National Institute of Standards and Technology (NIST) dengan pendekatan Header Analysis menghasilkan pola pemalsuan email yang berupa subjek, alamat dan tanggal email yang palsu. Selain itu investigasi email forensik ini juga menghasilkan Alamat email pengirim email palsu, memeriksa protokol inisiasi pesan (HTTP, SMTP), memeriksa ID pesan, dan alamat IP pengirim.

Majeed Raji, dkk (2018) yang berjudul Analyzing Data from an Android Smartphone while Comparing between Two Forensic Tools. Penelitian ini difokuskan untuk menganalisis data dari telepon Android sambil membandingkan dua alat forensik. Perbandingan akan dilakukan dengan menggunakan alat forensik sumber terbuka dan komersial alat. Sedangkan metode yang digunakan adalah Institut Nasional standar dan Teknologi (NIST).

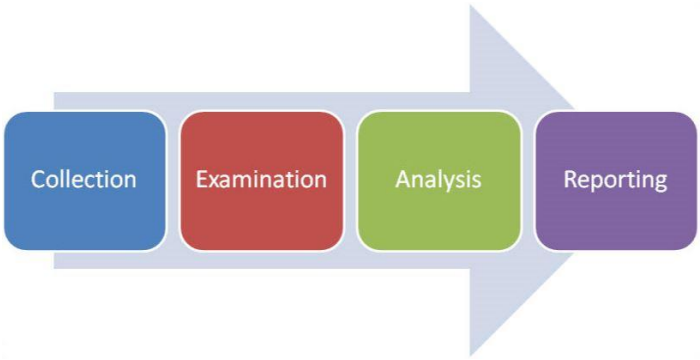
Khushboo Rathi, dkk (2018) yang berjudul Forensic Analysis of Encrypted Instant Messaging Applications on Android. penelitian ini bertujuan untuk menganalisis penyimpanan data lokasi aplikasi IM yang berbeda sering digunakan di perangkat Android. Studi dilakukan dengan menggunakan ponsel Android dengan berbagai versi Android OS. Tools yang digunakan dalam penelitian ini adalah Universal ADB Driver, WhatsApp KeyDB Extractor, WhatsApp Viewer Dan SQLiteSpy.

Ming Sang Chang, dkk (2018) yang berjudul Forensic Analysis of LINE Messenger on Android. Penelitian menggunakan mesin virtual dengan instalasi standar Windows OS 10. BlueStacks aplikasi diinstal pada Windows 10. Kemudian kita root BlueStacks. Pemain App BlueStacks dirancang untuk memungkinkan aplikasi Android untuk dijalankan pada PC Windows dan Macintosh komputer. Penelitian ini menunjukkan bahwa penggunaan garis untuk Android meninggalkan materi berdasar atas kenyataan yang berguna di volatile memori dan memori non-volatile. Dalam tulisan ini, mereka mempelajari dan laporan Forensik Analisis sekejap pesan yaitu baris Sistem Android. Karena keterbatasan percobaan biaya mereka menggunakan BlueStacks untuk meniru Android OS sistem. Implementasi dapat bervariasi antara dev akhir yang berbeda.

Hao Zhang, dkk (2018) yang berjudul Digital Forensic Analysis of Instant Messaging Applications on Android Smartphones. Dalam penelitian ini mereka mengikuti metode android forensik prosedur yang ditulis oleh Hoog, dengan langkah-langkah Identification, Preservation, Analysis, dan Presentation. Kesimpulan dari hasil penelitian ini adalah Metode enkripsi untuk kedua aliran data online chat dan artefak database lokal dibahas dan diringkas. Dalam tabel II, mereka merangkum temuan mengenai mode chatting yang berbeda dan status enkripsi sesuai artefak untuk setiap aplikasi. Hal ini dapat dilihat dari tabel yang Facebook messenger menggunakan mode privat untuk melindungi pesan Privasi, sedangkan garis dan WhatsApp menggunakan E2EE untuk mengenkripsi isi online chat. Sangat rentan untuk serangan dengan menangkap Paket menggunakan Wireshark jika tidak ada enkripsi end-to-end bekerja selama kegiatan chatting.

3. METODE PENELITIAN

Metode dalam penelitian ini menggunakan National Institute of Standard and Technology (NIST). Metode ini terdiri dari beberapa tahapan diantaranya yaitu: Pengumpulan (Collection), Pengujian (Examination), Analisa (Analysis), Laporan (Reporting), seperti yang terdapat pada gambar 1.1.



Gambar 1.1 Tahapan Metode NIST

Collection
Tahap ini merupakan proses identifikasi, pelabelan, perekaman, dan pengambilan data dari sumber data yang relevan dengan mengikuti prosedur penjagaan integritas data.

Examination
Merupakan tahap pemrosesan data yang dikumpulkan secara digital forensik menggunakan kombinasi dari berbagai skenario, baik otomatis maupun manual, serta menilai dan mengeluarkan data sesuai kebutuhan dengan tetap mempertahankan integritas data.

Analysis
Melakukan analisis pada hasil pemeriksaan dengan menggunakan metode dibenarkan secara teknik dan hukum untuk mendapatkan informasi yang berguna dan menjawab pertanyaan-pertanyaan yang menjadi pendorong untuk melakukan pengumpulan dan pemeriksaan.

Reporting
Melaporkan hasil analisis yang meliputi penggambaran tindakan yang dilakukan, penjelasan mengenai alat dan prosedur yang dipilih, penentuan tindakan lain yang perlu dilakukan (misalnya, pemeriksaan forensik dari sumber data tambahan, mengamankan celah yang teridentifikasi, atau meningkatkan control keamanan yang ada), dan memberikan rekomendasi untuk perbaikan kebijakan, prosedur, alat, dan aspek lain dari proses digital forensik.

Alat dan bahan yang digunaka dalam penelitian ini dapat dilihat pada tabel 1.1.

Tabel 1.1 alat dan bahan yang digunakan

NO	Alat Dan Bahan	Keterangan
1.	Laptop	Lenovo G40, Core i3, OS Windows 64bit.
2.	HP	Samsung GT-S5282, Samsung J7 2015
3.	Kingroot	Aplikasi Android digunakan sebagai alat bantu proses rooting
4.	OXYGEN Forensik	Aplikasi yang diigunakan untuk mengangkat bukti digital pada smartphone.
5.	MOBILedit Forensik	Aplikasi yang diigunakan untuk mengangkat bukti digital pada smartphone.
6.	Beetalk	Aplikasi instan messenger yang menjadi objek penelitian

4. HASIL DAN PEMBAHASAN

Penelitian ini diawali dengan membuat akun Beetalk pada dua handphone android yang sudah disiapkan, Selanjutnya melakukan skenario percakapan antara Akun A dan Akun B tentang prostitusi online melalui handphone android tersebut.

Langkah Selanjutnya melakukan proses rooting pada salah satu smartphone Android yang akan akusisi, proses rooting ini menggunakan aplikasi KingRoot, aplikasi ini adalah aplikasi root android yang digunakan untuk membantu memperoleh akses rooting.

Selanjutnya melakukan pemilihan tools untuk mengambil data dari akun Beetalk. Pertama adalah melakukan proses backup data dalam perangkat smartphone agar tidak corrupted. Tools yang digunakan untuk melakukan backup adalah MOBILedit Forensic. Setelaah itu melakukan Examination, tindakan ini bertujuan

untuk menampilkan data yang telah di backup tadi untuk melihat bukti-bukti apasaja yang ada di dalam perangkat tersebut. Tools yang akan digunakan untuk tahap Examination adalah OXYGEN Forensik, Alpikasi tersebut adalah aplikasi berbasis windows yang dapat digunakan untuk mengakusisi bukti digital pada smartphone Android yang telah di backup.

5. KESIMPULAN

Untuk hasil yang diharapkan dari penelitian ini adalah proses analisis bisa berjalan dengan baik dan mendapatkan barang bukti digital dari Beetalk pada smartphone Android yang digunakan sebagai objek penelitian selanjutnya.

DAFTAR PUSTAKA

Ammar. F., Imam. R, & Abdul. F, 2016. Analisis Forensik Digital Pada Line Messenger Untuk Penanganan Cybercrime, Prosiding Annual Research Seminar 2016 , Pp. 159-163.

Ambaranie. N.K.M. 2017. Ini Hasil Kerja Polri Perangi Kejahatan Siber Sepanjang 2017. https://nasional.kompas.com/read/2017/12/29/17233911/ini-hasil-kerja-polri perangi-kejahatan-siber-sepanjang-2017, Diakses 16 Oktober 2018

Clara M.T.D.H. 2018. Prostitusi di Apartemen Kalibata City Pakai Aplikasi BeeTalk. https://metro.tempo.co/read/1115067/prostitusi-di-apartemen-kalibata-city-pakai-aplikasi beetalk/full&view=ok. Diakses 20 November 2018.

Hafid. W., Imam. R, & Sunardi, 2017. Analisis Forensik Digital Aplikasi Telegram Pada Smartphone Berbasis Android, Prosiding Seminar Nasional Teknologi Informasi dan Komunikasi 2017, Pp. 95-98.

Hao. Z., Lei. C. & Qingzhong. L. 2018. Digital Forensic Analysis of Instant Messaging Applications on Android Smartphones. Jurnal ICNC 5(3), pp. 647-651.

Imam. M.N., Imam. R. & Rusydi, U. 2018. Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute Of Justice (Nij). Electronics, Informatics, and Vocational Education. 3(1), pp. 71-81.

Ikhwan. A., Anton, Y. & Imam. R. 2018. Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist. IT Journal Research and Development 3(1), pp. 13-20.

Khushboo. R, & Umit. K. 2018. Forensic Analysis of Encrypted Instant Messaging Applications on Android . Jurnal IEEE 7(3), pp. 254-259.

Majeed. R, B, N. & Mudrik, A. 2018. Analyzing Data from an Android Smartphone while Comparing between Two Forensic Tools. Jurnal IEEE 3(3), pp. 2-7.

Ming. S.C. & Chih. Y.C. 2016. Forensic Analysis of LINE Messenger on Android. Jurnal Journal of Computers 19(1), pp. 11-19.

Muhamad. C.F.P., Imam. R. & Anton. Y. 2018. Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute Of Justice (NIJ). Jurnal Teknik Informatika dan Sistem Informasi 4(2), pp. 219-226.

Mustafa, Rusdy. Imam. R. & Rusdy. U, 2018. Rancangan Investigasi Forensik Email Dengan Metode National Institute Of Standards And Technology (Nist), Prosiding SNST ke-9 2018, Pp. 122-124.

Rauhulloh. A.K.N.B., Rusdy. U, & Anton. Y, 2018. Perancangan Perbandingan Live Forensics Pada Keamanan Media Sosial Instagram, Facebook Dan Twitter Di Windows 10, Prosiding SNST ke-9 2018, Pp. 125-127.

Roni. A.P., Abdul. F. & Imam. R. 2017. Forensik Digital Pada Smartwatch Berbasis Android . JURTI 1(1), pp. 41-46.

Ruuhwan., Imam. R. & Yudi. P, 2017. Penerapan Integrated Digital Forensic Investigation Framework v2 (IDFIF) pada Proses Investigasi Smartphone. Jurnal Edukasi dan Penelitian Informatika 2(1), pp. 1-9.

Seruni c. 2018. Prostitusi Online di Manado, Tawarkan 7 Cewek via Aplikasi BeeTalk, Ini Tarifnya. https://seruindonesia.com/2018/02/25/prostitusi-online-di-manado-tawarkan-7-cewek-via-aplikasi-beetalk-ini-tarifnya/. Diakses 20 November 2018.

Wisnu. A.M., Siti. U.M. & Dewi. K. 2017. Analisa Dan Perbandingan Bukti Forensik Aplikasi Media Sosial Facebook Dan Twitter Pada Smartphone Android. Jurnal Teknik Informatika 10(1), pp. 74-83.

Zulkarnaen. A., Hayden. W. & Rami. J.H. 2016. Whatsapp Forensics Pada Android Smartphone: A Survey. Jurnal SINERGI 20(3), pp. 207-211.