KLASIFIKASI POLA DATA FORENSIK WHATSAPP PADA *SMARTPHONE* ANDROID MENGGUNAKAN METODE *SUPPORT VECTOR MACHINE* (SVM)

TESIS

OLEH :
UBAIDILLAH
09042681620001

PROGRAM STUDI MAGISTER TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2018

KLASIFIKASI POLA DATA FORENSIK WHATSAPP PADA *SMARTPHONE* ANDROID MENGGUNAKAN METODE *SUPPORT VECTOR MACHINE* (SVM)

Diajukan untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Magister

OLEH :
UBAIDILLAH
09042681620001

PROGRAM STUDI MAGISTER TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2018

LEMBAR PENGESAHAN

KLASIFIKASI POLA DATA FORENSIK WHATSAPP PADA *SMARTPHONE* ANDROID MENGGUNAKAN METODE *SUPPORT VECTOR MACHINE* (SVM)

TESIS

Diajukan untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Magister

OLEH :
UBAIDILLAH
09042681620001

Palembang, Desember 2018

Pembimbing

Deris Stiawan, M.T., Ph.D.
NIP. 197806172006041002

Mengetahui,
Koordinator Program Studi
Magister Teknik Informatika

Dr. Ir. Sukemi, M.T.
NIP. 196612032006041001

HALAMAN PERSETUJUAN

Pada hari Jum'at tanggal 28 Desember 2018 telah dilaksanakan ujian sidang Tesis II oleh Magister Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.

N a m a	:	Ubaidillah
N I M	:	09042681620001
Judul	:	Klasifikasi Pola Data Forensik Whatsapp pada *Smartphone* Android Menggunakan Metode *Support Vector Machine* (SVM)

1. Pembimbing

   Deris Stiawan, M.T., Ph.D.
   NIP. 197806172006041002 .....

2. Penguji I

   Prof. Dr. Ir. Siti Nurmaini, M.T.
   NIP. 196908021994012001 .....

3. Penguji II

   Syamsuryadi, M.Kom., Ph.D.
   NIP. 197102041997021003 .....

Mengetahui,
Koordinator Program Studi
Magister Teknik Informatika

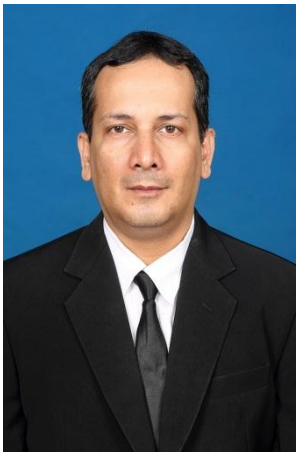
Dr. Ir. Sukemi, M.T.
NIP. 196612032006041001

LEMBAR PERNYATAAN

Nama	:	Ubaidillah
NIM	:	09042681620001
Program Studi	:	Magister Teknik Informatika
Judul Tesis	:	Klasifikasi Pola Data Forensik Whatsapp pada *Smartphone* Android Menggunakan Metode *Support Vector Machine* (SVM)

Hasil Pengecekan Software *iThenticate / Turnitin* : 15%

Menyatakan tesis saya merupakan hasil karya sendiri dan bukan penjiplakan / plagiat. Apabila ditemukan unsur penjiplakan / plagiat dalam laporan Tesis ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku. Demikian, pernyataan ini saya buat dengan sebenarnya dan tidak ada paksaan dari siapapun.



Palembang, 27 Desember 2018

Ubaidillah
NIM. 09042681620001

KATA PENGANTAR

Segala puji dan syukur penulis panjatkan kehadirat Allah SWT yang telah melimpahkan segala rahmat-Nya sehingga penulis dapat menyelesaikan tesis dengan judul "Klasifikasi Pola Data Forensik WhatsApp pada *Smartphone* Android Menggunakan Metode *Support Vector Machine* (SVM)" guna memenuhi sebagian persyaratan untuk memperoleh gelar Magister Komputer pada Magister Teknik Informatika Universitas Sriwijaya.

Pada kesempatan ini, penulis ingin menyampaikan ucapan terima kasih yang tak terhingga kepada pihak-pihak yang telah memberikan dukungan, bimbingan dan motivasi kepada penulis untuk menyelesaikan tesis ini, yaitu kepada:

1. Bapak Jaidan Jauhari, S.Pd., M.T., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
2. Bapak Dr. Ir. Sukemi, M.T., sebagai Koordinator Program Studi Magister Teknik Informatika yang telah memberikan dukungan kepada kami.
3. Bapak Deris Stiawan, M.T., Ph.D., sebagai pembimbing tesis yang telah meluangkan waktu untuk memberikan saran dan kritik dalam penyusunan tesis ini.
4. Ibu Prof. Dr. Ir. Siti Nurmaini, M.T., selaku penguji pertama.
5. Bapak Syamsuryadi, M.Kom., Ph.D., selaku penguji kedua.
6. Dosen-dosen Magister Teknik Informatika Universitas Sriwijaya yang telah memberikan ilmunya.
7. Ayahanda Muhdi Shahab (Alm), ibunda Nur Satri, ayah mertua Hasan Alwi (Alm), ibu mertua Raudoh serta istriku tercinta Sy. Patemah dan anak-anakku tersayang Sabrina Zafirah, Farhana, Ali Zainal Abidin, Aisyah Humairah dan Muhammad Umar yang selalu memberikan doa dan dukungan sehingga tesis ini dapat terselesaikan.

8. Kepada seluruh teman-teman dan para staf Magister Teknik Informatika Universitas Sriwijaya yang tidak bisa saya sebutkan satu per satu.

Penulis menyadari bahwa tesis ini masih banyak kekurangannya dan jauh dari kata sempurna. Semoga tesis ini dapat bermanfaat tidak hanya bagi penulis tetapi juga bagi para pembaca.

Palembang, 31 Desember 2018

Penulis

CLASSIFICATION OF WHATSAPP FORENSIC DATA PATTERN ON ANDROID SMARTPHONE USING SUPPORT VECTOR MACHINE

Ubaidillah

Abstract

WhatsApp have reached more than a billion users, making WhatsApp one of the most widely used private mobile messaging applications. Beside as tool of communication, WhatsApp messages can also be used as digital evidence to assist the criminal investigation process. Artifacts left on WhatsApp messages are analyzed forensically or correlated one by one. In the conventional method, the analysis and classification of forensic data is done manually. Therefore, in this study will use machine learning so that the investigation process can be carried out effectively and efficiently. One machine learning method that is reliable in classification and minimizing errors is Support Vector Machine (SVM). This study uses four types of kernerls namely: RBF, Linear, Sigmoid and Polynomial. Evaluation of the results of the classification of the best parameter values was obtained at a data ratio of 80%: 20%, iterations = 200, C = 1 and ε = 0.1. The results showed that the Linear SVM kernel had the highest accuracy value of 98.3% and the lowest accuracy value in the Polynomial kernel was 89.6%. In addition, the AUC value was 99.5%, which was statistically very good.

Keywords: Classification, WhatsApp, Mobile Forensic, Android, Smartphone, Support Vector Machine

KLASIFIKASI POLA DATA FORENSIK WHATSAPP PADA *SMARTPHONE* ANDROID MENGGUNAKAN METODE *SUPPORT VECTOR MACHINE* (SVM)

Ubaidillah

Abstrak

Pengguna WhatsApp telah mencapai satu milyar lebih, sehingga menjadikan WhatsApp sebagai salah satu aplikasi pesan seluler pribadi yang paling banyak digunakan. Selain sebagai sarana komunikasi, pesan WhatsApp juga dapat dijadikan sebagai bukti digital untuk membantu proses investigasi kriminal. Artefak yang tertinggal pada pesan WhatsApp dianalisis secara forensik atau dikorelasikan satu per satu. Pada metode konvensional, analisis dan pengelompokan data forensik dilakukan secara manual. Oleh karena itu, dalam penelitian ini akan menggunakan komputasi cerdas agar proses investigasi dapat dilakukan secara efektif dan efisien. Salah satu metode komputasi cerdas yang andal dalam pengelompokan dan meminimalisir error adalah *Support Vector Machine* (SVM). Penelitian ini menggunakan empat jenis kernel, yaitu RBF, Linear, Sigmoid dan Polynomial. Evaluasi hasil klasifikasi nilai parameter terbaik didapatkan pada rasio data 80%:20%, iterasi=200, C=1 dan $\varepsilon = 0.1$. Hasil penelitian menunjukan bahwa kernel SVM Linear mempunyai nilai akurasi tertinggi yaitu 98,3% dan nilai akurasi terendah pada kernel Polynomial yaitu 89,6%. Selain itu juga diperoleh nilai AUC sebesar 99,5%, dimana secara statistik nilai yang didapat tergolong sangat baik.

Kata Kunci: Klasifikasi, WhatsApp, *Mobile Forensic*, Android, *Smartphone*, *Support Vector Machine*

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

BAB I. PENDAHULUAN

1.1. Latar Belakang

WhatsApp telah dibeli facebook tahun 2014 seharga US$19 milyar (Nicole Arce, 2015). Sekarang sudah lebih dari satu milyar pengguna di seluruh dunia menggunakan WhatsApp, menjadikan WhatsApp sebagai salah satu aplikasi pesan seluler pribadi yang paling banyak digunakan, baik sebagai pengiriman teks maupun konten gratis (yaitu audio, video, gambar, lokasi dan kontak). WhatsApp baru mengeluarkan fitur fitur *voice call* pada 05 Maret 2015 dan fitur *video call* pada versi 2.16.318.

WhatsApp dijadikan *platfom* banyak komunitas untuk sarana berkomunikasi (termasuk berbagai macam konten yang ada di dalamnya). Pesan singkat WhatsApp merupakan salah satu komponen penting penyajian bukti kasus persidangan (Walnycky, dkk, 2015). Berbagai persidangan dan investigasi kriminal terbantukan dengan bukti digital pesan WhatsApp.

Penelitian Anglano (2014) membuktikan suatu panggilan atau konten pesan WhatsApp yang dilakukan tanggal dan waktu tertentu dapat dijadikan rangkaian cerita sebuah kasus. Penelitiannya memaparkan langkah-langkah forensik seperti mengenali artefak, ekstraksi artefak, dekripsi, dan analisis data. Artefak yang tertinggal pada pesan WhatsApp dianalisis secara forensik (dikorelasikan satu per satu).

Sebagian besar *platform* forensik seluler seperti : Cellebrite LTD, Micro Systemation, Oxygen Forensics, Compelson Labs mampu memecahkan kode berbagai data yang disimpan WhatsApp, mereka tidak memberikan penjelasan bagaimana penguraiannya dilakukan, tidak memberikan bagaimana mengkorelasikan bukti untuk merekonstruksi aktivitas pengguna secara keseluruhan. Sehingga tidak mungkin menilai kelengkapan kebenaran hasil yang didapatkan mereka (Anglano, 2014).

Seperti yang disebutkan Rogers (2015), penelitian digital forensik yang berfokus pengumpulan data menggunakan penyelidikan manual dan sedikit yang

memperhatikan pemeriksaan pada implementasi solusi cerdas. Penelitian forensik analisis data menggunakan *machine learning* dilakukan penelitian Clarke dan kawan-kawan (2014), Ntantogian dan kawan-kawan (2014), Al Fahdi dan kawan-kawan (2013).

Penelitian Ertam dan Kaya (2018) dan penelitian Ucar dan Ozhan (2017) melakukan forensik jaringan internet menggunakan metode *support vector machine* (SVM), mereka melakukan ekstraksi file log firewall sistem jaringan server, penelitiannya mengukur akurasi menganalisis pola-pola serangan dengan metode SVM, menggunakan empat kernel, yaitu Linear, Polynomial, Sigmoid dan RBF.

Penelitian Marturana dan Tacconi (2013) melakukan forensik *smartphone* juga menggunakan *machine learning* dengan mengusulkan metodologi secara otomatis, untuk meringkas jenis file pada media seperti *hard drive* atau perangkat seluler dengan membandingkan beberapa algoritma seperti (Naive Bayes, Decision Trees dan SVM).

Berdasarkan ulasan permasalahan di atas, untuk meningkatkan analisis forensik WhatsaApp perlu dilakukan kajian pola-pola data yang terdapat pada WhatsApp pada *smartphone* android untuk mengklasifikasikan menggunakan metode *support vector machine* (SVM).

1.2. Perumusan Masalah

Berdasarkan latar belakang di atas terdapat beberapa isu, seperti: penelitian digital forensik berfokus pada pengumpulan data menggunakan cara penyelidikan dengan *tool* forensik memiliki keterbatasan, yaitu (i) menampilkan hanya data yang diekstrak saja, (ii) sulit mendapatkan pola-pola yang dijadikan atribut untuk dikorelasikan satu per satu, (iii) perlunya implementasi solusi cerdas menggunakan *machine learning*.

Untuk itu, pertanyaan penelitian sebagai jawaban permasalahan di atas adalah sebagai berikut :

1. Bagaimana melakukan proses decoding dan interpretasi semua artefak dan data, melakukan fitur ekstraksi.
2. Bagaimana melakukan klasifikasi data hasil ekstraksi pada WhatsApp.

3. Bagaimana melakukan perhitungan, terkait akurasi klasifikasi data forensik WhatsApp dengan metode support

1.3. Tujuan Penelitian

Tujuan penelitian ini adalah:

1. Melakukan ekstraksi atribut-atribut paket data WhatsApp pada *smartphone* android.
2. Mengimplementasikan metode *support vector machine* (SVM) untuk mengklasifikasikan pola-pola paket data WhatsApp.
3. Mendapatkan nilai akurasi terbaik dari hasil klasifikasi data WhatsApp.

1.4. Manfaat Penelitian

Manfaat penelitian ini adalah:

1. Dapat menghasilkan atribut-atribut untuk paket obrolan dan panggilan di WhatsApp.
2. Dapat mengembangkan sistem pengklasifikasian paket data WhatsApp.
3. Dapat memberikan rekomendasi terkait aplikasi pengolah pesan yang terbaik pada bidang forensika digital.

1.5. Batasan Masalah

Batasan masalah yang akan dibahas pada penelitian ini adalah:

1. Data yang digunakan adalah data hasil dari *smartphone* android.
2. Pembuktian hasil analisa artefak WhatsApp dengan cara membaca pola-pola dan diklasifikasikan.
3. Membagi data klasifikasi menjadi dua kelas.

1.6. Sistematika Penulisan

Sistematika penulisan laporan proposal tesis ini adalah sebagai berikut :

1. BAB I. Pendahuluan

   Bab ini berisi penjelasan mengenai latar belakang, rumusan masalah, tujuan, manfaat, batasan masalah, dan sistematika penulisan yang digunakan untuk menyusun laporan proposal tesis ini.

2. BAB II. Tinjauan Pustaka

   Bab ini berisi landasan dasar teori yang berhubungan dengan klasifikasi pola forensik data WhatsApp pada *smartphone* android dengan metode *Support Vector Machine* (SVM) dan penelitian sebelumnya yang akan digunakan sebagai dasar dalam melakukan penelitian.

3. BAB III. Metodologi Penelitian

   Bab ini berisi metode yang dilakukan dalam melakukan penelitian agar dapat membantu dalam pengimplementasian, dan juga berisi penjelasan secara bertahap dan terperinci tentang fase-fase (metodologi) yang dilalui dalam mencapai tujuan penelitian.

4. BAB IV. Hasil dan Pembahasan

   Bab ini menjelaskan mengenai hasil pengujian yang telah dilakukan dan pembahasan terhadap hasil yang diperoleh.

5. BAB V. Kesimpulan dan Saran

   Kesimpulan yang didapat dari penelitian disampaikan pada bagian ini. Berdasarkan hasil penelitian juga disampaikan saran yang perlu dilakukan pada penelitian selanjutnya.

DAFTAR PUSTAKA

504ENSICS Labs. (2016). **Linux memory extractor (lime)**. Retrieved from http://codeload.github.com/504ensicsLabs/LiME/zip/master

Al Barghuthi, N. B., & Said, H. (2013). **Social networks IM forensics: Encryption analysis**. *Journal of Communications*, *8*(11), 708–715. https://doi.org/10.12720/jcm.8.11.708-715

Al Fahdi, M., Clarke, N. L., & Furnell, S. M. (2013). **Challenges to digital forensics: A survey of researchers & practitioners attitudes and opinions**. *2013 Information Security for South Africa - Proceedings of the ISSA 2013 Conference*, 1–8. https://doi.org/10.1109/ISSA.2013.6641058

Al Mutawa, N., Baggili, I., & Marrington, A. (2012). **Forensic analysis of social networking applications on mobile devices**. *Digital Investigation*, *9*(SUPPL.). https://doi.org/10.1016/j.diin.2012.05.007

Anglano, C. (2014). **Forensic analysis of whatsapp messenger on Android smartphones**. *Digital Investigation*, *11*(3), 201–213. https://doi.org/10.1016/j.diin.2014.04.003

Anglano, C., Canonico, M., & Guazzone, M. (2017). **Forensic analysis of Telegram Messenger on Android devices**. *Digital Investigation*, 1–7. https://doi.org/10.1109/ICTS.2016.7910263

Barmpatsalou, K., Cruz, T., Monteiro, E., & Simoes, P. (2018). **Mobile Forensic Data Analysis: Suspicious Pattern Detection in Mobile Evidence**. *IEEE Access*, *6*(c), 59705–59727. https://doi.org/10.1109/ACCESS.2018.2875068

Beebe, N. L., Maddox, L. A., Liu, L., & Sun, M. (2013). **Sceadan: Using concatenated N-gram vectors for improved file and data type classification**. *IEEE Transactions on Information Forensics and Security*,

8(9), 1519–1530. https://doi.org/10.1109/TIFS.2013.2274728

Cellebrite Android Forensic. (2013). Cellebrite LTD. Retrieved from https://www.cellebrite.com/en/product/

Clarke, N. L., Kasiaras, D., Zafeiropoulos, T., & Clarke, N. (2014). **Android Forensics : Correlation Analysis**, (September 2015). https://doi.org/10.1109/ICITST.CITATIONS

Ertam, F., & Kaya, M. (2018). **Classification of firewall log files with multiclass support vector machine**. *6th International Symposium on Digital Forensic and Security, ISDFS 2018 - Proceeding*, *2018–Janua*(2), 1–4. https://doi.org/10.1109/ISDFS.2018.8355382

Fitzgerald, S., Mathews, G., Morris, C., & Zhulyn, O. (2012). **Using NLP techniques for file fragment classification**. *Digital Investigation*, *9*(SUPPL.). https://doi.org/10.1016/j.diin.2012.05.008

Google. (2016). Retrieved December 13, 2018, from https://developer.android.com/studio/run/emulator

Gorunescu, F. (2010). **Data Mining Concepts,Models and Techniques**.

Husain, M. I., & Sridhar, R. (2010). **iForensics: Forensic analysis of instant messaging on smart phones**. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*, *31 LNICST*(Vim), 9–18. https://doi.org/10.1007/978-3-642-11534-9_2

Iqbal, A., Marrington, A., & Baggili, I. (2014). **Forensic artifacts of the ChatON Instant Messaging application**. *Int. Workshop Syst. Approaches Digit. Forensics Eng., SADFE*, (August 2014). https://doi.org/10.1109/SADFE.2013.6911538

Jung, J., Jeong, C., Byun, K., & Lee, S. (2011). **Sensitive privacy data acquisition in the iPhone for digital forensic analysis**. *Communications in Computer and Information Science*, *186 CCIS*, 172–186.

https://doi.org/10.1007/978-3-642-22339-6_21

Karpisek, F., Baggili, I., & Breitinger, F. (2015). **WhatsApp network forensics: Decrypting and understanding the WhatsApp call signaling messages**. *Digital Investigation*, *15*, 110–118. https://doi.org/10.1016/j.diin.2015.09.002

Mahajan, A., S. Dahiya, M., & P. Sanghvi, H. (2013). **Forensic Analysis of Instant Messenger Applications on Android Devices**. *International Journal of Computer Applications*, *68*(8), 38–44. https://doi.org/10.5120/11602-6965

Marturana, F., & Tacconi, S. (2013). **A Machine Learning-based Triage methodology for automated categorization of digital media**. *Digital Investigation*, *10*(2), 193–204. https://doi.org/10.1016/j.diin.2013.01.001

Nicole Arce. (2015). **WhatsApp Calling For Android And iOS: How To Get It And What To Know**. Retrieved from http://www.techtimes.com/articles/38291/20150309/whatsapp-calling-for-android-and-ios-how-to-get-it-and-what-to-know.htm

Norouzizadeh Dezfouli, F., Dehghantanha, A., Eterovic-Soric, B., & Choo, K. K. R. (2016). **Investigating Social Networking applications on smartphones detecting Facebook, Twitter, LinkedIn and Google+ artefacts on Android and iOS platforms**. *Australian Journal of Forensic Sciences*, *48*(4), 469–488. https://doi.org/10.1080/00450618.2015.1066854

NoxPlayer. (2015). Retrieved July 23, 2018, from https://id.bignox.com/

Ntantogian, C., Apostolopoulos, D., Marinakis, G., & Xenakis, C. (2014). **Evaluating the privacy of Android mobile applications under forensic analysis**. *Computers and Security*, *42*, 66–76. https://doi.org/10.1016/j.cose.2014.01.004

Oracle Corp. (2013). Retrieved December 12, 2018, from https://www.virtualbox.org/

Oxygen Forensics. (2013). Oxygen Forensics, Inc. Retrieved from https://www.oxygen-forensic.com/en/

Polat, K., & Güneş, S. (2007). **Breast cancer diagnosis using least square support vector machine**. *Digital Signal Processing: A Review Journal*, *17*(4), 694–701. https://doi.org/10.1016/j.dsp.2006.10.008

Rogers, M. K. (2015). **Psychological profiling as an investigative tool for digital forensics**. *Digital Forensics: Threatscape and Best Practices*. Elsevier Inc. https://doi.org/10.1016/B978-0-12-804526-8.00003-4

Shortall, A., & Azhar, M. A. H. Bin. (2016). **Forensic Acquisitions of WhatsApp Data on Popular Mobile Platforms**. *Proceedings - 2015 6th International Conference on Emerging Security Technologies, EST 2015*, 13–17. https://doi.org/10.1109/EST.2015.16

Singla, N., & Garg, D. (2012). **String Matching Algorithms and their Applicability in various Applications**, (6), 218–222.

Thakur, N. S. (2013). **Forensic Analysis of WhatsApp on Android Smartphones**. https://doi.org/10.1016/j.diin.2014.04.003

Tso, Y., Wang, S.-J., Huang, C.-T., & Wang, W. (2012). **iPhone social networking for evidence investigations using iTunes forensics**. *Proceedings of the 6th International Conference on Ubiquitous Information Management and Communication - ICUIMC '12*, 1. https://doi.org/10.1145/2184751.2184827

Ucar, E., & Ozhan, E. (2017). **The Analysis of Firewall Policy Through Machine**. *Wireless Personal Communications*. https://doi.org/10.1007/s11277-017-4330-0

Vapnik, V. N. (1995). **The Nature of Statistical Learning Theory**. *Springer-Verlag New York*. https://doi.org/10.1007/978-1-4757-2440-0

Vidas, T., Zhang, C., & Christin, N. (2011). **Passe-partout: A general collection**

methodology for android devices. *Digital Investigation*, S14–S24. https://doi.org/10.1109/TIFS.2013.2285360

Volatility Foundation. (2016). **An advanced memory forensics framework**. Retrieved from http://volatilityfoundation.org/

Walnycky, D., Baggili, I., Marrington, A., Moore, J., & Breitinger, F. (2015). **Network and device forensic analysis of Android social-messaging applications**. *Digital Investigation*, *14*(S1), S77–S84. https://doi.org/10.1016/j.diin.2015.05.009

Witten Ian H, Frank Eibe, H. M. A. (2011). **Data Mining**. Elsevier Ltd.

YouWave. (2013). Retrieved December 13, 2018, from https://youwave.com/

Yusoff, M. N., 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. Contemporary Digital Forensic Investigations of Cloud and Mobile Applications**. Elsevier Inc. https://doi.org/10.1016/B978-0-12-805303-4.00004-6

Zhao, Y., Wat, P., Laser, M. S., & Medvidović, N. (2018). **Empirically assessing opportunities for prefetching and caching in mobile apps**. *Proceedings of the 33rd ACM/IEEE International Conference on Automated Software Engineering - ASE 2018*, 554–564. https://doi.org/10.1145/3238147.3238215

Zheng, N., Wu, T., Wang, J., & Xu, M. (2015). **A fragment classification method depending on data type**. *Proceedings - 15th IEEE International Conference on Computer and Information Technology, CIT 2015, 14th IEEE International Conference on Ubiquitous Computing and Communications, IUCC 2015, 13th IEEE International Conference on Dependable, Autonomic and Se*, 1948–1953. https://doi.org/10.1109/CIT/IUCC/DASC/PICOM.2015.288