Available online at https://ejournal.almaata.ac.id/index.php/IJUBI
Indonesian Journal of Business Intelligence
Volume 1 | Issue 1 | June (2018)
IJUBI
Indonesian Journal ---- of ---- Business Intelligence

LIVE FORENSIK UNTUK ANALISA ANTI FORENSIK PADA WEB BROWSER STUDI KASUS BROWZAR

Tri Rochmadi[1]
[1]Program Studi Sistem Informasi, Fakultas Komputer, Universitas Alma Ata
trirochmadi@almaata.ac.id
Jalan Brawijaya No.99 Yogyakarta

Keywords:

live forensic, web browser forensic, anti-forensic.

Abstract

Cybercrime continues to increase and innovate along with the rapid development of internet and more easily accessible everywhere. Most business organizations have used the internet for its operations so that the use of browsers is a necessity to support work. So that the browser also adjusts to improve security on the user's side so that information accessed by users cannot be known by other users. Browzar is a browser that answers these challenges, where Browzar can run without having to be installed on the computer and automatically deletes information generated by the use of the browser itself. However, these advantages become a challenge for investigators because these advantages can be exploited by cybercriminals to eliminate, minimize existing digital evidence. This study intends to analyze and find digital evidence in criminal cases using Browzar with Live Forensic. Digital evidence is obtained using dumpit for data acquisition and forensic volatility memory and winhex to analyze data and information on RAM. Results of the study were able to obtain information that could be used for digital evidence on Browzar web browser, namely URL history, account used log in, namely username and password, timestamp, that is, the user access time to a web page.

Kata Kunci:

live forensik, forensik web browser, anti-forensik.

Abstrak

Cybercrime terus meningkat dan berinovasi seiring dengan perkembangan internet yang cepat dan lebih mudah diakses di mana-mana. Sebagian besar organisasi bisnis telah menggunakan internet untuk operasinya sehingga penggunaan browser adalah suatu keharusan untuk mendukung pekerjaan. Sehingga browser juga menyesuaikan untuk meningkatkan keamanan di sisi pengguna sehingga informasi yang diakses oleh pengguna tidak dapat diketahui oleh pengguna lain. Browzar adalah browser yang menjawab tantangan ini, di mana Browzar dapat berjalan tanpa harus diinstal di komputer dan secara otomatis menghapus informasi yang dihasilkan oleh penggunaan browser itu sendiri. Namun, keuntungan ini menjadi tantangan bagi penyelidik karena keuntungan ini dapat dimanfaatkan oleh penjahat cyber untuk menghilangkan atau setidaknya meminimalkan bukti digital yang ada. Penelitian ini bermaksud untuk menganalisis dan menemukan bukti digital dalam kasus kriminal menggunakan Browzar dengan Live Forensik. Bukti digital diperoleh dengan menggunakan dumpit untuk akuisisi data dan memori volatilitas forensik dan winhex untuk menganalisis data dan informasi pada RAM. Hasil penelitian ini dapat memperoleh informasi yang dapat digunakan untuk bukti digital pada browser web Browzar, yaitu riwayat URL, login akun yang digunakan, yaitu nama pengguna dan kata sandi, timestamp, yaitu waktu akses pengguna ke halaman web.

Pendahuluan

Pesatnya perkembangan internet telah berdampak pada perubahan organisasi bisnis di pemerintahan, pendidikan, kesehatan dan sektor lainnya. Meski menghadirkan kemudahan dan kelebihan lainnya, internet juga menjadi masalah, yaitu kejahatan di dunia maya atau cybercrime yang semakin beragam. Pada umumnya akses internet di sebuah organisasi menggunakan web browser untuk aktifitas mereka di keseharian kerjanya untuk mengakses sistem yang ada [1]. Web browser adalah peranti lunak yang dibuat dengan menyimpan informasi apa pun seperti URL history, search keyword, timestamp, password, dan segala sesuatu yang dilakukan pengguna saat menjelajah di internet [2]. URL history adalah kumpulan alamat web yang diakses oleh pengguna, search keyword adalah kata kunci yang dicari atau diketik di halaman web pengguna dan timestamp adalah istilah yang menunjukkan waktu mengakses web. Untuk meningkatkan privasi pengguna web browser, dalam hal ini, Browzar memiliki fitur bahwa informasi yang dihasilkan oleh web browser tidak disimpan di komputer atau di web browser lain disebut sebagai Private Browsing Mode [3]. Selain fitur-fitur ini, Browzar juga memiliki fitur bahwa browzar adalah portable web browser dan melakukan penghapusan registry pada sistem komputer ketika Browzar ditutup sehingga informasi yang dapat digunakan sebagai bukti digital semakin kabur [4], dalam hal ini, disebut metode anti forensik. Fitur ini digunakan oleh oknum untuk melakukan kejahatan dunia maya di samping keuntungan Browzar dalam menjaga privasi pengguna. Portable web browser adalah web browser yang dapat dijalankan tanpa diinstal di komputer, sehingga hanya disimpan dalam media penyimpanan eksternal sehingga tidak meninggalkan file program di komputer [3]. Registry adalah informasi atau basis data di komputer yang mencatat setiap aktivitas di komputer baik ketika ada aktivitas perangkat keras atau perangkat lunak baru yang berjalan. Jadi itu menjadi tantangan bagi penyelidik ketika melakukan forensik atau menyelidiki aktivitas internet yang dicurigai dalam kasus kejahatan dunia maya yang memungkinkan menggunakan web browser browzar.

Penelitian tentang masalah ini adalah penyelidikan forensik digital untuk menganalisis proses anti-forensik pada web browser Browzar. Penelitian sebelumnya pada web browser terbatas pada sisi portable dari mode private web browser [4] ketika melakukan aktivitas di internet. Pemecahan masalah dalam penelitian ini yaitu web browser Browzar dengan menggunakan metode live forensik. Metode ini sangat cocok untuk penanganan insiden yang lebih cepat dan memungkinkan memperoleh data lebih banyak dan informatif yang ada dalam RAM [5] karena sifat Browzar yang merupakan web browser yang dilengkapi dengan anti-forensik, sehingga harus dilakukan ketika komputer masih menyala. Live forensik adalah metode forensik untuk mendapatkan data volatil yang terkandung dalam RAM, sehingga kejahatan dapat diketahui dari analisis data volatil yang terdapat pada RAM tersebut [6]. Penelitian ini memiliki manfaat sebagai metode atau framework baru yang dapat digunakan dalam menangani kasus web browser yang di dalamnya terdapat unsur anti-forensik. Maka dengan penelitian ini diharapkan dapat menambah pengetahuan dan berkontribusi secara akademis dan praktis. Oleh karena itu penelitian ini difokuskan pada live forensik untuk analisa web browser Browzar.

Landasan Teori

Web Browser

Web browser adalah perangkat lunak yang digunakan untuk mengakses halaman web untuk mendapatkan informasi yang jelas dan mudah dibaca. Sumber informasi diidentifikasi dengan Uniform Resource Identifier (URI) dan akan menjadi halaman web, gambar, video atau konten lainnya [7]. Saat ini banyak jenis web browser dengan berbagai engine browser yang ada dalam perangkat lunak. Diantaranya yang paling banyak digunakan adalah Chrome, Firefox, Seamonkey Safari dan Opera. Dalam mode private, semua vendor browser mengatakan bahwa history, cookie, dan download file atau lainnya tidak akan disimpan di komputer. Sementara di sisi Browzar mereka mengklaim bahwa aplikasi Browzar baik digunakan untuk Perbankan dan Cloud. Selain itu, Browzar secara otomatis membersihkan data web browser dan menghapusnya dengan baik dari apa yang

dihasilkan saat aktifitas menggunakan web browser Browzar.

Forensik Web Browser

Forensik web browser adalah sebuah aktivitas investigasi untuk menganalisis apa yang dihasilkan dari penggunaan web browser. Analisis ini adalah untuk menemukan bukti digital dari aktivitas penggunaan terhadap web browser seperti cache, histori, cookie, timestamp, session, dan file unduhan [8]. Bukti digital sangat penting karena dengan bukti digital dapat mengungkapkan kejahatan dan melacak pelaku kejahatan yang dimaksud. Jadi seorang investigator setidaknya dalam analisis forensik we browser dapat menemukan bukti digital yang terdapat dalam web browser tersebut [9].

Anti-Forensik

Anti-forensik adalah sebuah upaya untuk meminimalkan dan bahkan menggagalkan dari proses analisis forensik yang dilakukan [10]. Kegiatan ini bertujuan untuk menghindari insiden respon, menghabiskan waktu pada proses penyelidikan sehingga membuat keraguan pada laporan forensik yang dilakukan oleh para ahli. Dalam forensik digital, kegiatan anti-forensik ini memiliki empat kategori metode yang dapat digunakan [11].

Hiding Data

Hiding data adalah menyembunyikan data sehingga tidak dapat dibaca dengan menggunakan teknik seperti enkripsi, steganografi, dan lainnya [12].

Artifact Wiping

Artifact wiping adalah teknik yang digunakan untuk menimpa data pada hard drive sehingga tidak dapat dipulihkan [13].

Trail Obfuscation

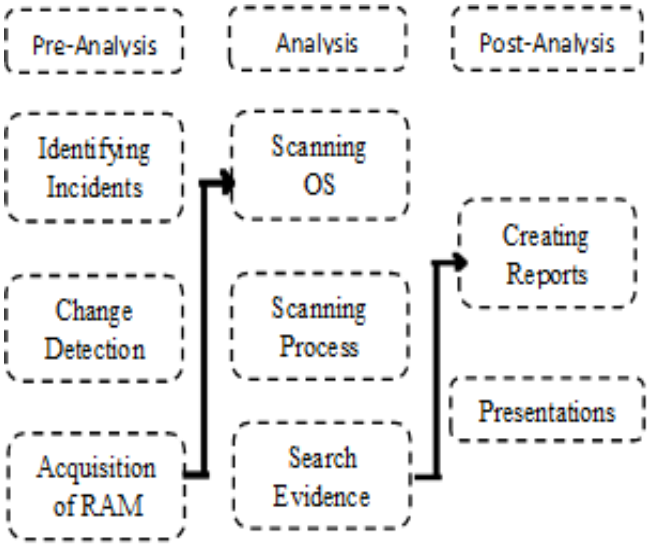
Trail Obfuscation bertujuan untuk menyesatkan atau mengelabui penyelidik dengan menyembunyikan atau menghapus bukti tentang sumber dan sifat serangan [11]. Teknik ini dapat menggunakan pembersih log untuk memodifikasi file log metadata atau memodifikasi timestamps.

Attack Against Forensics Prosess or Tool

Attacks Against Forensics Process or Tools adalah metode anti-forensik yang langka karena bekerja langsung pada prosedur penyelidikan atau bug yang ada di tool forensik. Penyerang atau oknum penjahat cybercrime membutuhkan lebih banyak pengetahuan dan pengalaman tentang cara kerja alat dan prosedur [10].

Metode

Metode dalam penelitian ini menggunakan metode pengembangan metode Generic Computer Forensic Investigation Model (GCFIM), metode ini terdiri dari 3 tahap utama, yaitu Pra Analisis, Analisis, dan Pasca Analisis, seperti yang ditunjukkan pada Gambar 1.



Gambar 1. Usulan Metode Live Forensik Web Browser

Pra Analisa

Tahapan awal melakukan investigasi sebelum analisa dilakukan termasuk identifikasi kejadian hingga akuisisi data.

Analisa

Tahap analisa dimulai dengan memindai sistem operasi hingga menemukan bukti digital yang dapat digunakan sebagai bukti hukum di pengadilan.

Pasca Analisa

Tahap di mana laporan dibuat dari awal investigasi sehingga kredibilitas dapat dipertahankan dalam melakukan investigasi untuk digunakan sebagai bahan untuk presentasi di pengadilan.

Simulasi

Penelitian ini membutuhkan skenario simulasi kasus untuk mendapatkan bukti digital. Simulasi dibuat lengkap hingga tahap anti-forensik. Tujuan dari simulasi ini adalah untuk menjadi

pedoman bagi informasi untuk diidentifikasi sebagai kasus kriminal menggunakan Browzar. Simulasi ini menggunakan perangkat keras dan perangkat lunak yang ditunjukkan pada Tabel 1.

Tabel 1. Perangkat Keras dan Perangkat Lunak

Perangkat Keras	Perangkat Lunak
Laptop Core i5 2GB RAM	Windows 7 SP 2
Flashdrive A-DATA 2 GB	Web Browser Browzar Black
Flashdrive TOSHIBA 8 GB	Clean After Me Portable
	ProcMon Portable
	DumpIt
	Winhex
	Volatility Memory Forensic

Penelitian ini disimulasikan ketika web browser Browzar ditutup dan anti-forensik dilakukan menggunakan Clean After Me untuk menghapus sistem registry pada komputer. Simulasi dari penelitian adalah sebagai berikut:

- Menjalankan web browser Browzar
- Membuka google.com
- Mencari Xman (berita dan gambar)
- Mengakses email google (gmail)

Penjelasan lebih jelas dari simulasi di atas dapat dilihat pada Tabel 2.

Tabel 2. Aktifitas Penggunaan Browzar

Web Browser	Aktifitas yang dilakukan (Keyword)
Browzar	Google.com – Pencarian (Xman) – Gambar – eMail Google (gmail)

Analisa dan Hasil

Penelitian ini dilakukan dengan menggunakan sistem operasi laptop Windows 7 SP 2 32 Bit yang digunakan sebagai tersangka dan laptop masih hidup tetapi tidak ada aplikasi terbuka. Laptop dibiarkan hidup dan tidak dilakukan aktifitas apapun dari laptop untuk menghindari kehilangan bukti digital. Sebelum memulai analisis, tahap awal yaitu insiden respons dideteksi dengan mendeteksi perubahan dalam sistem diikuti oleh akuisisi memori komputer menggunakan DumpIt untuk mendapatkan salinan file dari memori RAM dengan Live Forensik. Kemudian mulai menganalisis untuk menemukan bukti dari browser web menggunakan Forensic Memory Volatility dan WinHex.

Pra Analisa

Identifikasi Insiden dan Pendeteksian

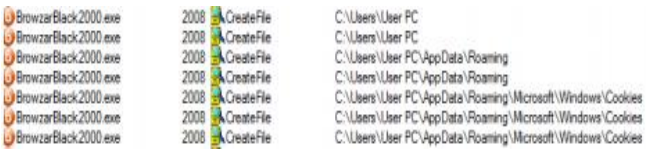
Tahap ini bertujuan untuk mencari informasi dan mengumpulkan semua data yang ada dan dimungkinkan untuk menemukan penyimpangan dari sistem yang sedang berjalan.

Pada tahap awal ini, keanehan ditemukan karena perubahan dalam registry yang ditunjukkan pada Tabel 3 dan juga pembuatan file baru pada drive komputer yang ditunjukkan pada Gambar 2. Tahap ini penting untuk membantu menentukan tool atau plugin yang tepat untuk menemukan bukti digital menggunakan memori forensik yang mudah hilang karena sifatnya volatile.

Tabel 3. Deteksi Perubahan Registry

Web Browser	Process	Location
Browzar	RegOpenKey	HKLM\SOFTWARE\Microsoft\Cryptography\ Offload
Browzar	RegCloseKey	HKLM\SOFTWARE\Microsoft\Cryptography\
Browzar	RegQueryKey	HKLM\SOFTWARE\Policies\Microsoft\Cryptography\

Proses deteksi diketahui memiliki perubahan registri dalam sistem, yaitu penggunaan Browzar yang menimpa data yang digunakan oleh Internet Explorer, ini sangat penting untuk diketahui karena sebagai referensi untuk analisis selanjutnya.

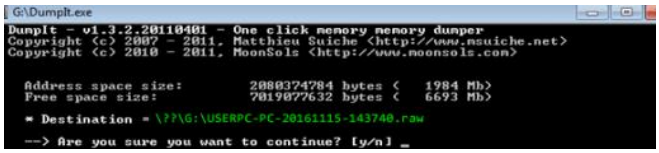


Gambar 2. File Baru Ketika Browzar Dijalankan

Ketika Browzar dijalankan, tidak ada file baru yang dibuat pada drive USB tetapi terjadi di sistem komputer, yaitu di beberapa tempat di mana sumber awalnya di folder C folder Pengguna - folder PC Pengguna - folder AppData.

Akuisisi RAM

Akuisisi RAM dilakukan ketika komputer masih hidup dengan menggunakan DumpIt. Live forensik yang digunakan dalam penelitian ini menggunakan DumpIt karena memiliki fitur memori dan dapat mengambil data dan informasi yang terkandung dalam RAM, termasuk dari aplikasi yang sebelumnya berjalan pada laptop. Dari hasil akuisisi, file ekstensi .raw ditunjukkan pada Gambar 3.



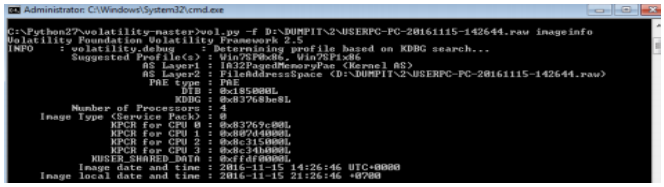
Gambar 3. Akuisisi RAM

Proses lama atau cepatnya akuisisi data dalam RAM tergantung pada jumlah kapasitas pada RAM, semakin besar kapasitas RAM, semakin lama akuisisi yang dijalankan, dan sebaliknya. Dari hasil akuisisi ini, file dump akan dianalisis menggunakan alat analisis forensik, Winhex dan Forensic Volatile Memory.

Analisa

Scanning Sistem Operasi

Scanning dimaksudkan untuk mengetahui informasi sistem operasi yang digunakan oleh komputer seperti yang ditunjukkan pada Gambar 4.



Gambar 4. Hasil Scanning Sistem Operasi

Hasil scanning sistem operasi menunjukkan bahwa komputer yang digunakan adalah Windows 7 Service Pack 1 dengan 32 bits seperti pada gambar tertulis Win7SP1x86.

Scanning Proses Aplikasi

Scanning proses dimaksudkan untuk menentukan ID dari proses perangkat lunak yang digunakan sehingga proses ID dapat membantu memfasilitasi kecepatan analisa karena telah memfilter ID proses ketika scanning pencarian bukti digital, seperti yang ditunjukkan pada Gambar 5.

Offset(V)	Name	PID	PPID	Thds	Hnds	Sess
0x975db408	Internet Explo	1924	1324	8	129	1
0x85f0a030	Internet Explo	4416	1324	12	445	1
0x85f4e780	Internet Explo	2108	4416	30	777	1
0x860be908	FirefoxPortabl	2408	1940	3	148	1
0x860bf788	firefox.exe	4872	2408	57	701	1
0x86a70740	GoogleChromePo	1536	1940	1	83	1
0x894df768	chrome.exe	772	1536	29	788	1
0x868ef660	chrome.exe	240	772	6	74	1
0x89609d40	chrome.exe	5748	772	5	165	1
0x97496628	chrome.exe	4952	772	14	355	1
0x894a4030	chrome.exe	5692	772	4	170	1
0x86a95bb8	BrowzarBlack20	2288	1940	28	609	1

Gambar 5. Hasil Scanning Process

Scanning Pencarian Bukti Digital

Scanning pencarian bukti digital dilakukan dengan 2 cara yaitu dengan Volatility Memory Forensic dan Winhex.

Volatility Memory Forensics

Proses penemuan bukti digital menggunakan Volatility Memory Forensic ditunjukkan pada Tabel 4.

Tabel 4. Bukti Digital yang Didapatkan Menggunakan Volatility Memory Forensics

Target	Analysis	Bukti
ID process is based on scanning 4.2.2	Proccess	2288 Browzar Black20
Accessed URL and keyword	Location	Visited User PC@https://www.google.co.id/search?hl=id&source=hp&biw=&bih=&q=xman&gbv=1
URL access time	Last accessed	2016-11-15 14:20:20 UTC+000

Winhex

Untuk mendukung proses investigasi dan untuk mendapatkan bukti digital maksimum dan dapat digunakan sebagai bukti digital yang sah dan meningkatkan kepercayaan dalam proses pengadilan, analisis tambahan dilakukan dengan

menggunakan tool forensik Winhex. Dari analisis menggunakan Winhex, URL history dan timestamp dapat ditemukan, seperti menggunakan tool forensik sebelumnya, yaitu Volatility Memory Forensic, dan untuk kata sandi atau password yang digunakan untuk masuk ke email google dapat ditemukan, seperti yang ditunjukkan pada Gambar 5.

Gambar 5. Password yang Ditemukan di RAM dari Browzar

Pasca Analisa

Pasca analisa terdiri dari laporan dan presentasi. Laporan ini terdiri dari semua informasi terperinci dari awal insiden kasus dan semua dokumentasi dari tahapan sebelum proses analisis dan analisis. Dan presentasi ini adalah tentang bukti digital apa yang dapat diperoleh selama investigasi dan digunakan untuk menjelaskannya di pengadilan.

Hasil dan Pembahasan

Teknik live forensik dapat diterapkan pada proses pengambilan bukti digital dari aplikasi web browser Browzar berbasis desktop pada sistem operasi Windows 7 menggunakan tool dumpit, volatility memori forensic dan winhex. Setelah melakukan beberapa simulasi dan beberapa tahapan analisis, hasil analisis dalam penelitian ini dapat dilihat pada Tabel 5.

Tabel 5. Kesimpulan Hasil Investigasi

Web Browser Portable	History	Timestamp	Password
Browzar Black2000	√	√	√

History, timestamp dan password pada web browser Browzar dapat ditemukan dengan baik dengan tool Volatility Memory Forensic dan WinHex.

Penelitian ini juga dapat dilakukan pada simulasi kasus kriminal lainnya yang mendukung teknik live forensik. Kompleksitas dalam menemukan dan memperoleh atau menganalisis bukti digital di browser portabel dengan menerapkan anti-forensik pada laptop yang masih berjalan membutuhkan lebih banyak pengetahuan dan pengalaman. Sehingga juga memerlukan tool forensik lain yang dapat mendukung untuk mendapatkan lebih banyak informasi dan lebih banyak bukti digital.

Kesimpulan dan Saran

Live forensik dapat diterapkan untuk memperolehan bukti digital dari we browser Browzar pada sistem operasi Windows 7 menggunakan tool DumpIt dan dianalisis menggunakan Forensic Memory Volatility dan Winhex berhasil mendapatkan 3 bukti digital potensial terkait kasus kriminal di internet. Bukti digital tersebut adalah URL atau alamat situs web yang dikunjungi dan history atau daftar URL yang telah dikunjungi oleh pelaku, timestamp, yaitu waktu mengakses URL oleh pelaku, dan kata sandi atau password yang merupakan akun pelaku yang digunakan untuk masuk ke akun Gmail. Hasil dari proses investigasi ini dapat menjadi sanggahan dari Browzar yang menyatakan bahwa bukti digital tidak disimpan di komputer yang digunakan. Teknik live forensik ini dilakukan dalam keadaan bahwa laptop masih berjalan untuk mengambil data yang ada dalam RAM sehingga data tidak hilang atau berkurang ketika laptop dimatikan sebelumnya.

Beberapa saran untuk penelitian lebih lanjut adalah melakukan forensik dengan metode lain, aplikasi web browser lain, dan sistem operasi lain yang digabungkan ke dalam topik penelitian yang mendukung teknik live forensik untuk mendapatkan hasil penelitian yang berbeda dan lebih akurat. Penggunaan tool live forensik dan analisis forensik pada RAM juga dapat digabungkan dengan tool lain, untuk mendapatkan lebih banyak infomasi yang berkualitas dan bukti digital yang lebih sehingga lebih mudah untuk mengungkap kasus-kasus kejahatan yang terjadi.

Referensi

[1] [1] G. Patel, "Anti-Forensics Techniques for browsing artifacts," 2014.

[2] J. Oh, S. Lee, and S. Lee, "Advanced evidence collection and analysis of web browser activity 5," vol. 8, pp. 0–8, 2011.

[3] D. G. Dharan, "Forensic Evidence Collection by Reconstruction of Artifacts in Portable Web Browser," 2014.

[4] G. Aggarwal, E. Burzstein, C. Jackson, and D. Boneh, "An Analysis of Private Browsing Modes in Modern Browsers," California, 2010.

[5] S. Rahman and M. N. A. Khan, "Review of Live Forensic Analysis Techniques," vol. 8, no. 2, pp. 379–388, 2015.

[6] Garcia, Gabriela Limon, "Forensic Physical Memory Analysis: An Overview of Tools and Techniques Technical Report," Helsinki University of Technology, 2007.

[7] A. Jain and V. Richariya, "Implementing a Web Browser with Phishing Detection Techniques," *World Comput. Sci. Inf. Technol. J.*, vol. 1, no. 7, pp. 289–291, 2011.

[8] L. Ran and H. Jin, "Analysis Framework to Detect Artifacts of Portable Web Browser," 2012.

[9] B. R. Jones, *Internet Forensics*, no. October. 2005.

[10] Li, W, "Anti-forensic Digital Investigation for Unauthorized Intrusion on a Wireless Network," Auckland, 2013.

[11] M. K. Rogers, R. Mislan, J. Goldman, T. Wedge, and S. Debrota, "Computer Forensics Field Triage Process Model," *Conf. Digit. Forensics, Secur. Law*, vol. 1, no. 2, pp. 27–40, 2006.

[12] Rekhis, S., & Boudriga, N., "A System for Formal Digital Forensic Investigation Aware of Anti-Forensic Attacks," Information Forensics and Security, 635-650, 2012.

[13] Sammons, J, "The Basics of Digital Forensics," Waltham: Syngress, 2012.