Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) DOI: 10.25126/jtiik.201961465
Vol. 6, No. 6, Desember 2019, hlm. 703-712 p-ISSN: 2355-7699
Akreditasi KEMENRISTEKDIKTI, No. 30/E/KPT/2018 e-ISSN: 2528-6579

FORENSIK *INTERNET OF THINGS* PADA *DEVICE LEVEL BERBASIS EMBEDDED SYSTEM*

Eri Haryanto[1], Imam Riadi[2]

[1] Departemen Informatika, Universitas Islam Indonesia, Indonesia
[2] Departemen Sistem Informasi, Universitas Ahmad Dahlan Yogyakarta, Indonesia
Email: [1]14917119@students.uii.ac.id, [2]imam.riadi@is.uad.ac.id

(Naskah masuk: 23 Februari 2019, diterima untuk diterbitkan: 11 November 2019)

Abstrak

Perangkat *Internet of Things* (IoT) merupakan perangkat cerdas yang memiliki interkoneksi dengan jaringan internet global. Investigasi kasus yang menyangkut perangkat IoT akan menjadi tantangan tersendiri bagi investigator forensik. Keberagaman jenis perangkat dan teknologi akan memunculkan tantangan baru bagi investigator forensik. Dalam penelitian ini dititikberatkan forensik di level *internal device* perangkat IoT. Belum banyak bahkan belum penulis temukan penelitian sejenis yang fokus dalam analisis forensik perangkat IoT pada level *device*. Penelitian yang sudah dilakukan sebelumnya lebih banyak pada level jaringan dan level *cloud server* perangkat IoT. Pada penelitian ini dibangun *environment* perangkat IoT berupa *prototype smart home* sebagai media penelitian dan kajian tentang forensik level *device*. Pada penelitian ini digunakan analisis model forensik yang meliputi *collection*, *examination*, *analysis*, dan *reporting* dalam investigasi forensik untuk menemukan bukti digital. Penelitian ini berhasil mengungkap benar-benar ada serangan berupa injeksi *malware* terhadap perangkat IoT yang memiliki sistem operasi Raspbian, Fedberry dan Ubuntu Mate. Pengungkapan fakta kasus mengalami kesulitan pada perangkat IoT yang memiliki sistem operasi Kali Linux. Ditemukan 1 IP *Address* komputer penyerang yang diduga kuat menanamkan *malware* dan mengganggu sistem kerja perangkat IoT.

Kata kunci: *digital forensic, IoT device, device level forensic, IoT forensic, embedded system, internet of things*

DEVICE LEVEL FORENSIC ON INTERNET OF THINGS DEVICES EMBEDDED BASED SYSTEM

Abstract

The Internet of Things (IoT) is an smart device that has interconnection with global internet networks. Investigating cases involving IoT devices will be a challenge for forensic investigators. The diversity of types of equipment and technology will create new challenges for forensic investigators. In this study focused on forensics at the IoT device's internal device level, there have not been many similar research that focuses on forensic analysis of IoT devices at the device level. Previous research has been done more at the network level and cloud level of IoT device's. In this study an IoT environment was built a smart home prototype as a object for research and studies on forensic level devices. This study, using forensic model analysis which includes collection, examination, analysis, and reporting in finding digital evidence. This study successfully revealed that there was really an attack in the form of malware injection against IoT devices that have Raspbian, Fedberry and Ubuntu Mate operating systems. Disclosure of the fact that the case has difficulties with IoT devices that have the Kali Linux operating system. Found 1 IP Address of an attacker's computer that is allegedly strongly infusing malware and interfering with the work system of IoT devices.

Keywords: *digital forensic, IoT device, device level forensic, IoT forensic, embedded system, internet of things*

1. PENDAHULUAN

Internet menjadi teknologi yang merupakan cikal bakal lahirnya teknologi baru dengan berbagai inovasi. Jaringan internet telah menghubungkan banyak komputer di seluruh penjuru dunia sehingga antar komputer tersebut dapat saling bertukar data. Interkoneksi jaringan internet saat ini dapat menghubungkan perangkat selain komputer personal. Salah satu contohnya adalah perangkat *Internet of Things* (IoT). Perangkat tersebut adalah perangkat

elektronik cerdas yang memanfaatkan internet sebagai media komunikasi dan transfer data.

Menurut Osman (Osman, Osei, & Narendra, 2016), masa depan internet adalah sebuah dunia baru berupa jaringan yang kuat dari perangkat *smart* yang secara independen dapat berkomunikasi satu sama lain dengan sedikit intervensi manusia, atau bahkan tanpa intervensi sama sekali. Imbas dari hal tersebut akan memunculkan teknologi baru bernama *internet of things* (IoT).

Perangkat IoT merupakan perangkat elektronik berupa mikrokontroler yang terhubung dengan sensor, memiliki interkoneksi dengan jaringan internet, dan pada sisi lain perangkat juga terhubung ke *server* sebagai media penyimpanan data mentah yang dihasilkan oleh sensor. Antar satu perangkat IoT dengan perangkat IoT yang lainnya memiliki kemampuan untuk saling berkomunikasi. Sehingga dapat memberikan banyak manfaat dan kemudahan bagi orang yang mengimplementasikan perangkat IoT.

Pada aplikasi *smarthome*, IoT dapat berperan sebagai asisten dari pemilik rumah yang dapat mengatur peralatan elektronik seperti lampu, mesin cuci, lemari es, AC, gerbang, dan televisi. Dengan diterapkannya IoT di rumah, rumah tersebut akan menjadi sebuah *smart home* yang selalu mengirimkan data keluaran dari sensor ke *server* untuk bisa dilakukan monitoring melalui platform khusus yang dibangun. *Smart home* bertujuan memberikan kontrol penuh atas penggunaan peralatan elektronik yang ada di rumah sehingga bisa dilakukan *remote* dari jarak jauh.

Pembangunan perangkat IoT sebagian besar dibuat berbasis *embedded system,* perangkat akan ditanamkan sebuah sistem komputer sebagai pengendali perangkat. (Barua, Hoque, & Akter, 2014) mendefinisikan *embedded system* sebagai sistem komputer dengan tipe khusus yang melakukan beberapa hal yang spesifik. Pada *embedded system* program telah dirancang khusus dan ditentukan sebelumnya, biasanya digunakan pada sistem mekanik maupun listrik dengan skala besar termasuk implementasi pada perangkat IoT.

Seiring berjalannya waktu jumlah perangkat IoT di dunia ini semakin meningkat. Diperkirakan jumlah perangkat ini pada tahun 2020 bisa mencapai 50,1 milyar perangkat (Wilianto & Kurniawan, 2018). Jumlah yang sangat besar dari sebuah perangkat digital. Dengan bertambahnya jumlah perangkat IoT akan menumbuhkan banyak ancaman keamanan. IoT yang pada aplikasinya menggunakan media jaringan internet, menjadi sasaran penyerangan yang akan dilakukan oleh penyerang. Isu keamanan menjadi sangat penting karena berkaitan dengan sensitivitas data personal yang dihasilkan oleh perangkat IoT.

Sebuah sistem yang terkoneksi ke jaringan internet global akan memiliki potensi untuk diserang karena memiliki banyak celah keamanan. Oleh karenanya dalam membangun perangkat IoT juga perlu untuk ditambahkan modul keamanan di dalam perangkat tersebut. Sebagai contoh, penggunaan protokol *Secure Socket Layer* (SSL) sebagai enkripsi pada pengiriman datanya. *Security awareness* terhadap perangkat IoT harus senantiasa ditingkatkan terutama oleh produsen untuk menjamin keamanan perangkat IoT.

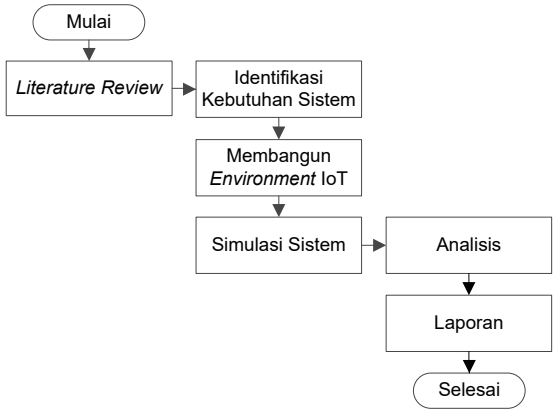
Keberagaman jenis perangkat dan teknologi akan memunculkan tantangan bagi investigator forensik digital (Rizal, Riadi, & Prayudi, 2018). Perangkat IoT melibatkan tiga unsur forensik pada proses investigasinya, yaitu *cloud forensic, network forensik, dan device level forensic* (Zawoad & Hasan, 2015). Ketiga unsur tersebut memiliki tantangan yang menarik dalam mendapatkan barang bukti digital sehingga perlu dikaji lebih mendalam.

Pada level *cloud* dan *network* telah banyak penelitian yang telah mengkaji *scope* tersebut akan tetapi level forensik perangkat IoT yang fokus di sisi *device* belum banyak ditemukan. Oleh karena hal tersebut pada penelitian ini dilakukan kajian lebih lanjut mengenai tahapan dan metode untuk mendapatkan barang bukti digital yang berasal dari *internal device* perangkat IoT.

Pada penelitian ini dilakukan proses forensik perangkat IoT pada *device level* secara sistematis sehingga didapatkan karakteristik bukti digital yang ditemukan. Untuk mendukung proses forensik dikembangkan juga purwarupa perangkat *Internet of Things* berupa sistem *smart home*.

2. METODOLOGI PENELITIAN

Proses penelitian dibuat sistematis sehingga dapat digunakan dalam menyelesaikan masalah dan membuat analisa terhadap hasil penelitian. Pada Gambar 1 dapat dilihat tahapan penelitian yang dilakukan.



Gambar 1. Alur Metodologi Penelitian

2.1 *Literature Review*

Literatur review dilakukan untuk mendapatkan informasi terbaru terkait topik-topik yang akan diteliti yang didapatkan dari referensi buku, artikel, dokumen, atau bahan tertulis lain yang berupa laporan hasil penelitian terdahulu yang telah dipublikasikan. Referensi tersebut didapatkan dari

sumber bersifat daring (*online*) maupun luring (*offline*).
Informasi terbaru dari topik-topik terkait penelitian yang akan dilakukan perlu digali secara mendalam untuk mendapatkan informasi hal-hal yang sudah pernah dilakukan dan belum dilakukan pada topik penelitian ini.

Liu (Liu, 2015) menyampaikan beberapa kasus yang terjadi menyangkut infrastruktur perangkat *Internet of Things*. Infrastruktur IoT harus dibangun secara matang sehingga meminimalisir adanya kerentanan celah keamanan. Menurut (Oriwoh, Jazani, Epiphaniou, & Sant, 2013) perangkat IoT dapat melibatkan *cloudsystem,* sistem virtualisasi, perangkat *mobile, fixed computer*, teknologi sensor serta RFID, dan teknologi kecerdasan buatan. Investigasi forensik dapat mencakup seluruh elemen tersebut.

Penelitian yang dilakukan (Jeong, Park, Lee, & Kang, 2015) menjelaskan proses investigasi forensik *cloud computing* pada *environment* IoT. Beberapa penelitian lainnya seperti yang dilakukan (Tilva & Rohokale, 2016) juga telah melakukan proses forensik pada perangkat IoT yang berfokus pada forensik jaringan yang menjadi media perangkat IoT dalam bertransfer data. Senada dengan penelitian tersebut (Rizal, Riadi & Prayudi, 2018) juga telah melakukan penelitian untuk melakukan forensik jaringan pada perangkat IoT yang menghasilkan temuan bukti digital yang dapat mendeteksi adanya serangan pada perangkat IoT.

Penelitian yang telah dilakukan oleh (Zawoad & Hasan, 2015) menyimpulkan bahwa kegiatan forensik digital pada perangkat IoT memiliki tiga level forensik yaitu *cloud forensic*, *network forensic*, dan *device level forensic*.

Menurut (Kebande & Ray, 2016) teknik digital forensik yang ada tidak sepenuhnya dapat diterapkan pada infrastruktur *Internet of Things*. Saat ini prosedur dan *tools* forensik digital yang ada tidak dapat memenuhi keberagaman akan sifat infrastruktur perangkat *Internet of Things* yang terdistribusi. Belum dibuatnya standar memunculkan tantangan tersendiri bagi *investigator* forensik dengan obyek *environment* IoT.

Penelitian yang dilakukan oleh (Watson & Dehghantanha, 2016) menemukan kompleksitas forensik digital pada *embedded system* (IoT) antara lain penyimpanan data pada *embedded system* tidak dapat dilakukan dengan metode forensik digital tradisional, dataset bisa berada di banyak lokasi yang berbeda dan data yang berhasil diakusisi terkadang tidak terbaca atau tidak dapat diakses oleh *tool* forensik yang ada. Meffert (Meffert et al., 2017) pada penelitian yang dilakukan membangun *environment* IoT yang *digital forensic friendly.* Bertujuan agar segala aktifitas yang ada pada perangkat dapat terekam dalam sebuah *log* sehingga mudah dalam mengungkap fakta apabila terjadi sebuah insiden. Hal tersebut sebagai antisipasi awal sebelum sebuah insiden kasus terjadi.

Pada penelitian selanjutnya yang dilakukan oleh Perumal (Perumal, Md Norwawi, & Raman, 2015) menyimpulkan bahwa tantangan riset IoT bagi investigator forensik berkaitan dengan ukuran dari obyek *environment* IoT, relevansi, batas jaringan yang tidak jelas pada perangkat IoT, dan terutama metode untuk melakukan penyelidikan pada kasus yang menyangkut IoT menjadi hambatan bagi *investigator*. Sehingga penelitian spesifik sangat perlu dilakukan pada investigasi forensik *environment* IoT.

Pada penelitian (Boztas, Riethoven, & Roeloffs, 2015) dilakukan proses forensik perangkat IoT dengan metode *static forensic* pada *storage* perangkat IoT berupa *Smart* TV. Pada penelitiannya bukti-bukti digital dapat ditemukan dari file-file *log* dari aplikasi *browser* dan *log* jaringan. Penelitian lain (Ramadhan, Prayudi, & Sugiantoro, 2017) menyampaikan bahwa pemilihan *tool* yang tepat dalam kegiatan forensik cukup penting karena akan berpengaruh pada keberhasilan penemuan barang bukti digital, pada penelitian ini telah berhasil melakukan kegiatan forensik dengan metode *static forensic* menggunakan bantuan *tool* Autopsy yang dikembangkan oleh Sleuth Kit. Pada penelitian ini *tool* tersebut akan menjadi *tool* utama dalam melakukan analisis forensik. Senada dengan hal tersebut pada penelitian (Riadi, Umar, & Nasrulloh, 2018) dilakukan perbandingan tiga *tool* forensik dalam melakukan pencarian bukti digital yaitu OSForensic, Autopsy, dan Winhex. Diantara tiga *tool* tersebut didapatkan Autopsy merupakan *tool* yang paling banyak dalam menemukan bukti digital pada investigasi *static forensic.*

2.2 Identifikasi Kebutuhan Sistem

Pada penelitian ini akan dibangun *prototype* perangkat *internet of things* yang diterapkan dalam sebuah rumah. Perangkat *internet of things* tersebut akan menjadikan rumah tersebut menjadi sebuah rumah cerdas. Dalam membangun *environment* IoT sebagai obyek penelitian ini dibutuhkan dukungan *hardware* serta *software*.

Spesifikasi kebutuhan *hardware* dalam penelitian ini yaitu Raspberry pi 3 Model B+ sebagai pengendali perangkat IoT yang dilengkapi dengan *s*ensor suhu DHT22, *LED, photoresistor* (sensor cahaya), dan modul sensor hujan MD-0127. Selanjutnya untuk kebutuhan investigasi forensik menggunakan komputer PC dengan spesifikasi prosesor AMD APU A8, RAM 8GB, LCD monitor, k*eyboard* dan *mouse.* Selain itu dibutuhkan komputer dengan spesifikasi standar komputer *server* untuk tempat menginstal *platform* IoT.

Kebutuhan perangkat lunak yang digunakan untuk perangkat *internet of things* dan kebutuhan forensik dalam penelitian ini antara lain sistem operasi Centos *server* untuk *server platform* IoT.

Sistem operasi Raspbian, Fedberry, Ubuntu Mate, dan Kali Linux yang ditanamkan pada Raspberry pi 3 Model B+ *board.* Untuk proses investigasi dibutuhkan sistem operasi Windows 10 dan serta perangkat lunak *tool* forensik yaitu FTK Imager, Thumbscrew USB Writeblocker, OS Forensic, dan Autopsy.

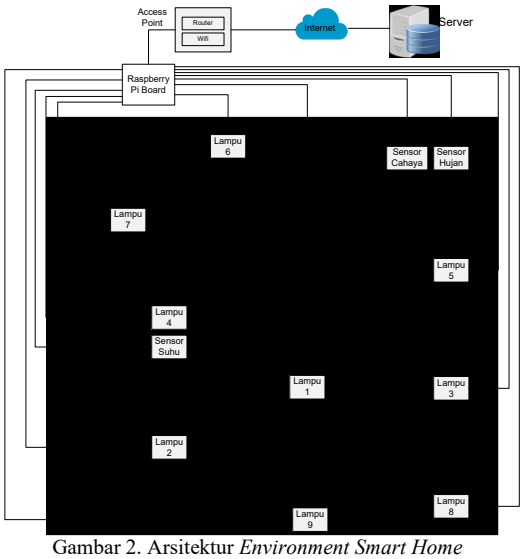
3. PERANCANGAN SISTEM

Seperti yang sudah disampaikan pada bagian sebelumnya, pada penelitian ini dikembangkan *prototype* perangan IoT berupa *smart home* yang selanjutnya dilakukan simulasi kasus serta analisis forensik pada level *device. Prototype* perangkat IoT didukung oleh perangkat komputer mini Raspberry pi 3 Model B+. Menurut (Akbar, Henryranu, Handono, & Basuki, 2017) perangkat Raspberry pi yang dilengkapi dengan *port* GPIO (*General Purpose Input Output*) dapat digunakan sebagai pengendali sebuah perangkat rumah cerdas. Dalam penelitian ini Raspberry pi akan dijadikan pengendali pada *environment* IoT berbentuk *smart home.* Dengan menerapkan sistem *smart home* pada rumah dapat menekan biaya pengeluaran untuk kebutuhan listrik karena apabila pemilik rumah lupa mematikan perangkat elektronik, dari jarak jauh dapat mengendalikan perangkat tersebut (Masykur & Prasetiyowati, 2017).

Perangkat IoT dikendalikan Raspberry pi yang ditanamkan pada perangkat IoT. Raspberry pi layaknya sebuah komputer mini yang dapat diinstall sistem operasi dan aplikasi. Proses forensik pada sistem komputer pada umumnya telah banyak ditemukan *framework* yang telah dibuat yang sudah menjadi standar. Namun proses forensik pada perangkat IoT belum banyak ditemukan *framework* standar yang menjadi sebuah kesepakatan.

3.1. Arsitektur *Prototype* Perangkat *Smart Home*

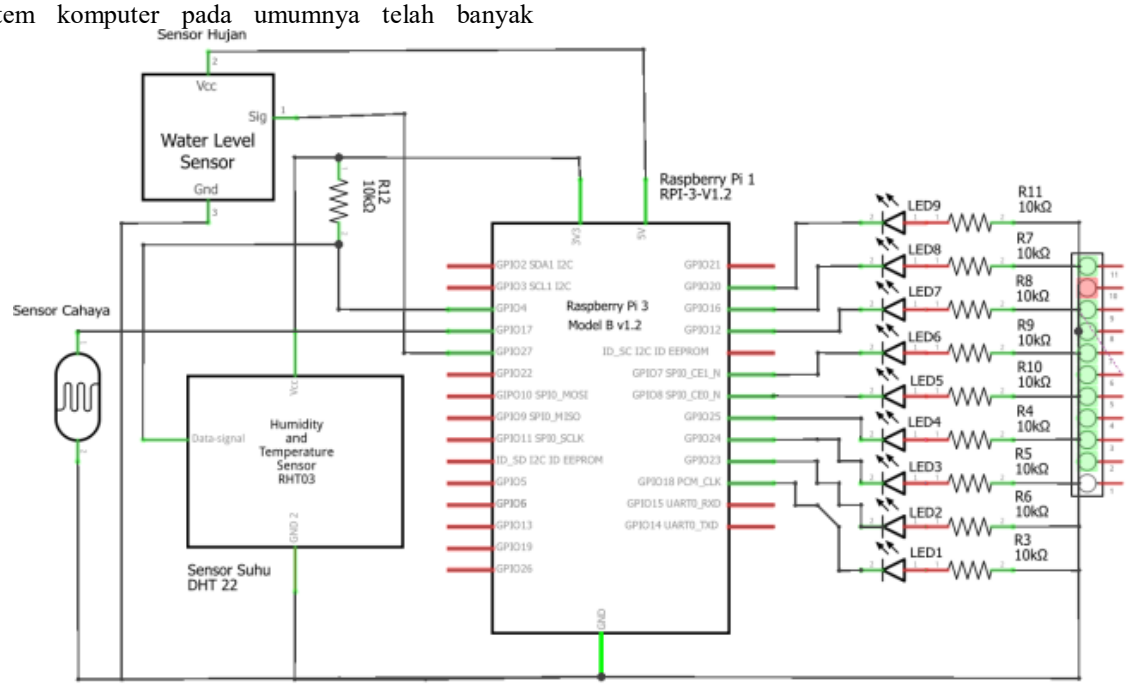
Rancangan arsitektur perangkat *smart home* dapat dilihat pada Gambar 2.



Gambar 2. Arsitektur *Environment Smart Home*

3.2. Skema Rangkaian Modul Sensor IoT

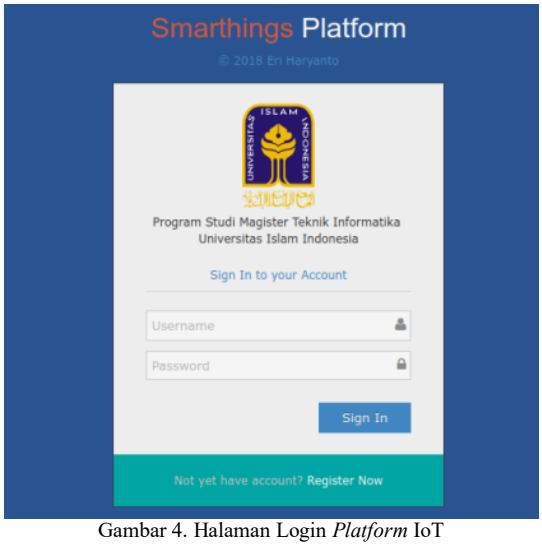
Pada Gambar 3 dapat dilihat skema elektronik perangkat IoT berupa komponen sensor dan komponen keluaran.



Gambar 3. Skema rangkaian modul sensor IoT

3.3. Skema Rangkaian Modul Sensor IoT

Pada penelitian ini turut dikembangkan sebuah *platform* IoT berbasis web yang dipasang pada *server*.

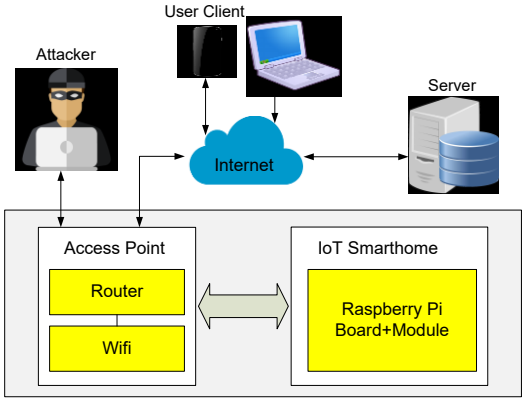


Gambar 4. Halaman Login *Platform* IoT

Gambar 4 menunjukkan halaman login *platform* IoT yang menjadi *dashboard* untuk melakukan *monitoring* dan *remote* perangkat IoT.

3.4. Simulasi Kasus

Pada gambar 5 dapat dilihat topologi skenario kasus yang akan diungkap dan ditemukan fakta kasus oleh investigator forensik.



Gambar 5. Simulasi Kasus pada Perangkat *Internet Of Things*

Penyerang menyusup ke dalam perangkat IoT melalui perangkat *access point* yang digunakan oleh sistem *smart home.* Penyerang akan menanamkan sebuah *malware* ke dalam sistem *smart home*.

Pada Gambar 6 menunjukkan alur penyerangan yang menyerang sistem *smart home.*

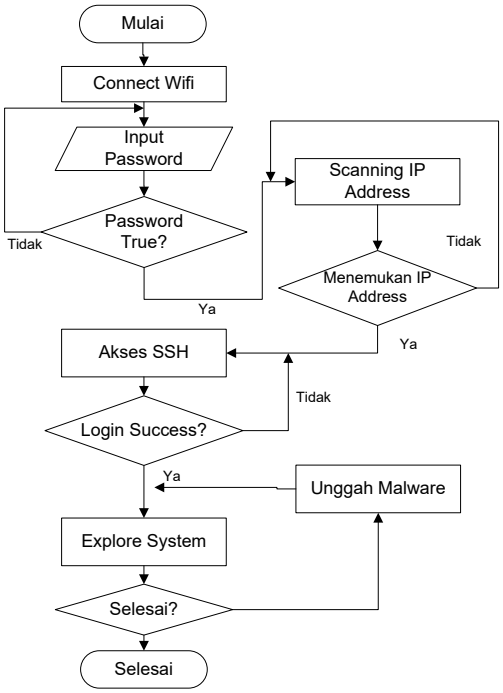
4. HASIL DAN PEMBAHASAN

4.1. Implementasi Forensik Perangkat IoT pada level *Device*

Forensik perangkat IoT pada level *device* akan melibatkan media penyimpanan perangkat IoT yaitu *storage (*media penyimpanan) yang berbentuk kartu *micro* SD. Ruang lingkup penelitian ini adalah untuk mengetahui karakteristik barang bukti yang dapat ditemukan pada berbagai sistem operasi Raspberry pi yang digunakan untuk mengendalikan perangkat IoT.

Media penyimpanan pada perangkat Raspberry pi akan dilakukan *imaging* atau duplikasi dengan *tool* FTK *Imager*. File hasil *imaging* ini yang selanjutnya akan dilakukan pengolahan lebih lanjut untuk dilakukan forensik untuk menemukan bukti-bukti digital. Untuk menjaga integritas file *image*, maka perlu dilakukan *hashing* pada file tersebut menggunakan algoritma MD5 *Hash*. Setiap bukti digital ditemukan akan dicatat dan disajikan pada laporan. Proses tersebut akan dilakukan pada 4 sistem operasi yang digunakan pada penelitian ini yaitu Raspbian, Fedberry, Ubuntu Mate, dan Kali Linux

Untuk melestarikan bukti-bukti digital maka investigasi forensik dilakukan sesuai dengan prinsip-prinsip digital forensik. Bertujuan agar barang bukti legal untuk dibawa ke meja persidangan. Investigasi menggunakan analisis model forensik *collection, examination, analysis,* dan *reporting.*



Gambar 6. Alur Penyerangan ke Sistem *Smart Home*

4.2. Analisis Model Forensik

4.2.1. Tahap Pengumpulan (*Collection*)

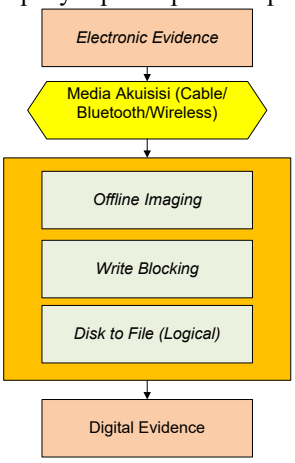
Pada penelitian ini untuk mendapatkan karakteristik barang bukti dari bermacam-macam sistem operasi, maka perangkat Raspberry pi akan diinstall 4 sistem operasi berbeda yang mendukung perangkat yang berbasis arsitektur ARM ini. Sistem operasi yang diinstal dapat dilihat pada tabel 1.

Tabel 1. Daftar Sistem Operasi Pengendali Perangkat IoT

No	Sistem Operasi	Basis	Pengembang
1	Raspbian	Linux	Raspberry Pi Foundation
2	Fedberry	Linux	Fedberry Organization
3	Ubuntu Mate	Linux	Ubuntu MATE Team
4	Kali Linux	Linux	Offensive Security

Pada tahap ini investigator mendapatkan informasi awal mengenai sistem operasi yang digunakan pada perangkat IoT. Empat sistem operasi yang menjadi obyek penelitian diketahui berbasis Linux. Sistem operasi Linux merupakan sistem operasi dengan sumber terbuka dan gratis dalam distribusinya.

Selanjutnya akan dilakukan pengumpulan barang bukti dari hasil akuisisi data *image* pada sistem operasi yang mengendalikan perangkat IoT. Proses akuisisi perangkat IoT dapat dilakukan menggunakan dua metode, metode pertama perintah atau *command* akuisisi dijalankan langsung pada *terminal console* sistem operasi pengendali *smart home* yaitu raspberry pi 3 Model B+ pada saat sistem dalam keadaan hidup. Metode selanjutnya perintah atau proses akuisisi dijalankan dengan menggunakan komputer investigator dengan melakukan *cloning* "2 *bit stream*" terhadap barang bukti, dalam hal ini adalah media penyimpanan pada Raspberry pi.



Gambar 7. Proses Akuisisi Perangkat *Smart Home*

Metode akuisisi dengan *live system* saat sistem sedang berjalan rentan adanya kontaminasi ke dalam sistem IoT, maka pada penelitian ini digunakan metode yang kedua yaitu *investigator* melakukan *cloning* "2 *bit stream*" media penyimpanan Raspberry Pi berbentuk kartu *Micro* SD yang merupakan sumber barang bukti dalam keadaan sistem mati (OFF), barang bukti diambil dan dianalisis tanpa menghidupkan sistem. Dengan metode ini menurut (Albanna & Riadi, 2017) pencarian bukti digital dapat dilakukan dengan berbagai teknik antara lain *recover deleted file*, *carving tipe file*, pencarian dengan string, dll. Proses akuisisi yang dilakukan ditunjukkan pada Gambar 7.

Proses akusisi barang bukti media penyimpanan perangkat IoT dilakukan dengan menggunakan bantuan *tool* FTK Imager buatan Perusahaan Access Data. Untuk menjaga agar barang bukti tidak terkontaminasi oleh akses sistem maka terlebih dahulu pada komputer *investigator* dilakukan pemasangan *tool* untuk mencegah USB *WriteAccess* dengan menggunakan *tool* Thumbscrew *USB WriteBlocker*. Selanjutnya *Hash* dari *image file* akan dibuat untuk menjaga integritas barang bukti.

4.2.2.Tahap Pemeriksaan (*Examination*)

Investigator akan memeriksa *image file* yang telah didapatkan dari hasil akuisisi sistem operasi perangkat IoT yang menjalankan *smart home.* Proses pemeriksaan akan melakukan *mounting* dan ekstraksi data pada *image file* dan investigator forensik akan mengeksplorasi data yang mencurigakan sebagai data pendukung dalam mengungkap kasus. Skenario kasus pada bagian sebelumnya menjelaskan bahwa penyerang melakukan akses ilegal terhadap sistem IoT melalui protokol SSH yang ada pada sistem. Sesuai arsitektur *environment* IoT yang ada, perangkat IoT terhubung ke sebuah perangkat jaringan berupa *router* untuk terhubung ke jaringan internet global.

4.2.3. Tahap Analis (*Analysis*)

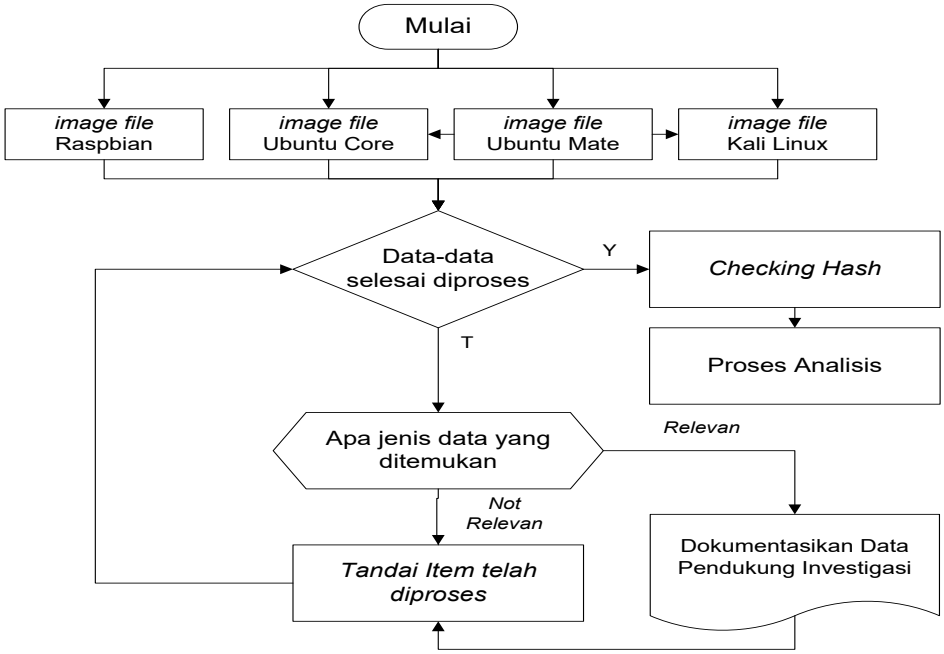
Tahap ini dilakukan analisis mendalam dari temuan file pada tahap pemeriksaan. Pada tahap sebelumnya ditemuan bukti-bukti digital yang dikategorikan sebagai berikut: *log* SSH, histori perintah terminal, *log browser*, konfigurasi jaringan, wifi ssid, file crontab, file *malware*, dan *logsystem*.

Dari pemeriksaan komprehensif artefak digital yang ditemukan, investigator merumuskan *timeline* dari fakta kasus berupa *timestamp* dan aktifitas penyerang. Dalam proses forensik, *timestamp* ibarat tambang emas dikarenakan ditemukannya sebuah bukti digital yang dilengkapi atribut *timestamp* yang relevan dapat mengantarkan investigator untuk mendapatkan fakta kasus yang ingin diungkap.

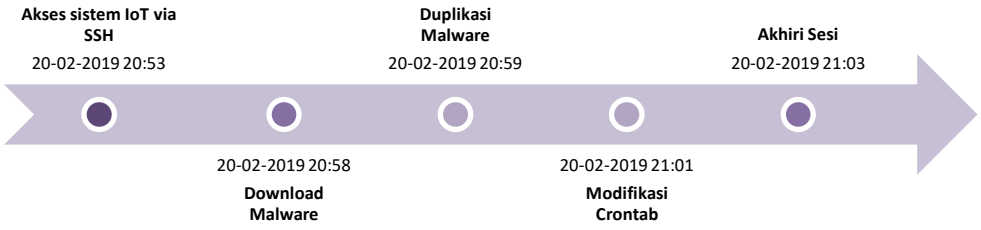
Ditemukan jejak berupa artefak digital pada hasil pemeriksaan *image file* perangkat IoT dengan sistem operasi Raspbian. Aktifitas penyerang dapat dilihat pada Gambar 9. Dari *timeline* terlihat jelas aktifitas penyerang terhadap sistem, didukung timestamp yang menunjukkan terjadinya serangan.

Gambar 10 menunjukkan penemuan jejak berupa artefak digital pada hasil pemeriksaan *image file* perangkat IoT dengan sistem operasi Fedberry. Dari *timeline* terlihat jelas aktifitas penyerang terhadap sistem, didukung *timestamp* yang menunjukkan terjadinya serangan.

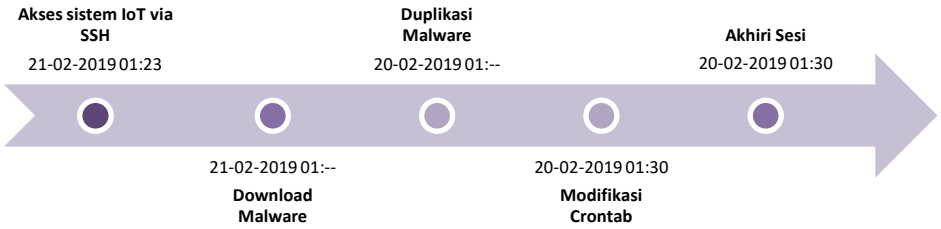
Ditemukan jejak berupa artefak digital pada hasil pemeriksaan image file perangkat IoT dengan sistem operasi Ubuntu Mate. Aktifitas penyerang dapat dilihat pada Gambar 11. Dari *timeline* terlihat jelas aktifitas penyerang terhadap sistem, didukung *timestamp* yang menunjukkan terjadinya serangan.



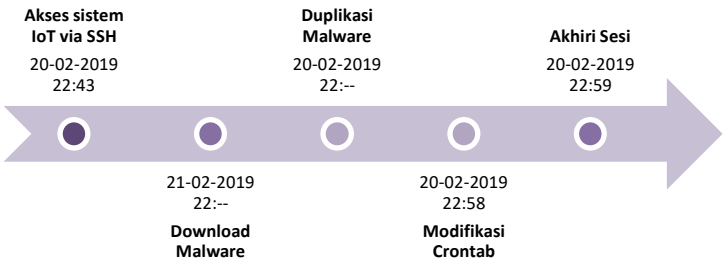
Gambar 8. Proses pemeriksaan barang bukti.



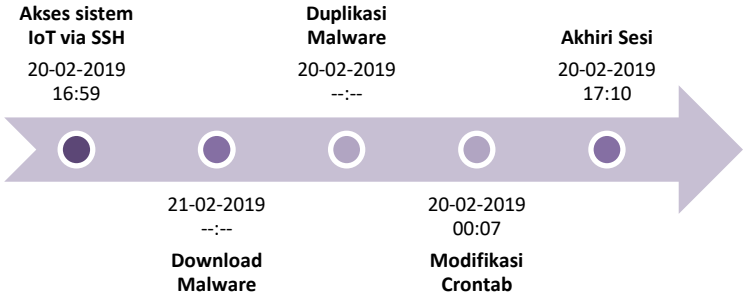
Gambar 9. *Timeline* Aktifitas Penyerang pada Sistem IoT dengan OS Raspbian



Gambar 10. *Timeline* Aktifitas Penyerang pada Sistem IoT dengan OS Fedberry



Gambar 11.*Timeline* Aktifitas Penyerang pada Sistem IoT dengan OS Ubuntu Mate



Gambar 12.*Timeline* Aktifitas Penyerang pada Sistem IoT dengan OS Kali Linux

Ditemukan jejak berupa artefak digital pada hasil pemeriksaan image file perangkat IoT dengan sistem operasi Kali Linux. Aktifitas penyerang dapat dilihat pada Gambar 12. Namun dari *timeline* terlihat ada kejanggalan yang ditemukan. Pada aktifitas "akhiri sesi" memiliki timestamp yang jauh lebih awal dari aktifitas modifikasi crontab. Dari temuan ini investigator tidak dapat menyimpulkan bahwa pengungkapan kasus berhasil dilakukan pada OS ini. Karena ketidakkonsistenan timestamp tersebut akan sulit dalam pembuktian di meja persidangan.

4.2.4. Tahap Pelaporan (*Reporting*)

Berdasarkan hasil analisis dan pengamatan dari kegiatan forensik perangkat IoT pada level *device* menunjukkan bahwa perangkat Raspberry pi 3 Model B+ yang mengendalikan sistem *smart home* dapat dilakukan akuisisi dengan dibuat *cloning* dari media penyimpanan perangkat tersebut. Akuisisi akan membentuk sebuah *image file* yang besarnya sekitar 16 GB sama dengan ukuran kartu Micro SD yang menjadi media penyimpanan yang terpasang pada perangkat.

Proses akuisisi memakan waktu yang berbeda-beda dari masing-masing sistem operasi yang digunakan. Raspberry pi dengan OS Raspbian memakan waktu akuisisi selama 9 menit 48 detik, dengan OS Fedberry memakan waktu akuisisi selama 10 menit 3 detik, dengan OS Ubuntu Mate memakan waktu akuisisi selama 9 menit 43 detik dan dengan OS Kali Linux memakan waktu akuisisi selama 13 menit 51 detik. Hasil *cloning* berbentuk *image file* dilakukan *hashing* untuk mendapatkan kode *hash* dengan algoritma md5 dan sha1. Kode *hash* tersebut akan menjamin integritas *image file* selama dilakukan perpindahan atau distribusi file, mulai dari tahap *collection* sampai dengan *reporting.*

Hasil analisis membuktikan bahwa serangan terhadap *environment* IoT dengan menginfeksi sistem dengan *malware malware* dapat diungkap fakta kasusnya berdasarkan temuan-temuan yang dijadikan barang bukti digital. Diketahui bahwa penyerang adalah pemilik komputer dengan IP Address 192.168.8.104 yang ditemukan pada log SSH.

4.3.Komparasi Karakteristik Bukti-bukti Digital

Dengan membandingkan hasil analisis forensik dari 4 sistem operasi (Raspbian, Fedberry, Ubuntu Mate, Kali Linux) yang diinstal pada Raspberry pi IoT maka didapatkan karakteristik bukti-bukti digital yang ditemukan. Karakteristik ini akan berupa perbedaan-perbedaan yang mungkin ada dari analisis temuan bukti digital. Pada tabel 2 dapat dilihat karakteristik lama waktu akuisisi barang bukti.

Tabel 2. Komparasi Karakteristik Lama Waktu Akuisisi Barang Bukti

item pembanding	raspbian	fedberry	ubuntu mate	kali linux
waktu akuisisi	9 menit 48 detik	10 menit 3 detik	9 menit 43 detik	13 menit 51 detik
ukuran file	15193 MB	15193 MB	15193 MB	15193 MB

Pada tabel 3 dapat dilihat karakteristik lokasi bukti digital yang ditemukan pada perangkat IoT.

Pada tabel 4 dapat dilihat karakteristik relevansi temuan bukti digital terhadap fakta kasus.

Pada analisis image file perangkat IoT dengan sistem operasi Kali Linux dapat disimpulkan bahwa ditemukan ketidakkonsistenan timestamp pada rumusan timeline. Sehingga fakta kasus tidak dapat ditemukan secara pasti.

Tabel 4. Komparasi Karakteristik Relevansi Bukti Digital terhadap Kasus

kategori	raspbian	fedberry	ubuntu mate	kali linux
***log* ssh**	✓	✓	✓	✓
histori perintah terminal	✓	✓	✓	✓
log browser	✓	×	×	×
konfigurasi jaringan	×	×	×	×
wifi ssid	✓	×	✓	✓
file crontab	✓	✓	✓	✓
file *malware*	✓	✓	✓	✓
logsystem	×	×	×	×

Tabel 3. Komparasi Karakteristik Lokasi Bukti Digital

kat.	raspbian	fedberry	ubuntu mate	kali linux
Log SSH	/var/log/auth.log	/var/log/ secure	/var/log/auth.log	/var/log/auth.log
Histori perintah terminal	/root/.bash_history	/root/.bash_history	/root/.bash_history	/root/.bash_history
Log browser	/home/pi/.config/chromium/Default/ History /home/pi/.config/chromium/Default/ Current Session /home/pi/.config/chromium/Default/ DownloadMetadata	/home/pi/.config/chromium/Default/ History /home/pi/.config/chromium/Default/ Current Session /home/pi/.config/chromium/Default/ DownloadMetadata	/home/pi/.mozilla/firefox/mjufxgzi.default/Cookies.sqlite /home/pi/.mozilla/firefox/mjufxgzi.default/Places.sqlite	/root/.mozilla/firefox/13dokg21.default/Cookies.sqlite /root/.mozilla/firefox/13dokg21.default/ Places.sqlite
Konfigurasi Jaringan	/etc/network/ interfaces	/etc/NetworkManager/ NetworkManager.conf	/etc/NetworkManager/ NetworkManager.conf	/etc/NetworkManager/NetworkManager.conf
Wifi SSID	/etc/wpa_supplicant/ wpa_supplicant.conf	/etc/wpa_supplicant/ wpa_supplicant.conf	/etc/ NetworkManager/system-connection/Mister_A_wifi	/etc/ NetworkManager/system-connection/Mister_A_wifi
File Crontab	/var/spool/cron/crontab/root	/var/spool/cron/crontab/root	/var/spool/cron/crontab/root	/var/spool/cron/crontab/root
File Malware	/home/sim/ malware.py /var/tmp/ malware.py	/home/sim/ malware.py /var/tmp/ malware.py	/home/sim/ malware.py /var/tmp/ malware.py	/home/sim/ malware.py /var/tmp/ malware.py
Log System	/var/log/ syslog	-	/var/log/ syslog	/var/log/ syslog

Pada tabel 5 dapat dilihat karakteristik keberhasilan pengungkapan fakta kasus.

Tabel 5. Komparasi Keberhasilan Pengungkapan Kasus Berdasarkan Analisis *Timeline*

	raspbian	fedberry	ubuntu mate	kali linux
berhasil	✓	✓	✓	
gagal				✓

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Environment berupa *smarthome* berhasil menjadikan rumah biasa menjadi rumah cerdas yang dilengkapi dengan sensor suhu, sensor hujan, sensor cahaya, dan modul lampu yang dapat dipantau dan dikendalikan dari jarak jauh.

Investigasi menggunakan analisis model forensik *collection*, *examination*, *analisys*, dan *reporting* pada investigasi forensik level *device* perangkat IoT telah membantu investigator dalam menemukan barang bukti digital untuk mengungkap kasus. Sehingga dapat disajikan bukti digital yang legal untuk dibawa di meja persidangan.

Didapatkan karakteristik barang bukti digital dari ekstraksi *image file* hasil akuisisi media penyimpanan perangkat Raspberry pi 3 Model B+. Sistem operasi Raspbian, Fedberry, Ubuntu Mate dan Kali Linux menyimpan bukti-bukti digital yang berbeda-beda lokasi walaupun sama-sama berbasis Linux. Dari temuan bukti-bukti digital tidak seluruhnya relevan dengan pengungkapan fakta kasus yang terjadi.

5.2 Saran

Untuk melengkapi penelitian ini, pada penelitian berikutnya dapat dikembangkan dengan penggunaan beberapa aplikasi akuisisi untuk membandingkan temuan barang bukti digital. Mengingat ruang lingkup forensik pada *environment* IoT sangat luas pada penelitian ini hanya fokus pada forensik *device level* perangkat IoT, sehingga pada penelitian selanjutnya dapat dikembangkan *framework* forensik perangkat IoT yang mengintegrasikan 3 level forensik IoT, yaitu level perangkat, level jaringan, dan level *cloud server*.

DAFTAR PUSTAKA

AKBAR, S. R., HENRYRANU, B., HANDONO, M. T., & BASUKI, A.,2017. Implementasi Purwarupa Perangkat Rumah Cerdas Pervasif Berbasis Protokol Universal Plug And Play (UPnP) Dan Raspberry Pi General Purpose Input/Output (GPIO). *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *2*(2), 116. https://doi.org/10.25126/jtiik.201522143

ALBANNA, F., & RIADI, I., 2017. Forensic Analysis of Frozen Hard Drive Using Static Forensics Method. *International Journal of Computer Science and Information Security*, *15*(1), 173–178. https://doi.org/10.13140/RG.2.1.2967.0003

BOZTAS, A., RIETHOVEN, A. R. J., & ROELOFFS, M., 2015. Smart TV forensics: Digital traces on televisions. *Digital Investigation*, *12*(S1), S72–S80. https://doi.org/10.1016/j.diin.2015.01.012

JEONG, D., PARK, J., LEE, S., & KANG, C., 2015. Investigation methodology of a virtual desktop

infrastructure for IoT. *Journal of Applied Mathematics*, *2015*. https://doi.org/10.1155/2015/689870

KEBANDE, V. R., & RAY, I., 2016. A generic digital forensic investigation framework for Internet of Things (IoT). *Proceedings - 2016 IEEE 4th International Conference on Future Internet of Things and Cloud, FiCloud 2016*, 356–362. https://doi.org/10.1109/FiCloud.2016.57

LIU, J., 2015. IoT Forensics Issues strategies and challenges. *12 IDF Annual Conference*.

MASYKUR, F., & PRASETIYOWATI, F., 2017. Aplikasi Rumah Pintar (Smart Home) Pengendali Peralatan Elektronik Rumah Tangga Berbasis Web. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *3*(1), 51. https://doi.org/10.25126/jtiik.201631156

MEFFERT, C. S., CLARK, D. R., BAGGILI, I., BREITINGER, F., MEFFERT, C., & CLARK, D., 2017. Digital Commons @ New Haven Forensic State Acquisition from Internet of Things (FSAIoT): A General Framework and Practical Approach for IoT Forensics through IoT Device State Acquisition Forensic State Acquisition from Internet of Things (FSAIoT): A gener, *2017*. Retrieved from http://digitalcommons.newhaven.edu/%0Ahttps://doi.org/10.1145/3098954.3104053

ORIWOH, E., JAZANI, D., EPIPHANIOU, G., & SANT, P., 2013. Internet of Things Forensics: Challenges and Approaches. *Proceedings of the 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing*, (December), 608–615. https://doi.org/10.4108/icst.collaboratecom.2013.254159

OSMAN, Y., OSEI, A., & NARENDRA, B. C., 2016). A Review of Prospects and Challenges of Internet of Things. *International Journal of Computer Applications*, *139*(April), 33–39. https://doi.org/10.5120/ijca2016909390

PERUMAL, S., MD NORWAWI, N., & RAMAN, V., 2015. Internet of Things(IoT) digital forensic investigation model: Top-down forensic approach methodology. *2015 5th International Conference on Digital Information Processing and Communications, ICDIPC 2015*, 19–23. https://doi.org/10.1109/ICDIPC.2015.7323000

RAMADHAN, R. A., PRAYUDI, Y., & SUGIANTORO, B., 2017. Implementasi dan Analisis Forensika Digital Pada Fitur Trim Solid State Drive (SSD). *Teknomatika*, *9*(2), 1–13. Retrieved from http://teknomatika.stmikayani.ac.id/wp-content/uploads/2017/07/1.pdf

RIADI, I., UMAR, R., & NASRULLOH, I. M., 2018. Analisis Forensik Digital Pada Frozen Slod State Drive Dengan Metode National Institute of Justice (Nij), *3*(May), 70–82. https://doi.org/10.21831/elinvo.v3i1.19308

RIZAL, R., RIADI, I., & PRAYUDI, Y., 2018. Network Forensics for Detecting Flooding Attack on Internet of Things (IoT) Device. *Int. J. Cyber-Security Digit. Forensics*, *7*(4), 382–390.

TILVA, M., & ROHOKALE, V., 2016. Network Forensics for detection of malicious packets in Internet of Things (IoT), (June), 114–118.

WATSON, S., & DEHGHANTANHA, A., 2016. Digital forensics: the missing piece of the Internet of Things promise. *Computer Fraud and Security*, *2016*(6). https://doi.org/10.1016/S1361-3723(15)30045-2

WILIANTO, & KURNIAWAN, A., 2018. Sejarah , Cara Kerja Dan Manfaat Internet of Things. *Matrix*, *8*(2), 36–41.

ZAWOAD, S., & HASAN, R., 2015. FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things. *Proceedings - 2015 IEEE International Conference on Services Computing, SCC 2015*, 279–284. https://doi.org/10.1109/SCC.2015.46