BAB 2
Tinjauan Pustaka

2.1 Kajian Penelitian Terdahulu

Sudah dilakukan berbagai analisis yang bertujuan melakukan forensik terhadap perangkat *Internet of Things*, salah satunya yang telah dilakukan oleh Boztas (Boztas, Riethoven, & Roeloffs, 2015). Forensik dilakukan pada perangkat *smart* TV. Perangkat tersebut biasanya dimanfaatkan untuk menonton video, media sosial, dan pesan instan. *Smart* TV dilengkapi kemampuan untuk terhubung ke internet, USB *flashdisk* dan *smart phone.* Hal tersebut menjadikan *Smart* TV menjadi sumber barang bukti digital yang berpotensi untuk dilakukan forensik. Pada penelitian tersebut diusulkan prosedur untuk akuisisi, analisa, dan investigasi *Smart TV*.

Penelitian yang dilakukan oleh Jeong (Jeong, Park, Lee, & Kang, 2015), telah dilakukan eksperimen untuk mendapatkan barang bukti digital dari infrastruktur *internet of things*. Barang bukti didapatkan dari infrastruktur *cloud computing* yang berbentuk *virtual machine*. Saat ini banyak perusahaan yang memanfaatkan solusi *cloud computing* untuk memangkas biaya dan efisiensi kerja dari *server*. Dalam melakukan investigasi pada infrastruktur IoT ini, dibuat prosedur investigasi yang sistematis untuk meminimalkan adanya kerusakan barang bukti. Dalam penelitian yang dilakukan diusulkan metode investigasi untuk infrastruktur IoT di sisi penyimpanan data pada komputer virtual.

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. Pada penelitian tersebut mengenalkan model untuk melakukan identifikasi obyek forensik dalam proses investigasi yang menggabungkan *triage model* dan 1-2-3 *zone model*. Dengan pendekatan 1-2-3 *zone model* proses forensik melibatkan 3 zona forensik yaitu: zona 1 yang merupakan zona internal yang melibatkan seluruh *hardware* dan *software* IoT seperti sensor dan modul jaringan, zona 2 merupakan zona komunikasi perangkat dengan *cloud server* melalui jaringan internet, dan zona 3 melibatkan seluruh *hardware* dan *software* di luar perangkat IoT (Oriwoh, Jazani, Epiphaniou, & Sant, 2013). Pada zona 3 barang bukti dapat berasal dari *cloud server* atau *Internet Service Provider* (ISP).

Liu (Liu, 2015) menyampaikan beberapa kasus yang terjadi menyangkut infrastruktur perangkat *Internet of Things*. Infrastruktur IoT harus dibangun secara matang sehingga meminimalisir adanya celah yang bisa saja dimanfaatkan oleh pihak yang tidak bertanggung jawab. Pada penelitian yang dilakukan disampaikan ada perusahaan perangkat jaringan yang telah memproduksi ribuan perangkat *Internet of Things* yang ternyata memiliki celah dan celah tersebut berhasil diekspos ke publik oleh *hacker*. Atas kejadian tersebut perusahaan mendapatkan sanksi memberikan ganti rugi kepada pihak yang dirugikan. Sebagai contoh lain juga disampaikan sebuah kasus skandal yang melibatkan sebuah perusahaan otomotif. Perangkat IoT yang ditanamkan di kendaraan yang diproduksinya telah melakukan manipulasi hasil uji tes emisi. Sehingga hasil penilaian uji emisi pada kendaraan tersebut tidak valid karena pada kenyataannya kendaraan yang lolos uji emisi tersebut sebenarnya menghasilkan emisi *nitrogen oxides* (Nox) yang 40 kali lebih besar dari batas emisi yang diijinkan oleh undang-undang negara setempat. Penelitian tersebut juga memaparkan tantangan dalam melakukan forensik perangkat *Internet of Things* antara lain:

1. Forensik pada perangkat *Internet of Things* adalah cabang forensik digital baru atau bahkan bisa menjadi sebuah cabang forensik sendiri.
2. Apapun yang berhubungan dengan teknologi IoT senantiasa berubah-ubah.
3. IoT merupakan evolusi era digital.
4. IoT merupakan *environment* baru baik di sisi perangkat keras maupun perangkat lunak.
5. Dunia *cyber* yang menjadi domain IoT membutuhkan usulan undang-undang hukum baru agar lebih bisa diterima oleh masyarakat.
6. Perlu adanya kerjasama antar negara untuk investigasi infrastruktur IoT, karena melibatkan banyak negara dalam melakukan investigasinya.

Penelitian yang telah dilakukan oleh Zawoad (Zawoad & Hasan, 2015) telah memberikan pencerahan kepada investigator forensik. Menurutnya forensik digital pada perangkat *Internet of Things* memiliki tiga level forensik, yaitu *cloud forensic*, *network forensic*, dan *device level forensic*. Forensik pada IoT adalah cabang forensik digital yang spesial dimana proses identifikasi, koleksi, organisasi, dan presentasi berhubungan dengan infrastruktur IoT. Proses tersebut memiliki tujuan yaitu mengungkapkan fakta atas tindakan kriminal yang terjadi. *Model Forensics-aware* IoT (FAIoT) menjadi usulan dalam penelitian yang dilakukannya untuk mendukung investigasi forensik pada *environment Internet of Things*.

Teknik digital forensik yang ada tidak sepenuhnya dapat diterapkan pada infrastruktur *Internet of Things* (Kebande & Ray, 2016). Saat ini prosedur dan *tools* forensik digital yang ada tidak dapat memenuhi keberagaman akan sifat infrastruktur perangkat *Internet ofThings* yang terdistribusi. Pada penelitiannya telah dihasilkan *Digital Forensic Investigation Framework* untuk IoT (DFIF-IoT) yang dapat mendukung investigasi perangkat IoT di masa akan datang. *Framework* dibuat sesuai dengan ISO/IEC 27043: 2015 yang merupakan standar internasional tentang teknologi informasi, keamanan, serta memuat prinsip dan proses investigasi atas sebuah kejadian. Menurut Kebande, dengan DFIF-IoT *framework* akan membuat proses investigasi forensik digital dari perangkat *Internet of Things* lebih efisien.

Menurut Tilva (Tilva & Rohokale, 2016) kemajuan teknologi baru dalam segala bidang juga memunculkan tantangan baru di bidang investigasi forensik khususnya bagi investigator forensik digital. Alur proses dan peralatan forensik yang ada tidak dapat memenuhi kebutuhan infrastruktur IoT. Menemukan barang bukti digital pada komponen yang terinfeksi sampai dengan menganalisa barang bukti tersebut pada perangkat IoT menjadi tantangan bagi investigator. Fokus yang dilakukan di dalam penelitian tersebut adalah membangun *environment* IoT untuk simulasi forensik jaringan.

Pada kasus yang melibatkan perangkat *embedded system,* yang menjadi tantangan bagi investigator forensik dalam melakukan investigasi forensik antara lain, perangkat *wearable, drone*, *prototyping* mikrokontroler, peralatan medis, teknologi jaringan sensor, otomatisasi rumah, *Internet of Things*, kendaraan, *printer* 3D, sistem keamanan, sistem akses kontrol, *mobile phone,* dan berbagai alat yang terhubung (Watson & Dehghantanha, 2016). Menurut mereka kompleksitas forensik digital pada *embedded system* antara lain :

1. Penyimpanan data pada *embedded system* tidak dapat dilakukan dengan metode forensik digital tradisional.
2. Dataset bisa berada di banyak lokasi yang berbeda.
3. Data yang berhasil diakusisi terkadang tidak terbaca atau tidak dapat diakses oleh *tool* forensik yang ada.

Pada beberapa kondisi, teknik dalam akuisisi data yang diterapkan untuk mengambil data pada *hardisk* dan *image* perangkat *mobile* juga dapat diterapkan pada teknologi *embedded system.*

Menurut Osman (Osman, Osei, & Narendra, 2016), masa depan internet adalah sebuah dunia baru berupa jaringan yang sangat kuat dari perangkat *smart* yang secara independen dapat berkomunikasi satu sama lain dengan sedikit intervensi oleh manusia,

atau bahkan tanpa intervensi sama sekali. Imbas dari hal tersebut akan memunculkan *smart phones*, *smart homes*, *smart offices*, *smart vehicles*, *smart classrooms*, *smart factories*, *smart farm* dan lingkungan *smart* lainnya yang disebut dengan *internet of things* (IoT). Penelitian tersebut menjelaskan tantangan dan bagaimana forensik digital perangkat IoT sampai dengan mendapatkan barang bukti untuk dibawa ke meja persidangan. Untuk mendapatkan barang bukti dilakukan *realtime digital forensic* untuk mendeteksi dan menganalisa kejadian sesegera mungkin agar mendapatkan barang bukti dari perangkat IoT.

Penelitian yang dilakukan oleh Meffert (Meffert et al., 2017) mengusulkan sebuah *framework* umum untuk melakukan forensik pada perangkat IoT. *Framework* tersebut dirancang agar perangkat IoT dapat selalu mengirimkan kondisi *(state)* ke penyimpanan tersentral, sehingga apabila ada kejadian dapat dilakukan akuisisi pembacaan *state* pada *timestamp saat* kejadian berlangsung. Pada penelitian ini dihasilkan *state of the art* yaitu keterbatasan *log* untuk menyimpan histori akses dan data yang dihapus. Dengan *framework* yang dibuat tidak dapat melakukan akusisi data histori yang ada pada sisi perangkat IoT.

Dari berbagai penelitian berkaitan dengan forensik perangkat IoT belum banyak pembahasan tentang investigasi forensik pada level *device,* hal ini disebabkan cakupan forensik pada infrastruktur IoT sangat luas. Senada dengan yang disampaikan oleh Perumal (Perumal et al., 2015), bahwa kegiatan forensik pada perangkat IoT dapat diklasifikasikan menjadi tiga zona forensik, yaitu *cloud forensic*, *network forensic*, dan *device level forensic*. Hal ini mendorong penulis untuk melakukan penelitian terkait forensik perangkat perangkat IoT fokus pada *device level forensic*.

Agar lebih jelas maka *literatur review* dapat dilihat pada tabel 2.1

Tabel 2.1 *Literature Review* Forensik Level *Device* Perangkat IoT

No	Paper Utama	Proses Forensik	Model	*Scope* Penelitian	Pengujian
1	Jeong, Park, Lee, & Kang, 2015	InvestigasiInfrastuktur *Server*IoT	*Framework* untuk investigasi IoT VDI (*virtual desktop infrastructure)*	IoT *Forensic*	Uji coba akuisisi data dari tiga VDI menggunakan *thin client* komputer
2	Boztas, Riethoven, & Roeloffs, 2015	Akuisisi data dari *smart TV*	Prosedur untuk akuisisi, analisa, dan investigasi *smart television*	IoT *Forensic*	Skenario kasus, demonstrasi keberhasilan sistem sesuai dengan skenario
3	Perumal, Md Norwawi, & Raman, 2015	Komprehensif mulai dari planning sampai dengan penyimpanan barang bukti	Mengintegrasikan model *triage* dan model 1-2-3 *zone*	IoT *Forensic*	-
4	Liu, 2015	-	Tantangan pada forensik IoT, meliputi tahap *identification, preservation, analysis,* dan *presenation*	IoT *Forensic*	-
5	Zawoad & Hasan, 2015	-	Konsep *Forensics-aware* IoT (FAIoT) untuk investigasi infrastruktur IoT	IoT *Forensic*	*Prototype* Sistem dan *Environment*.
6	Kebande & Ray, 2016	Investigasi dengan berpegang pada standar ISO/IEC 27043: 2015	*Generic Digital Forensic Investigation Framework* untuk IoT (DFIF-IoT)		*Prototype* Sistem dan *Environment*.

7	Tilva & Rohokale, 2016	Forensik jaringan pada infrastruktur IoT	Model forensik jaringan untuk mendeteksi *malicious* paket berbasis log	*IoT Network Forensic*	*Prototype* Sistem dan *Environment* serta studi kasus
8	Watson & Dehghantanha, 2016	Akuisisi data pada IoT	-		Komparasi *tools* forensik
9	Osman, Osei, & Narendra, 2016	Forensik digital pada *Internet of Things*	*Realtime Digital Forensic Techniques*	IoT *Forensic*	Studi kasus, melengkapi kekurangan teknik forensik digital tradisional
10	Meffert et al., 2017	Akuisisi log kondisi sensor-sensor pada perangkat IoT	*General Framework and Practical Approach for IoT Forensics through IoT Device State Acquisition* (FSAIoT)	IoT *Forensic*	*Prototype* sistem dan uji coba pembuktian
11	(Babun, Sikder, Acar, & Uluagac, 2018)	Forensik perangkat IoT berbasis log yang dibuat oleh perangkat IoT	IoTDots *Framework*	IoT *Forensic*	*Prototype* sistem dan uji coba pembuktian
Usulan Penelitian					

Solusi yang diusulkan	Analisa forensik infrastruktur IoT yang berfokus pada forensik level *device* pada perangkat IoT	Algoritma forensik *device level* perangkat IoT	IoT *Device Level Forensic*	*Prototype* Sistem dan *Environment*, Skenario kasus, serta demonstrasi keberhasilan *device level forensic* perangkat IoT untuk mendapatkan barang bukti digital.
Usulan Penelitian				
Solusi yang diusulkan	Pertumbuhan perangkat IoT sangat pesat harus diimbangi dengan dibangunnya ekosistem yang baik dan aman. Ketika terjadi insiden yang melibatkan perangkat IoT, investigator forensik bertugas untuk mengumpulkan barang bukti dari perangkat tersebut. Zona forensik IoT yang cukup luas membuat pekerjaan investigator menjadi sangat berat. Kegiatan forensik pada IoT mencakup area *cloud forensic*, *network forensic*, dan *device level forensic.* Saat ini telah banyak dibuat panduan forensik berupa algoritma maupun *framework* dalam investigasi *cloud forensic* dan *network forensic,* akan tetapi belum banyak atau bahkan belum ada solusi *framework* untuk investigasi *device level forensic.* Forensik di level perangkat IoT menjadi solusi yang diusulkan di dalam penelitian ini. Forensik di level ini akan mendapatkan berbagai informasi penting sebagai barang bukti atas sebuah insiden yang terjadi.			

2.2 Landasan Teori

2.2.1 *Internet of Things*

Menurut (Ovidiu & Friess, 2013) *internet of things* merupakan konsep dan paradigma yang luas mencakup lingkungan obyek-obyek yang menggunakan koneksi dengan kabel atau *wireless* yang memiliki alamat unik serta antar obyek dapat berinteraksi satu sama lain dan bekerjasama untuk membuat sebuah *service* baru untuk mencapai tujuan. Tujuan *internet of things* adalah membuat obyek (*thing*) dapat berhubungan kapanpun, dimanapun, dengan apapun, dengan siapapun menggunakan jaringan dan layanan yang ada. Dari definisi tersebut IoT dapat disimpulkan adalah jaringan dari banyak obyek fisik. Internet saat ini tidak hanya merupakan jaringan komputer tetapi telah berkembang menjadi jaringan dari berbagai perangkat dengan banyak tipe dan ukuran, seperti: kendaraan, *smartphone, home applicance,* mainan, gedung, dan obyek lainnya yang saling terhubung dan berkomunikasi serta berbagi informasi berdasarkan protokol yang ditetapkan.

(Patel & Patel, 2016) mendefinisikan IoT menjadi tiga kategori, yaitu *people to people, people to machine (things*), dan *machine* (*things*) *to machine* (*things*) yang berinteraksi melalui internet. Dapat dibayangkan bahwa IoT akan menjadi teknologi yang perkembangannya sangat cepat karena menyentuh berbagai lini kehidupan manusia. Internet yang pada awalnya digunakan hanya sebagai jaringan komputer saat ini telah berkembang dengan menghubungkan berbagai perangkat dan obyek.

2.2.2 *Embedded System*

Embedded System merupakan kombinasi dari perangkat keras dan perangkat lunak komputer serta bagian tambahan lainnya yang berwujud mekanis maupun elektronik yang dirancang melakukan fungsi khusus (Feynman, 2007). *Embedded system* didesain untuk memiliki fungsi yang spesifik sehingga berbeda dengan personal komputer. Walaupun sebenarnya antara *embedded system* dan personal komputer memiliki kesamaan yaitu memiliki prosesor, RAM, dan media penyimpanan. Dari definisi tersebut dapat diketahui bahwa *embedded system* adalah sebuah sistem komputer yang memiliki fungsi spesifik (*special purpose*) pada sebuah *environment* atau sebuah alat yang didesain sedemikian rupa.

(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. Tanpa disadari aplikasi dari *embedded system* telah banyak ditemukan dalam kehidupan sehari-hari, pada tabel di bawah ini dapat dilihat contoh aplikasi *embedded system* yang telah ada.

Tabel 2.2 Aplikasi *Embedded System* Pada Kehidupan Sehari-hari (Barua et al., 2014)

Home Applications	Mesin pencuci piring, mesin cuci, oven microwave, *set-top box*, sistem keamanan rumah, pemutar dvd, mesin penjawab, sistem penyiram taman, sistem pencahayaan, *remote control*, ac
Electronic Products	Ponsel, telepon tanpa kabel, kamera digital, perekam video, pemutar dvd, tv, kalkulator, pemutar mp3, sistem stereo, *tuner* tv kabel, jam tangan digital, personal pda, iphone.
Industrial applications	Personal smart phone, mesin fax, mesin fotokopi foto, *printer*, *scanner*, *assembly line*, sistem pengumpulan data, sistem monitoring (tekanan, tegangan, arus, suhu), sistem pendeteksi bahaya, robot industri.
Business Equipment	ATM, kas register, sistem alarm, pembaca kartu, detektor sidik jari, sistem tol otomatis, pengenal suara, mesin vendor cerdas
Automobile	GPS, pengendali injeksi bahan bakar, sistem rem *anti-locking*, *controller* transmisi, suspensi aktif, sistem *airbag*, AC
Communication Systems	*Router*, hub, telepon seluler, webcam, modem, *network card*, sistem *tele-conferencing*.
Aerospace	Sistem GPS, automatic landing system, radar
Medical Technology	CT *scanner*, EKG, EEG, EMG, MRI, monitor glukosa, monitor tekanan darah, perangkat diagnostik, mesin sinar-x, monitor *pulse digital*
Security Systems	Sistem pengenal wajah, pengenal sidik jari, pengenal iris mata, sistem keamanan gedung, sistem keamanan bandara, sistem alarm, kartu akses digital, kartu pintar berbasis sidik jari.
Classroom applications	*Smart board, smart room*, OCR, kalkulator, *smart cord*, sistem stereo, proyektor.
Game and Entertainment	*Video games, robot, mp3, mind storm, smart toy*

2.2.3 *Digital Forensic*

Digital forensics menurut (Palmer, 2001) adalah penggunaan metode ilmiah dalam pelestarian, pengumpulan, validasi, identifikasi, analisa, interpretasi, dokumentasi, dan penyajian bukti digital yang bersumber dari sumber digital yang bertujuan memfasilitasi atau melakukan rekontruksi kejadian tindakan kriminal atau kejadian yang melibatkan tindakan yang tidak memiliki otorisasi terhadap sebuah operasi yang direncanakan. Berdasarkan definisi tersebut kegiatan rekonstruksi kejadian akan sulit dilakukan apabila tidak dilengkapi bukti yang lengkap.

Dari hasil investigasi forensik pada perangkat digital dapat ditemukan barang bukti bersifat digital yang dapat membantu mengungkap fakta dari sebuah kejadian. Barang bukti digital membutuhkan penanganan secara khusus mulai dari pelestarian, pengumpulan, validasi, identifikasi, analisa, interpretasi, dokumentasi, dan penyajian agar dapat dijadikan landasan kuat pada proses persidangan. Penanganan khusus tersebut yaitu dengan memperhatikan *standart operation procedure* (SOP) yang ada serta menggunakan metode ilmiah yang memang dibuat dalam penanganan bukti digital.

Dalam proses forensik digital terdapat empat fase dasar (Kent, Chevalier, Grance, & Dang, 2006), antara lain:

1. *Collection*

   Pada fase pertama ini dilakukan identifikasi, pembuatan label, perekaman, dan akuisisi data dari sumber data yang relevan dengan didasari pedoman dan prosedur yang ada untuk menjaga integritas data. Pada fase pengumpulan data (*collection)* ini perlu dilakukan tepat waktu karena data yang bersifat dinamis akan mudah hilang ketika baterai habis, contohnya seperti pada *smartphone* dan *tablet*.

2. *Examination*

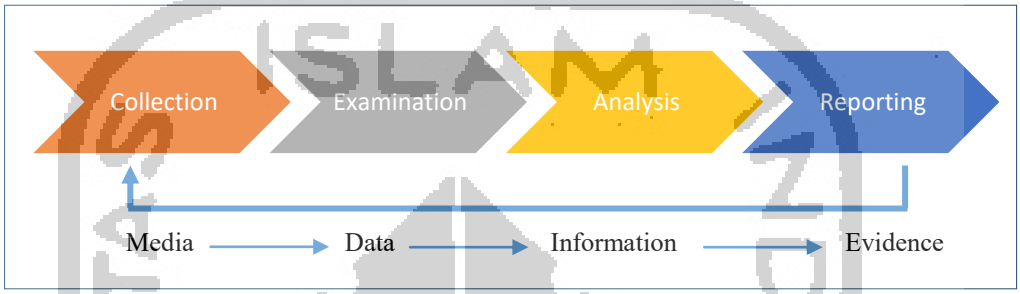
   Fase ini akan menangani jumlah data yang besar untuk dilakukan forensik dengan menggunakan kombinasi metode manual dan otomatis untuk mencari dan melakukan ekstrak data. Dalam fase ini juga perlu diperhatikan terkait integritas data.

3. *Analysis*

   Pada fase ini akan dilakukan analisa hasil dari fase sebelumnya yaitu *examination*, menggunakan metode dan teknik yang dapat dibenarkan secara hukum, untuk memperoleh informasi bermanfaat yang menjawab pertanyaan-pertanyaan yang merupakan motivasi dilakukannya *collection* dan *examination*.

4. *Reporting*

Tahap akhir adalah melaporkan hasil analisa, yang menggambarkan tindakan yang dilakukan, menjelaskan bagaimana alatdan prosedur yang dipilih, menentukan tindakan lain yang perlu dilakukan (misalnya, pemeriksaan forensik terhadap sumber data tambahan, mengamankan kerentanan yang teridentifikasi, memperbaiki kontrol keamanan yang ada), dan memberikan rekomendasi untuk perbaikan terhadap kebijakan, pedoman, prosedur, peralatan, dan aspek lain dari proses forensik.

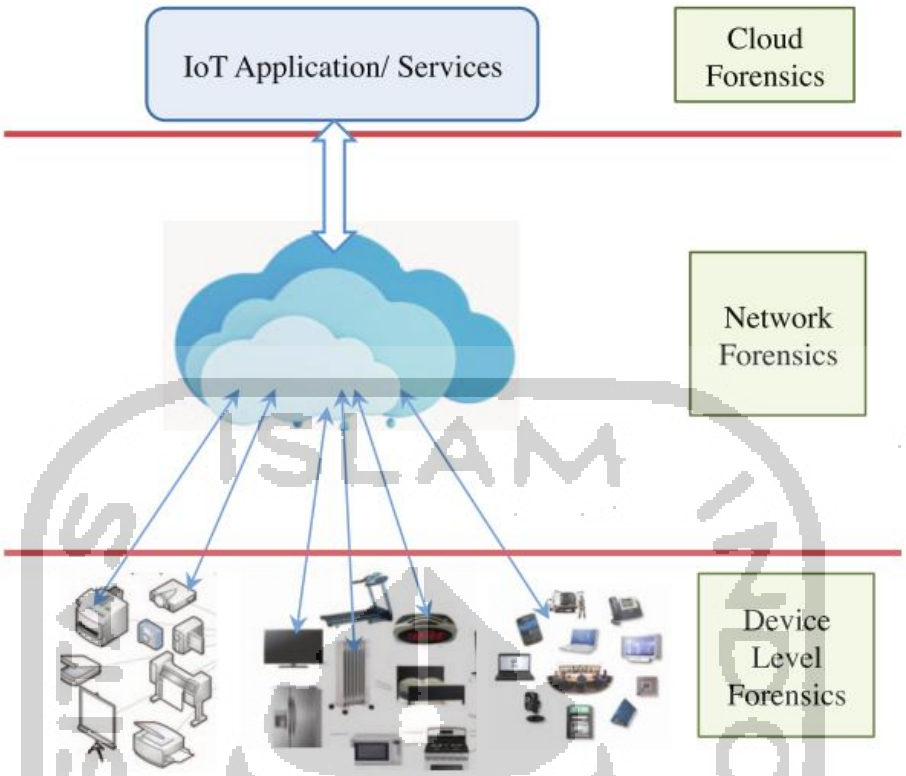


Gambar 2.1 Proses *digital forensic* (Kent et al., 2006).

Pada gambar 2.1 menunjukkan transformasi media menjadi *evidence* (barang bukti), selanjutnya barang bukti tersebut akan diperlukan dalam penegakan hukum atau penggunaan internal sebuah organisasi. Transformasi pertama terjadi saat data yang dikumpulkan (*collection*) diperiksa, data dilakukan ekstraksi dari media dan diubah menjadi format yang dapat dikenali oleh *tool* forensik. Kedua, data ditransformasi menjadi informasi melalui analisa. Selanjutnya informasi ditransformasi dan menghasilkan barang bukti untuk bisa dibuat laporan.

2.2.4 *Internet of Things Forensic*

Forensik perangkat IoT adalah cabang forensik digital yang spesial dimana proses identifikasi, koleksi, organisasi, dan presentasi disesuaikan dengan infrastruktur IoT untuk mengungkapkan fakta atas insiden yang terjadi (Zawoad & Hasan, 2015). Forensik perangkat IoT merupakan kombinasi dari tiga level (skema) forensik digital, yaitu forensik pada level perangkat, forensik jaringan, dan forensik *cloud server.* Cakupan yang terbilang cukup luas untuk bidang forensik digital. Skema tersebut dapat dilihat pada gambar di bawah ini.



Gambar 2.2 Forensik pada perangkat IoT (Zawoad & Hasan, 2015).

Gambar 2.2 memperlihatkan pembagian level forensik dari perangkat IoT. Level forensic pada perangkat IoT terbagi menjadi 3 level, yaitu *cloud forensic, network forensic,* dan *device level forensic.* Pada tabel di bawah ini menunjukkan sumber ditemukannya barang bukti digital.

Tabel 2.3 Tabel skema Forensik Perangkat IoT

Level Forensik	**Sumber Barang Bukti**
Device Level Forensic	Barang bukti digital didapatkan dari internal perangkat IoT
Network Forensic	Barang bukti digital didapatkan dari log jaringan
Cloud Forensic	Barang bukti digital didapatkan dari penyimpanan *cloud server*

Infrastruktur IoT saat ini belum memiliki standar *framework* untuk investigasi forensik, oleh karenanya masih perlu dikembangkan algoritma dan *framework* forensik yang spesifik untuk mendukung kegiatan forensik di lingkungan ini (Kebande & Ray, 2016). Forensik pada infrastruktur IoT memiliki karakterisktik yang berbeda dengan pendekatan forensik tradisional.Kompleksitas IoT adalah tantangan yang perlu dihadapi

oleh investigator forensik. Oriwoh (Oriwoh et al., 2013) memaparkan beberapa perbedaan pendekatan terkait forensik tradisional dengan forensik perangkat IoT, antara lain:

1. Sumber barang bukti

   Forensik komputer biasa mendapatkan barang bukti pada PC, c*loud*, virtualisasi, perangkat *mobile phone, web client*, media sosial, *server* otentikasi dan otorisasi, *proxy server*, dll. Sedangkan pada forensik IoT barang bukti didapatkan dari perangkat elektronik rumah, mobil, *tag*, *reader*, *embedded system*, jaringan sensor, implan di dunia medis, dan perangkat IoT lainnya.
2. Jumlah perangkat

   Jumlah perangkat pada konteks forensik digital mencapai milyaran perangkat, sedangkan perangkat IoT pada tahun 2020 diperkirakan 50 milyar sampai trilyunan perangkat.
3. Jumlah dan tipe data

   Tipe data sebagai barang bukti pada perangkat IoT dapat berupa format apapun dan tidak terbatas suatu format. Sedangkan forensik biasa hanya mengakomodir format standar berupa dokumen digital, jpeg, mp3, dll.
4. Lokasi barang bukti

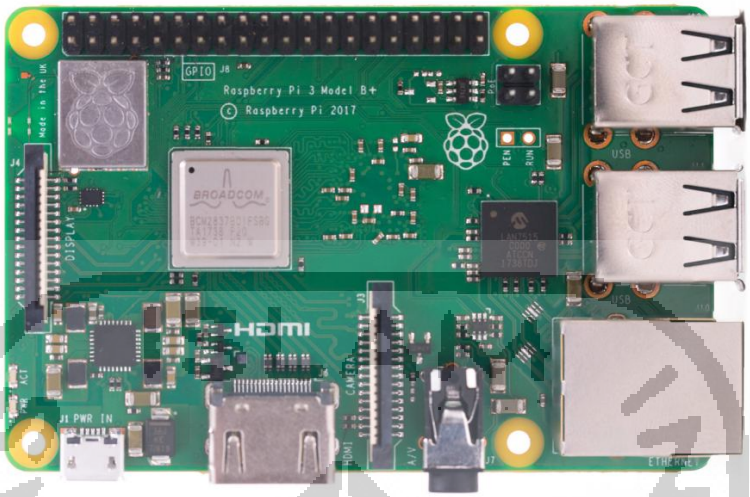
   Perangkat IoT memiliki karakter memiliki bentuk fisik akan tetapi dapat dilakukan *remote* dari jarak jauh. Penyimpanan data dapat berada di luar sistem, bisa terbagi ke beberapa tempat berbeda. Antar sensor dapat memiliki lokasi yang berjauhan tetapi terintegrasi ke satu penyimpanan data pada *cloud server.*
5. Batas sistem

   Forensik perangkat IoT memiliki kesulitan tersendiri karena tidak jelas batas sistem yang ada, khususnya batas jaringan. Sebuah perangkat IoT dapat memiliki banyak sensor dan dapat terhubung dengan perangkat IoT lainnya sehingga cakupan jaringan menjadi cukup besar. Berbeda dengan pendekatan forensik tradisional yang biasanya sudah jelas batasan sistemnya. Batasan tersebut biasanya didasarkan atas kepemilikan sistem.

2.2.5 *Raspberry Pi 3 Model B+*

Raspberry Pi merupakan perangkat komputer mini yang dikemas dalam papan PCB tunggal yang memiliki spesifikasi seperti komputer personal (PC). Perangkat ini dilengkapi dengan modul GPIO (*General Purpose Input Output*) yang sangat berguna untuk diterapkan pada peralatan berbasis *embedded system*. Raspberry Pi telah dilengkapi dengan

semua fungsi layaknya sebuah komputer lengkap, menggunakan teknologi SoC (*System-on-a-chip*) berbasis arsitektur prosesor ARM (Yuwono & Nugroho, 2015).



Gambar 2.3 Raspberry Pi 3 Model B+.

Raspberry Pi 3 Model B+ adalah model terbaru dari Raspberry pi yang memiliki spesifikasi prosesor quad core dengan kecepatan clock 1,4 Ghz. Untuk spesifikasi lengkapnya dapat dilihat di bawah ini:

- *Processor* : Broadcom BCM2837B0, Cortex-A53 64-bit SoC @ 1.4GHz
- *Memory* : 1GB LPDDR2 SDRAM
- *Connectivity* : 2.4GHz and 5GHz IEEE 802.11.b/g/n/ac *wireless* LAN, *Bluetooth* 4.2, BLE Gigabit *Ethernet over* USB 2.0 (*max* 300Mbps), 4 × USB 2.0 *ports*
- *Access* *: Extended* 40-pin GPIO *header*
- *Video & sound* : 1 × *full size* HDMI, MIPI DSI *display port*, MIPI CSI *camera port* , 4 *pole stereo output and composite video port*
- *Multimedia* : H.264, MPEG-4 *decode* (1080p30); H.264 *encode* (1080p30); OpenGL ES 1.1, 2.0 *graphics*
- SD *card support* : Micro SD
- *Input power* : 5V/2.5A DC *via micro* USB *connector*, 5V DC *via* GPIO *header*, *Power over Ethernet* (PoE)–*enabled* (*requires separate* PoE HAT)
- *Environment* *: Operating temperature*, 0–50°C