BAB 1
Pendahuluan

1.1 Latar Belakang

Internet menjadi teknologi yang merupakan cikal bakal lahirnya teknologi baru dengan berbagai inovasi. Jaringan internet telah menghubungkan banyak komputer di seluruh penjuru dunia yang berinterkoneksi. Dengan interkoneksi tersebut komputer dapat saling bertukar data. Saat ini tidak hanya komputer yang terhubung ke jaringan internet, akan tetapi perangkat selain komputer yang telah didesain sedemikian rupa juga dapat terhubung ke jaringan internet. Salah satu contohnya adalah perangkat *Internet of Things* (IoT). Perangkat tersebut adalah perangkat elektronik cerdas yang memanfaatkan internet sebagai media komunikasi dan transfer data.

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. Dengan munculnya IoT melahirkan sistem cerdas seperti *smarthome, smart farm, smart city, smart building, smart health, smart transport,* dll.

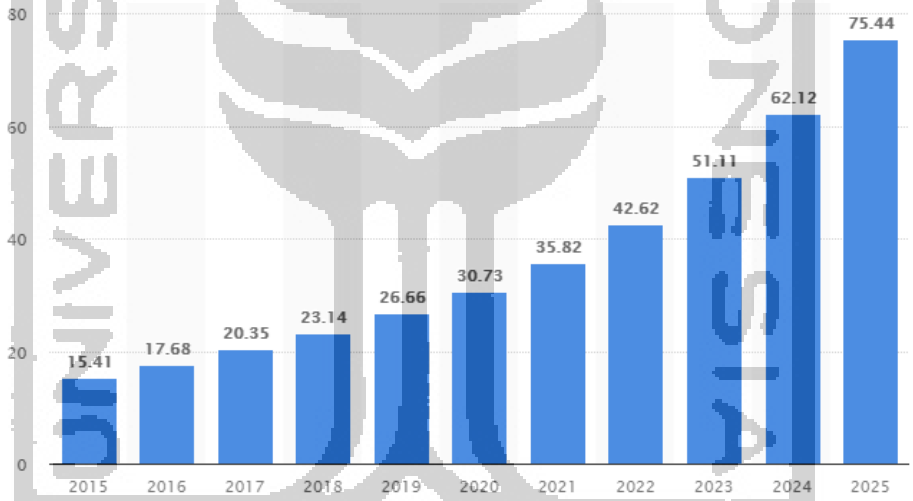
Pada aplikasi *smarthome,* IoT dapat berperan sebagai asisten dari pemilik rumah yang dapat mengatur peralatan elektronik seperti lampu, mesin cuci, lemari es, AC, gerbang, televisi, dan perangkat lainnya yang terhubung ke internet. Dengan diterapkannya IoT di rumah, rumah tersebut akan menjadi sebuah *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.

Sebagai contoh aplikasi lain dari IoT yaitu diterapkannya IoT di dunia kesehatan. Masalah kesehatan menjadi sebuah masalah yang semakin meningkat dari waktu ke waktu. Pola makan tidak teratur dan pola hidup yang kurang baik menjadi pemicu seseorang jatuh sakit. Ketika sudah sakit rumah sakit akan menjadi tempat tujuan untuk memulihkan kesehatannya. Di rumah sakit pasien ada kalanya perlu dipasang berbagai macam alat

monitoring seperti suhu badan, tekanan darah, detak jantung, dan sebagainya. Agar pasien tersebut dapat terpantau oleh dokter dan paramedis maka dikembangkan sistem *smarthealth* yang membantu petugas medis memantau pasien dari manapun melalui jaringan internet. Adanya *smart health* membantu mempercepat penanganan dan tindakan kepada pasien di saat tindakan itu dibutuhkan.

Seiring berjalannya waktu jumlah perangkat IoT di dunia ini semakin meningkat. Lembaga riset Postscapes dan Harbor Research (2014) dalam penelitian yang telah dilakukan sedikitnya pada tahun 2014 telah ada sejumlah 6 milyar perangkat IoT yang dibangun dan terhubung ke internet. Dan diperkirakan pada tahun 2020 akan meningkat hingga 27 milyar perangkat IoT yang meliputi penerapan di dunia industri, infrastruktur, kesehatan, dan rumah.

Lembaga penelitian Statista pada tahun 2017 berdasarkan penelitian yang dilakukan menyampaikan bahwa dari tahun ke tahun jumlah perangkat IoT yang terhubung ke internet semakin meningkat. Data tersebut dapat dilihat dari gambar di bawah ini.



Gambar 1.1 Jumlah perangkat IoT terpasang.

Sumber: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

Berdasarkan data dari dua lembaga riset tersebut pada tahun 2020 memiliki perkiraan yang hampir sama berkaitan dengan jumlah perangkat IoT yang akan terpasang di jaringan internet. Pertumbuhan yang bisa dibilang sangat pesat dari tahun-tahun sebelumnya.

Seiring 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. Akan menjadi sangat fatal apabila data tersebut dilakukan penyadapan maupun manipulasi oleh penyerang.

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.

Pada tahun 2013 telah terjadi serangan terhadap perangkat IoT yang diproduksi oleh salah satu perusahaan produsen alat jaringan. Perusahaan tersebut telah memproduksi perangkat IoT berupa *Internet Camera* yang ternyata memiliki kelemahan di dalam sistemnya yaitu pada pengaturan *default* perangkat tersebut tidak mewajibkan pengguna untuk membuat *password*. Sehingga celah tersebut akhirnya telah terbongkar sehingga data-data pengguna yang berupa *streaming* video yang bersifat personal dapat dibuka oleh khalayak umum. Atas kejadian tersebut akhirnya perusahaan diberikan sanksi ganti rugi kepada pengguna yang jumlahnya tidak sedikit. Dari kasus ini *security awareness* terhadap perangkat IoT harus senantiasa ditingkatkan terutama oleh produsen.

Investigasi kasus yang menyangkut perangkat *Internet of Things* akan menjadi tantangan tersendiri bagi investigator forensik. Keberagaman jenis perangkat dan teknologi akan memunculkan tantangan baru bagi investigator forensik (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.

Dalam penelitian ini akan dititikberatkan forensik di level internal *device* dari 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 level ini diharapkan dapat menemukan berbagai artefak digital berupa program dan *service* berupa *malware* yang ada di sistem, sehingga dapat menjadi referensi *investigator* dalam mengungkap fakta dalam sebuah kasus.

Pada penelitian ini akan dibangun sebuah *environment* perangkat IoT sebagai media penelitian dan kajian tentang forensik level *device*. Pada penelitian ini dipilih model perangkat IoT berupa *smart home*. Model perangkat IoT berupa *smart home* dipilih karena

perangkat ini adalah perangkat yang di masa mendatang akan menjadi perangkat IoT yang jumlahnya bisa sangat banyak dan diterapkan di setiap rumah dalam sebuah keluarga.

1.1 Rumusan Masalah

Rumusan masalah dalam penelitian ini adalah:

1. Bagaimana mengembangkan *environment* perangkat *Internet of Things* untuk mendukung proses forensik?
2. Bagaimana proses forensik *device level* pada perangkat *Internet of Things* berbasis *Embedded System*?
3. Bagaimana karakteristik bukti digital yang ditemukan dari hasil forensik *device level* dari perangkat IoT yang berjalan pada sistem operasi Raspbian, Fedberry, Ubuntu Mate, dan Kali Linux?

1.2 Batasan masalah

Batasan masalah dalam penelitian ini meliputi:

1. Forensik dilakukan pada media penyimpanan perangkat *Internet of things* yang dibangun berbasis Raspberry Pi 3 Model B+.
2. *Platform* IoT dibangun berbasis *web application* dengan didukung apache *server* dan mysql *database server*.
3. Barang bukti digital didapatkan dari hasil akuisisi media penyimpanan perangkat *Internet of Things*.
4. Sistem operasi perangkat IoT yang diteliti meliputi Raspbian, Fedberry, Ubuntu Mate, dan Kali Linux.

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dibuat maka dapat diambil tujuan penelitian ini sebagai berikut:

1. Mengembangkan *environment* berupa *prototype* IoT bertajuk *smart home* untuk media penelitian dan simulasi.
2. Melakukan forensik *device level* pada perangkat IoT berbasis *embedded system.*
3. Untuk mendapatkan karakteristik bukti digital pada forensik *device level* yang berjalan pada sistem operasi Raspbian, Fedberry, Ubuntu Mate, dan Kali Linux.

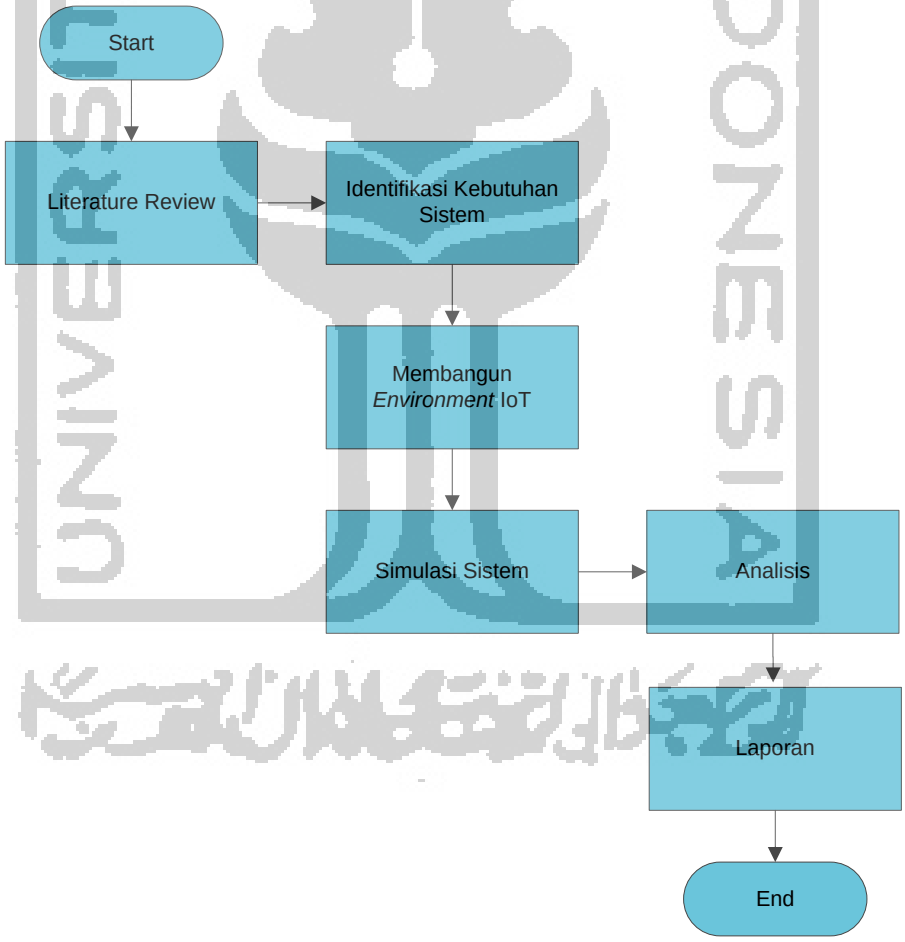
1.4 Manfaat Penelitian

Manfaat yang dapat diperoleh dari hasil penelitian adalah sebagai berikut:

1. Memberikan acuan kepada investigator forensik digital dalam melakukan analisis forensik *device level* pada perangkat *Internet of Things.*
2. Mengetahui karakteristik barang bukti yang didapat dari forensik *device level* pada perangkat *Internet of Things.*
3. Sebagai bahan referensi bagi peneliti lain dalam mengembangkan penelitian lebih lanjut pada kajian penelitian yang sama.

1.5 Metode Penelitian

Susunan laporan penelitian ini perlu metodologi penyelesaian secara sistematis, penelitian ini menggunakan beberapa tahap yaitu:



Gambar 1.2 Alur metodologi penelitian.

1. *Literatur Review*

   Studi literatur dilakukan untuk mendapatkan informasi mengenai topik yang menjadi domain penelitian yang dapat bersumber dari dokumen, buku, artikel, atau bahan

tertulis lainnya yang berupa teori, laporan penelitian, atau penemuan sebelumnya, baik bersifat *online* maupun *offline*.

2. Identifikasi Kebutuhan Sistem

   Merupakan tahap identifikasi kebutuhan dalam membangun *environment* IoT. IoT adalah perangkat yang kompleks sehingga diperlukan tahapan yang matang dalam perancangan dan pembuatannya.

3. Membangun *Environment* IoT

   Tahap selanjutnya yaitu membangun *environment* perangkat *Internet of Things.* Pada tahapan ini akan dibuat perangkat IoT dengan konsep *smart home* untuk simulasi sistem.

4. Simulasi Sistem

   Merupakan tahap dilakukannya simulasi langsung pada sistem yang menjalankan perangkat IoT. Memastikan *environment* berjalan sesuai dengan fungsinya. Pada tahap ini akan dilakukan simulasi skenario kasus yang bertujuan untuk melakukan pengujian serangan pada perangkat IoT.

5. Analisis

   Tahap ini dilakukan untuk melakukan investigasi dalam menemukan barang bukti serangan, mengelompokkan barang bukti yang ditemukan dari hasil forensik perangkat IoT pada *level device*.

6. Laporan

   Tahap ini dilakukan untuk membuat laporan semua data yang telah di analisis yang digunakan sebagai bukti digital yang sah dan dapat diterima secara umum.

1.6 Sistematika Penulisan

Untuk mempermudah proses pembahasan dalam penelitian, maka dibuat sistematika penulisan pada penelitian ini:

BAB I PENDAHULUAN

Bab Pendahuluan merupakan pengantar terhadap permasalahan yang akan dibahas. Didalamnya menguraikan tentang gambaran suatu penelitian yang terdiri dari latar belakang, rumusan masalah, batasan masalah, manfaat penelitian, tujuan penelitian, metodologi penelitian, serta sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini menjelaskan kajian penelitian terdahulu dan teori-teori yang digunakan untuk memecahkan masalah dalam penelitian ini. Teori yang dibahas pada bagian ini merupakan teori yang berhubungan dengan forensik perangkat *Internet of Things* pada level *device*.

BAB III METODOLOGI PENELITIAN

Bab ini membahas tentang langkah-langkah penelitian dan gambaran umum langkah penyelesaian.

BAB IV ANALISIS DAN HASIL

Bab ini berisi tentang pemaparan hasil penelitian dalam penyelesaian masalah yang diangkat yaitu dengan melakukan analisis dan uji coba.

BAB V KESIMPULAN DAN SARAN

Kesimpulan dan Saran memuat kesimpulan dari hasil penelitian dan saran yang perlu diperhatikan berdasarkan hasil yang ditemukan serta asumsi-asumsi yang dibuat selama melakukan penelitian dan juga rekomendasi yang dibuat untuk pengembangan penelitian selanjutnya.