1. Pendahuluan

Latar Belakang

Tidak ada definisi yang jelas mengenai konsep IoT namun dapat disepakati bersama bahwa IoT adalah langkah evolusi dari Internet, dimana objek dapat berbagi data antara satu dengan yang lainnya. Contoh konsep IoT yang berkaitan dengan objek sehari-hari adalah kunci pintu pintar, monitor bayi, kamera keamanan, robot rumah tangga, thermostat pintar, dan masih banyak lagi. Namun terdapat beberapa resiko pada IoT yang yang dapat menimbulkan hal-hal yang tidak kita inginkan dan penyalahgunaan IoT contohnya seperti *Smart Car* yang digunakan untuk tujuan mencelakai seseorang, kamera pengintai bayi yang digunakan untuk memata-matai kita dan masih banyak resiko lainnya.

Asosiasi perdagangan nirlaba CompTIA memperkirakan bahwa jumlah objek yang terhubung ke IoT akan mencapai 50,1 miliar pada tahun 2020 atau sederhananya 6,3 item yang terhubung untuk setiap orang yang terhubung di dunia rata-rata [1]. Tentu saja IoT akan tumbuh dengan cepat dan diharapkan menjadi teknologi yang wajib ada bagi kehidupan manusia tapi sudah seberapa siap kita menghadapinya. Sebuah survey yang dilakukan oleh CompTIA terhadap perusahaan-perusahaan IT mengungkapkan bahwa 43% perusahaan mengakui bahwa mereka tidak diperlengkapi untuk berurusan dengan sebagian besar atau beberapa wilayah IoT [1]. Tentu saja dibutuhkan prosedur digital forensik pada wilayah IoT.

Dalam IoT, mikrokontroler mempunyai peranan penting karena mikrokontroler memfasilitasi pengoprasian sistem elektromekanis pada IoT. Dalam memori mikrokontroler terdapat SDRAM, EPROM atau EEPROM dan memori *flash* [12]. mikrokontroler dirancang dengan memori *onboard* yang memadai dan menawarkan pin untuk operasi I/O umum, sehingga dapat langsung berinteraksi dengan sensor dan komponen lainnya. Bukti digital bisa saja berada pada mikrokontroler karena memori penyimpanan data dalam mikrokontroler, maka dari itu diperlukan prosedur yang efektif, efisien untuk menganalisis isi memori pada mikrokontroler. Namun sebelum melakukan analisis, terlebih dahulu melakukan tahap akuisisi.

Untuk melakukan akusisi pada perangkat sistem tertanam seperti memori mikrokontroler dapat dilakukan menggunakan metode fisik, berdasarkan penelitian yang dilakukan [2] akuisisi paling aman dan efektif adalah dengan menggunakan JTAG. Dengan menggunakan JTAG kita mendapatkan data dari memori *flash*. Jika pin PCB pada mikrokontroler sudah terhubung dengan emulator JTAG maka semua area memori fisik dapat di *dump* dengan pendekatan *bit-by-bit.*

Berdasarkan latar belakang dari penelitian terkait yang sebelumnya tentang kemungkinan IoT digunakan untuk tindak kejahatan dan mikrokontroler sebagai perangkat penting dalam IoT maka dalam tugas akhir ini mengajukan prosedur yang tepat dalam melakukan proses akuisisi dalam digital forensik pada mikrokontroler.

Topik dan Batasannya

Berdasarkan latar belakang diatas akuisisi fisik pada mikrokontroler menggunakan metode fisik. Berikut topik dan batasan penelitian ini:

- Akuisisi pada mikrokontroler menggunakan JTAG.
- Mikrokontroler yang digunakan untuk penelitian ini telah disediakan oleh kami.
- Penelitian ini berfokus pada tahap akuisisi.

Tujuan

Penelitian ini bertujuan untuk menganalisis prosedur digital forensik pada memori mikrokontroler. Akusisi pada memori mikrokontroler menggunakan metode fisik dengan menggunakan JTAG, dan menganalisis prosedur akuisisi yang telah diusulkan.

Organisasi Tulisan

Penelitian ini disusun dengan struktur sebagai berikut:

1. Pada bagian pertama dijelaskan pendahuluan.
2. Studi terkait
3. Perancangan prosedur akuisisi.
4. Evaluasi hasil analisis prosedur foresik digital.
5. Kesimpulan dan saran untuk penelitian selanjutnya.