BAB II

LANDASAN TEORI

2.1 *State of The Art*

Penelitian mengenai *Internet of Things* (IoT) telah banyak dilakukan. Beberapa di antaranya membahas menganai tantangan yang hadir seiring dengan perkembangan IoT tersebut (Atlam, et al., 2018), (Bastos, et al., 2018), (Bouchaud, et al., 2018), (MacDermott, et al., 2018) (Zulkipli, et al., 2017).

Aine MacDermott, Thar Baker, dan Qi Shi (MacDermott, et al., 2018) dalam penelitiannya yang berjudul *"IoT Forensics: Challenges For The IoA Era"* menjelaskan bagaimana tantangan untuk investigasi forensik yang berbasis IoT. Perangkat IoT yang semakin meningkat menyebabkan semakin kompleksnya prosedur yang dibutuhkan untuk melakukan investigasi. Perangkat ini menghasilkan, mengakses, dan menggunakan jumlah data personal dan sensitif yang besar. Tantangan yang muncul yaitu untuk menganalisis data dalam volume besar secara tepat waktu dengan mengumpulkan bukti forensik terkait kejahatan yang sedang diselidiki, sembari mendeteksi keberadaan aktifitas IoT. Tantangan selanjutnya yaitu belum adanya prinsip-prinsip yang terdefinisi untuk forensik IoT, investigator akan secara signifikan mengandalkan pada sifat mekanik dan fisik dari perangkat IoT.

Penelitian serupa oleh Zulkipli (Zulkipli, et al., 2017) menjelaskan mengenai tantangan pada investigasi forensik IoT dalam hal akuisisi barang bukti digital. Akuisisi data memiliki peranan penting dalam proses investigasi forensik. Akuisisi

barang bukti harus baik proses penanganannya agar dapat diterima di pengadilan. Perangkat IoT bersifat unik, biasanya memiliki *power* terbatas, pemrosesan bawaan yang ringan, penyimpanan terbatas, dan berbagi jaringan. Investigator harus memperhatikan apakah perangkat harus dimatikan atau tetap berjalan saat investigasi. Berdasarkan permasalahan tersebut diusulkan dua buah pendekatan, yaitu menekankan pada tahapan prainvestigasi dan proses forensik IoT secara *real time.*

Penelitian di atas menjadi dasar untuk adanya penelitian ini. Penelitian ini akan berfokus pada tahapan prainvestigasi sebelum melakukan akuisisi data. Karakteristik perangkat IoT yang berbeda menyebabkan berbeda pula teknik akuisisi datanya. Penelitian ini akan mencoba untuk memberikan usulan teknik akuisisi data yang dapat digunakan pada perangkat IoT tergantung dari karakteristik yang dimiliki oleh perangkat tersebut.

Berikut merupakan tabel *literature review* mengenai IoT dan teknik akuisisi data yang tersaji pada tabel 2.1 dan 2.2. Matriks penelitian berdasarkan penelitian terdekat akan disajikan berikutnya pada tabel 2.3.

Tabel 2.1 *Literature Review* Terkait IoT

No.	Konten	Deskripsi
1.	**Paper ke-1**	
	Judul Paper	*IoT Forensic: Bridging the Challenges in Digital Forensic and the Internet of Things*
	Penulis	Nurul Huda Nik Zulkipli; Ahmed Alenezi; Gary B. Wills (2017)
	Jurnal/Konferensi	*Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security (IoTBDS 2017)*
	URL	https://www.scitepress.org/papers/2017/63087/63087.pdf

No.	Konten	Deskripsi
	Permasalahan	Perangkat IoT dapat dengan mudah diserang, diperlakukan, dan dieksploitasi oleh penjahat cyber di mana perangkat pintar tersebut dapat memberikan data yang salah sehingga dapat menyebabkan interpretasi dan aktuasi yang salah kepada pengguna yang sah.
	Kontribusi	Mengusulkan dua pendekatan dalam investigasi forensic IoT yang menekankan pada tahap prainvestigasi dan mengimplementasikan investigasi *real-time* untuk memastikan data dan barang bukti potensial terkumpul dan dapat dihadirkan selama proses investigasi.
	Metode/Solusi	Untuk memenuhi karakteristik IoT, dua pendekatan menuju penyelidikan untuk forensik IoT diusulkan dengan menekankan fase pra-investigasi dan mengimplementasikan penyelidikan real-time untuk memastikan data dan bukti potensial dikumpulkan dan disimpan selama penyelidikan.
	Hasil Utama	- Blok bangunan IoT terdiri dari lima modul utama sebagai berikut: modul sensor; modul pemrosesan; modul aktuasi; modul komunikasi; modul energi. - Karakteristik IoT: *existence*; *sense of self*; konektivitas; interaktivitas; dinamika; skalabilitas; keterbatasan komputasi; keterbatasan sumber daya - Pendekatan dalam forensik IoT: 1. Mempersiapkan kesiapan forensik IoT terutama selama fase pra-investigasi. 2. Mengadopsi elemen *real-time* selama investigasi.
	Batasan	Dua pendekatan pada forensik IoT diperlukan pengembangan selanjutnya.
2.	**Paper ke-2**	
	Judul Paper	*IoT Forensics: Challenges For The IoA Era*
	Penulis	Áine MacDermott; Thar Baker; Qi Shi (2018)
	Jurnal/Konferensi	2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)
	URL	https://www.researchgate.net/publication/324177822_Iot_Forensics_Challenges_for_the_Ioa_Era
	Permasalahan	- Meningkatnya pemanfaatan layanan cloud dalam operasi sehari-hari oleh organisasi, dan meningkatnya pemanfaatan perangkat pintar berarti bahwa penyelidikan forensik digital yang melibatkan sistem tersebut akan melibatkan perolehan dan analisis bukti digital yang lebih kompleks. - IoT merupakan penggabungan tanpa batas dari dunia nyata dan digital, dengan perangkat baru yang dibuat yang menyimpan dan menyebarkan data, harus menemukan cara baru untuk mengambil dan mengamankan data ini untuk memastikan bahwa tidak ada gangguan pada barang bukti.

No.	Konten	Deskripsi
	Kontribusi	Menjabarkan mengenai tantangan pada forensik IoT.
	Metode/Solusi	Menganalisis bagaimana berbagai bentuk barang bukti dapat disita, disimpan, diekstraksi, dan dianalisis.
	Hasil Utama	- Tidak ada prinsip yang terdefinisi untuk forensik IoT, karena itu, investigasi akan sangat bergantung pada sifat mekanik dan fisik perangkat pintar, karena mengidentifikasi sumber bukti merupakan tantangan utama. Bukti dapat dikumpulkan dari sensor tetap di rumah dan bangunan, sensor bergerak yang ditanam ke dalam mobil dan perangkat yang dapat didengar, perangkat komunikasi, penyimpanan cloud dan bahkan log ISP. - Tantangan utama yang ditimbulkan oleh TKP berbasis IoT dari sudut pandang penyelidik meliputi: ukuran objek forensik, lokasi, relevansi perangkat yang diidentifikasi dan dikumpulkan, masalah hukum/yurisdiksi, batas-batas jaringan buram/jaringan tak bertepi, alat yang tersedia . - Cloud forensik juga akan memainkan peran utama dalam memperkuat praktik terbaik keamanan siber, karena semua data yang dihasilkan oleh komponen IoT akan disimpan di cloud karena skalabilitas, kapasitas, dan kenyamanannya. - Sumber bukti pada perangkat berbasis IoT dapat dikategorikan ke dalam tiga kelompok: semua bukti dikumpulkan dari perangkat pintar dan sensor; semua bukti yang dikumpulkan dari perangkat keras dan perangkat lunak yang menyediakan komunikasi antara perangkat pintar dan dunia eksternal; semua bukti dikumpulkan dari perangkat keras dan lunak yang berada di luar jaringan yang sedang diselidiki.
	Batasan	Penelitian untuk mengidentifikasi metode untuk melakukan analisis forensik digital berbasis IoT sangat esensial. Tujuan jangka panjangnya untuk pembangunan standar forensik digital yang dapat digunakan dalam investigasi yang berbasis IoT.

Tabel 2.1 di atas merupakan penelitian sebelumnya. Penelitian tersebut menjelaskan mengenai tantangan dalam forensik IoT dan berfokus pada akuisisi barang bukti data digital.

Tabel 2.2 *Literature Review* Terkait Teknik Akuisi Data

No.	Konten	Deskripsi
	Judul Paper	Live Vs Dead Computer Forensic Image Acquisition
	Penulis	Mahesh Kolhe; Purnima Ahirao
	Jurnal/Konferensi	International Journal of Computer Science and Information Technologies
	URL	https://ijcsit.com/docs/Volume%208/vol8issue3/ijcsit20170800331.pdf
	Permasalahan	Konsep *forensic imaging* kerap kali membingungkan dalam bidang forensik komputer.
	Kontribusi	Menyarankan metode akuisisi terbaik yang digunakan untuk suatu kasus dalam investigasi forensik.
	Metode/Solusi	- *Live acquisition* - *Dead acquisition*
	Hasil Utama	- *Live acquisition* digunakan pada investigasi yang membutuhkan identifikasi pada file yang paling terakhir digunakan dan perangkat seperti SSD. - *Dead acquisition* memerlukan waktu yang lebih singkat dibanding *live*, tetapi tidak dapat menangkap data *volatile.* - Dikarenakan meningkatnya kejahatan siber, analisis *live* merupakan cara terbaik untuk menginvestigasi sistem target karena lebih banyak keuntungan.
	Batasan	Penelitian ini menggunakan contoh kasus analisis *malware.*

Tabel 2.2 merupakan penelitian yang menjelaskan mengenai perbedaan teknik akuisisi data yang dapat digunakan. *Live acquisition* dapat menangkap data *volatile*, sedangkan *dead acquisition/write block* tidak.

Berikut merupakan tabel matriks penelitian terdekat yang dijadikan bahan rujukan untuk melakukan penelitian ini:

Tabel 2.3 Matriks Penelitian Terkait Investigasi Forensik

No.	Penelitian/ Tahun	Judul	Metode	Objek	Teknik Akuisisi Data
1.	Eri Haryanto, Imam Riadi	Forensik *Internet of Things* pada *Device Level* Berbasis *Embedded System*	*collecting, examination, analysis, reporting* (NIST)	perangkat IoT *smart home*	*write block*
2.	Nur Widiyasono; Imam Riadi; Ahmad Luthfi	*Investigation on the Services of Private Cloud Computing by Using ADAM Method*	ADAM	komputer *server*, *desktop*, *laptop* dan *smartphone*	*live* dan *write block*
3.	Faulinda Ely Nastiti, Nindya Dwi Anggana, Heri Gunawan, dan Uning Kristiana	Akuisisi Barang Bukti Digital Pada *Smart CCTV* Menggunakan Standarisasi ACPO DAN SNI ISO/IEC 27037:2014	ACPO DAN SNI ISO/IEC 27037:2014	*smart CCTV*	logikal/*live* dan fisikal/*write block*
4.	A. Boztas, A.R.J. Riethoven, M. Roeloffs	*Smart TV forensics: Digital traces on televisions*	*selection, acquisition, analysis*	*smart TV*	*static/write block*
5.	Lubi Arsada dan Aries Muslim	Penerapan Metode NIST untuk Analisis Serangan *Denial of Service* (DoS) pada Perangkat *Internet of Things (IoT)*	NIST	perangkat IoT	*live*
6.	Lulu Hazirotul Quds	Klasifikasi Perangkat IoT untuk Teknik Akuisisi Bukti Data Digital	NIST	perangkat IoT *smart home*	*live* dan *write block*

Tabel 2.3 menerangkan mengenai penelitian terdekat yang telah dilakukan sebelumnya. Metode atau kerangka kerja diterapkan, di antaranya kerangka kerja investigasi dasar, ADAM, NIST, ACPO & SNI ISO/IEC 27037:2014. Teknik akuisisi yang digunakan berupa *live* dan *write block.*

Penelitian oleh (Haryanto, et al., 2019) melakukan investigasi forensik pada objek berupa perangkat IoT yang terdapat pada *smart home*. Perangkat tersebut memiliki media penyimpanan berupa sebuah *SD card.* Teknik akuisisi data yang digunakan merupakan *write block*.

Penelitian oleh (Widiyasono, et al., 2016) melakukan investigasi *cloud computing* pada objek berupa komputer *server*, *desktop*, *laptop* dan *smartphone*. Teknik akuisisi data yang digunakan pada penelitian tersebut berupa *live* dan *write block.*

Penelitian oleh (Nastiti, et al., 2020) dilakukan investigasi forensik pada objek berupa sebuah *smart CCTV. Smart CCTV* tersebut memiliki media penyimpanan sehingga teknik akuisisi data yang digunakan berupa *live* dan *write block.*

Penelitian oleh (Boztas, et al., 2015) melakukan investigasi pada *smartTV* menggunakan teknik akuisisi data *write block*. Perangkat *smartTV* tersebut memiliki media penyimpanan.

Penelitian selanjutnya oleh (Arsada, et al., 2021) pada perangkat IoT menggunakan metode *live*. Perangkat ini tidak memiliki media penyimpanan.

2.2 Tinjauan Pustaka

2.2.1 *Internet of Things* (IoT)

Internet of Things (IoT) merupakan suatu konsep yang diciptakan untuk mencakup infrastruktur dan utilitas yang saling terhubung (MacDermott, et al., 2018). Perangkat IoT merupakan perangkat keras dengan sensor yang mentransmisikan data dari satu tempat ke tempat lain melalui Internet. Jenis perangkat IoT termasuk sensor nirkabel, perangkat lunak, aktuator, dan perangkat komputer. Mereka dapat tertanam ke dalam perangkat seluler, peralatan industri, sensor lingkungan, perangkat medis, dan banyak lagi.

2.2.2 Digital Forensik

Digital forensik merupakan aplikasi bidang ilmu pengetahuan dan teknologi komputer untuk kepentingan pembuktian hukum, yang dalam hal ini adalah untuk membuktikan kejahatan berteknologi tinggi atau kejahatan komputer secara ilmiah hingga bisa mendapatkan bukti-bukti digital yang dapat digunakan untuk menjerat pelaku kejahatan tersebut (Al-Azhar, 2012).

2.2.3 Barang Bukti Elektronik

Barang bukti elektrotik bersifat fisik dan dapat dikenali secara visual. Jenis-jenis barang bukti elektronik pada IoT seperti: *smart TV, IP CCTV, smart refrigator,* dll.

2.2.4 Barang Bukti Data Digital

Bukti data digital adalah setiap informasi pembuktian yang disimpan atau disalurkan dalam bentuk digital yang mana pihak dalam kasus hukum dapat gunakan untuk pemeriksaan pengadilan (Al-Azhar, 2012). Barang bukti digital dalam IoT dapat hadir dengan beragam bentuk, seperti *IP address, log, history activity,* dll.

2.2.5 Teknik Akuisisi Data

Akuisi data merupakan tindakan yang berfungsi untuk mengambil, mengumpukan dan menyiapkan serta memproses data untuk menghasilkan data yang dikehendaki.

Teknik akuisisi data pada forensik digital terbagi menjadi dua, yaitu *live* dan *dead acquisition/write block* (Kolhe, et al., 2017). *Live acquisition* merupakan teknik akuisisi yang dilakukan terhadap sistem yang hidup, sedangkan *write block acquisition* dilakukan apabila sistem dalam keadaan mati. Apabila suatu perangkat memiliki media penyimpanan, seperti *memory card, harddisk,* dll, maka diperlukan teknik *write block acquisition.* Teknik ini digunakan untuk memblok perintah *write* apapun yang dapat mempengaruhi barang bukti yang tengah diperiksa. (Lessing, et al., 2008).

2.2.6 *Smart home*

Smart home memungkinkan pemilik rumah memasang perangkat pintar untuk mengontrol pekerjaan rumah (Atlam, et al., 2018). Perangkat IoT *smart home* menawarkan keamanan, efisisensi listrik, kenyamanan, dll ((Bastos, et al., 2018).

2.2.7 NIST

NIST merupakan salah satu kerangka kerja yang mengandung tahapan dasar pada proses investigasi forensik. Kerangka kerja ini banyak digunakan karenakan mengatur standar pedoman, dan praktek terbaik dalam mengelola resiko terkait segala bentuk yang berkaitan dengan sains, teknologi informasi (Arsada, et al., 2021). Metode ini tidak sampai mempertimbangkan prinsip keamanan dan privasi.

Tahapan pada NIST berupa:

a. *Collection*, tahap pengumpulan barang bukti potensial.
b. *Examination*, tahap akuisisi data pada barang bukti potensial.
c. *Analysis*, tahap analisis terhadap hasil yang didapatkan.
d. *Report*, pelaporan hasil investigasi.