BAB 1
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi digital yang semakin maju diikuti dengan meningkatnya berbagai tindak kejahatan dan kriminalitas yang memanfaatkan teknologi digital, seperti kamera*, smartphone* dan teknologi digital lain yang memiliki fitur perekam dan menyimpan data. Fungsi teknologi digital saat ini tidak hanya menangkap aktivitas atau tindak kejahatan, tetapi juga sebagai barang bukti digital sebagai contoh, kasus tindak kejahatan Jessica Kumala Wongso yang menggunakan rekaman perangkat CCTV sebagai barang bukti elektronik (Mualfah dkk., 2022). Perangkat *Closed-Circuit Television* (CCTV) umumnya digunakan untuk memantau dan merekam aktivitas di area tertentu di antaranya rumah, toko, bank, kantor dan fasilitas publik lainnya dengan tujuan pemantauan dan keamanan. Hingga saat ini teknologi CCTV sudah berkembang dengan pesat dan memiliki berbagai fitur canggih, di antaranya kecerdasan buatan, *cloud*, dan integrasi dengan sistem lain.

Peran perangkat CCTV dibutuhkan sebagai sistem pengamanan dalam kehidupan sehari-hari, penggunaan perangkat CCTV tidak hanya untuk mencegah tindak kejahatan, pada saat tertentu perangkat CCTV dapat dijadikan sebagai barang bukti digital kasus tindak kejahatan (Mualfah & Ramadhan, 2021). Dalam beberapa kasus tindak kejahatan, perangkat CCTV digunakan sebagai barang bukti elektronik. Dalam investigasi dan analisis Barang bukti yang dapat disajikan dalam persidangan di antaranya rekaman berupa video. Rekaman video tersebut dikategorikan sebagai barang bukti digital yang potensial. Barang bukti elektronik perangkat CCTV dan barang bukti digital rekaman perangkat CCTV termasuk sebagai barang bukti yang sah (Ramadhanti dkk., 2021).

Barang bukti digital pada perangkat CCTV dapat dikategorikan sebagai barang bukti yang sah. Beberapa penelitian terkait investigasi dan analisis perangkat CCTV mengacu pada standar forensik di antaranya *National Institute Of Standard Technology* (NIST), Standar Nasional Indonesia (SNI) ISO/IEC 27037:2014, dan *Association of Chief Police Officers* (ACPO). Tahapan

investigasi dan analisis forensik berdasarkan NIST SP 800-86 di antaranya *collection, examination, analysis,* dan *reporting* (Kent dkk., 2006). Tahapan berdasarkan SNI ISO/IEC 27037:2014 di antaranya *identification, collection, acquisition,* dan *preservation* (Hariyadi, 2022). Tahapan berdasarkan ACPO di antaranya *Plan, capture, analysis,* dan p*resent* (Association of Chief Police Officers, 2012). Penelitian yang dilakukan oleh Ilham Asy'ari (Asy'ari dkk., 2024) menggunakan metode NIST untuk mengakuisisi barang bukti *Digital Video Recorder* (DVR) dan perangkat CCTV serta barang bukti digital berupa video rekaman CCTV, memberikan hasil analisa yang terstruktur dan dapat dipertanggung jawabkan. Selanjutnya, penelitian yang dilakukan oleh Danang Mulyadipa Suratno (Suratno dkk., 2022) membahas terkait investigasi dan analisis perangkat CCTV dengan menggabungkan standar SNI ISO/IEC 27037:2014 dan *Scientific Working Group on Imaging Technology* (SWGIT) dalam investigasi dan analisis perangkat CCTV.

Perangkat *smart* CCTV menjadi perangkat elektronik yang penting sebagai solusi pengamanan rumah. Penelitian yang dilakukan oleh Sujono (Sujono & Prayitno, 2021) membahas terkait penggunaan *smart* CCTV. *Smart* CCTV dirancang untuk memudahkan dalam *monitoring* kondisi sekitar karena menggunakan aplikasi berbasis android sebagai antarmuka pengguna. Penelitian lain yang dilakukan oleh Dedy Hariyadi (Hariyadi dkk., 2018) yang membahas terkait akuisisi barang bukti dari perangkat CCTV yang menggunakan *Digital Video Recorder* (DVR), *Network Video Recorder* (NVR), dan *smart* NVR berbasis *cloud computing* dalam memproses dan menyimpan data. Menggunakan standar ACPO dan SNI ISO/IEC 27037:2014. *Smart* NVR adalah ekosistem perekam video yang memanfaatkan teknologi *cloud computing* untuk penyimpanan dan *monitoring* menggunakan *smartphone* yang terintegrasi dalam ekosistem *smart home.*

Ekosistem *smart home* adalah kumpulan perangkat elektronik yang terhubung dalam sistem untuk otomatisasi dan *monitoring* jarak jauh. Penelitian yang dilakukan oleh Faulinda Ely Nastiti (Nastiti dkk., 2020) membahas terkait teknik akuisisi *smart* CCTV merek Xiaomi tipe Xiaofang yang menggunakan

aplikasi Mi Home pada *smartphone* bersistem operasi Android menggunakan teknik akuisisi *physical* dan *logical* sesuai standar ACPO dan SNI ISO/IEC 27037:2014. Barang bukti digital yang di dapat berupa *image* SD Card *smart* CCTV, hasil *image* SD Card *smartphone*, dan kumpulan berkas dari aplikasi Mi Home. Penelitian yang dilakukan oleh Evy Kusumaningrum (Kusumaningrum dkk., 2024) membahas terkait integrasi perangkat *smart* CCTV dengan Ekosistem *Internet of Things* (IoT) berbasis aplikasi *Home Assistant* dan aplikasi Tuya, supaya dapat memantau kondisi dan keamanan lingkungan sekolah secara *real-time*. Dalam penelitian Mauro Conti (Conti dkk., 2018) membahas tentang arsitektur di IoT yang tidak hanya menerapkan *enkripsi* pada *endpoint*, tetapi juga memperhitungkan *integrasi* dengan infrastruktur *cloud* dan *Software Defined Networking* (SDN). Karena serangan terhadap lapisan SDN atau *cloud* dapat dengan mudah menjalar ke seluruh jaringan IoT, sistem deteksi intrusi tradisional sering kali tidak memadai dalam menangani sektor serangan yang lintas lapis tersebut menunjukkan bahwa arsitektur IoT yang efektif harus mengombinasikan mekanisme keamanan perangkat *device level*, kontrol lalu lintas jaringan *network level*, hingga proteksi data di *cloud* agar ancaman dapat dicegah atau dideteksi sebelum merusak ekosistem secara luas. Kasus tindak kejahatan yang dianalisis oleh Ilham Asy'ari (Asy'ari dkk., 2024) sering terjadi dan terekam perangkat CCTV, seperti kasus tindak kejahatan pencurian di sebuah minimarket. Kasus tindak kejahatan yang analisis oleh Zul Khaidir Kadir (Kadir, 2023) berupa pencurian burung dengan kekerasan yang dilakukan oleh anak di bawah umur.

Penelitian yang telah dilakukan oleh Dedy Hariyadi (Hariyadi dkk., 2018a) tidak membahas terkait akuisisi perangkat *smart* CCTV yang terintegrasi dengan ekosistem *smart home*. Penelitian tentang akuisisi perangkat *smart* CCTV telah dilakukan oleh peneliti terdahulu tetapi belum terintegrasi dengan ekosistem *smart home*. Hal ini menimbulkan tantangan dalam proses pengumpulan barang bukti elektronik dan/atau digital, mengingat kompleksitas ekosistem *smart home* yang digunakan di antaranya perangkat *smart* CCTV, *smart home*. Maka dari itu, penelitian ini mengusulkan metode olah Tempat Kejadian Perkara (TKP) dalam proses pengumpulan dan/atau akuisisi barang bukti elektronik dan/atau digital

sesuai dengan standar ACPO dan SNI ISO/IEC 27037:2014, serta selaras dengan peraturan perundang-undangan yang berlaku di Indonesia. Perangkat yang digunakan pada ekosistem *smart home* yang terintegrasi ini di antaranya, perangkat *smart* CCTV, *Home Assistant*, dan Tuya aplikasi. Pemilihan perangkat *smart* CCTV dalam penelitian ini didasarkan pada pengumpulan bukti digital yang akurat dan autentik dari sumber yang memiliki kemampuan *monitoring* secara *real-time*. Penelitian ini hanya menggunakan ekosistem *Home Assistant* dan Tuya App dipilih karena sebuah aplikasi *open-source* dan mendukung integrasi perangkat *Internet of Things* (IoT) yang memberikan kontrol terpusat pada ekosistem *smart home*. Sedangkan Tuya App digunakan sebagai aplikasi untuk mengelola perangkat berbasis *cloud* yang telah terintegrasi dengan *smartphone*. *Smartphone* yang digunakan dalam penelitian ini juga sudah dalam keadaan *rooted* agar memudahkan dalam proses akuisisi. Proses akuisisi dalam penelitian ini akan menggunakan pendekatan teknik *physical* dan *logical* untuk mengumpulkan barang bukti digital dari berbagai media penyimpanan sesuai dengan standar ACPO dan SNI ISO/IEC 27037:2014.

1.2 Perumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, penelitian terdahulu belum melakukan akuisisi perangkat *smart* CCTV yang terintegrasi dengan ekosistem *smart home*. Hal ini menimbulkan tantangan dalam proses pengumpulan barang bukti elektronik dan/atau digital, mengingat kompleksitas ekosistem *smart home* yang digunakan di antaranya perangkat *smart* CCTV, *Home Assistant*, dan Tuya aplikasi.

Untuk menjaga fokus dan ruang lingkup penelitian tidak terlalu meluas, penelitian ini dibatasi pada perangkat-perangkat tertentu, yaitu *smart* CCTV, Raspberry Pi, dan *smart*phone Xiaomi. Sistem *smart* home yang digunakan dalam penelitian ini adalah *Home Assistant*, sementara aplikasi yang dijalankan di *smartphone* adalah Tuya. Batasan ini ditetapkan agar penelitian tetap terarah dan lebih mudah dikelola.

1.3 Pertanyaan Penelitian

Berdasarkan perumusan masalah, maka dapat diuraikan menjadi beberapa pertanyaan penelitian, di antaranya:

1. Bagaimana mengimplementasikan metode olah TKP yang menggabungkan standar ACPO dan SNI ISO/IEC 27037:2014 dalam mengakuisisi barang bukti digital dari perangkat *smart* CCTV dalam ekosistem *smart home*?
2. Bagaimana proses akuisisi barang bukti digital dari perangkat *smart* CCTV yang terintegrasi dalam ekosistem *smart home* dapat diterima sebagai barang bukti yang sah sesuai dengan perundang-undangan yang berlaku di Indonesia?

1.4 Tujuan Penelitian

Tujuan dari penelitian ini di antaranya:

1. Mengembangkan teknik olah TKP menggunakan standar ACPO dan SNI ISO/IEC 27037:2014 pada perangkat *smart* CCTV yang terintegrasi dalam ekosistem *smart home* yang sesuai dengan peraturan perundang-undangan yang ada di Indonesia.
2. Mengidentifikasi barang bukti digital pada perangkat *smart* CCTV yang terintegrasi dalam ekosistem *smart home*.

1.5 Manfaat Hasil Penelitian

Penelitian ini diharapkan dapat memberikan manfaat dalam mengembangkan metode akuisisi bukti digital dari perangkat *smart* CCTV yang terintegrasi dalam ekosistem *smart home* menggunakan standar ACPO dan SNI ISO/IEC 27037:2014, di antaranya :

1. Menghasilkan metode olah TKP yang selaras dengan peraturan perundang-undangan yang ada di Indonesia.
2. Menghasilkan petunjuk barang bukti digital yang selaras dengan peraturan perundang-undangan yang ada di Indonesia.

BAB 2
TINJAUAN PUSTAKA DAN LANDASAN TEORI

2.1 Tinjauan Pustaka

Penelitian yang dilakukan oleh Dedy Hariyadi (Hariyadi dkk., 2021) tentang akuisisi pada Xiaomi *Smart* Router Metode yang digunakan dalam akuisisi ini menggabungkan *web scraping* untuk router dan ADB untuk *smartphone* sesuai standar SNI ISO/IEC 27037:2014 sehingga bukti digital tetap otentik. Akuisisi secara langsung pada barang bukti elektronik *smart* router Xiaomi melalui *web interface* dengan menggunakan teknik *web scraping* yang memanfaatkan XPath dari *web interface smart* router Xiaomi untuk mendapatkan barang bukti digital berupa router *log* yang tersimpan secara *real-time* dan akuisisi secara langsung pada aplikasi Mi Wi-Fi yang terpasang pada *smartphone* Xiaomi untuk mendapatkan barang bukti digital berupa *file database*dari aplikasi MI Wi-Fi. Hasilnya peneliti berhasil memperoleh *log* router secara *real-time* dan *file database*Mi Wi-Fi yang menyimpan jejak aktivitas pengguna dan perangkat.

Akuisisi langsung pada pada *smartphone* Android dengan barang bukti digital *database* juga dilakukan oleh Soni (Soni dkk., 2021) yang menggunakan aplikasi WeChat dengan metode *Integrated Digital Forensics Process Model* (IDFPM) berbasis SNI ISO/IEC 27037:2014. Adapun tahapan IDFPM adalah tahap identifikasi, akuisisi, analisis, dan dokumentas. Merode ini dimulai dengan membuat *image smartphone* menggunakan ADB dan mencatat nilai *hash* MD5 serta SHA1 untuk menjaga *integritas* data. Kemudian *file database* WeChat (Enmicromsg.db) yang terenkripsi SQLCipher di dekripsi menggunakan *MobileEdit Forensic Express* dengan kunci gabungan IMEI dan UIN pengguna. Hasilnya seluruh percakapan, termasuk pesan *Cyberbullying*, beserta *metadata timestamp* berhasil dipulihkan, lengkap dengan verifikasi hash, sehingga dapat di identifikasi akun pelaku dan waktu pengiriman pesan secara akurat.

Selain itu, pendekatan berbasis NIST juga diterapkan dalam analisis forensik rekaman CCTV, seperti penelitian yang dilakukan oleh Desti Mualfah (Mualfah & Ramadhan, 2021) pada rekaman DVR CCTV menggunakan tools seperti *MediaInfo*

dan *ExifTool*. Proses tersebut mencakup pengumpulan, pemeriksaan, analisis, dan pelaporan, serta mendokumentasikan hasilnya dalam *Chain of Custody* menggunakan pendekatan 4W1H untuk menjaga keaslian dan integritas barang bukti digital. Metode ini dimulai dari tahap *collection*, *investigator* menyalin rekaman dari DVR dan menghitung hash MD5 pada *file* video untuk memastikan integritas data. Selanjutnya tahap *examination*, MediaInfo digunakan untuk mengekstrak *metadata* video di antaranya format, *codec*, durasi, ukuran dan *ExifTool* untuk mencatat *timestamp* pembuatan, *modifikasi*, dan akses *file*. Pada tahap *analysis*, *metadata* tersebut dianalisis untuk mengidentifikasi karakteristik rekaman seperti format .AVI berdurasi 14 menit 50 detik dan *codec* AVC serta merangkai kronologi peristiwa berdasarkan informasi *timestamp*. Hasilnya penelitian ini memperoleh *metadata* lengkap seperti *header*, isi dan *footer* yang memungkinkan rekonstruksi kejadian secara akurat dan menjamin bukti digital dapat dipertanggungjawabkan di pengadilan..

Menindaklanjuti hal tersebut, pengujian keaslian video CCTV juga dilakukan oleh Desti Mualfah (Mualfah dkk., 2022) menggunakan metode *Localization Tampering* yang menganalisis *frame* demi *frame* dengan pendekatan histogram RGB. Peneliti membuat dua video asli dan *tampering* kemudian menghitung hash MD5 untuk mendeteksi perbedaan *integritas*, mengekstrak *metadata* dengan *MediaInfo* untuk melihat perbedaan format dan *bit rate*, serta mengurai *frame* menjadi gambar untuk dianalisis nilai RGB-nya menggunakan JPEGSnoop dan *K-means clustering* dan analisis histogram menggunakan Matlab. Hasilnya terlihat perbedaan distribusi *pixel* pada *frame-frame* tertentu, sehingga manipulasi terlokalisasi pada frame ke-6 hingga frame ke-8. Hasil ini membuktikan bahwa metode *Localization Tampering* secara efektif dapat menentukan titik-titik manipulasi pada rekaman CCTV dengan akurasi tinggi. Metode ini mampu mengidentifikasi adanya manipulasi seperti penambahan atau penghapusan *frame* serta membandingkan *metadata* antara video asli dan video hasil manipulasi memastikan integritas bukti digital.

Seiring berkembangnya metode akuisisi, pendekatan akuisisi secara *hybrid* mulai diterapkan untuk menangkap lebih banyak data dari lingkungan jaringan

yang kompleks. Pada penelitian yang dilakukan oleh Dedy Hariyadi (Hariyadi dkk., 2023) membahas tentang metode akuisisi *hybrid* pada forensik digital berbasis ISO/IEC 27037:2012 menggunakan *port mirroring* dan *single board computer.* Menggunakan 2 metode akuisisi, yaitu metode akuisisi *live forensics* pada barang bukti elektronik router dan akuisisi *physical* pada barang bukti elektronik kartu memori. Metode akuisisi melibatkan konfigurasi *port mirroring* pada Mikrotik RB1100HX2 untuk membelokkan *traffic* ke Raspberry Pi yang menjalankan Maltrail, kemudian Raspberry Pi merekam *log* lalu lintas tersebut pada kartu memori sebelum dilakukan akuisisi *pysical* berdasarkan ISO/IEC 27037:2012. Hasilnya Maltrail berhasil mendeteksi berbagai anomali lalu lintas seperti *known attacker, malware, mass scanner*, dan *domain suspicious*. Sehingga bukti digital dari kedua sumber ini dapat digunakan untuk analisis forensik yang lebih komprehensif.

Pendekatan *mobile forensics* dikembangkan untuk menangani kasus yang lebih spesifik terutama pada perangkat *smartphone*. Salah satu penelitian yang dilakuakan oleh Amru Rizal Fakhriansyah (Fakhriansyah & Luthfi, 2024) membahas tentang fitur *second space* pada *smartphone* Xiaomi menggunakan metode akuisisi *mobile forensic* menggunakan pendekatan *live forensics* sesuai dengan standar SNI/ISO 27037:2014 pada barang bukti elektronik *smartphone* Xiaomi. Dalam penelitian ini, proses akuisisi melibatkan pengaktifan mode pengembang dan USB *debugging*, pemasangan *connector* MobilEdit Forensic Express Pro pada *First Space* dan *Second Space*, serta dua kali proses ekstraksi citra digital sesuai standar SNI/ISO 27037:2014. Hasilnya *framework* yang dikembangkan berhasil menghasilkan dua *file* ekstraksi terpisah sekaligus mengidentifikasi persyaratan akses *Second Space* (*password*, sidik jari).

Mobile forensic tidak hanya perangkat dan fitur bawaan saja, aplikasi pihak ketiga yang digunakan dalam komunikasi digital juga menjadi objek dalam analisis forensik digital yang menerapkan metode akuisisi langsung. pada penelitian yang dilakukan oleh Mahaputra Giovani (Giovani, 2024) membahas tentang forensik aplikasi Discord pada android berdasarkan ACPO *framework*. Penelitian ini menggunakan ADB untuk melakukan *kloning* data dari perangkat, kemudian

menjalankan MOBILedit *Forensic Express Pro* dan *Autopsy* sesuai kerangka ACPO untuk mengekstrak artefak Discord seperti pesan teks, gambar, video, dan dokumen. Akuisisi dilakukan pada *smartphone* Android untuk mendapatkan barang bukti digital. Hasilnya dari empat skenario yang diuji, tiga skenario berhasil memulihkan 57,8% bukti digital berupa pesan dan media, sedangkan skenario ketika aplikasi telah dihapus tidak menghasilkan bukti, ini menunjukkan bahwa akuisisi efektif ketika aplikasi tersebut masih terpasang.

Dari penelitian sebelumnya yang dijadikan acuan dalam melakukan akuisisi menunjukkan bahwa setiap metode yang digunakan memberikan informasi tentang proses akuisisi barang bukti digital. Seperti standar ACPO dan *Integrated Digital Forensics Process Model* (IDFPM) yang digunakan dalam beberapa penelitian termasuk SNI ISO/IEC 27037:2014 dan NIST SP 800-86. Termasuk penelitian yang dilakukan oleh Quang Do (Do dkk., 2018) yang membahas tentang potensi pengumpulan informasi forensik dari perangkat *smart home* dengan menggunakan dua perangkat IoT yang umumnya dianggap minim menyimpan data, yaitu lampu pintar LIFX *Original* 1000 dan saklar pintar *Belkin WeMo Switch*. Model *Adversary Forensic* terdiri dari tiga konstruksi di antaranya *Forensic Passive Adversary*, *Forensic Active Adversary*, dan *Real-time Active Adversary.* Dua Adversary pertama diwajibkan mematuhi prinsip *forensic soundness* yakni menjaga *integritas* dan keaslian bukti sepanjang proses pengumpulan sementara *Real-time Active Adversary* beroperasi tanpa batasan forensik untuk merepresentasikan penyerangan di dunia nyata. Pada lampu LIFX *Original* 1000, *Adversary pasif* melakukan *sniffing* paket UDP *StateWifiInfo* dan *State* yang dikirim ke lampu setiap lima detik untuk memperoleh status *on/off,* warna, intensitas, kekuatan sinyal, dan label pengguna tanpa interaksi langsung. *Adversary* aktif mengirim perintah UDP *GetService* dan serangkaian perintah *GetHostInfo*, *GetVersion*, *GetPower*, *GetInfo*, serta *Get* untuk mengekstrak *metadata* perangkat tanpa *autentikasi*. *Adversary Real-time* menggunakan *ARP spoofing* untuk *intercept* dan memodifikasi paket kontrol lampu seperti mengubah *brightness* atau warna sehingga lampu dapat berfungsi sebagai kanal kovert untuk *eksfiltrasi* data atau serangan *photosensitive epilepsy trigger*.

Penelitian yang akan dilakukan oleh penulis memiliki beberapa kesamaan dengan penelitian sebelumnya terutama dalam metode akuisisi *mobile* forensik dan akuisisi *hybrid*, juga dalam pengumpulan informasi dalam ekosistem *smart home*. Namun ada perbedaan dalam objek yang digunakan dalam penelitian ini secara khusus hanya menargetkan perangkat *smart* CCTV yang terintegrasi ekosistem *smart home*.

Berdasarkan Tabel 2.1 dan penjelasan sebelumnya dapat disimpulkan bahwa metode dan hasil penelitian terdapat beberapa persamaan dalam hal pendekatan akuisisi dan standar forensik, penelitian ini memiliki perbedaan tersendiri, yaitu *smart* CCTV yang terintegrasi dengan ekosistem *smart home* dan belum ada penelitian yang melakukan akuisisi pada perangkat *smart* CCTV yang terintegrasi dengan ekosistem *smart home.* Maka penelitian ini memberikan kontribusi baru dalam forensik IoT.

Tabel 2.1 Tinjauan Pustaka

No	Nama	Barang Bukti Digital	Barang Bukti Elektronik	Metode	Hasil
1	Dedy Hariyadi, 2021	1. Router *log* 2. *Database*aplikasi Mi Wi-Fi	1. *Smart* Route Xiaomi 2. *Smartphone* Xiaomi	*Live acquisition*, SNI ISO/IEC 27037:2014, dan NIST SP 800-86	Mendapatkan barang bukti digital berupa *log* hasil dari *smart* router Xiaomi dan *database* dari Xiaomi aplikasi Mi Wi-Fi.
2	Mualfah dkk., 2021	*Metadata* rekaman CCTV	DVR CCTV	NIST (4 tahap: akuisisi, pemeriksaan, analisis, pelaporan)	*Metadata* diverifikasi dengan MediaInfo & ExifTool; *Chain of Custody*

No	Nama	Barang Bukti Digital	Barang Bukti Elektronik	Metode	Hasil
3	Soni, 2021	*Databas e*aplikasi WeChat	*Smartphone* Android	*Integrated Digital Forensics Process Model* (IDFPM) berbasis SNI ISO/IEC 27037:2014	Mengamankan barang bukti digital dalam bentuk *database* hasil dari akuisisi aplikasi Wechat yang berisikan pesan percakapan verbal dan nilai *hashing* md5 dan sha1 yang autentik, serta *metadata* atau *timestamp* pada pesan percakapan aplikasi media sosial WeChat.
4	Mualfah dkk., 2022	Video *frame* & histogram RGB	Video rekaman CCTV	*Localization Tampering*	Identifikasi manipulasi *frame* & *metadata* video
5	Dedy Hariyadi, 2023	*Log* Maltrail	1. Router (Mikrotik RB1100HX2) 2. Raspberry Pi 3. Memory	Akuisisi *hybrid* dan *live acquisition*	Mengakuisisi *log* maltrail dari Raspberry Pi

No	Nama	Barang Bukti Digital	Barang Bukti Elektronik	Metode	Hasil
			Card		
6	Fakhriansyah & Luthfi, 2024	*Database* fitur *Second Space*	*Smartphone* Xiaomi	*Mobile forensic acquisition* berbasis SNI/ISO 27037:2014 untuk *Second Space* pada perangkat *Smart*phone Xiaomi	Mendapatkan barang bukti digital dalam bentuk *database* hasil dari akuisisi fitur *second space.*
7	Giovani Mahaputra, 2024	*Database* aplikasi Discord	*Smartphone* Android	Analisis forensik menggunakan ACPO *Framework*	Mendapatkan barang bukti digital dalam bentuk *database* hasil dari akuisisi aplikasi Discord yang menggunakan empat skenario.

No	Nama	Barang Bukti Digital	Barang Bukti Elektronik	Metode	Hasil
8	Ahmad Naufal, 2025	*Databas e*aplikasi Tuya, *Imaging smart* CCTV dan *Home Assistant*.	1. BARDI *Smart* IP *Camera Outdoor* PTZ. 2. Raspberry Pi 4. 3. SD *Card.* 4. *Smartpho ne* Xiaomi 5 Plus (*Rooted)*.	ACPO dan SNI ISO/IEC 27037:2014, menggunaka n 2 metode akuisisi *physical* dan *logical*.	

2.2 Landasan Teori

2.2.1 Forensik Digital

Forensik Digital adalah cabang ilmu yang berhubungan dengan barang bukti elektronik dan digital untuk mengidentifikasi bukti tersebut dalam penegakan hukum. Proses ini melibatkan investigasi tindak kejahatan di dunia siber yang melibatkan perangkat elektronik. Tindak kejahatan digital terbagi menjadi dua, yaitu *computer crime* dan *computer-related crime. Computer crime* melibatkan pelaku yang menggunakan perangkat elektronik untuk merusak sistem komputer, seperti *web defacement*. Sementara itu, *computer-related crime* menggunakan perangkat elektronik untuk melakukan tindakan tidak etis, seperti ancaman melalui pesan singkat atau pencemaran nama baik di media sosial (Hariyadi, 2022).

Forensik digital juga didukung oleh berbagai teori ilmiah yang menjadi fondasi dalam memastikan keabsahan bukti dan proses investigasi. Salah satu teori mendasar adalah *Locard's Exchange Principle* yang menyatakan bahwa setiap

aktivitas digital akan meninggalkan jejak. Jejak digital ini bisa berupa *file log, cache,* atau artefak lain yang dapat dianalisis oleh penyidik. Teori ini diperkuat oleh konsep *Digital Evidence Dynamics*, yang menjelaskan bahwa bukti digital dapat berubah akibat aktivitas sistem atau manipulasi, sehingga penting untuk menjaga integritasnya melalui prinsip *chain of custody* (Olivier, 2016).

Dalam kasus dengan data yang rusak atau tidak lengkap, pendekatan berbasis *Rough Set Theory* sangat berguna. Teori ini memungkinkan penyidik mengidentifikasi bukti relevan meskipun informasinya tidak sempurna, serta meningkatkan akurasi proses klasifikasi data (Gupta dkk., 2022). Sedangkan untuk pengembangan organisasi dan riset forensik, *Grounded Theory* dipakai untuk membentuk teori baru berdasarkan praktik nyata di lapangan, terutama dalam pengelolaan laboratorium forensik dan kapabilitas penyidik digital (Almarzooqi dkk., 2016).

Barang bukti adalah benda yang disita dan diajukan ke persidangan untuk keperluan pembuktian (Hardhika, 2024). Adapun *Rules of Evidence* merupakan sebuah pengaturan barang bukti di mana barang bukti harus memiliki keterkaitan dengan kasus yang diinvestigasi dan memiliki kriteria seperti pada Tabel 2.2.

Tabel 2.2 Kriteria Barang Bukti RFC

No	Kriteria	Keterangan
1.	Layak dan dapat diterima (*Admissible*)	Barang bukti harus dapat diterima dan digunakan demi hukum, mulai dari kepentingan penyidikan sampai ke pengadilan.
2.	Asli (*Authentic*)	Barang bukti harus mempunyai hubungan keterkaitan yang jelas secara hukum dengan kasus yang diselidiki dan bukan rekayasa.
3.	Akurat (*Accurate*)	Barang bukti harus akurat dan dapat dipercaya.
4.	Lengkap (*Complete*)	Barang bukti dikatakan lengkap jika di dalamnya terdapat petunjuk-petunjuk yang

No	Kriteria	Keterangan
		lengkap dan terperinci dalam membantu proses investigasi.

Menurut Zuhri, e*vidence* yang dimaksud dalam kasus forensik pada umumnya tidak lain adalah informasi dan e*vidence*. Menurut salah satu ahli forensik Indonesia Muhammad Nuh, beberapa klasifikasi barang bukti forensik yaitu: (Juman, 2018)

a) Barang Bukti Elektronik

Barang bukti elektronik adalah barang bukti yang bersifat fisik dan dapat dikenali secara visual, sehingga data. Cara pandangnya sama saja, tetapi dalam kasus komputer forensik, kita mengenal subjek tersebut sebagai *Digital investigator* dan analis forensik harus sudah memahami barang bukti tersebut ketika sedang melakukan proses pencarian barang bukti di TKP. Barang bukti elektronik dapat dicontohkan di antaranya, komputer PC, laptop, *tablet*, *flash disk*, *hard disk*, router/switch/hub, kamera digital, musik/video *player*, *smartphone*, *floppy disk*, CD/DVD, kamera video, CCTV, *digital recorder*.

b) Barang Bukti Digital

Barang bukti digital adalah data-data yang dikumpulkan dari semua jenis penyimpanan digital yang menjadi subjek pemeriksaan forensik komputer. Barang bukti digital bersifat digital yang diekstrak dari barang bukti elektronik. Barang bukti digital dapat dicontohkan di antaranya, *logical file, deleted file, lost file, file slack, log file, encrypted file.*

2.2.2 SNI ISO/IEC 27037:2014

Standar ini memberikan panduan kepada individu berkenaan dengan situasi-situasi umum yang dihadapi sepanjang proses penanganan bukti digital dan membantu organisasi dalam prosedur penegakan disiplinnya serta dalam memudahkan pertukaran bukti digital potensial antara yurisdiksi (*Terjemahan SNI ISO/IEC 27037 "Teknologi Informasi - Teknik Keamanan Panduan Identifikasi,*

Koleksi, Akuisisi dan Preservasi Bukti Digital," 2014). Kerangka kerja SNI ISO/IEC 27037:2014 ini memiliki tahapan seperti pada Gambar 2.1.

Gambar 2.1 Tahapan kerangka kerja SNI ISO/IEC 27037:2014

Standar ini memberikan pedoman untuk kegiatan yang spesifik dalam menangani bukti digital, yaitu:

1. Identifikasi (*Identification*)

   Proses identifikasi melibatkan pencarian, pengenalan, dan dokumentasi bukti digital potensial. Proses identifikasi harus mengenali media penyimpanan digital dan perangkat pemrosesan yang berisi bukti digital potensial yang relevan dengan perkara.
2. Koleksi (*Collection*)

   Koleksi adalah proses penanganan bukti digital ketika perangkat yang berisi bukti digital potensial dipindahkan dari lokasi asli ke laboratorium atau lingkungan lain yang terkendali untuk akuisisi dan analisis selanjutnya.
3. Akuisisi (*Acquisition*)

   Proses akuisisi melibatkan penghasilan salinan bukti digital (misalnya *hard disk* utuh, partisi, *file* terpilih) dan mendokumentasikan metode yang digunakan dan tindakan yang dilakukan.
4. Preservasi (*Preservation*)

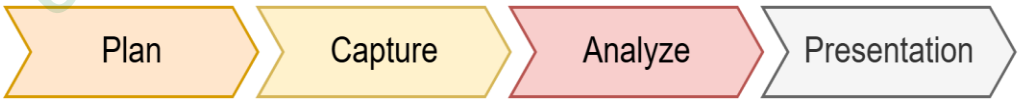
   Bukti digital potensial harus dipelihara untuk menjamin kegunaannya dalam investigasi. Melindungi integritas dari bukti menjadi hal yang penting. Proses preservasi melibatkan pengamanan bukti digital potensial dan perangkat digital yang mengandung bukti digital potensial dari perusakan atau pengubahan. Proses preservasi dimulai dan dikelola pada seluruh proses penanganan bukti digital, sejak dari identifikasi perangkat digital yang mengandung bukti digital potensial.

Prinsip dalam penanganan barang bukti elektronik dan barang bukti digital berdasarkan SNI ISO/IEC 27037:2014, di antaranya: (*Terjemahan SNI ISO/IEC 27037 "Teknologi Informasi - Teknik Keamanan Panduan Identifikasi, Koleksi, Akuisisi dan Preservasi Bukti Digital,"* 2014):

1. Meminimalkan penanganan perangkat digital asli atau bukti digital potensial.
2. Memperhitungkan perubahan apa pun dan mendokumentasikan tindakan yang diambil.
3. Mematuhi aturan pedoman bukti lokal.
4. Penanggap Pertama Bukti Digital dan Spesialis Bukti Digital tidak boleh melakukan tindakan melebihi kompetensi mereka.

2.2.3 Standar ACPO

Asosiasi kepolisian di Inggris, *Association of Chief Police Officers* (ACPO) bekerja sama dengan perusahaan keamanan informasi *7safe* membuat petunjuk penanganan barang bukti elektronik dan/atau digital. Petunjuk yang dibuat tersebut tidak hanya dapat diterapkan di lingkungan kepolisian Inggris, tetapi dapat diterapkan pada kepolisian di negara lain termasuk penyidik swasta untuk sektor khusus. Kepolisian Republik Indonesia melalui Pusat Laboratorium Forensik juga menerapkan petunjuk dari ACPO dalam penanganan barang bukti elektronik dan/atau digital (Hariyadi dkk., 2018b). Kerangka kerja ini memiliki Tahapan seperti pada Gambar 2.



Gambar 2.2 Tahapan Kerangka Kerja ACPO

Tahapan-tahapan tersebut dijelaskan secara rinci sebagai berikut:

1. *Plan*

   Merupakan tahap perencanaan dan perancangan segala sesuatu yang akan dilakukan selama penelitian berlangsung. Di dalamnya berisi

pembuatan proses penelitian, dan menentukan *software* atau *tools* yang akan digunakan.

2. *Capture*

   Tahap ini melakukan akuisisi data berupa penyalinan data dari *smart*phone yang digunakan dengan menggunakan *tools* yang tersedia.

3. *Analyze*

   Tahap ini menganalisis data yang telah didapatkan untuk mengetahui barang bukti apa saja yang dapat dimanfaatkan sebagai barang bukti digital.

4. *Presentation*

   Tahap ini adalah merilis data penelitian yang kini menjadi informasi yang relevan dan dapat dipertanggungjawabkan. Tindakan dan hasil penelitian diberikan secara lengkap. Saran-saran yang terkait dengan hasil penelitian juga diberikan.

Adapun Prinsip dalam penanganan barang bukti elektronik dan barang bukti digital berdasarkan ACPO, di antaranya: *(Association of Chief Police Officers*, 2012):

1. Menjaga Integritas

   Tidak ada tindakan yang diambil yang dapat mengubah data yang tersimpan pada perangkat digital termasuk komputer atau telepon seluler yang selanjutnya dapat dijadikan bukti di pengadilan.

2. Kompetensi Teknis (hanya diakses oleh ahli)

   Apabila seseorang merasa perlu untuk mengakses data asli yang tersimpan pada perangkat digital, orang tersebut harus kompeten untuk melakukannya dan mampu menjelaskan tindakannya serta implikasi tindakan tersebut pada bukti digital tersebut kepada Pengadilan.

3. Jejak Audit

   Jejak atau rekaman semua tindakan yang telah dilakukan dan diterapkan pada bukti digital harus dibuat dan disimpan. Pakar forensik pihak ketiga yang independen harus dapat memeriksa proses tersebut dan mencapai kesimpulan yang sama.

4. Tanggung Jawab Investigatif

   Bahwa individu yang bertanggung jawab atas investigasi memiliki tanggung jawab keseluruhan untuk memastikan bahwa prinsip-prinsip ini dipatuhi.

2.2.4 Investigasi Forensik

Investigasi forensik digital adalah disiplin ilmu yang berkembang untuk menganalisis bukti elektronik dalam berbagai kasus, seperti kejahatan siber, pelanggaran kebijakan perusahaan, dan investigasi hukum. Teori lain yang mendukung adalah *Locard's Exchange Principle* yang menyatakan bahwa setiap interaksi dalam sistem digital meninggalkan jejak yang dapat dianalisis sebagai bukti. Selain itu, *Digital Evidence Dynamics* membahas bagaimana bukti digital dapat berubah karena aktivitas sistem atau manipulasi manusia, sehingga penting untuk menjaga integritasnya dengan rantai penjagaan bukti (*Chain of Custody*) (Olivier, 2016).

Proses investigasi forensik digital terdiri dari beberapa langkah utama: pengumpulan bukti, analisis data, dan pelaporan hasil. Setiap langkah harus dilakukan dengan hati-hati untuk memastikan bahwa bukti tetap utuh dan dapat diterima di pengadilan (Uwatun, 2024).

Pendekatan *Narrative Theory* dan *Surrealism Theory* juga mulai diterapkan untuk memahami pola bukti sebagai rangkaian cerita digital. *Narrative Theory* melihat media penyimpanan sebagai narasi multidimensi yang saling berkaitan, sedangkan Surrealism digunakan untuk menginterpretasi artefak digital yang tampak tidak beraturan atau fragmentaris (Pollit, 2009).

2.2.5 Data *Carving*

Data *Carving* didasarkan pada asumsi bahwa dalam kondisi di mana struktur dan *metadata* sistem berkas hilang atau korup seperti akibat proses pemformatan, penghapusan, atau keberadaan data pada ruang "*lost*" dan "*unallocated*" satu-satunya cara untuk memulihkan berkas digital adalah dengan mengekstraksi potongan data mentah berupa *raw* data. Metode ini menitikberatkan pada pencarian

pola tanda tangan berkas yaitu *byte-signature* khusus yang terdapat pada bagian awal/*header* dan bila tersedia bagian akhir/*footer* suatu berkas. Karena setiap format berkas memiliki *signature* yang khas seperti JPEG diawali FF D8 FF E0, MP4 diawali 66 74 79 70 atau 69 73 6F 6D, MOV diawali 6D 6F 6F 76, dan AVI diawali 41 56 49 20 atau 4C 49 53 54. penelusuran *signature* tersebut pada aliran *byte* mentah memungkinkan ekstraksi seluruh isi berkas, selama *byte-signature* belum tertimpa atau terkorupsi oleh data lain. Teori ini memformulasikan beberapa pendekatan *carving* sesuai karakteristik format berkas:

1. *Header-Footer Carving*

   Signature awal dan akhir teridentifikasi dalam data mentah, semua *byte* di antara kedua tanda tersebut di ekstraksi sebagai satu unit berkas.

2. *Header-Embedded Length Carving*

   Format berkas ZIP memuat informasi panjang berkas di dalam *header*. Dengan demikian setelah menemukan *header*, membaca nilai panjang berkas dan mengekstrak data sebanyak itu tanpa perlu mencari *signature* akhir.

3. *File Structure Based Carving*

   Format dengan struktur internal kompleks seperti PDF atau format video AVI analisis dilakukan pada elemen-elemen struktural internal guna memverifikasi konsistensi data yang diambil dengan skema format berkas. Pendekatan ini secara signifikan menurunkan tingkat *false positive*.

4. *Carving with Validation*

   Berkas yang diperoleh divalidasi melalui pemeriksaan spesifik format misalnya memverifikasi *marker* JPEG secara menyeluruh. Jika pemeriksaan tidak konsisten berkas dianggap rusak dan diabaikan.

5. *Header-Max File Size Carving*

   Format yang tidak memiliki *footer* atau informasi panjang berkas akan dilakukan ekstraksi hingga mencapai batas ukuran maksimum yang telah ditetapkan berdasarkan jenis berkas, sehingga mencegah pengekstrakan data non-berkas.

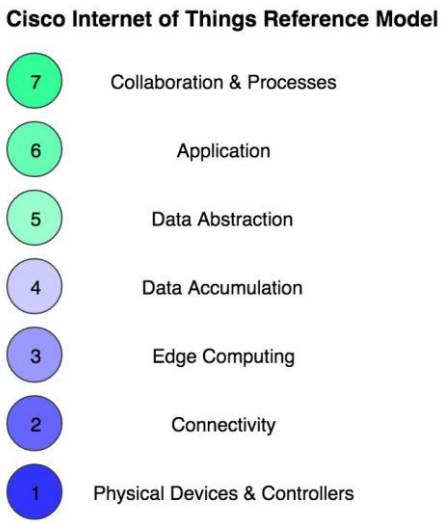
Teori *carving* juga menekankan optimalisasi proses pencarian *signature*. Memindai setiap *byte* secara berurutan dapat digunakan algoritme *string search* efisien seperti Boyer Moore dan pembatasan pada *byte-byte* awal setiap *cluster* atau sektor yang berpotensi memuat berkas terhapus (Povar & Bhadran, 2011).

2.2.6 Arsitektur *Internet of Things*

Arsitektur IoT menurut Mauro Conti (Conti dkk., 2018) adalah struktur yang memungkinkan perangkat, layanan *cloud*, dan protokol saling terhubung untuk menciptakan ekosistem IoT. Jaringan ini terdiri dari sensor, *controller* konektivitas dan elemen terhubung lainnya yang memungkinkan aliran data dari sumber fisik melalui jaringan ke penyimpanan di *cloud*.

Tujuan arsitektur ini adalah mengelola informasi yang dikumpulkan oleh perangkat IoT sehingga dapat dianalisis atau diproses sesuai kebutuhan. Perangkat, sensor, dan infrastruktur jaringan semuanya harus bekerja sama agar komunikasi berjalan dengan sukses. Dengan itu maka data yang dikumpulkan dapat di analisa memenuhi tugas-tugas tertentu (Buyya & Dastjerdi, 2016).

Arsitektur di IoT tidak hanya menerapkan *enkripsi* pada *endpoint*, tetapi juga memperhitungkan integrasi dengan infrastruktur *cloud* dan *Software Defined Networking* (SDN). Karena serangan terhadap lapisan SDN atau *cloud* dapat dengan mudah menjalar ke seluruh jaringan IoT, sistem deteksi intrusi tradisional sering kali tidak memadai dalam menangani vektor serangan yang lintas lapis tersebut menunjukkan bahwa arsitektur IoT yang efektif harus mengombinasikan mekanisme keamanan perangkat *device level*, kontrol lalu lintas jaringan *network level*, hingga proteksi data di *cloud* agar ancaman dapat dicegah atau dideteksi sebelum merusak ekosistem secara luas. Pada gambar 2.3 merupakan contoh 7-layer arsitektur IoT *by* Cisco.



Gambar 2.3 *7-Layer*Arsitektur Internet of Things *by* Cisco (Smith dkk., 2020).

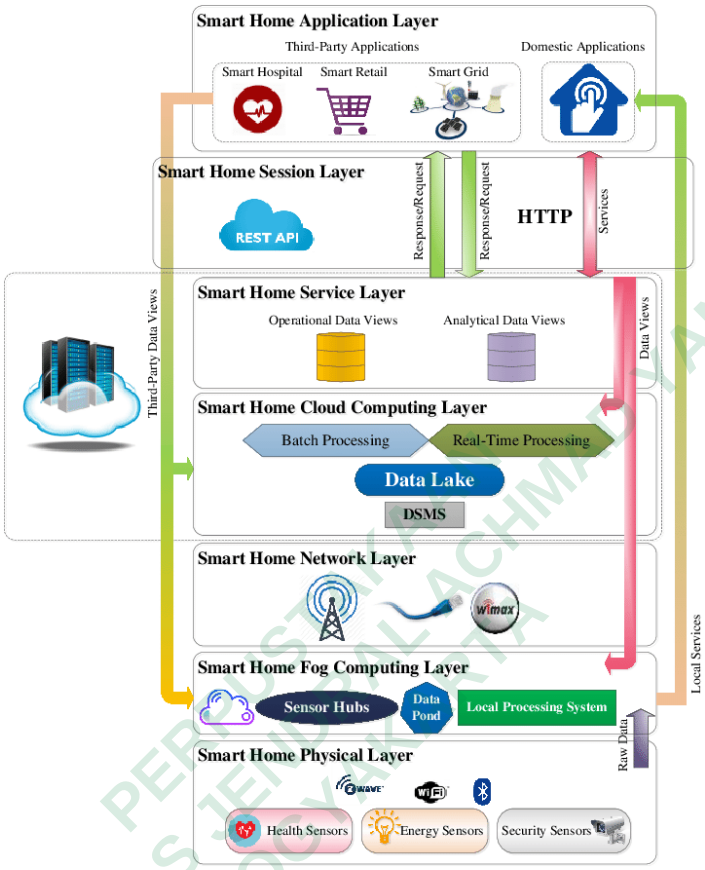
2.2.7 Ekosistem *Smart Home*

Ekosistem *smart home* adalah konsep yang mengintegrasikan perangkat elektronik berbasis Internet of Things (IoT) untuk mengendalikan berbagai perangkat elektronik secara otomatis dan jarak jauh. Melalui ekosistem *smart home* perangkat elektronik seperti lampu, pendingin udara, sistem keamanan, dan peralatan elektronik lainnya yang dapat dikendalikan melalui *smart*phone, tablet, atau perangkat lain yang terhubung ke internet (Imam, 2023).

Menurut Tang dan Inoue, tiga hal penting yang menentukan keberhasilan ekosistem *smart home* yaitu *interoperabilitas* adalah kemampuan antar perangkat untuk saling berkomunikasi, *modularitas* adalah kemudahan untuk menambah dan mengganti perangkat serta hubungan antar pengguna. Model seperti ini menjadi dasar dari berbagai aplikasi terkenal seperti *Google Home, Apple HomeKit*, dan *Amazon Alexa* (Tang & Inoue, 2021).

Menurut Mladenova ekosistem *smart home* bekerja dengan menghubungkan berbagai perangkat melalui protokol komunikasi seperti Wi-Fi, Zigbee, atau Bluetooth, yang kemudian dikendalikan oleh sebuah *hub* pusat atau aplikasi. Arsitekturnya biasanya terdiri dari empat lapisan: sensor dan aktuator, pengendali, *cloud* atau server lokal, dan aplikasi *mobile* atau *web*. Sistem ini mendukung otomatisasi berdasarkan preferensi pengguna, misalnya lampu otomatis menyala

saat sensor gerak mendeteksi keberadaan, atau AC menyala saat suhu ruangan naik (Mladenova & Cankov, 2023). Seperti pada gambar 2.4.

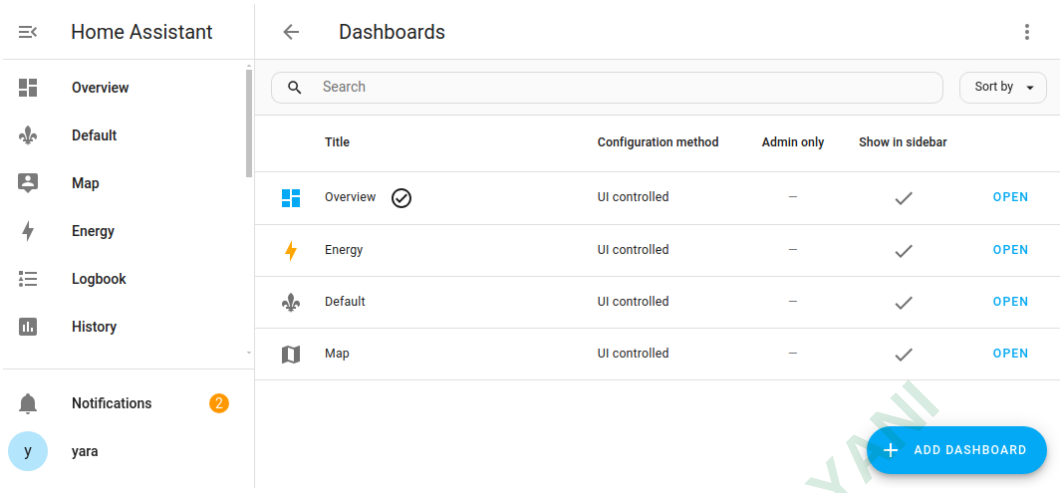


Gambar 2.4 Arsitektur Ekosistem *Smart Home* (Mokhtari dkk., 2019)

2.2.8 *Home Assistant*

Home Assistant adalah sistem otomatisasi rumah yang mengintegrasikan ekosistem *smart home* dan berbagai perangkat pintar dalam satu aplikasi untuk meningkatkan kenyamanan, efisiensi, dan keamanan rumah. Konsep ini didasarkan pada beberapa teori utama, di antaranya. *Internet of Things* (IoT) yang menghubungkan perangkat rumah tangga agar dapat berkomunikasi dan dikendalikan dari jarak jauh melalui internet (Tamanna & Lima, 2023).

Home Assistant juga mendukung ribuan integrasi dengan perangkat dari berbagai merek dan protokol seperti Zigbee, Z-Wave, dan Wi-Fi. Membangun sistem otomatisasi yang fleksibel dan dapat di *costume* sesuai kebutuhan. *Home Assistant* dapat dijalankan pada perangkat Raspberry Pi, komputer mini, atau server lokal (Assistant, 2025). Dashboard *Home Assistant* seperti pada Gambar 2.5



Gambar 2.5 *Dashboard Home Assistant*

Cara kerja *Home Assistant* ini sama seperti ekosistem *smart home* bekerja dengan menghubungkan berbagai perangkat melalui protokol komunikasi seperti Wi-Fi, Zigbee, atau Bluetooth, yang kemudian dikendalikan oleh sebuah hub pusat atau aplikasi (Mladenova & Cankov, 2023).

2.2.9 Tuya App

Tuya App adalah sebuah aplikasi yang dikembangkan oleh Tuya *Smart* Inc. dengan fitur pengguna mengendalikan peralatan rumah tangga mereka dari jarak jauh. Dengan aplikasi ini pengguna dapat menambahkan dan mengendalikan beberapa perangkat sekaligus. Aplikasi ini juga memungkinkan pengguna berbagi perangkat dan menerima peringatan secara *real-time* untuk memastikan keamanan (Tuya *Smart*, 2025).

Aplikasi Tuya App ini berbasis *cloud* yang memungkinkan pengguna untuk mengendalikan perangkat dari jarak jauh melalui *smartphone*. Pada Gambar 2.6 merupakan tampilan *dashboard* dari aplikasi Tuya yang diakses menggunakan *smartphone*. *Dashboard* ini menyajikan antarmuka yang intuitif dan *user friendly*, memudahkan pengguna dalam memantau status perangkat, mengatur jadwal otomatisasi, serta menerima *notifikasi* secara *real-time.* Selain itu, Tuya App juga mendukung integrasi dengan berbagai *smartphone*, sehingga memberikan fleksibilitas dan kenyamanan dalam mengelola ekosistem *smart home* secara efisien melalui satu aplikasi.

Gambar 2.6 *Dashboard* Tuya App

Cara kerja Tuya App ini sama seperti ekosistem *smart home* dan *Home Assistant* bekerja dengan menghubungkan berbagai perangkat melalui protokol komunikasi seperti Wi-Fi, Zigbee, atau Bluetooth, yang kemudian dikendalikan oleh sebuah *hub* pusat atau aplikasi (Mladenova & Cankov, 2023).

2.2.10 *Closed-Circuit Television* (CCTV)

CCTV atau *Closed-Circuit Television* adalah sistem pengawasan yang bekerja dengan menangkap, mentransmisikan, dan menampilkan gambar dari area tertentu secara tertutup. Proses kerjanya diawali oleh kamera CCTV yang merekam aktivitas di sekitarnya. Kamera ini bisa berupa jenis ana*log* atau digital, tergantung pada sistem yang digunakan. Hasil rekaman tersebut kemudian dikirimkan ke perangkat penyimpanan, seperti DVR untuk sistem ana*log* atau NVR untuk sistem digital, melalui kabel atau koneksi jaringan seperti Wi-Fi atau LAN.

CCTV digunakan untuk memantau dan merekam aktivitas di area tertentu dengan tujuan keamanan, pemantauan, atau investigasi. Teknologi pengawasan CCTV di mana sejumlah kamera video dihubungkan dalam sirkuit dengan gambar yang dihasilkan dikirim ke monitor televisi pusat atau direkam. Kemajuan teknologi sekarang memungkinkan sistem CCTV bekerja pada jaringan nirkabel, dioperasikan dari jarak jauh, dan dilihat dari beberapa lokasi.

Saat ini CCTV digunakan sebagai istilah umum untuk berbagai teknologi pengawasan video termasuk *Police Observation Devices* (POD) atau *Portal Overt Digital Surveillance Systems* (PODS). Salah satu instrumen yang dapat mengurangi tindak kejahatan di suatu daerah adalah lokasi penempatan CCTV (Ratcliffe, 2021). Ada tiga jenis peletakan CCTV:

1. *Open System*, pemasangan di area yang dapat dilihat dengan jelas oleh masyarakat dan diberi penanda bahwa ada CCTV yang terpasang.
2. *Open System*, Tersembunyi, CCTV dipasang di area yang dapat dilihat dengan jelas oleh masyarakat namun dilindungi oleh *casing* transparan satu arah.
3. *Hidden System*, CCTV dipasang di area tersembunyi sehingga masyarakat tidak menyadari bahwa area tersebut sedang dipantau oleh CCTV.