JUSTISE
E-ISSN : XXXX-XXXX
Journal Data Science, Technology, Informatics and Security (JuSTISe)
Volume 2 No 2 Desember 2024

INVESTIGASI DIGITAL FORENSIK PADA PERANGKAT *IOT* DALAM SISTEM RUMAH PINTAR (*SMART HOME*) MENGGUNAKAN *FRAMEWORK APPLICATION SPECIFIC INVESTIGATION MODEL (FASIM)*

Deni Koswara[1], Deni Suprihadi[2]
Program Studi Teknik Informatika, Universitas Kebangsaan Republik Indonesia, Bandung
Email : denidexler@gmail.com[1], dens.tesis99@gmail.com[2]

ABSTRAK

Perkembangan pesat Internet of Things (IoT) memberikan peluang dan tantangan baru dalam konteks keamanan siber, khususnya dalam sistem rumah pintar (smart home). Penelitian ini bertujuan untuk menginvestigasi keamanan dan privasi perangkat IoT di lingkungan smart home menggunakan framework Application Specific Investigation Model (FASIM). Fokus penelitian ini adalah pada proses akuisisi, analisis, dan pelaporan bukti digital dari perangkat-perangkat IoT seperti pengontrol lampu, kamera keamanan, pengontrol suhu, dan pengunci pintu. Metode yang digunakan meliputi identifikasi perangkat IoT, analisis data menggunakan tools seperti Hercules, WireShark, FFMPEG, dan Fing, serta penggunaan hashing MD5 untuk memastikan integritas data. Hasil penelitian menunjukkan bahwa setiap perangkat IoT dalam sistem rumah pintar mampu memberikan jejak digital yang valid dan dapat diolah lebih lanjut dalam investigasi digital forensik. Penelitian ini diharapkan dapat memberikan kontribusi signifikan dalam meningkatkan keamanan dan privasi pada sistem rumah pintar, serta sebagai dasar bagi pengembangan penelitian di masa depan terkait investigasi forensik digital pada perangkat IoT.

Kata kunci : *Internet of Things, Smart Home,* Digital Forensik.

ABSTRACT

The rapid development of the Internet of Things (IoT) presents new opportunities and challenges in cybersecurity, particularly in smart home systems. This study aims to investigate the security and privacy of IoT devices in smart home environments using the Application Specific Investigation Model (FASIM) framework. The research focuses on the processes of acquisition, analysis, and reporting of digital evidence from IoT devices such as light controllers, security cameras, temperature controllers, and door locks. The methods include identifying IoT devices, analyzing data using tools such as Hercules, WireShark, FFMPEG, and Fing, as well as utilizing MD5 hashing to ensure data integrity. The findings reveal that IoT devices in smart home systems can provide valid digital traces that can be further processed in digital forensic investigations. This study is expected to contribute significantly to enhancing the security and privacy of smart home systems and serve as a foundation for future research on digital forensic investigations of IoT devices.

***Keywords*:** *Internet of Things, Smart Home, Digital Forensics.*

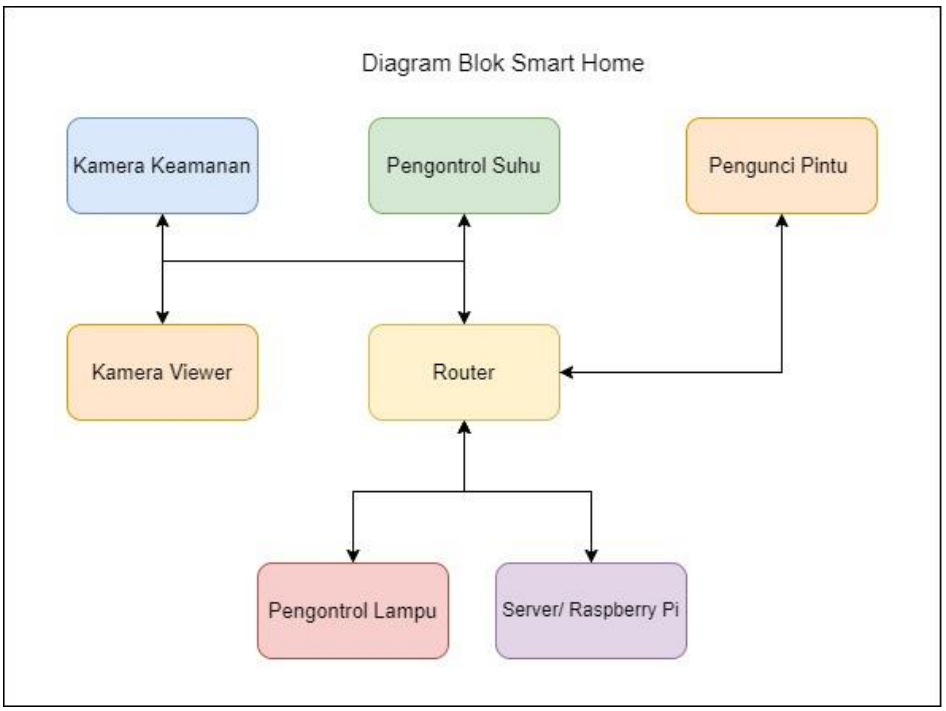
1. PENDAHULUAN

Internet of Things (IoT) berkembang pesat, menciptakan peluang sekaligus tantangan dalam investigasi kejahatan, termasuk serangan siber dan intrusi fisik. Rumah pintar dan lingkungan IoT lainnya yang saling terhubung, dinamis, dan dapat diakses jarak jauh membuat perangkat IoT menjadi saksi digital yang mampu merekam jejak aktivitas. Perangkat ini dapat menjadi sumber bukti berharga jika penyelidik mampu mengelola data dalam jumlah besar, keragaman perangkat, heterogenitas protokol, serta sifat distribusinya.

Berdasarkan data, jumlah perangkat IoT global diperkirakan meningkat dari 15,1 miliar pada 2020 menjadi lebih dari 29 miliar pada 2030, dengan China memimpin di angka 8 miliar perangkat. Namun, studi Hewlett Packard (2015) menunjukkan 80% perangkat IoT memiliki risiko privasi, dan 60% tidak memiliki mekanisme validasi pembaruan keamanan, membuatnya rentan terhadap manipulasi firmware. Kerentanan ini terlihat dalam serangan Mirai botnet 2016 yang memanfaatkan kata sandi default lemah untuk melancarkan serangan DDoS besar-besaran.

Jarangnya pembaruan perangkat lunak memperburuk kerentanan IoT, sehingga inovasi berkelanjutan menjadi kebutuhan utama. Dalam konteks forensik digital, investigasi perangkat IoT dapat memastikan integritas data dan menyediakan bukti signifikan dalam proses hukum. Penelitian ini menggunakan framework *Application Specific Investigation Model* untuk menganalisis bukti digital dari perangkat IoT, yang diharapkan dapat membantu pihak berwenang menyelesaikan kasus terkait IoT.

2. METODE PENELITIAN

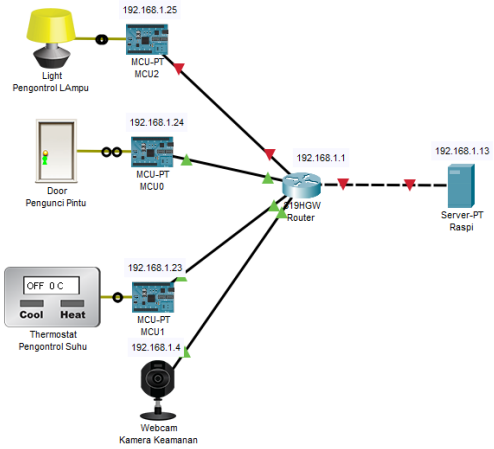


Gambar 1. Diagram Blok Smart Home

Penelitian ini menggunakan metode *Model of Devices DNA and Genes* pada *Framework Application Specific Investigation Model*. *Model of Devices DNA and Genes* adalah tahapan pendekatan pada perangkat IoT, sebelum melakukan investigasi maka kita melakukan pendekatan dulu ke perangkat IoT dengan cara mengidentifikasi masing masing perangkat IoT. Untuk mengumpulkan data dari berbagai perangkat *IoT*, menggunakan aplikasi Hercules, FTK, WireShark untuk identifikasi dan pengumpulan data dari perangkat *IoT*. Data dan informasi yang diambil dalam penelitian ini adalah data pada perangkat *IoT* yang meliputi data Pengontrol Lampu, Kamera Keamanan, Pengaontrol Suhu dan pengunci pintu, aktivitas dalam jaringan Smart Home. Data yang dipakai dalam penelitian ini diambil dari Perangkat *IoT*. Proses pengumpulan data dan informasi sebagai pendukung penelitian ini harus memiliki tujuan yang jelas.

3. HASIL DAN PEMBAHASAN

Skenario smart home di tempat objek penelitian yaitu setiap sensor dihandel oleh mcu masing-masing, terhubung ke router yang sama sehingga semua sensor dapat terintegrasi kemudian semua data tersebut di simpan di server, dibawah ini untuk konsep jaringan smart home di tempat objek penelitian sebagai berikut:



Gambar 2. Konsep Jaringan Smart Home

Terlihat pada foto konsep jaringan di atas masing masing perangkat mempunyai ip tersendiri, berikut daftar tabel ip dari gambar diatas:

Tabel 1. Ip Masing-Masing Perangkat

Nama Perangkat	IP
Pengontrol Lampu	192.168.1.25
Kamera Keamanan	192.168.1.4
Pengontrol Suhu	192.168.1.23
Pengunci Pintu	192.168.1.24
Router	192.168.1.1
Raspberry	192.168.1.13

3.1 Konfigurasi *Model of Devices DNA and Genes*.

Pada tahap ini peneliti melakukan identifikasi pada masing-masing perangkat menggunakan metode *Model of Devices DNA and Genes*. Sebagai contoh pada tabel 2 perangkat kamera kemanan mempunyai DNA yaitu *Owner* nya adalah PT.WPI, *Subcriber* nya adalah Anggara, *User* nya adalah anggara dengan *serial number* T090060-2B1 *Location* di Ciganitri, Bandung, Indonesia, mempunyai *Device Type* Tapo C310, CCTV.

Tabel 2. Tabel DNA

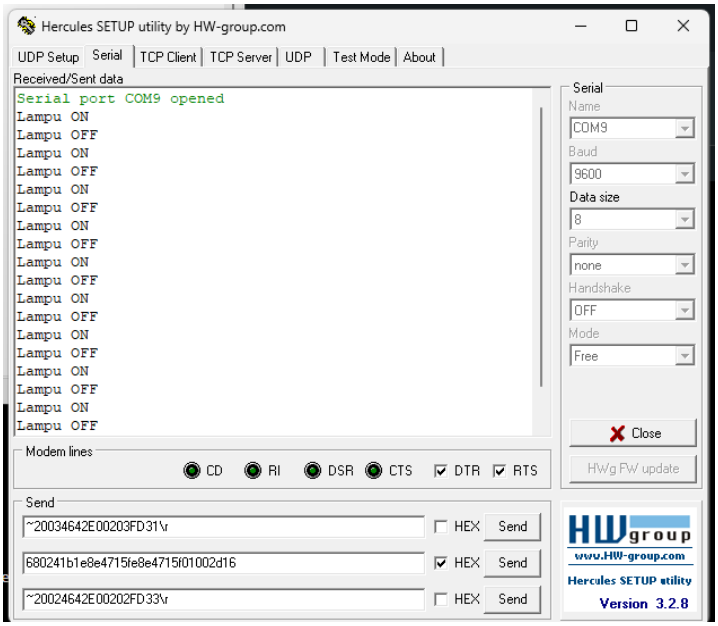
Device	Genes					
	owner	Subcriber	User	Serial Number	Location	Device Type
Pengontrol lampu	PT. WPI	Anggara	Anggara	Krc-AQ-007	Ciganitri, Bandung, Indonesia	Songle, Relay
Kamera Keamanan	PT. WPI	Anggara	Anggara	T090060-2B1	Ciganitri Bandung, Indonesia	Tapo C310, CCTV
Pengontrol Suhu	PT. WPI	Anggara	Anggara		Ciganitri Bandung, Indonesia	Termostat
Pengunci Pintu	PT. WPI	Anggara	Anggara	P208	Ciganitri Bandung, Indonesia	Door Lock

3.2 Framework FASIM

Pada tahap ini peneliti melakukan akuisisi data pada perangkat yang ada di tempat objek penelitian:

1. Pengontrol Lampu

Pada Tahapan ini peneliti mengakuisisi data dari pengontrol lampu menggunakan *tools* Hercules. Berdasarkan gambar 3 data dari perangkat pengontrol lampu yaitu status perangkat sedang ON(hidup) atau OFF(mati).



MD5 : 20892cdb1c9bc9631000fe969dc02b83

Gambar 3. Metadata dari Pengontrol lampu

Di tahap tools tersebut yang terlihat pada gambar 4.9 perangkat bekerja sesuai dengan fungsinya, sehingga menghasikan kesimpulan bahwa pengontrol lampu bekerja dengan baik dengan indikasi lampu ON dan OFF.

2. Kamera Keamanan

Pada Tahapan ini peneliti mengaquisisi data dari kamera keamanan menggunakan tools MMPEG dan Fing, berdasarkan gambar 4 detail data untuk stream kamera keamanan mempunyai data waktu real time yaitu 2024-04-18 13 : 44 : 56 sesuai dengan waktu pada saat peneliti melakukan akuisisi data.

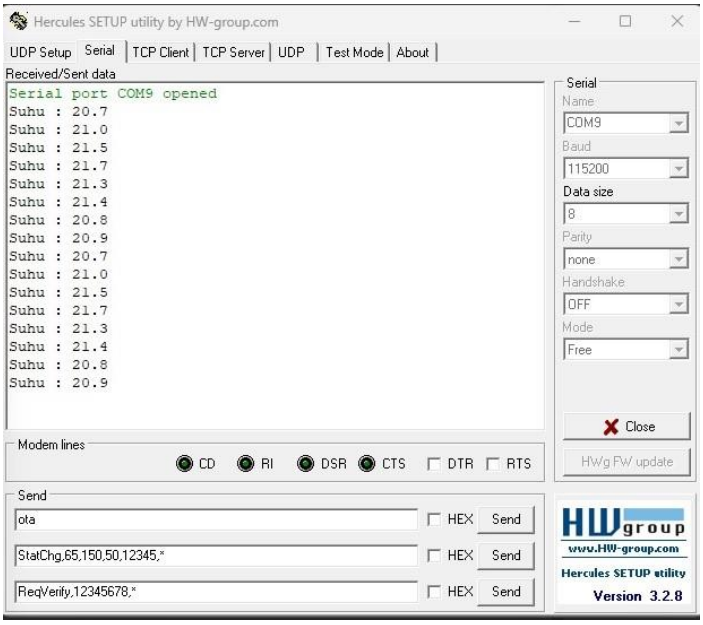
MD5 : 5d197fbcc19878c4fb1bc004350df12e

Gambar 4. Stream CCTV di FFMPEG

Berdasarkan untuk detail keneksi jaringan pada perangkat kamera keamanan yang di akuisisi melalui aplikasi fing mempunyai IP 192.168.1.4 dengan MAC Address 9C:A2:F4:5F:E3:77 dari brand TP-Link dengan model Tapo C310.

3. Pengontrol Suhu

Pada Tahapan ini peneliti mengaquisisi data dari pengontrol Suhu menggunakan tools Hercules dan Fing. Berdasarkan gambar 4.13 data dari perangkat pengontrol suhu yaitu data parameter pebacaan suhu.



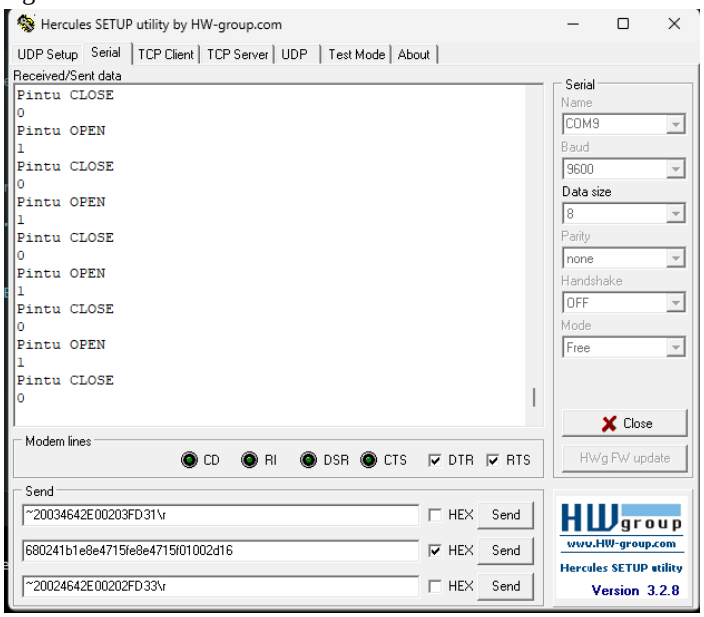
MD5 : 0f5c1b47ec5dbd81b17f7e10c64be32b

Gambar 5. Metadata dari Pengontrol Suhu di Hercules

Di tahap tools tersebut yang terlihat pada gambar 4.13 perangkat bekerja sesuai dengan fungsinya, sehingga menghasikan kesimpulan bahwa pengontrol suhu bekerja dengan baik dengan indikasi perangkat mengeluarkan data suhu.

4. Pengunci Pintu

Pada Tahapan ini peneliti mengaquisisi data dari Pengunci Pintu menggunakan tools Hercules dan Fing. Berdasarkan gambar 4.15 data dari perangkat pengunci pintu yaitu status sedang OPEN atau CLOSE dengan logic 1/0.



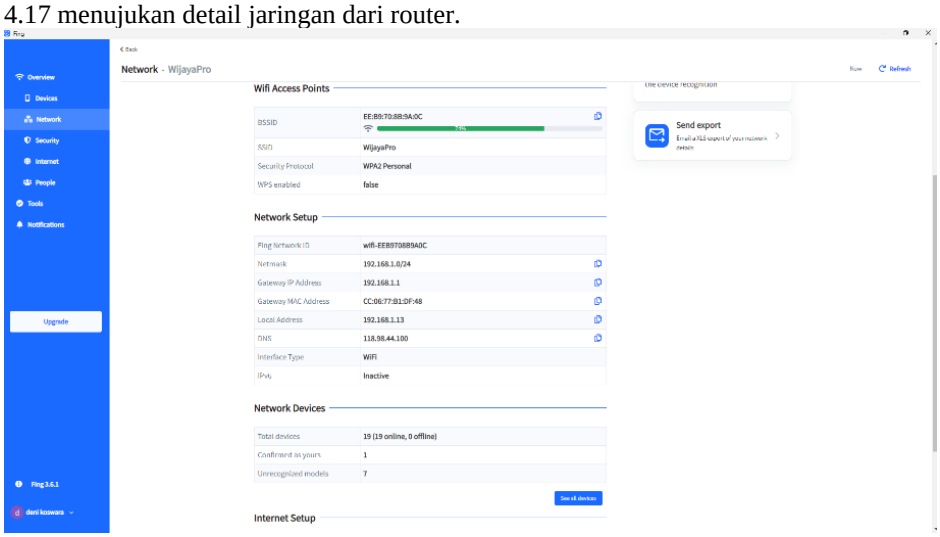
MD5 : 30c8182568299d73b3a70294e586740a

Gambar 6. Metadata dari Pengunci Pintu di Hercules

Di tahap tools tersebut yang terlihat pada gambar 4.15 perangkat bekerja sesuai dengan fungsinya, sehingga menghasikan kesimpulan bahwa pengunci pintu bekerja dengan baik dengan indikasi perangkat mengeluarkan output OPEN dan CLOSE.

5. Router

Pada Tahapan ini peneliti mengaquisisi data dari Router menggunakan tools Fing, berdasarkan gambar 4.17 menujukan detail jaringan dari router.



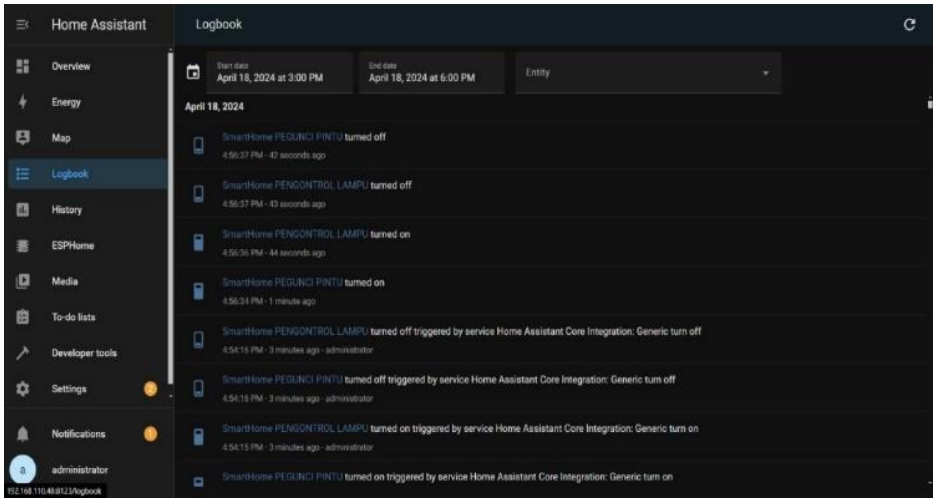
MD5 : 1a92c7081f0cc65054532005e89c7eb2

Gambar 7. Detail Network Router di Aplikasi Fing

Di tahap tools tersebut yang terlihat pada gambar 4.17 perangkat bekerja sesuai dengan fungsinya, sehingga menghasikan kesimpulan bahwa router bekerja dengan baik dengan indikasi perangkat terhubung ke jaringan dan terkonfigurasi dengan benar.

6. Raspberry Pi

Pada Tahapan ini peneliti mengaquisisi data dari Raspberry Pi menggunakan tools Home Assistant, berdasarkan gambar 4.22 menujukan Logbook dari perangkat smart home yang tersambung seperti Pengontrol Suhu, Pengunci Pintu dan Pengontrol Lampu.



MD5 : 65d6b4aaa3f79933ee1786fd418df913

Gambar 8. Log Perangkat di Server Home Assistant pada Raspberry Pi

Di tahap tools tersebut yang terlihat pada gambar 4.22 perangkat bekerja sesuai dengan fungsinya, sehingga menghasikan kesimpulan bahwa Raspberry pi bekerja dengan baik dengan indikasi perangkat menyimpan log activity semua perangkat yang terhubung.

3.3 Evidence Presentation and Preservetion of Data

Setelah melalui proses analisis dan interpretasi data, langkah selanjutnya adalah menyajikan temuan tersebut dengan cara yang mudah dimengerti dan bermanfaat. Ini dapat dicapai melalui berbagai medium, seperti laporan tertulis, presentasi grafis, atau *Chain of Custody*, yang disesuaikan dengan audiens dan tujuan komunikasi di bidang smart home.

Tabel 3. Bukti Dokumen MD5

NO	Nama Barang Bukti	Hash	Tahapan
1	Foto letak pengontrol lampu di lokasi	b7efdd36a32e719b9120b85a0dbb3b6e	4.1 Persiapan
2	Foto letak Kamera keamanan di lokasi	3082c26cbd172db45d10497afe803c31	4.1 Persiapan
3	Foto letak Pengontrol Suhu di Lokasi	538fc41074d182b00a22b882cddfb229	4.1 Persiapan
4	Foto letak Pengunci pintu di lokasi	180dcb269ac8f18b7125e8d70495b79b	4.1 Persiapan
5	Foto letak Router di lokasi	0c328ad891377e3e65f27e58c97ff458	4.1 Persiapan
6	Foto letak raspberry Pi di lokasi	3a6474471b95c5f20d71c4f90622965e	4.1 Persiapan
7	Metadata dari Pengontrol Lampu	20892cdb1c9bc9631000fe969dc02b83	4.3.1 Identification and Collection of data
8	Detail Jaringan Pengontrol Lampu di aplikasi Fing	24d615464ac7ca4f0657337da5ef4911	4.3.1 Identification and Collection of data
9	Stream CCTV di FFMPEG	5d197fbcc19878c4fb1bc004350df12e	4.3.1 Identification and Collection of data
10	Detail Jaringan Pengontrol suhu di aplikasi Fing	8038b0826cd571e1ba87d085ea9b09b0	4.3.1 Identification and Collection of data
11	Metadata dari Pengontrol Suhu di hercules	0f5c1b47ec5dbd81b17f7e10c64be32b	4.3.1 Identification and Collection of data
12	Detail Jaringan Pengontrol suhu di aplikasi Fing	42b33d5959fa5d550b006ca505847690	4.3.1 Identification and Collection of data
13	Metadata Dari Pengunci Pintu di Hercules	30c8182568299d73b3a70294e586740a	4.3.1 Identification and Collection of data
14	Detail Jaringan Pengunci Pintu di aplikasi Fing	972f86cc7d837e1035053cd27ea5ae93	4.3.1 Identification and Collection of data
15	Detail Network Router di Aplikasi Fing	1a92c7081f0cc65054532005e89c7eb2	4.3.1 Identification and Collection of data
16	Detail wifi access point router di aplikasi Fing	dce16a5c8dbb06b21c537db33ec4e96f	4.3.1 Identification and Collection of data
17	Detail Network Setup router di aplikasi Fing	df5a26348f193a748ff0d657634d2d8c	4.3.1 Identification and Collection of data
18	Detail Network Device router di aplikasi Fing	c6a3a0bcc39d7f8df019e260d0c3f403	4.3.1 Identification and Collection of data
19	Detail Internet Setup router di aplikasi Fing	68f383674d78d404effc45100a8846a9	4.3.1 Identification and Collection of data
20	Log Perangkat di server Home Assistant pada raspberry Pi	65d6b4aaa3f79933ee1786fd418df913	4.3.1 Identification and Collection of data

21	Detail jaringan Server/Raspberry Pi di aplikasi Fing	2eb44bf11cb66737321a9e875cb8cc29	4.3.1 Identification and Collection of data
22	Format data Pengontrol Lampu dalam jaringan	b7efdd36a32e719b9120b85a0dbb3b6e	4.3.2 Analisis
23	Data Bit Stream dari kamera keamanan	3082c26cbd172db45d10497afe803c31	4.3.2 Analisis
24	bit stream kamera	538fc41074d182b00a22b882cddfb229	4.3.2 Analisis
25	bit stream kamera	180dcb269ac8f18b7125e8d70495b79b	4.3.2 Analisis
26	bit stream kamera	0c328ad891377e3e65f27e58c97ff458	4.3.2 Analisis
27	Format data Pe+ngontrol Suhu dalam jaringan	3a6474471b95c5f20d71c4f90622965e	4.3.2 Analisis
28	Format data pengunci pintu dalam jaringan	20892cdb1c9bc9631000fe969dc02b83	4.3.2 Analisis
29	Data Dari Pengontrol Lampu	b7efdd36a32e719b9120b85a0dbb3b6e	4.3.3 Interpretasi
30	Data Kamera Keamanan	3082c26cbd172db45d10497afe803c31	4.3.3 Interpretasi
31	Data dari Pengontrol Suhu	538fc41074d182b00a22b882cddfb229	4.3.3 Interpretasi
32	Data dari Pengunci Pintu	180dcb269ac8f18b7125e8d70495b79b	4.3.3 Interpretasi
33	BitStream kamera keamanan saat sedang di jamming	42ce69286cc87f74b033cf0865ae035f	4.3.5 Conclution
34	Proses Compiler data bitstream yang terkena Serangan DDOS	014087d2f157ccb35ddcdc3f69fe5f56	4.3.5 Conclution

3.4 Hasil Penelitian dan Pengolahan Data pada Framework FASIM

1. Akuisisi

Pada tahap akuisisi, bukti digital yang diserahkan oleh Anggara berupa perangkat smarthome yang terdiri dari pengontrol lampu, kamera keamanan, pengtrol suhu, dan pengunci pintu, di ambil menggunakan tools Hercules, FFMPEG, dan Ping berupa data Fisikal.

2. Analisis

Pada tahap analisis metadata dari perangkat Smart Home berupa perangkat smarthome yang terdiri dari pengontrol lampu, kamera keamanan, pengtrol suhu, dan pengunci pintu di analisis menggunakan Data Sniffer dan BitStreamer Compiler berupa data logical, Sehingga ketemu format data dari setiap perangkat tersebut.

3. Interpretasi

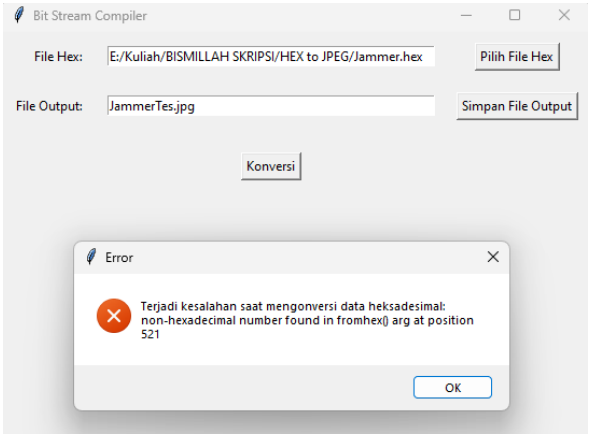
Pada tahap interpretasi semua data dari perangkat Smart Home berupa perangkat smarthome yang terdiri dari pengontrol lampu, kamera keamanan, pengtrol suhu, dan pengunci pintu yang sudah di aquisisi dan di analisis di teliti lebih dalam sehingga terdapat temuan bahwa perangkat itu berjalan dengan baik atau tidak terdapat anomali pada alat tersebut.

Hasil investigasi forensik pada smarthome anggara menunjukan tidak ada anomali atau kejanggalan yang terjadi. Oleh sebab itu penulis mencoba melakukan penyerangan pada salah satu perangkat smorthome anggara yaitu melakukan jamming pada kamera keamanan dengan teknik ddos, berikut yang terjadi pada kamera keamanan:

MD5: 42ce69286cc87f74b033cf0865ae035f

Gambar 9. BiteStream Kamera Keamanan Pada Saat Jamming

Pada gambar 4.42 terlihat data kamera keamanan pada perangkat smarthome anggara yang sedang dilakukan percobaan penyerangan menggunakan metode DDOS. Data menjadi kacau tidak beraturan sehingga menyebabkan gangguan fungsi pada kamera keamanan tersebut, seperti pada gambar berikut saat data bitstream dari kamera di coba untuk di compile.



MD5: 014087d2f157ccb35ddcdc3f69fe5f56

Gambar 10. Proses Compiler Data BitStream

Pada gambar 10 terlihat proses compiler data kamera keamanan pada perangkat smarthome anggara yang sedang dilakukan percobaan penyerangan menggunakan metode DDOS tidak bisa di compile dengan baik. Dikarenakan data tersebut telah mengalami gangguan akibat penyerangan tersebut. Sehingga dapat disimpulkan bahwa dengan ketika terjadi penyerangan pada salah satu perangkat, framework application specific investigation model dapat mengetahui jejak penyerangan tersebut.

Tabel 4. Dokumen Bukti Digital MD5

NO	Nama Barang Bukti	Hash	Tahapan
1	BitStream kamera keamanan saat sedang di jamming	42ce69286cc87f74b033cf0865ae035f	4.3.5 Conclution
2	Proses Compiler data bitstream yang terkena Serangan DDOS	014087d2f157ccb35ddcdc3f69fe5f56	4.3.5 Conclution

4. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan terhadap investigasi digital forensik pada perangkat IoT dalam sistem rumah pintar menggunakan Framework Application Specific Investigation Model (FASIM), beberapa kesimpulan dapat diambil. Pertama, framework FASIM terbukti efektif dalam melakukan investigasi digital forensik pada perangkat IoT, di mana proses identifikasi, pengumpulan, analisis, da interpretasi data dilakukan secara sistematis sehingga memastikan bahwa bukti digital dapat dikumpulkan dan dianalisis dengan tepat. Kedua, penelitian ini menunjukkan bahwa perangkat IoT dalam sistem rumah pintar memiliki kerentanan yang dapat dieksploitasi.

Melalui investigasi ini, keamanan dan privasi yang diperoleh dari masing-masing perangkat IoT seperti kamera keamanan, pengontrol suhu, dan pengunci pintu yang bekerja sesuai dengan fungsinya dan terhubung ke jaringan dapat dipastikan. Ketiga, selama fase interpretasi, ditemukan bahwa pemahaman mendalam terhadap makna data yang dianalisis memberikan dasar yang kuat untuk merumuskan rekomendasi praktis. Hasil analisis ini konsisten dengan hipotesis awal penelitian dan memberikan implikasi signifikan bagi peningkatan keamanan sistem rumah pintar. Keempat, untuk memastikan integritas barang bukti, seluruh temuan barang bukti dibungkus dengan format MD5, memastikan bahwa tidak ada perubahan yang terjadi pada barang bukti selama proses investigasi.

DAFTAR PUSTAKA

Pustaka yang berupa judul buku

[1] M. Cook. (2021). *Smart Home Automation: A Practical Guide.*

[2] A. McEwen. (2021). *Internet of Things: A Hands-On Approach*.

[3] J. C. Ryan. (2021). *The Complete Guide to Heating and Cooling Your Home*.

[4] Drs. Madijono. (2018). *The Concept of Investigation in Criminal Law: An Indonesian Perspective*.

Pustaka yang berupa jurnal ilmiah

[5] A. Chakraborty. (2023) "Journal of Electrical and Computer Engineering".

[6] I. Wahyudi and I. A. Rafiq.(2022). "Forensic Mobile Analysis on Social Media Using National Institute Standard of Technology Method," *International Journal of Safety & Security Engineering*, vol. 12, no. 6, pp. xx–xx.

[7] L. S. Vailshery. (2024). "Jumah perangkat yang terhubung dengan IoT di seluruh dunia pada tahun 2019-2023, dengan perkiraan hingga tahun 2030," *Articles Statista*.

[8] R. P. Sari. (2024). "Mengenal IoT Hacking dan Cara Pencegahannya," *Cloud Computing Indonesia*.

[9] Hossain. (2024). "Analysis of Internet of Things (IoT) Security: Principles, Practices, and New Perspectives,".

[10] K. K. Sindhu. (2012). "Digital Forensic Investigation Tools and Procedures," *International Journal of Computer Network and Information Security*, vol. 4, no. 4, pp. 39–48.

[11] F. Servida. (2019). "IoT forensic challenges and opportunities for digital traces,".

Pustaka yang berupa Prosiding Seminar:

[12] S. Zawoad S. Zawoad and R. Hasan. (2015). "FAIoT: Towards Building a Forensics Aware Ecosystem for the Internet of Things," in *Proc. 2015 IEEE Int. Conf. on Services Computing (SCC)*, pp. 279–284.

[13] S. Perumal, N. M. Norwawi, and V. Raman. (2015). "Internet of Things (IoT) Digital Forensic Investigation Model: Top-Down Forensic Approach Methodology," in *Proc. 2015 5th Int. Conf. on Digital Information Processing and Communications (ICDIPC)*, pp. 19–23.

[14] N. H. N. Zulkipli, A. Alenezi, and G. B. Wills. (2017). "IoT Forensic: Bridging the Challenges in Digital Forensic and the Internet of Things," in *Proc. IoTBDS*, pp. 315–324.

Pustaka yang berupa disertasi/thesis/skripsi::

[15] T. Wu. (2020). "Digital Forensic Investigation of IoT Devices: Tools and Methods," M.S. thesis.