Penerapan Metode NIST untuk Analisis Serangan *Denial of Service* (DoS) pada Perangkat *Internet of Things* (IoT)

Lubi Arsada[1] dan Aries Muslim[2]

[1] Magister Manajemen Sistem Informasi, Universitas Gunadarma
[2]Universitas Gunadarma
Jakarta
E-mail : arsada.lubi@gmail.com, aries.muslim09@gmail.com

Abstrak

Salah satu permasalahan IoT adalah banyaknya perangkat yang terhubung ke IoT di Era Industri 4.0, yang pada akhirnya mengalihkan perhatian peretas dari penyelesaian mekanisme keamanan. Salah satu faktor keamanan yang menjadi perhatian pada perangkat IoT ini adalah serangan berupa *Denial of Service* (DoS) pada jaringan perangkat *Internet of Things* (IoT) yang mengakibatkan suatu sistem dibanjiri data secara terus menerus dalam waktu singkat yang mana mengakibatkan trafik jaringan menjadi sangat padat sehingga perangkat IoT menjadi down. Untuk memperoleh bukti digital menggunakan metode NIST meliputi 3 proses yaitu Proses Penanganan, Proses Akuisisi, dan Proses Investigasi. Sehingga diperoleh alat bukti digital yang valid yang dapat dijadikan alat bukti hukum di pengadilan.

Kata kunci : Industri 4.0, IoT (*Internet of Things*), *Denial of Service*, NIST.

Pendahuluan

Saat ini kemajuan internet begitu pesat sehingga berdampak pada perkembangan yang inovatif dari perangkat elektronik yang semakin pintar. Perkembangan saat ini mengarah pada pengaplikasian *Internet of Things (IoT)* yang termasuk pada salah satu bagian industry 4.0. IoT merupakan identitas unik yang terhubung dengan internet yang fokusnya adalah bagaimana mengkonfigurasi, mengontrol dan monitoring melalui perangkat. Menurut laporan analisis GrowthEnabler tahun 2018 Pasar IoT global akan tumbuh dari $157 pada tahun 2016 menjadi $457 pada tahun 2020, mencapai tingkat pertumbuhan tahunan majemuk sebesar 38,3%. Dengan peningkatan penggunaan IoT yang begitu pesat dapat membawa banyak kemajuan yang signifikan dalam teknologi aplikasi dan layanan komputasi. Menurut BI *Intelligence* pada tahun 2021 secara kumulatif, pengeluaran untuk IoT seluruh dunia hampir $5 Triliun diperkirakan dihabiskan oleh berbagai industry manufaktur dan keuangan [1].

Menurut laporan McAfee Labs Threats Report tahun 2018 – 2019. Serangan dilakukan dengan memanfaatkan celah yang ada pada perangkat jaringan yang digunakan. Teknik serangan yang dilakukan pun bermacam-macam beberapa diantaranya seperti *Malware, Vulnerability, Code Injection, Theft, Account Hijacking, Unauthorized Acces, DoS (Denial of Service), Target Attack, Defacement* [2].

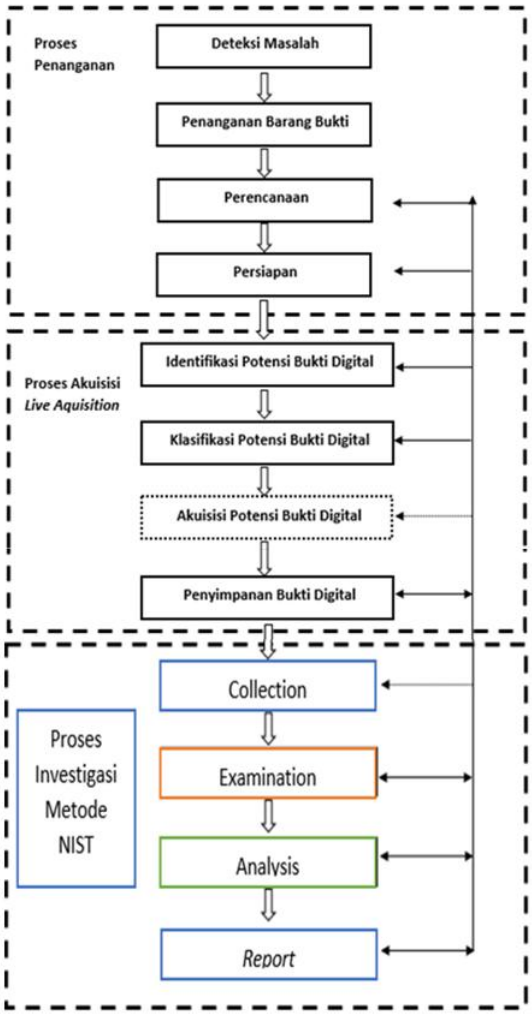
Menurut laporan analisis dari laporan *Enabler* tentang pertumbuhan penggunaan IoT dan *McAffe Laboratory.* Banyak serangan pada akhirnya mengalihkan perhatian peretas dalam memecahkan mekanisme keamanan. Perangkat IoT menjadi salah satu perangkat yang banyak diserang dilihat dari data data dari *Enabler* tahun 2018. Salah satu faktor keamanan yang menjadi perhatian dalam perangkat IoT ini adalah salah satu serangan DoS. "Serangan *Flooding* menjadi salah satu bentuk serangan *Denial of Service* (DoS) terhadap jaringan perangkat *Internet of Things* (IoT) yang mengakibatkan suatu sistem akan terbanjiri oleh data – data secara terus menerus dalam waktu singkat dan juga mengakibatkan lalu lintas jaringan menjadi sangat padat" [3] .

Untuk melakukan analisis serangan pada IoT, yaitu memanfaatkan aplikasi *Wireshark* yang memiliki fungsi menangkap paket data atau informasi dalam format Protokol yang berjalan dalam jaringan, sehingga data atau informasi tersebut langsung dapat dianalisis untuk memahami seber-

DOI : http://dx.doi.org/10.32409/jikstik.20.2.2724

apa rawan suatu sistem untuk pelanggaran keamanan [4].

Dalam penelitian ini untuk proses analisis deteksi jenis serangan DoS pada pada perangkat *Internet of Things* (IoT) sehingga dilakukan akuisisi data pada IoT untuk menentukan karakteristik bukti digital melalui metode *National Institute of Standards and Technology* (NIST).



Gambar 1: Alur Proses Penelitian

Penelitian Terdahulu

Penelitian tentang digital forensic Imam Riadi dan Yudi Prayudi dilakukan dengan menggunakan Model Proses Forensik Jaringan dengan metode *Live Forensic* tujuanya adalah melakukan explorasi terhadap bukti digital yang bisa didapatkan dari Sistem Operasi *Router* untuk memperoleh informasi yang digunakan dalam penyelidikan *forensic* [5].

Mempresentasikan model forensik jaringan untuk mendeteksi dan mengidentifikasi serangan berbahaya pada perangkat IoT untuk keperluan penyelidikan forensik. Sedangkan hasil penelitian dari Dimitriadis et al yaitu dengan metode *NIST & CYBER Kill Chain* untu melakukan explorasi terhadap bukti digital yang bisa didapatkan untuk memperoleh informasi yang digunakan dalam penyelidikan *forensic*. [6]

Metode Penelitian

Dalam penelitian ini dilakukan dalam beberapa tahap seperti tergambar dalam flowchart dibawah ini.. Diagram alir ini mengacu dari Penelitian Mumba & Venter, 2014 sebagai gambaran secara keseluruhan untuk sistem yang dibangun pada penelitian ini [7], lihat Gambar 1.

Hasil dan Pembahasan

Bab ini membahas langkah-langkah penelitian, analisis dan hasil yang telah dilakukan. Pembahasan dalam bab ini meliputi tahap melakukan simulasi kasus serangan *flooding* pada perangkat IoT, melakukan proses penanganan insiden, proses akuisisi untuk mengambil data dengan metode *Live Forensic* dan proses investigasi untuk mencari barang bukti dengan metode NISTmenjawab pertanyaan penelitian.

Serangan Flooding

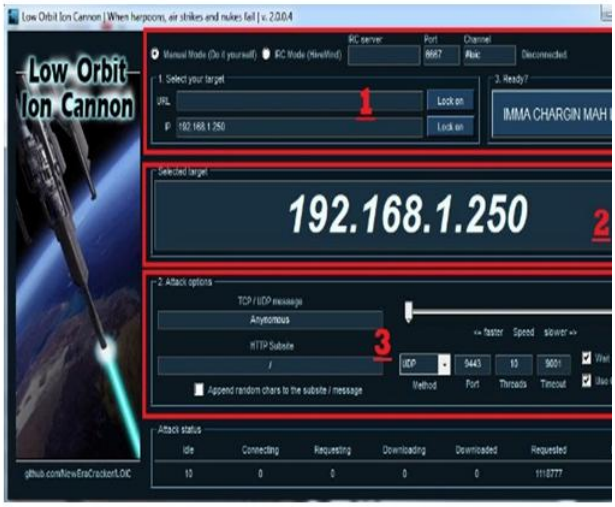
Dalam proses serangan ini menggunakan tool yang digunakan menyerang perangkat IoT adalah *Low Orbit Ion Canon* (LOIC). Berikut ini adalah prosedur untuk melakukan serangan *flooding*.

1. Memasukkan alamat IP target yang akan diserang.

2. Kemudian klik tombol lock on yang berada pada menu 1 (satu), selanjutkan menentukan jumlah *threads* yang akan dikirimkan sebanyak 10, target protokol adalah UDP, pilih target port adalah 9443, pilih kecepatan penyerangan pada menu 3 (Tiga).

3. Setelah semua konfigurasi kemudian melakukan serangan flooding dengan menekan tombol "IMMA CHARGIN MAH LAZER" dilakukan selama 5-10 menit.

Aplikasi LOIC ditunjukkan pada gambar 2.



Gambar 2: Serangan Flooding

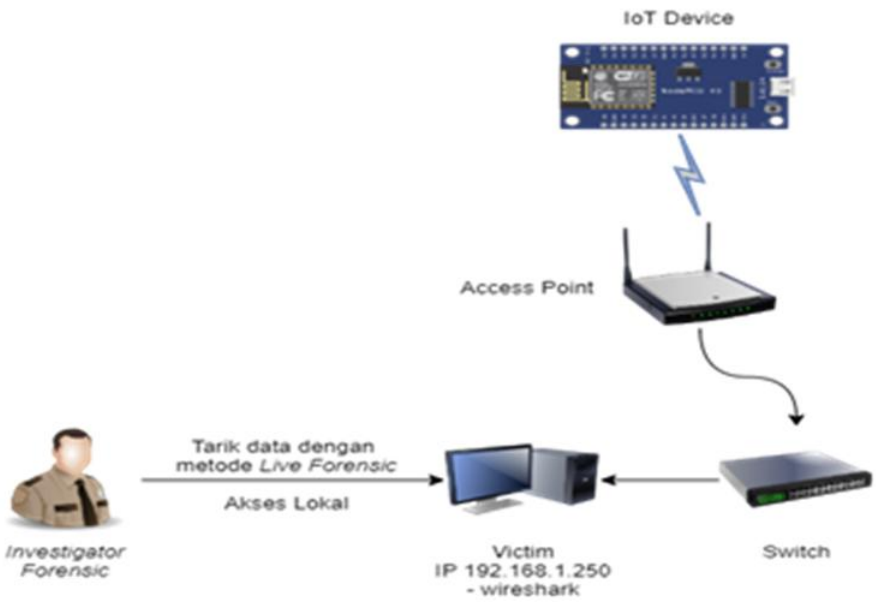
Gambar 3: Penanganan Barang Bukti

Penanganan Barang Bukti

Tahap penanganan ini dimaksudkan untuk menangani perangkat bukti yang memiliki potensi bukti digital. Selanjutnya memisahkan antara bukti pada kasus yang sedang ditangani dengan bukti kasus lainnya dengan cara memberikan label keterangan untuk barang bukti sebelum proses pemindahan menuju lokasi penyimpanan.

Proses Akuisis Bukti Digital

Proses akuisisi data dengan pengambilan log kemudian dikumpulkan file log tersebut agar bias dianalisis oleh investigator maka tahap selanjutnya adalah melakukan proses investigasi forensic. Metode yang digunakan adalah live forensic yaitu pengambilan data diambil saat system sedang berjalan.



Gambar 4: Proses Akuisisi

Proses Investigasi Forensic

Metode yang digunakan adalah pada proses investigasi adalah metode (NIST) National Institute of Standards and Tecknologi. NIST merupakan kerangka kerja yang sering digunakan, dikarenakan kerangka kerja NIST mengatur standar pedoman, dan praktek terbaik dalam mengelola resiko terkait segala bentuk yang berkaitan dengan sains, teknologi informasi.

Tahap Collection

Pengkoleksian barang bukti dalam penelitian ini menggunakan rekaman jaringan traffic log pada IoT. Proses mengambil payload sebagai file serangan flooding dalam penelitian ini. Dalam tahapan ini untuk melindungi bukti-bukti dari kerusakan, perubahan dan penghilangan oleh pihak-pihak tertentu. Untuk itu bukti harus benar-benar steril dan harus ada pengamanan terhadap barang bukti yang telah didapat dari TKP (Tempat Kejadian Perkara).

Tahap Examination

Investigator forensic dalam memeriksa log file yang ditemukan di log lalu lintas perangkat IoT di capture dengan memasukkan parameter yang akan dipassangkan. Proses pemeriksaan lalu lintass dengan aplikasi wireshark

Tahap Analysis

Dalam tahap proses ini untuk analisis dilakukan secara offline dengan menggunakan wireshark. hasilnya menunjukan peningkatkan traffic yang terlihat abnormal. Hasil dapat dilihat peningkatan traffic jaringan seperti pada gambar 5.

Setelah melihat traffic yang abnormal yang telah terdeksi oleh wireshark kemudian dilakukan pengecekan paket. Bisa dilihat pada Gambar 6.

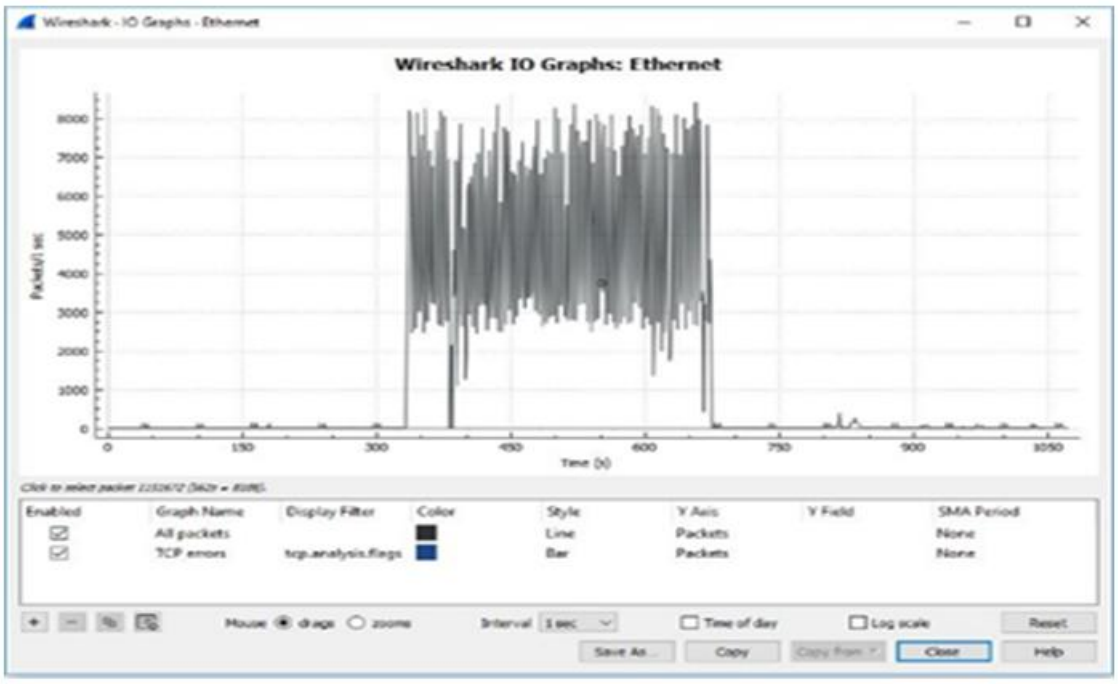
Selanjutnya dilakukan analisis lanjutan dengan modul statistic endpoin pengecekan paket. Dalam proses analisis endpoin terdapat jumlah serangan sejumlah 27 serangan dan UDP 254 Serangan. Bisa dilihat pada gambar 7.

Selanjutnya dilakukan analisis IP address penyerang lainnya seperti langkah-langkah sebelumnya. Kemudian data dikumpulkan untuk dianalisis sehingga dapat menemukan IP address yang melakukan serangan flooding terhadap perangkat IoT untuk dijadikan barang bukti. Tabel 1 adalah IP address yang terdeteksi melakukan serangan.

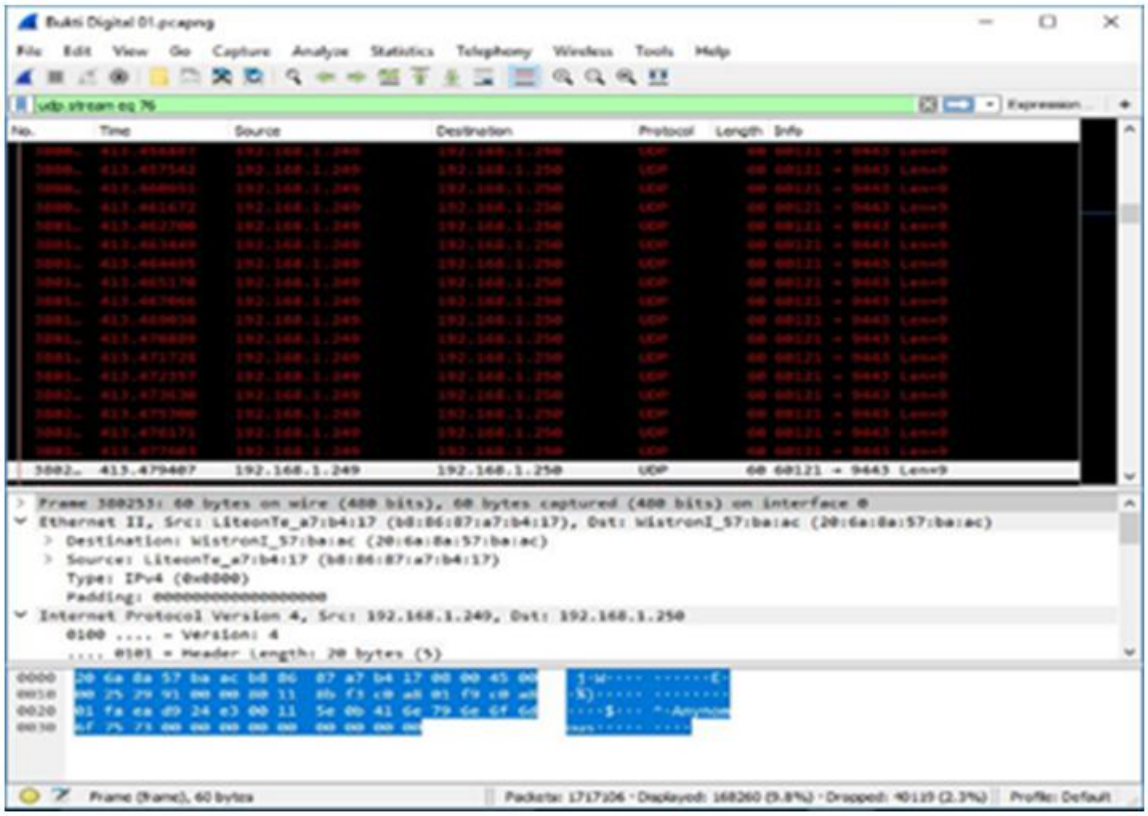
Tabel 1: Klasifikasi Paket Serangan

No.	IP Address	Source Part	Source Destination	Protocol	Jumlah Paket	Klasifikasi
1	192.168.1.254	192.168.1.254	192.168.1.250	UDP	2	LOW
2	192.168.1.255	192.168.1.255	192.168.1.250	UDP	461	LOW
3	192.168.1.247	192.168.1.247	192.168.1.250	UDP	1.789	MEDIUM
4	192.168.1.248	192.168.1.248	192.168.1.250	UDP	1.240	MEDIUM
5	192.168.1.249	192.168.1.249	192.168.1.250	UDP	1.109.243	HIGH

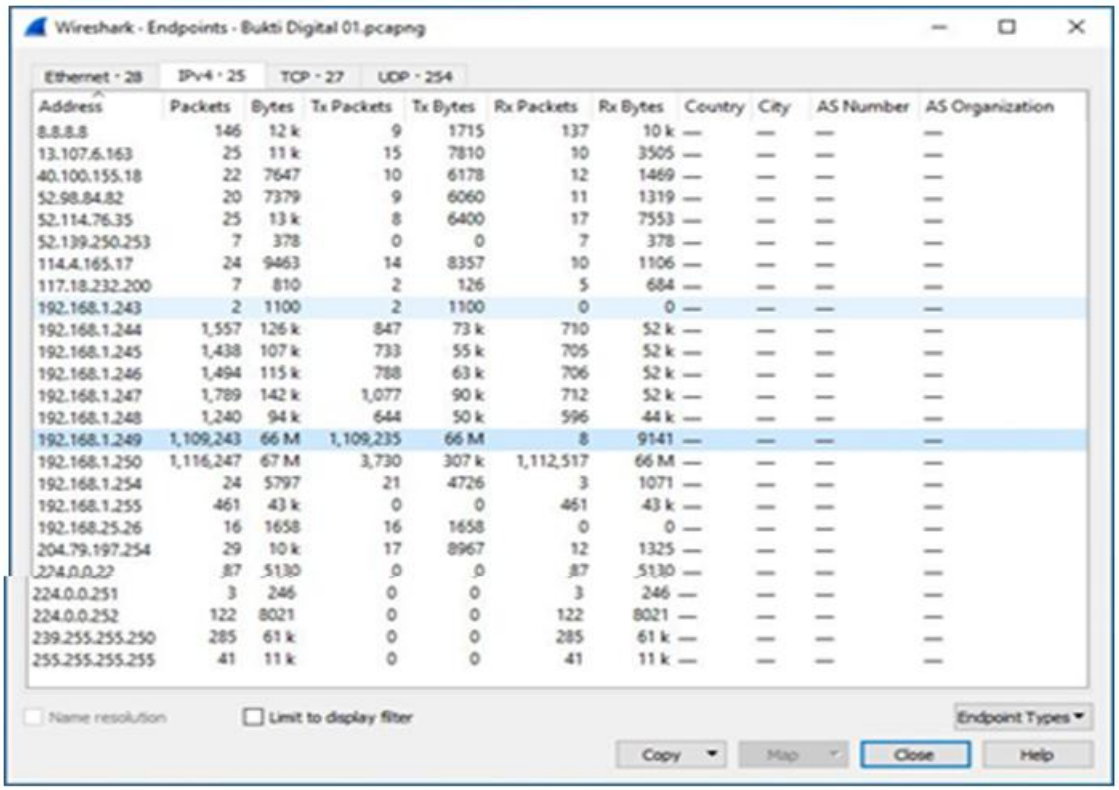
Dari Tabel 1 dapat dilihat klasifikasi paket serangan dari IP address 192.168.1.254 dan 192.168.1.255 masuk klasifikasi LOW dengan jumlah paket 2 sampai 461. Kemudian dari IP Address 192.168.1.247 dengan jumlah paket 1.789 dan IP Address 192.168.1.248 dengan jumlah paket 1.240 diklasifikasikan MEDIUM. Dan dari IP Address 192.168.1.249 dengan paket terbanyak diklasifikasikan HIGH dengan paket 1.109.243.



Gambar 5: Graph Traffic Log



Gambar 6: Pengecekan Paket



Gambar 7: Static Endpoin

Tahap Report

Pada tahap ini hal yang dilakukan adalah menyajikan hasil analisis yang telah dilakukan. Tahap ini adalah persentasi dari semua temuan dalam penelitian. Hasil analisis lebih lanjut dijelaskan pada tabel hasil analisis serangan DoS pada IoT di bawah ini.

Tabel 2: Laporan

No	Jenis Informasi Analisis	Keterangan
1	Serangan DoS pada IoT menggunakan aplikasi LOIC	Berhasil melakukan serangan secara bertubi-tubi pada perangkat IoT
2	Aplikasi Wireshark berhasil menangkap aktivitas lalu-lintas yang mencurigakan melalui protocol UDP	diperoleh informasi bahwa adanya penyerang dengan serangan flooding
3	Port serangan berhasil ditembus	protocol UDP
4	Port protocol penyerang	59925
5	Port protocol target	9443
6	Log activity	Terdapat aktivitas yang tidak wajar yaitu terjadi serangan yang bertubi-tubi pada perangkat IoT yang terdeteksi oleh wireshark
7	IP Address list penyerang	192.168.1.249
8	IP Address list target	192.168.1.250

Dari Table 2 dapat dilihat informasi analisis yang dilakukan untuk laporan kegiatan pendeteksian serangan DoS pada IoT menggunakan aplikasi LOIC, bahwa adanya serangan flooding atau serangan pembanjiran paket secara bertubi-tubi dari IP Address 192.168.249 dengan port 59925 menuju 192.168.1.250 dengan port 9443 dengan protocol UDP, aktivitas ini ditandai pada log activity yang terekam oleh wireshark.

Penutup

Berdasarkan hasil yang didapat pada proses implementasi, hasil dan bahasan, maka pada penelitian dan analisa forensic pada perangakat IoT dapat ditarik keimpulan bahwa:

1. Aplikasi wireshark dapat mengidentifikasi adanya serangan flooding dari dari IP 192.168.1.249 kepada IP 192.168.1.250
2. Metode NIST dapat mengidentifikasi lalulintas serangan yang didapatkan pada jaringan IoT, dan hasilnya dapat digunakan sebagai bukti digital yang legal berupa laporan.
3. Simulasi yang dilakukan menggunakan aplikasi LOIC untuk serangan perangkat IoT berhassil dilakukan attacker menuju target berupa perangkat victim dengan IP 192.168.1.250 Port 9443 dari IP penyerang 192.168.1.249 port 59925 dengan protocol UDP, 10 threads, timeout 9001, kecepatan faster.
4. Proses akuisisi data pada perangkat IoT menggunakan metode NIST dengan pendekatan secara Live Forensic yaitu dilakukan dengan kondisi On. Dapat disimpulkan bahwa adanya aktivitas yang tidak wajar yang dilakukan dari IP 192.168.1.249 menuju IP target 192.168.1.250. hasil penelitian ini berhasil mengidentifikasi IP address dari penyerang yaitu IP 192.168.1.249 dengan port protocol penyerang 59925, port destination target 9443 dan port serangan berhasil ditembus dengan Protocol UDP.Karakteristik bukti digital pada perangkat IoT yang dapat dijadikan sebagai laporan atau hasil temuan penelitian terkait analisis serangan DoS pada pernagkat IoT, meliputi jenis serangan yang masuk, Port jenis serangan yang masuk, Port Protocol penyerang, Port destination target yang diserang, dan untuk proses analisis History penyerangan diketahui melalui Log Activity dan IP Address List Penyerangan.

Daftar Pustaka

[1] Koustav Routh, Tannistha Pal, "A survey on technological, business and societal aspects of Internet of Things by Q3", 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU), p. 1–4, 2018.

[2] McAfee Labs, "McAfee Labs Threats Report McAfee Global Threat Intelligence analyzed", 1–21, 2018.

[3] Randi Rizal, Imam Riadi, & Yudi Prayudi, "Network Forensics for Detecting Flooding Attack on Internet of Things (IoT) Device", International Journal of Cyber-Security and Digital Forensics (IJCSDF), Vol. 7 No.4, 382–39, 2018.

[4] V. Sahiti, P. Tilakchand, B. Kowshik, P. Avinash, & S.L. Kavya, "Penetration testing using wireshark and defensive mechanisms against mitm", International Journal of Recent Technology and Engineering, Vol. 7 No. 6, 880–885, 2019.

[5] M. Alim, Imam Riadi, & Yudi Prayudi, "Live Forensics Method for Analysis Denial of Service (DOS) Attack on Routerboard", International Journal of Computer Applications, Vol. 180, No. 35, 23–30, 2018.

[6] Athanasios Dimitriadis, Nenad Ivezic, Boonserm Kulvatunyou, & Ioannis Mavridis, "D4I - Digital forensics framework for reviewing and investigating cyber attacks", Array, Vol. 9, 100015, 2020.

[7] Emilio Raymond Mumba, H. S. Venter, "Mobile forensics using the harmonised digital forensic investigation process", 2014 Information Security for South Africa - Proceedings of the ISSA 2014 Conference, 2014.

[8] Precilla M. Dimpe, Okuthe P. Kogeda, "Generic Digital Forensic Requirements", 2018 Open Innovations Conference, OI 2018, P. 240-245, 2018.

[9] Rusydi Umar, Anton Yudhana, M Nur Faiz, "Analisis Kinerja Metode Live Forensics Untuk Investigasi Random Access Memory Pada Sistem Proprietary", Prosiding Konferensi Nasional Ke- 4 Asosiasi Program Pascasarjana Perguruan Tinggi Muhammadiyah (APPPTM), P. 207-211, 2016.

[10] Jania Astrid Saucedo Martínez, Magdiel Pérez-Lara, José Antonio Marmolejo-Saucedo, Tomás Eloy Salais-Fierro, Pandian Vasant, "Industry 4.0 framework for management and operations: a review", Journal of Ambient Intelligence and Humanized Computing, Vol. 9, P. 789-801, 2018.