Analisis Log Menggunakan *Jupyter Notebook* pada Kasus *Cyber Threat Hunting*

Sutra Ovi Yansa dan Ferdiansyah

Teknik Informatika, Universitas Bina Darma, Palembang, Indonesia
Jl. Jenderal A. Yani No. 3 Palembang Sumatera Selatan, Indonesia
E-mail: sutraovi@gmail.com, ferdi@binadarma.ac.id

Abstrak

Forensik Digital merupakan disiplin ilmu yang menerapkan investigasi dan identifikasi dalam menindak kejahatan digital. Salah satu tahapan utama dalam menginvestigasi tindak kejahatan yaitu mengumpulkan barang bukti digital. Untuk menemukan barang bukti digital pada malware, dibutuhkan analisis lebih mendetail agar dapat mendeteksi aktifitas sebuah malware serta mempelajari bagaimana sebuah malware menginfeksi dan berkembang dalam sebuah sistem . Dengan melakukan analisis terhadap malware dapat mengetahui tentang bagaimana sebuah malware bekerja dan menginfeksi terhadap sistem yang diserang, komputer dan perangkat jaringan menghasilkan catatan atau log yang mendokumentasikan aktivitas pada sistem. Events log windows dapat membantu proses analisis serangan malware dengan melihat setiap peristiwa yang telah disimpan, menggunakan open source jupyter notebook untuk menganalisa dataset events log sehingga menghasilkan barang bukti digital berupa Visualisasi IP dari serangan malware, mengetahui file yang terinfeksi oleh malware dengan mengekstrak dan menghasilkan sumber informasi dari asal serangan malware dan memberikan panduan dalam melakukan investigasi digital forensik terhadap ancaman serangan malware yang dapat dipertanggung jawabkan didalam persidangan.

Kata kunci : Digitial Forensic, Cyber Secuirty, Data Mining, Visualisasi Data

Pendahuluan

Dengan meningkatnya aktivitas kejahatan yang terjadi pada kasus digital crime berbagai model investigasi digital forensik sudah dikembang, dalam investigasi digital forensik praktik ada lebih dari ratusan prosedur investigasi yang telah dikembangkan diseluruh dunia[1]. Setiap organisasi dan negara cenderung mengembangkan prosedurnya sendiri, beberapa fokus pada aspek teknologinya dan dibagian analisis data penyidikan yang memanfaatkan teknologi dan perangkat digital ini akan menjadi hal tepenting bagi investigasi digital untuk mengembangkan strategi pemikiran yang baik sehingga dapat menganalisis data kejahatan pada komputer seperti worm, ransomware, rootkit ataupun malware[2].

Forensik Digital merupakan disiplin ilmu yang menerapkan investigasi dan identifikasi dalam menindak kejahatan digital [3]. Salah satu tahapan utama dalam menginvestigasi tindak kejahatan yaitu mengumpulkan barang bukti digital. Untuk menemukan barang bukti digital pada malware, dibutuhkan analisis lebih mendetail agar dapat mendeteksi aktifitas sebuah malware serta mempelajari bagaimana sebuah malware menginfeksi dan berkembang dalam sebuah sistem. Ada dua tipe analisis dalam melakukan analisis pada malware yaitu dengan analisis statis (analisa kode) dan analisis dinamis [4]. Meskipun dari kedua tipe analisis tersebut mempunyai tujuan yang sama yaitu menjelaskan tentang bagaimana sebuah malware bekerja namun peralatan, waktu dan kemampuan yang dibutuhkan dalam menganalisa sangatlah berbeda [5].

Dalam Penelitian [6], yang dapat digunakan selama investigasi digital untuk mendeteksi anomali dan penipuan, yang melibatkan malware, phising dan penipuan digital. Mendeteksi malware menjadi masalah utama karena malware sangat pesat perkembangannya dan sangat diperlukan metode baru untuk memerangi kejahatan cyber crime dan membantu penyelidikan digital[7].

Dalam penelitian [8], penanganan serangan malware atau incidence response of malware attack menggunakan metode analisa reverse engineering untuk ekstraksi data informasi yang ada didalam malware, dengan mengetahui bagaimana malware tersebut bekerja dan membuat celah untuk melakukan serangan kedalam sistem komputer.

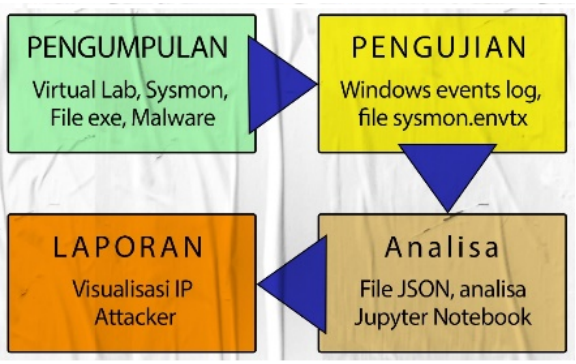
Berdasarkan latar belakang diatas perlu di-

DOI : http://dx.doi.org/10.32409/jikstik.21.2.3063

lakukan penelitian lanjutan untuk menemukan bukti digital dari catatan serangan malware terhadap sistem dengan melanjutkan penelitian sebelumnya menggunakan jupyter notebook untuk mengelola log yang terurai dan menganalisis log untuk mengklasifikasikan proses system dalam tingkat keamanan uang berbeda pada proses investigasi.

Metode Penelitian

Metode yang digunakan penulis dalam menyelsaikan penelitian ini yaitu metode forensik. Komputer forensik atau digital forensik merupakan penelitian yang dilakukan dengan menganalisis barang bukti digital hingga mendapatkan hasil penelitian yang relevan dan dapat dipertanggung jawabkan di pengadilan [9], lihat Gambar 1.



Gambar 1: Metode Forensik Komputer

Tahap dalam penelitian yaitu[9] :

1. Pengumpulan Dalam tahap pertama ini peneliti melakukan pengumpulan data yang merupakan proses identifikasi, pelabelan, rekaman dan pengambilan data dari sumber data yang relevan dengan mengikuti prosedur berikut untuk menjaga integritas data. Membangun Virtual Lab, Sysmon, Instal file exe yang sudah dipersiapkan dan Proses Malware Identifikasi. Selain mengumpulkan dan mendokumentasikan, pada tahap ini dilakukan persiapan dan perencanaan bagaimana malware akan dianalisis dan menggunakan alat apa yang dibutuhkan selama proses analisis.

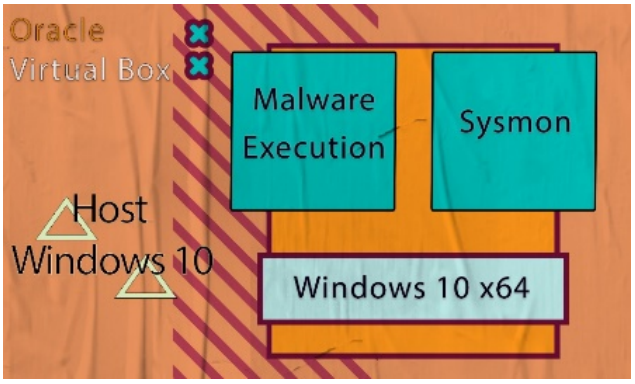
2. Pengujian mencakup pengolahan data yang dikumpulkan dalam forensik dan mengeluarkan data sesuai kebutuhan sehingga menjaga integritas data. Data yang digunakan dalam penelitian ini yaitu events log windows dan Log sysmon dikeluarkan menjadi file format JSON. Tahap ini dilakukan untuk memelihara bukti digital untuk memastikan keaslian dari dataset yang diambil.

3. Analisa ini akan dilakukan analisa mencakup proses hasil pemeriksaan dengan menggunakan metode digital forensic dibenarkan secara Teknik dan hukum untuk mendapatkan informasi yang berguna dan menjawab pertanyaan – pertanyaan yang menjadi pendorong untuk melakukan pengumpulan dan pemeriksaannya. Pada proses ini menggunakan dataset dari events log windows 10, yang akan diekstrak menjadi file JSON untuk mempermudah dalam menganalisa menggunakan Jupyter Notebook.

4. Laporan merupakan fase terakhir ini melaporkan hasil analisis yang meliputi penggambaran tindakan yang dilakukan dalam menganalisa malware, seperti mengetahui proses penyebaran malware dan mengamankan celah yang teridentifikasi sehingga ditingkatkan keamanan sistem, Barang bukti digital dapat digunakan dalam persidangan.

Perancangan Virtual Lab

Peneliti akan merancang sebuah Virtual lab atau mesin virtual, merupakan sebuah rekayasa perangkat yang memiliki fungsi yang sama seperti halnya komputer fisik, rekayasa yang mampu melakukan aktivitas misalnya menginstal aplikasi, menjalankan program, membuat, instal sistem operasi, pembaruan system dan konfigurasi[10]. Dapat dilihat pada Gambar 2 bahwa peneliti akan menggunakan sistem operasi windows 10 sebagai target dan didalamnya peneliti akan mengeksekusi sebuah sample malware yang dipersiapkan.



Gambar 2: Rancangan Virtual Lab

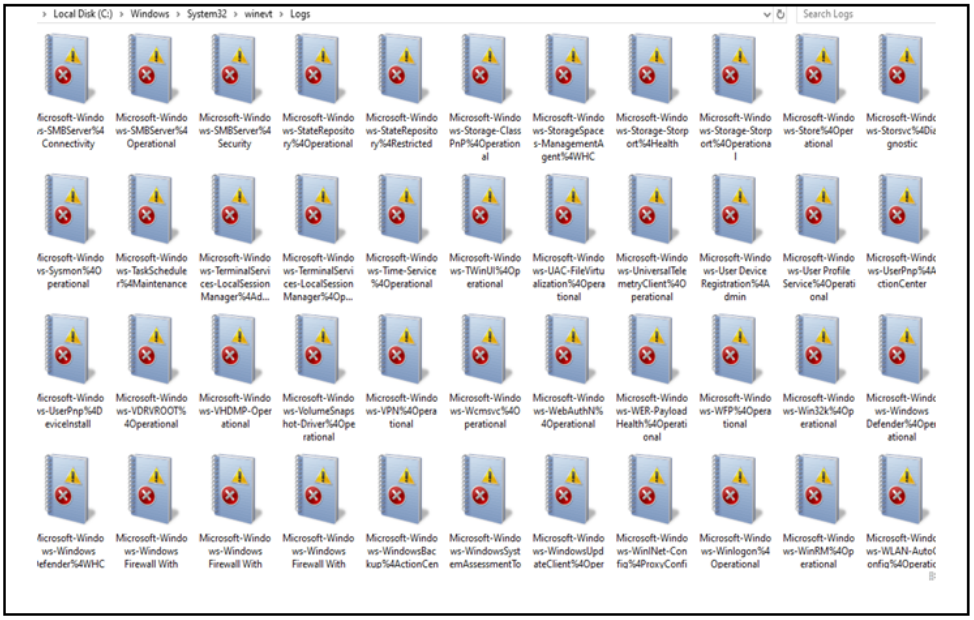
Sysmon

Peneliti menggunakan sysmon dalam menganalisa sistem monitor dikarenakan sysmon mampu merekam secara akurat meskipun komputer mengalami restart [11]. Sysmon sangat handal dalam mengawasi aktivitas dan insiden yang terjadi pada sistem, sysmon dipasang sebelum dieksekusinya malware zeuz banking, lihat Gambar 3.

Microsoft-Windows-Sysmon%4Operational_1 Number of events: 55.156

Level	Date and Time	Source	Event ID	Task Category
Information	21/08/2021 13:12:00	Sysmon	1	Process Create (rule: Pro.
Information	21/08/2021 13:12:00	Sysmon	13	Registry value set (rule: ...
Information	21/08/2021 13:12:00	Sysmon	3	Network connection det.
Information	21/08/2021 13:11:59	Sysmon	13	Registry value set (rule: ...
Information	21/08/2021 13:11:58	Sysmon	22	Dns query (rule: DnsQue.
Information	21/08/2021 13:11:58	Sysmon	22	Dns query (rule: DnsQue.
Information	21/08/2021 13:11:58	Sysmon	22	Dns query (rule: DnsQue.
Information	21/08/2021 13:11:58	Sysmon	22	Dns query (rule: DnsQue.
Information	21/08/2021 13:11:58	Sysmon	22	Dns query (rule: DnsQue.
Information	21/08/2021 13:11:58	Sysmon	22	Dns query (rule: DnsQue.
Information	21/08/2021 13:11:57	Sysmon	3	Network connection det.
Information	21/08/2021 13:11:56	Sysmon	3	Network connection det.
Information	21/08/2021 13:11:55	Sysmon	3	Network connection det.
Information	21/08/2021 13:11:54	Sysmon	3	Network connection det.
Information	21/08/2021 13:11:53	Sysmon	22	Dns query (rule: DnsQue.
Information	21/08/2021 13:11:53	Sysmon	3	Network connection det.
Information	21/08/2021 13:11:52	Sysmon	3	Network connection det.
Information	21/08/2021 13:11:51	Sysmon	3	Network connection det.
Information	21/08/2021 13:11:48	Sysmon	13	Registry value set (rule: ...
Information	21/08/2021 13:11:46	Sysmon	22	Dns query (rule: DnsQue.
Information	21/08/2021 13:11:45	Sysmon	1	Process Create (rule: Pro.

Gambar 3: Sysmon



Gambar 4: Events Log

Dataset

Peneliti ini akan mengambil dataset yang telah dikumpulkan menggunakan "Sysmon" pada tanggal 21 Agustus 2021 dan disimpan pada events log dari sistem operasi windows 10 yang sudah terinfeksi oleh malware zeuz banking invoice_2318362983713_82393 1342io.pdf.exe. File events log yang diambil peneliti yaitu Microsoft-Windows-Sysmon%4Operational.evtx, selanjutnya peneliti akan melakukan analisis terhadap dataset tersebut. Event log sendiri mengacu pada kejadian yang direkam dalam konteks suatu proses dan menyimpan setiap peristiwa, insiden atau aktivitasnya secara lengkap. Seperti logs level, jam dan tanggal, source, event_id dan task kategori., lihat Gambar 4

Hasil Penelitian

Berdasarkan hasil dari prooses pengolahan dari dataset events log windows 10 (evtx) yang telah diekstrak menjai file format JSON, lihat Gambar 5. Sehingga akan dilakukan analisis untuk melihat aktivitas apa saja yang dilakukan malware zeuz banking terhadap system menggunakan jupyter noterbook.

```
invoke_sysmon_df = pd.read_json('Microsoft-Windows-Sysmon%4Operational.evtx.json', lines=True)
```

```
invoke_sysmon_df.head()
```

	event_record_id	timestamp	winlog	log	event	@timestamp
0	64	2021-08-22 17:18:43.275620+00:00	{'channel': 'Microsoft-Windows-Sysmon/Operatio...	{'file': {'name': 'Microsoft-Windows-Sysmon%4O...	{'code': 5, 'created': '2021-08-22T17:18:43.27...	2021-08-22T17:18:43.275620Z
1	63	2021-08-22 17:18:43.236126+00:00	{'channel': 'Microsoft-Windows-Sysmon/Operatio...	{'file': {'name': 'Microsoft-Windows-Sysmon%4O...	{'code': 5, 'created': '2021-08-22T17:18:43.23...	2021-08-22T17:18:43.236126Z
2	62	2021-08-22 17:18:36.582629+00:00	{'channel': 'Microsoft-Windows-Sysmon/Operatio...	{'file': {'name': 'Microsoft-Windows-Sysmon%4O...	{'code': 5, 'created': '2021-08-22T17:18:36.58...	2021-08-22T17:18:36.582629Z
3	61	2021-08-22 17:18:38.387945+00:00	{'channel': 'Microsoft-Windows-Sysmon/Operatio...	{'file': {'name': 'Microsoft-Windows-Sysmon%4O...	{'code': 1, 'created': '2021-08-22T17:18:38.38...	2021-08-22T17:18:38.387945Z
4	60	2021-08-22 17:18:30.852287+00:00	{'channel': 'Microsoft-Windows-Sysmon/Operatio...	{'file': {'name': 'Microsoft-Windows-Sysmon%4O...	{'code': 1, 'created': '2021-08-22T17:18:30.86...	2021-08-22T17:18:30.852287Z

Gambar 5: Dataset JSON

```
In [11]: invoke_sysmon_flat.columns

Out[11]: Index(['event_record_id', 'timestamp', '@timestamp', 'winlog.channel',
       'winlog.computer_name', 'winlog.event_id', 'winlog.opcode',
       'winlog.provider_guid', 'winlog.provider_name', 'winlog.record_id',
       'winlog.task', 'winlog.version', 'winlog.process.pid',
       'winlog.process.thread_id', 'winlog.event_data.Image',
       'winlog.event_data.ProcessGuid', 'winlog.event_data.ProcessId',
       'winlog.event_data.RuleName', 'winlog.event_data.UtcTime',
       'winlog.event_data.Status', 'log.file.name', 'event.code',
       'event.created', 'winlog.event_data.CommandLine',
       'winlog.event_data.Company', 'winlog.event_data.CurrentDirectory',
       'winlog.event_data.Description', 'winlog.event_data.FileVersion',
       'winlog.event_data.Hashes', 'winlog.event_data.IntegrityLevel',
       'winlog.event_data.LogonGuid', 'winlog.event_data.LogonId',
       'winlog.event_data.OriginalFileName',
       'winlog.event_data.ParentCommandLine', 'winlog.event_data.ParentImage',
       'winlog.event_data.ParentProcessGuid',
       'winlog.event_data.ParentProcessId', 'winlog.event_data.Product',
       'winlog.event_data.TerminalSessionId', 'winlog.event_data.User',
       'winlog.event_data.SchemaVersion', 'winlog.event_data.State',
       'winlog.event_data.Version', 'winlog.event_data.Configuration',
```

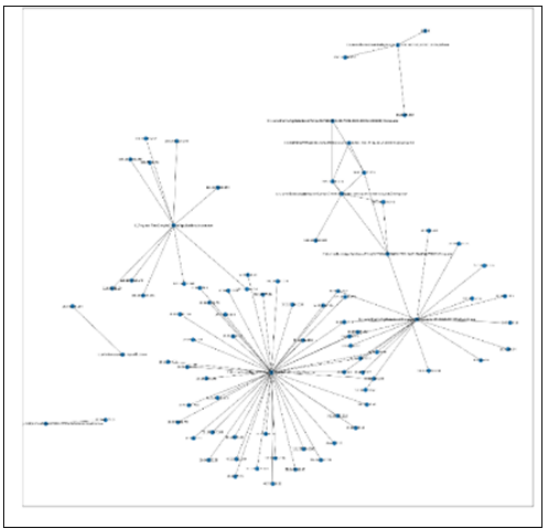
Gambar 6: Dataframe

Dataframe

Pada tahap ini peneliti akan melihat index data sysmon menggunakan invoke_sysmon_flat. columns seperti pada Gambar 6. Sehingga peneliti bisa melakukan pengelompokan (grouping) pada dataframe. Proses ini bertujuan untuk melihat data yang dikompilasi pada kolom dan baris dan berurutan, sehingga dapat dengan mudah melihat event id atau aktivitas terhadapap sistem.

Visualisasi IP

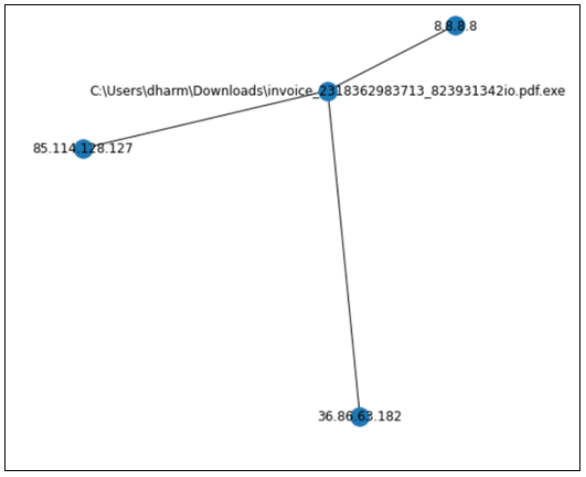
Pada tahap ini peneliti akan menggunakan library networkx untuk menampilkan hasil visualisasi IP dari dataset windows events log ,visualisasi ditunjukan pada Gambar 7 grafik yang menyertakan lebih banyak informasi mengenai IP didalam grafik dan mempunyai node yang saling berhubungan.



Gambar 7: Visualisasi IP

Node 1

Pada tahap ini peneliti akan menggunakan *library networkx* untuk menampilkan hasil visualisasi IP dari *dataset windows events log* ,visualisasi ditunjukan pada Gambar 8, grafik yang menyertakan lebih banyak informasi mengenai IP didalam grafik dan mempunyai node yang saling berhubungan, lihat Tabel 1. Berdasarkan gambar 8 peneliti telah melihat sebuah simpul tengah menunjukan tiga koneksi, bagaimana proses penyebaran sebuah malware zeuz banking-invoice_2318362983713_8239313 42io.pdf.exe terhadap sistem operasi serta menghubungkan pada target dan server ke dalam jaringan.



Gambar 8: Node 1

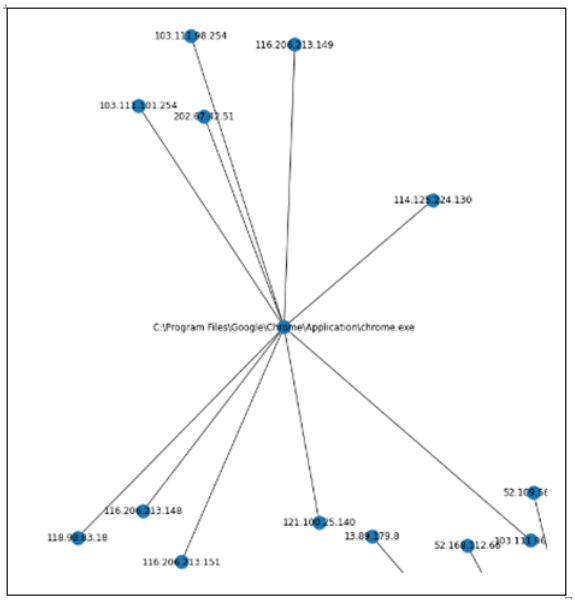
Tabel 1: Node 1

Ip Address	Hostname	Lokasi
85.114.128.127	Srv11028.dus4.fastwebserver.de	Germany Hubbelrath Fast It Colocation
8.8.8.8	dns.google	United State mountain view google
36.86.63.182	Telkom.co.id	Indonesia Jakarta PT.Telkom

Node 1 merupakan pola dari malware zeuz banking terhadap sistem, yang mana malware ini berasal dari titik 85.114.128.127 yaitu IP server malware zeuz banking yang terhubung pada titik 8.8.8.8 sebagai DNS dari google, dan titik 36.86.63.182 IP router ISP Telkom.

Node 2

Selanjunya pada node 2 ini akan menampilkan proses dari C:\Program Files\ Google\Chrome\Applic Chrome.exe. Terlihat pada Gambar 9 yang mempunyai simpul dan berbagai koneksi atau proses didalamnya, dengan daftar IP tersaji pada Tabel 2.



Gambar 9: Node 2

Tabel 2: Node 2

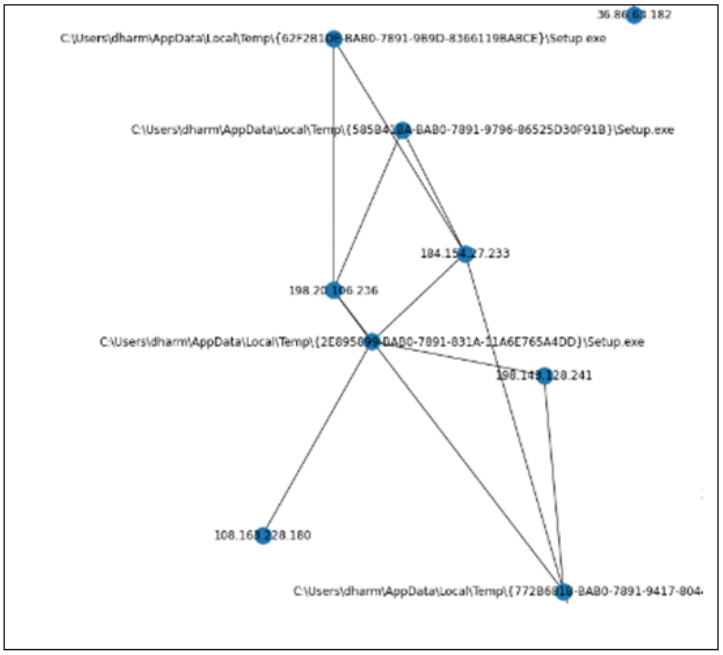
IP Address	Lokasi
103.111.101.254	Surabaya Pt.Mitra Lintas Mutimedia
202.67.42.51	Pt.Hutchison cp Telecommunication Jakarta Selatan
103.111.99.254	Surabaya Pt.Mitra Lintas Mutimedia
116.206.213.149	Pt.Giga Patra Multimedia Lampung timur
114.125.224.130	Pt. Telekomunikasi Selular (telkomsel) Indonesia
103.111.86.254	Dumai Cv. Solution Technology
121.100.25.140	Palembang Pt. Sakti Putra Mandiri
116.206.213.151	Pt. Giga Patra Multimedia Lampung timur
116.206.213.148	Pt. Giga Patra Multimedia Lampung timur
118.98.83.18	Pt. Telkom Indonesia Jakarta

Node 3

Pada tahap ini node 3 akan menampilkan proses dari C:\Users\dharm\ local\temp\{2E89099-BABO-7891-831A-21A6E765A4DD}\Setup.exe. Terlihat pada gambar 10 yang mempunyai simpul dan berbagai koneksi atau proses didalamnya.

Tabel 3: Node 3

Ip Adderess	Lokasi
198.20.106.236	SingleHop LLC Amsterdam Netherlands
184.154.27.233	SingleHop LLC Chicago Illinois United States
198.143.128.241	SingleHop LLC Chicago Illinois United States
108.163.228.180	SingleHop LLC Chicago Illinois United States



Gambar 10: Node 3

Destination IP Berdasarkan Gambar 10 menampilkan daftar file.exe serta mengetahui daftar *destinationIP* dan *destinationPor*t lebih sepesifik, model akan menampilkan daftar dari IP tersebut (lihat Tabel 3) . IP ini kemudian akan digunakan untuk mengetahui darimana asalnya malware zeuz banking itu sendiri, lihat Gambar 11.

Daftar File.exe Setelah visualisasi dilakukan, model kemudian akan menampilkan daftar file .exe yang tampil pada saat proses visualisasi IP. Daftar file tersebut dapat dilihat pada Gambar 12.

Hasil Akhir

Berdasarkan hasil dari prooses pengolahan dari dataset events log windows 10 (evtx) yang telah diekstrak menjai file format JSON. Sehingga akan dilakukan analisis untuk melihat aktivitas apa saja yang dilakukan malware zeuz banking terhadap system menggunakan jupyter noterbook, lihat Gambar 13.

	winlog.event_data.ParentProcessGuid	winlog.event_data.ParentCommandLine	winlog.event_data.Image_x	winlog.computer_name	winlog.ev
0	F3081BA1-8C0C-611E-1B00-000000000900	C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule	C:\Windows\System32\rundll32.exe	DESKTOP-U4N7R4A	
1	F3081BA1-8C0C-611E-1B00-000000000900	C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule	C:\Windows\System32\rundll32.exe	DESKTOP-U4N7R4A	
2	F3081BA1-8C0B-611E-0F00-000000000900	C:\Windows\system32\svchost.exe -k DcomLaunch -p	C:\Windows\System32\rundll32.exe	DESKTOP-U4N7R4A	
3	F3081BA1-AC82-6122-960A-000000000900	C:\Windows\system32\regsvr32.exe -s C:\Users\dharm\DOWNLO~1\DanaBot.dll f1 C:\Users\dharm\DOWNLO~1\DanaBot.exe@3964	C:\Windows\SysWOW64\rundll32.exe	DESKTOP-U4N7R4A	
4	F3081BA1-8C0C-611E-1B00-000000000900	C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule	C:\Windows\System32\rundll32.exe	DESKTOP-U4N7R4A	
5	F3081BA1-06CA-6123-0F00-000000000B00	C:\Windows\system32\svchost.exe -k DcomLaunch -p	C:\Windows\System32\rundll32.exe	DESKTOP-U4N7R4A	
6	F3081BA1-06CB-6123-1B00-000000000B00	C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule	C:\Windows\System32\rundll32.exe	DESKTOP-U4N7R4A	
7	F3081BA1-4447-6123-4703-000000000B00	"C:\Users\dharm\AppData\Local\Temp\{2E895899-BAB0-7891-831A-11A6E765A4DD}\setup.exe"	C:\Windows\SysWOW64\rundll32.exe	DESKTOP-U4N7R4A	
8	F3081BA1-447C-6123-5403-000000000B00	C:\Windows\system32\rundll32.exe "C:\Program Files (x86)\Babylon\Babylon-Pro\Utils\BabylonDocTranslation64PI.dll",AdminAction64 1 0	C:\Windows\System32\rundll32.exe	DESKTOP-U4N7R4A	
9	F3081BA1-4447-6123-4703-000000000B00	"C:\Users\dharm\AppData\Local\Temp\{2E895899-BAB0-7891-831A-11A6E765A4DD}\setup.exe"	C:\Windows\SysWOW64\rundll32.exe	DESKTOP-U4N7R4A	
10	F3081BA1-447D-6123-5903-000000000B00	C:\Windows\system32\rundll32.exe "C:\Program Files (x86)\Babylon\Babylon-Pro\Utils\BabylonOffice64PI.dll",AdminAction64 1 0	C:\Windows\System32\rundll32.exe	DESKTOP-U4N7R4A	
11	F3081BA1-4447-6123-4703-000000000B00	"C:\Users\dharm\AppData\Local\Temp\{2E895899-BAB0-7891-831A-11A6E765A4DD}\setup.exe"	C:\Windows\SysWOW64\rundll32.exe	DESKTOP-U4N7R4A	
12	F3081BA1-449A-6123-8303-000000000B00	C:\Windows\system32\rundll32.exe "C:\Program Files (x86)\Babylon\Babylon-Pro\Utils\BabylonOffice64PI.dll",AdminAction64 3 0	C:\Windows\System32\rundll32.exe	DESKTOP-U4N7R4A	

Gambar 11: Destination IP

winlog.event_data.DestinationIp	winlog.event_data.DestinationPort	
103.111.101.254	8080.0	2
103.111.96.254	8080.0	2
103.111.98.254	8080.0	2
104.46.162.224	443.0	1
104.46.162.226	443.0	9
108.163.228.180	80.0	2
114.125.224.130	8080.0	2
116.206.213.148	8080.0	2
116.206.213.149	8080.0	2
116.206.213.151	8080.0	2
118.98.83.18	8080.0	2
121.100.25.140	8080.0	2
13.107.42.12	443.0	20
13.107.43.12	443.0	50
13.69.239.72	443.0	5
13.69.239.73	443.0	2
13.78.111.198	443.0	6
13.89.179.10	443.0	2
13.89.179.8	443.0	1
131.253.14.230	443.0	1
184.154.27.233	80.0	36
198.143.128.240	80.0	2
198.143.128.241	80.0	4
198.20.106.236	80.0	8
20.150.43.196	443.0	1
20.150.77.68	443.0	1
20.150.88.132	443.0	1
20.150.88.164	443.0	1
20.150.95.132	443.0	1
20.150.95.196	443.0	1
20.189.173.14	443.0	1
20.189.173.15	443.0	4
20.189.173.3	443.0	6
20.189.173.5	443.0	4
20.189.173.6	443.0	2
20.190.144.140	443.0	1
20.197.71.89	443.0	4
20.198.162.76	443.0	7
20.198.162.78	443.0	4
20.42.65.84	443.0	4
20.42.65.85	443.0	1

Gambar 12: File Exe

```
(
invoke_sysmon_flat[["winlog.event_data.DestinationHostname","winlog.event_data.DestinationIp"
                    ,"winlog.event_data.DestinationPort"
                    ,"winlog.event_data.DestinationPortName"
                    ,"winlog.event_data.Protocol"
                    ,"winlog.event_data.SourceIp","winlog.event_data.SourcePort"
                    ,'timestamp','winlog.event_id','winlog.event_data.ProcessGuid'
                    ,"winlog.event_data.ParentProcessGuid",'winlog.event_data.ParentCommandLine'
                    ,"winlog.event_data.ParentImage","winlog.event_data.User"
                    ,"winlog.event_data.LogonGuid","winlog.event_data.CommandLine",
                   "winlog.event_data.Description",'winlog.event_data.Image',
                    'winlog.computer_name'
                   ]]

[(invoke_sysmon_flat['winlog.channel'] == 'Microsoft-Windows-Sysmon/Operational')
   & (invoke_sysmon_flat['winlog.event_id'] == 3)
   & (invoke_sysmon_flat["winlog.event_data.DestinationIp"]
   & (invoke_sysmon_flat["winlog.event_data.DestinationPort"]
      & ((invoke_sysmon_flat['winlog.event_data.Image'].str.contains('.*invoice_2318362983713_8239313421o.pdf.exe.*', regex=Tr
]

.head(20)
)
```

	winlog.event_data.DestinationHostname	winlog.event_data.DestinationIp	winlog.event_data.DestinationPort	winlog.event_data.DestinationPortName	winlog
2882	srv11028.dus4.fastwebserver.de	85.114.128.127	53.0	domain	
2883	-	36.86.63.182	80.0	http	
2884	dns.google	8.8.8.8	53.0	domain	

Gambar 13: Hasil Akhir

Penutup

Berdasarkan hasil penelitian "Analisis Log Menggunakan Jupyter Notebook Pada Kasus Cyber Threat Hunting", maka dapat diambil kesimpulan penelitian sebagai berikut: Memanfaatkan dataset events log windows 10 mampu mendapatkan bukti digital untuk mendukung investigasi serangan malware. Berdasarkan penelitian yang dilakukan, ditemukan asal malware, aplikasi yang terinfeksi, domain dan visualisasi IP. Penelitian selanjutnya menggunakan spesifikasi komputer yang lebih mumpuni dikarenakan memakan waktu pada saat menjalankan windows 10 di virtual box untuk mensimulasikan sample dan pengambilan dataset events log. Penggunaan aplikasi jupyter notebook serta didukung modul dapat menampilkan barang bukti digital berupa visualisasi IP. Ucapan Terima Kasih Terima kasih kepada Direktorat Jendral Pendidikan Tinggi, Riset dan Teknologi (Kemendikbudristek) yang telah memberi dana penelitian ini melalui Program Talenta Inovasi 2021.

Daftar Pustaka

[1] Haw Min Lu, Adrian Kwong & José Unpingco, "Securing Your Collaborative Jupyter

Notebooks In The Cloud Using Container and Load Balancing Services", Conference: Python in Science Conference, Cornel University, DOI:10.25080/Majora-342d178e-001, 2020.

[2] Kul Prasad Subedi, Daya Ram Budhathoki, Dipankar Dasgupta, "Forensic Analysis of Ransomware Families using Static and Dynamic Analysis", Conference: 12th International Workshop on Systematic Approaches to Digital Forensics Engineering, @ 2018 IEEE Security and Privacy. San Francisco, California, USA, DOI:10.1109/SPW.2018.00033, 2018.

[3] T. A. Cahyanto, V. Wahanggara dan D. Ramadana, "Analisis dan Deteksi Malware Menggunakan Metode Malware Analisis Dinamis dan Malware Analisis Statis", JUSTINDO, vol. 2, no. 1, p. 12, 2017.

[4] M. Moh, S. Pininti, S. Doddapaneni and T.-S. Moh, "Detecting Web Attacks Using Multi-stage Log Analysis", in 2016 IEEE 6th International Conference on Advanced Computing (IACC), Bhimavaram, India, DOI: 10.1109/IACC.2016.141, Feb. 2016.

[5] V Mavroeidis, A Jøsang, "Data-Driven Threat Hunting Using Sysmon", Proceedings of the 2nd International Conference on Cryptography, Security and Privacy, DOI:10.1145/3199478.3199490, 2018.

[6] Suyash Sharma, " Efficient Log Analysis Using Advanced", School Of Computing National Colleger Ireland, Ireland 2019.

[7] Dau Hoang, "Detecting Common Web Attacks Based on Machine Learning Using Web Log", Conference: Advances in Engineering Research and Application. ICERA 2020.At: Thai Nguyen, VietnamVolume: Springer LNNS Vol. 178, DOI:10.1007/978-3-030-64719-3_35, 2020.

[8] Stacey Omeleze Barror, Hein S.Venter, "A Taxonomy for Cybercrime Attack In the Public Cloud", Conference on cyber warfare and security, South Africa 2019.

[9] Ferdiansyah, "Analisis Aktivitas dan Pola Jaringan Terhadap Eternal Blue & Wannacry Ransomware", JUSIFO (Jurnal Sistem Informasi), vol.. 4, no. 1, DOI https://doi.org/10.19109/jusifo.v4i1.2077, 2018.

[10] Jimmy Moedhjahedy, "Forensik Komputer Studi Kasus : Universitas Klabat", Jurnal Sistem Informasi dan Teknologi Informasi (JUSITI), vol. 5, no.2, 2016.

[11] V. Kanimozhi and T. Prem Jacob, "Artificial Intelligence based Network Intrusuion Detection With Hyper-Parameter Optimization Tunning on the Realistic Cyber Dataset CSE-CIC IDS 2018 using cloud computing", Conference: 2019 International Conference on Communication and Signal Processing (ICCSP), DOI:10.1109/ICCSP.2019.8698029, 2019.