# DETEKSI SERANGAN *MALWARE RANSOMWARE* PADA *BITCOIN MINING* DENGAN METODE *K-MEANS CLUSTERING*

**Oleh :**

**FITRIANI**

**09011181621023**

**JURUSAN SISTEM KOMPUTER**
**FAKULTAS ILMU KOMPUTER**
**UNIVERSITAS SRIWIJAYA**
**2021**

# DETEKSI SERANGAN *MALWARE RANSOMWARE* PADA *BITCOIN MINING* DENGAN METODE *K-MEANS CLUSTERING*

**TUGAS AKHIR**

**Diajukan Untuk Melengkapi Salah Satu Syarat**
**Memperoleh Gelar Sarjana Komputer**


**Oleh :**

**FITRIANI**

**09011181621023**

**JURUSAN SISTEM KOMPUTER**
**FAKULTAS ILMU KOMPUTER**
**UNIVERSITAS SRIWIJAYA**
**2021**

# LEMBAR PENGESAHAN

## DETEKSI SERANGAN *MALWARE RANSOMWARE* PADA *BITCOIN MINING* DENGAN METODE *K-MEANS CLUSTERING*

**TUGAS AKHIR**

**Diajukan Untuk Melengkapi Salah Satu Syarat**
**Memperoleh Gelar Sarjana Komputer**

**Oleh :**

**FITRIANI**

**09011181621023**

**Inderalaya, Mei 2021**

**Pembimbing I Tugas Akhir**

**Deris Stiawan,M.T.,Ph.D**

**NIP.197806172006041002**

**Pembimbing II Tugas Akhir**

**Ahmad Heryanto,S.Kom.,M.T**

**NIP.198701222015041002**

**Mengetahui,**

**Ketua Jurusan Sistem Komputer**

**Dr.Ir.Sukemi, MT**

**NIP. 196612032006041001**

## HALAMAN PERSETUJUAN

Telah diuji dan lulus pada:

Hari : Kamis

Tanggal : 01 April 2021

**Tim Penguji:**

1. **Ketua** : **Sarmayanta Sembiring, S.SI., M.T.** (.....)
2. **Sekretaris** : **Rendyansyah, S.Kom., M.T.** (.....)
3. **Penguji** : **Huda Ubaya, S.T., M.T.** (.....)

**Mengetahui,**

**Ketua Jurusan Sistem Komputer**

UNIVERSITAS SRIWIJAYA FAKULTAS ILMU KOMPUTER JURUSAN SISTEM KOMPUTER

**Dr. Ir. Sukemi, MT**

**NIP. 196612032006041001**

# DETEKSI SERANGAN *MALWARE RANSOMWARE* PADA *BITCOIN MINING* DENGAN METODE *K-MEANS CLUSTERING*

**Fitriani (0901181621023)**

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email : fitrianibn0302@gmail.com

**ABSTRAK**

Deteksi serangan merupakan suatu kegiatan untuk menganalisa suatu data atau file apakah data tersebut terdapat serangan atau tidak. Snort IDS (intrusion detection system) membantu dalam menganalisa dan mendeteksi serangan pada suatu jaringan pada proses penambangn bitcoin. Serangan Malware Ransomware yaitu serangan yang sangat berbahaya karena meminta penebuasan sejumlah biaya agar dapat mengakses suatu file yang diinginkan. Serangan Ransomware biasanya menyerangan para penambang bitcoin yang sedang melakukan penambangan. Bitcoin Mining merupakan proses yang dilakukan para penambang untuk mendapatkan sebuah keuntungan yang keuntungannya biasa disebut Bitcoin. K-Means dapat digunakan untuk mendeteksi serangan yang terdapat pada dataset bitcoin mining. Pola serangan Malware Ransomware pada dataset bitcoin mining dapat dikenali dengan beberapa parameter seperti source port, Destination port, TTL dan protocol. Pada penelitian ini didapatkan hasil akurasi yaitu 99%, yang menandakan keakuratan dalam pengklasifikasian serangan malware pada penelitian ini.

**Kata kunci:** Deteksi Malware,snort IDS,malware ransomware,k-means clustering,bitcoin mining.

**Mengetahui**

| **Pembimbing I** | **Pembimbing II** |
|---|---|
| **Deris Stiawan,M.T.,Ph.D** | **Ahmad Heryanto,S.Kom.,M.T** |
| **NIP. 197806172006041002** | **NIP.198701222015041002** |

**Ketua Jurusan Sistem Komputer**

2/6/21

**Dr. Ir. H. Sukemi, M.T.**

**NIP. 196612032006041001**

# *DETECTION OF MALWARE RANSOMWARE ATTACKS ON BITCOIN MINING USING K-MEANS CLUSTERING*

**Fitriani (0901181621023)**

*Department of Computer Systems, Faculty of Computer Science,*

*Sriwijaya University*

Email : fitrianibn0302@gmail.com

***ABSTRACT***

*Attack detection is an activity to analyze data or files whether the data has an attack or not. Snort IDS (intrusion detection system) helps in analyzing and detecting attacks on a network in the bitcoin mining process. Malware Ransomware attack is a very dangerous attack because it requires a fee to be able to access the desired file. Ransomware attacks usually attack bitcoin miners who are doing the mining. Bitcoin Mining is a process carried out by miners to get a profit whose profits are commonly called Bitcoin. K-Means can be used to detect attacks on the bitcoin mining dataset. Malware Ransomware attack patterns on mining bitcoin mining datasets can recognized by several parameters such as source port, destination port, TTL, and protocol. In this study, the results obtained were 99% accuracy, which indicates the accuracy in the classification of malware attacks in this study.*

***Keywords:*** *Malware detection, snort IDS, ransomware malware, k-means clustering, bitcoin mining.*

**Mengetahui**

**Pembimbing I**

**Deris Stiawan,M.T.,Ph.D**

**NIP. 197806172006041002**

**Pembimbing II**

**Ahmad Heryanto,S.Kom.,M.T**

**NIP.198701222015041002**

**Ketua Jurusan Sistem Komputer**

4/6/21

**Dr. Ir. H. Sukemi, M.T.**

**NIP. 196612032006041001**

# HALAMAN PERNYATAAN

**Yang bertanda tangan dibawah ini:**

**Nama** : **Fitriani**

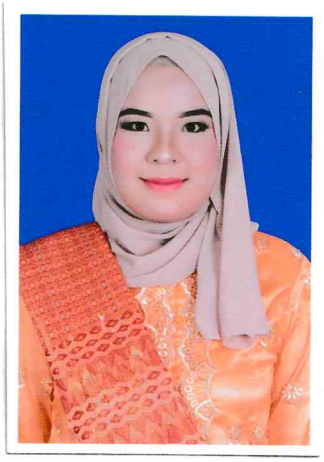
**NIM** : **09011181621023**

**Judul** : **Deteksi Serangan *Malware Ransomware* Pada *Bitcoin Mining* Dengan Metode *K-Means Clustering***

Hasil Pengecekan Software iThenticate/Turnitin : 13 %

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil pejiplakan / *plagiat*. Apabila ditemukan unsur penjiplakan / *plagiat* dalam laporan tugas akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian, Pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan.



**Inderalaya, Mei 2021**


**Fitriani**

**NIM. 09011181621023**

## HALAMAN PERSETUJUAN

Telah diuji dan lulus pada:

Hari : Kamis

Tanggal : 01 April 2021

**Tim Penguji:**

1. **Ketua** : **Sarmayanta Sembiring, S.SI., M.T.** (.....)
2. **Sekretaris** : **Rendyansyah, S.Kom., M.T.** (.....)
3. **Penguji** : **Huda Ubaya, S.T., M.T.** (.....)

**Mengetahui,**

**Ketua Jurusan Sistem Komputer**

UNIVERSITAS SRIWIJAYA FAKULTAS ILMU KOMPUTER JURUSAN SISTEM KOMPUTER

**Dr. Ir. Sukemi, MT**

**NIP. 196612032006041001**

# HALAMAN PERSEBAHAN

**Kutipan:**

**"Tahapan pertama dalam mencari ilmu adalah mendengarkan, kemudian diam dan menyimak dengan penuh perhatian, lalu menjaganya, lalu mengamalkannya, dan kemudian menyebarkannya." - Sufyan bin Uyainah**

**"Ilmu yang sejati, seperti barang berharga lainnya, tidak bisa diperoleh dengan mudah. Ia harus diusahakan, dipelajari, dipikirkan, dan lebih dari itu, harus selalu disertai doa."**

**Tugas Akhir Ini Kupesembahkan Untuk:**

- **ALLAH SWT**
- **Rasulullah Muhammad SAW**
- **Kedua orang tua yang tersayang dan tercinta.**
- **Saudaraku ( Sapriansyah, S.Ip, Pandriansyah, Octa Alpian A) dan Keluarga besarku yang tersayang.**
- **Sahabat – sahabatku yang selalu ada bersamaku disaat senang maupun susah (Widyana, Yen Mey, Diah, Icha, Ega, Octafian, Aji, Dll).**
- **Rekan – rekan seperjuangan di Sistem Komputer 2016**
- **Jurusan Sistem Komputer**
- **Almamaterku Universitas Sriwijaya**

# KATA PENGANTAR

Puji syukur penulis panjatkan atas kehadirat Allah Subhanahu Wata'ala yang telah melimpahkan rahmat dan karunianya, sehingga penulis dapat menyelesaikan Tugas Akhir ini yang **"Deteksi serangan *malware ransomware* pada *bitcoin mining* dengan metode *k-means clustering*"**. Shalawat serta salam tak lupa kita curahkan kepada junjungan kita Nabi Muhammad SAW beserta keluarga, Sahabat dan para pengikutnya yang insyaallah istiqomah hingga akhir zaman.

Selesainya penyusunan Tugas Akhir ini tidak terlepas dari peran serta semua pihak. Oleh karena itu, pada kesempatan ini penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada:

1. Allah Subhanahu Wata'ala yang telah memberikan berkah serta nikmat kesehatan dan kesempatan kepada penulis dalam menyusul Tugas Akhir ini.
2. Kepada kedua orang tua tercinta, yaitu bapak Burliansyah dan ibu Nursida yang selalu mendoakanku, semangat dalam bekerja demi kami dan yang selalu mendukungku dalam hal apapun yang terbaik untukku.
3. Saudara-saudaraku yang tersayang, kakak sapriansyah, adek pandriansyah dan adek okta alpian yang selalu mendukung dan memberi semangat dalam kelancaran dan kemudahan untuk menyelesaikan tugas akhir.
4. Keluarga besar yang tersayang, yang telah mendukung dalam hal apapun dan membantu dalam hal moral serta materil.
5. Bapak Dr. Ir. Sukemi, MT. selaku Ketua Jurusan Sistem Komputer Universitas Sriwijaya.
6. Ibu Sri Desi Siswanti, S.T.,M.T. selaku dosen Pembimbing Akademik.
7. Bapak Deris stiawan,M.T.,Ph.D. selaku Pembimbing 1 Tugas Akhir.
8. Bapak Ahmad Heryanto, S.Kom., M.T. selaku Pembimbing 2 Tugas Akhir.
9. Mbak Reny selaku Admin Jurusan Sistem Komputer yang telah membantu penulis dalam hal administrasi selama perkuliahan.
10. Bapak, Ibu dosen jurusan Sistem Komputer yang telah memberikan ilmunya serta pengalamannya kepada saya.
11. Keluarga besar HIMASISKO yang telah membersamai dan membantu dalam hal perkulihan selama ini.

12. Teman-teman sekelas SK16A Indralaya Universitas Sriwijaya , Terimakasih untuk setiap kebersamaan dan bantuannya selama mengerjakan tugas akhir dan perkuliahan.
13. Teman-teman seangkatan Kosentrasi jaringan yang juga anak bimbingan Bapak Deris Stiawan dan Bapak Ahmad Heryanto serta kakak dan adek tingkat yang telah membantu penulis dalam menyelesaikan Tugas Akhir ini.
14. Kakak-kakak tingkat yang satu riset dengan saya, kak Eko, kak Resti, kak Juanda, terimakasih telah membantu saya menyelesaikan tugas akhir ini.
15. Teman-teman kosan yang saya sayangi, Widyana aprianti, Siti Aisyah, Yen mey sutedja, Diah komariah, Ega wahyu ningsih, Octafian, Ahmad aji dan yang lainnya, terima kasih atas kebersamaannya selama ini.
16. Seluruh pihak yang tidak dapat penulis sebutkan satu persatu, yang telah memberikan semangat serta do'anya dalam penyelesaian Tugas Akhir.
17. Almamater.

Penulis menyadari dalam penyusunanlaporan Tugas akhir ini masih terdapat banyak kekurangan, karenanya penulis mengharapkan kritik dan saran untuk perbaikan. Semoga laporan Tugas akhir ini dapat bermanfaat bagi siapa saja yang membacanya.

Wassalamu'alaikum Warahmatulahi Wabarakatuh.

Inderalaya, Mei 2021

Penulis

Fitriani

NIM. 09011181621023

# DETEKSI SERANGAN *MALWARE RANSOMWARE* PADA *BITCOIN MINING* DENGAN METODE *K-MEANS CLUSTERING*

**Fitriani (0901181621023)**

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

Email : fitrianibn0302@gmail.com

**ABSTRAK**

Deteksi serangan merupakan suatu kegiatan untuk menganalisa suatu data atau file apakah data tersebut terdapat serangan atau tidak. Snort IDS (intrusion detection system) membantu dalam menganalisa dan mendeteksi serangan pada suatu jaringan pada proses penambangn bitcoin. Serangan Malware Ransomware yaitu serangan yang sangat berbahaya karena meminta penebuasan sejumlah biaya agar dapat mengakses suatu file yang diinginkan. Serangan Ransomware biasanya menyerangan para penambang bitcoin yang sedang melakukan penambangan. Bitcoin Mining merupakan proses yang dilakukan para penambang untuk mendapatkan sebuah keuntungan yang keuntungannya biasa disebut Bitcoin. K-Means dapat digunakan untuk mendeteksi serangan yang terdapat pada dataset bitcoin mining. Pola serangan Malware Ransomware pada dataset bitcoin mining dapat dikenali dengan beberapa parameter seperti source port, Destination port, TTL dan protocol. Pada penelitian ini didapatkan hasil akurasi yaitu 99%, yang menandakan keakuratan dalam pengklasifikasian serangan malware pada penelitian ini.

**Kata kunci:** Deteksi Malware,snort IDS,malware ransomware,k-means clustering,bitcoin mining.

**Mengetahui**

| **Pembimbing I** | **Pembimbing II** |
|---|---|
| **Deris Stiawan,M.T.,Ph.D** | **Ahmad Heryanto,S.Kom.,M.T** |
| **NIP. 197806172006041002** | **NIP.198701222015041002** |

**Ketua Jurusan Sistem Komputer**

2/6/21

**Dr. Ir. H. Sukemi, M.T.**

**NIP. 196612032006041001**

# *DETECTION OF MALWARE RANSOMWARE ATTACKS ON BITCOIN MINING USING K-MEANS CLUSTERING*

**Fitriani (0901181621023)**

*Department of Computer Systems, Faculty of Computer Science,*

*Sriwijaya University*

Email : fitrianibn0302@gmail.com

***ABSTRACT***

*Attack detection is an activity to analyze data or files whether the data has an attack or not. Snort IDS (intrusion detection system) helps in analyzing and detecting attacks on a network in the bitcoin mining process. Malware Ransomware attack is a very dangerous attack because it requires a fee to be able to access the desired file. Ransomware attacks usually attack bitcoin miners who are doing the mining. Bitcoin Mining is a process carried out by miners to get a profit whose profits are commonly called Bitcoin. K-Means can be used to detect attacks on the bitcoin mining dataset. Malware Ransomware attack patterns on mining bitcoin mining datasets can recognized by several parameters such as source port, destination port, TTL, and protocol. In this study, the results obtained were 99% accuracy, which indicates the accuracy in the classification of malware attacks in this study.*

***Keywords:*** *Malware detection, snort IDS, ransomware malware, k-means clustering, bitcoin mining.*

**Mengetahui**

**Pembimbing I**

**Deris Stiawan,M.T.,Ph.D**

**NIP. 197806172006041002**

**Pembimbing II**

**Ahmad Heryanto,S.Kom.,M.T**

**NIP.198701222015041002**

**Ketua Jurusan Sistem Komputer**

4/6/21

**Dr. Ir. H. Sukemi, M.T.**

**NIP. 196612032006041001**

## DAFTAR ISI

**Halaman**

**BAB III METODOLOGI PENELITIAN**

**BAB IV HASIL DAN ANALISA**



**BAB V KESIMPULAN DAN SARAN**

## DAFTAR GAMBAR

**Halaman**

## DAFTAR TABEL

**Halaman**

# BAB I

# PENDAHULUAN

## 1.1 Latar Belakang

Bitcoin adalah cryptocurrency paling yang populer berdasarkan buku besar digital, terdistribusi, publik dan biasanya disebut blockchain. Sistem bitcoin dirancang sedemikian rupa sehingga kompleksitas dalam penghitungan *checksum* meningkat ketika kapasitas dalam perhitungan dunia meningkat[1]. Node pada jaringan bitcoin menyimpan blockchain, dimana transaksi dicatat dalam satu unit blok, dan blockchain diperpanjang dengan menghasilkan blok-blok baru. Proses menghasilkan blok baru inilah yang disebut sebagai penambangan (Mining), dan yang melakukan kegiatan penambangan biasanya disebut sebagai penambang (Miner). Agar kegiatan menambang dapat berhasil dengan baik, maka para penambang harus menemukan solusi yang biasa disebut *proof-of-work* (PoW)[2].

Penambang menemukan bahwa meningkatnya biaya sumber daya yang terkait dengan penambangan bitcoin membuat nilainya kurang menarik, tetapi penjahat cyber menemukan cara tertentu untuk mengambil keuntungan dari penambangan bitcoin dan keuntungan yang dapat didapatkannya melalui produksi dan distribusi malware penambangan crypto. Malware ini menginfeksi komputer korban atau penambang dan mengkonfigurasi perangkat lunak penambangan cryptocurrency, mengalihkan semua pendapatan penambang langsung ke penyerang, yang tanpa mengeluarkan biaya[3]. Jadi dari itulah seorang penambang bitcoin sangat memerlukan sesuatu yang berguna dan bermanfaat untuk mengetahui atau mendeteksi bagaimana malware ransomware yang menginfeksi komputer dapat dideteksi dan dihilangkan oleh penambang bitcoin agar proses penambangan dapat berjalan dengan lancar dan sukses.

Mendeteksi malware yang menyerang komputer menggunakan *Network based intrusion detection system* (NIDS), sistem ini dapat mendeteksi bebabagai macam serangan yang salah satunya serangan malware ransomware. Selain mendeteksi malware diperlukan juga pengelompokan data serangan dan data

normal untuk memudahkan para penambang membedakan paket data yang terserang dan paket data normal sehingga proses penambangan dapat berjalan dengan lancar. Klasifikasi antara serangan dan normal membutuhkan suatu metode yang dapat melakukan proses pengelompokan data normal dan serangan secara akurat. Pengelompokan K-Means bertujuan untuk mengklasifikasi malware yang menyerang komputer yang sedang melakukan penambangan bitcoin. Agar metode ini berfungsi, pertama-tama harus menentukan yang mewakili masing-masing simpul sebagai vektor multi dimensi dalam ruang Euclidean[4]. Semakin populernya bitcoin kriminal pada ekosistem bitcoin semakin meningkat.

Pada penelitian [5] membahas estimasi pertama dari proporsi entitas kriminal di ekosistem bitcoin menggunakan *supervised machine learning,* dimana klasifikasi yang berbeda dari scikit learn diuji yang menghasilkan daftar empat klasifikasi teratas diantaranya random forest, extremely randomised forests, bagging,and gradient boosting classifiers dengan *cross validation* mendapatkan akurasi (77.38%, 76.47%, 78.46%, 80.76%). Pada penelitian[6] membahas perkirakan secara konservatif bahwa pendapatan ekosistem secara keseluruhan selama dua tahun terakhir lebih dari 16 juta USD yang diambil dari urutan 20.000 korban yang dilakukan malware ransomware perkiraan tersebut didapatkan dengan menjebak malware ransomware dengan metode *end to end*. Untuk menganalisis malware yang menyerang para penambang bitcoin menggunakan berbagai mekanisme yang telah diusulkan pada penelitian-penelitian sebelumnya.

Pada penelitian[7] membahas suatu mekanisme yang telah diusulkan sebagai sistem analisis malware yang resmi dan memiliki akurasi 96,3% dalam mendeteksi malware ransomware menggunakan sistem *kriptografi hybrid*. Mekanisme pemantauan pada dasarnya bersifat reaktif yang artinya operasi file berulang yang menyebabkan I/O sering menunjukkan bahwa ransomware secara aktif menyerang sistem para pengguna atau user penambang bitcoin.

Berdasarkan beberapa ulasan diatas, maka penelitian ini mengusulkan deteksi *malware ransomware* pada proses *bitcoin mining* dengan salah satu metode *unsupervised learning* yaitu metode *K-means Clustering*.

## 1.2 Tujuan

Adapun tujuan yang ingin dicapai dalam penelitian ini adalah sebagai berikut:

a. Mengenali pola serangan *malware* dan mendeteksi serangan *malware ransomware* dengan membandingkan hasil *alert snort* dengan dataset yang sudah diekstraksi.
b. Membedakan data normal dengan data serangan pada data *bitcoin miner*.
c. Mengklasifikasi serangan *ransomware* pada *bitcoin miner* dengan metode K-means.
d. Menghitung akurasi deteksi serangan *malware ransomware* pada *bitcoin miner* dengan algoritma *K-means clustering*.

## 1.3 Manfaat

Adapun tujuan yang ingin dicapai dalam penelitian ini adalah sebagai berikut:

a. Dapat mengetahui pola serangan pada data *bitcoin miner.*
*b.* Dapat membedakan data normal dan data serangan pada data *bitcoin miner*
*c.* Dapat mendeteksi serangan *malware ransomware* pada data *bitcoin miner.*
d. Dapat Menghitung akurasi deteksi serangan *malware ransomware* pada *bitcoin miner* dengan algoritma *K-means clustering*.

## 1.4 Rumusan Masalah

Berdasarkan latar belakang diatas, maka rumusan masalah yang akan dibahas pada penelitian ini adalah:

a. Bagaimana mengekstrak dataset pcap ke csv ?
b. Bagaimana mengenali pola serangan *malware ransomware* pada *bitcoin miner* ?

c. Bagaimana mendeteksi serangan *malware ransomware* pada *bitcoin miner* ?

d. Bagaimana *K-means clustering* mengenali serangan *malware ransomware* pada data *bitcoin miner* ?

## 1.5 Batasan Masalah

Batasan masalah pada Tugas Akhir ini yaitu sebagai berikut:

a. Menggunakan dataset *bitcoin miner*.csv
b. Mengenali pola serangan *malware ransomware* menggunakan perbandingan antara alert dan dataset yang sudah ekstraksi.
c. Mengklasifikasi serangan *malware ransomware* menggunakan algoritma *k-means clustering*.
d. Serangan yang dideteksi hanya serangan *malware ransomware*.

## 1.6 Metodologi Penelitian

Metodologi yang digunakan dalam penulisan Tugas akhir ini akan melalui beberapa tahapan sebagai berikut :

1. Studi Pustaka/Literatur

   Tahap ini dilakukan setelah masalah yang didapatkan sudah sesuai untuk dijadikan sebagai penelitian, membaca artikel, jurnal atau makalah yang berhubungan dengan tugas akhir ini.

2. Perancangan sistem

   Dalan tahapan ini mengenai bagaimana membangun dan menerapkan metode pada sistem Tugas Akhir, apa saja yang digunakan pada penelitian seperti software apa saja yang digunakan, terakhir bagaimana proses konfigurasi dan penerapan metode pada Tugas akhir.

3. Pengujian

   Pada tahap ini, merupakan tahapan pengujian berdasarkan metodologi penelitian dan penelitian sebelumnya sehingga didapatkan data hasil uji yang sesuai dan tepat dengan algoritma.

4. Analisa

Pada tahapan ini, yaitu menganalisa data hasil pengujian dengan diterapkan pendekatan tertentu, sehingga mendapatkan hasil yang sesuai objektif, dimana datanya diperoleh dari hasil pengujian.

5. Kesimpulan dan saran

Pada tahapan ini adalah tahap terakhir yaitu membuat kesimpulan dari permasalahan, studi pustaka, metodologi, dan analisa hasil pengujian. Selain itu beberapa saran yang dapat dijadikan penelitian selanjutnya.

## 1.7 Sistematika Penelitian

Adapun sistematika penulisan dalam Proposal Tugas Akhir ini adalah sebagai berikut:

**BAB I. PENDAHULUAN**

Pada Bab ini merupakan penjelasan mengenai landasan topik penelitian yang meliputi Latar Belakang, Tujuan, Manfaat, Rumusan Masalah, dan Batasan Masalah. Selain itu termasuk juga metodologi penelitian, dan sistematika penulisan.

**BAB II. TINJAUAN PUSTAKA**

Pada Bab ini berisi mengenai dasar teori dari penelitian tugas akhir tentang *bitcoin miner, malware ransomware, K-means clustering* dan yang berhubungan dengan penelitian.

**BAB III. METODOLOGI PENELITIAN**

Pada Bab ini akan membahas analisis pola dan deteksi serangan *malware ransomware* pada *bitcoin miner* dengan Metode *K-means Clustering.*

**BAB IV. PENGUJIAN DAN ANALISA**

Pada Bab ini berisi penjelasan tentang hasil pengujian yang dilakukan serta analisis dari data yang didapat dari hasil pengujian.

**BAB V. KESIMPULAN DAN SARAN**

Pada bab ini berisi kesimpulan tentang hasil pengujian yang telah dilakukan serta analisis dari data yang didapat dari hasil pengujian.

## DAFTAR PUSTAKA


[1] M. Thum, "The economic cost of bitcoin mining," *CESifo Forum*, vol. 19, no. 1, pp. 43–45, 2018.

[2] Y. Kwon, H. Kim, J. Shin, and Y. Kim, "Bitcoin vs. Bitcoin cash: Coexistence or downfall of bitcoin cash?," *Proc. - IEEE Symp. Secur. Priv.*, pp. 935–951, 2019.

[3] J. Burgess, D. Carlin, P. O'Kane, and S. Sezer, "MANiC: Multi-step assessment for crypto-miners," *2019 Int. Conf. Cyber Secur. Prot. Digit. Serv. Cyber Secur. 2019*, pp. 1–8, 2019.

[4] S. Lee, T.T.Phan "Anomaly Detection in the Bitcoin System - A Network Perspective",2017

[5] H. S. Yin and R. Vatrapu, "A First Estimation of the Proportion of Cybercriminal Entities in the Bitcoin Ecosystem using Supervised Machine Learning," pp. 3690–3699, 2017.

[6] D. Y. Huang *et al.*, "Tracking Ransomware End-to-end," *Proc. - IEEE Symp. Secur. Priv.*, no. 2, pp. 618–631, 2018.

[7] E. Kolodenker, W. Koch, G. Stringhini, and M. Egele, "PayBreak : Defense against cryptographic ransomware," *ASIA CCS 2017 - Proc. 2017 ACM Asia Conf. Comput. Commun. Secur.*, pp. 599–611, 2017.

[8] Q. Chen and R. A. Bridges, "Automated behavioral analysis of malware: A case study of wannacry ransomware," *Proc. - 16th IEEE Int. Conf. Mach. Learn. Appl. ICMLA 2017*, pp. 454–460, 2017.

[9] M. Salimitari, M. Chatterjee, M. Yuksel, and E. Pasiliao, "Profit Maximization for Bitcoin Pool Mining: A Prospect Theoretic Approach," *Proc. - 2017 IEEE 3rd Int. Conf. Collab. Internet Comput. CIC 2017*, pp. 267–274, 2017.

[10] A. Sari and S. Kilic, "Exploiting Cryptocurrency Miners with OISNT Techniques," *Trans. Networks Commun.*, vol. 5, no. 6, 2017.

[11] A. Z. Ausop and E. S. N. Aulia, “Teknologi Cryptocurrency Bitcoin Untuk Investasi Dan Transaksi Bisnis Menurut Syariat Islam,” *J. Sosioteknologi*, vol. 17, no. 1, pp. 74–92, 2018.

[12] R. Qin, Y. Yuan, S. Wang, and F. Y. Wang, “Economic Issues in Bitcoin Mining and Blockchain Research,” *IEEE Intell. Veh. Symp. Proc.*, no. 9, pp. 268–273, 2018.

[13] R. Recabarren and B. Carbunar, “Hardening Stratum, the Bitcoin Pool Mining Protocol,” *Proc. Priv. Enhancing Technol.*, no. 3, pp. 57–74, 2017.

[14] D. Maiorca, A. Demontis, B. Biggio, F. Roli, and G. Giacinto, “Adversarial Detection of Flash Malware: Limitations and Open Issues,” *Comput. Secur.*, vol. 96, p. 101901, 2020.

[15] M. Nakerekanti and V. B. Narasimha, “Analysis on Malware Issues in Online Social Networking Sites (SNS),” *2019 5th Int. Conf. Adv. Comput. Commun. Syst. ICACCS 2019*, pp. 335–338, 2019.

[16] L. A. Garcia, F. Brasser, M. H. Cintuglu, A.-R. Sadeghi, O. Mohammed, and S. A. Zonouz, “Hey, My Malware Knows Physics! Attacking PLCs with Physical Model Aware Rootkit”, 2017.

[17] L. Zhou and Y. Makris, “Hardware-Assisted Rootkit Detection via On-line Statistical Fingerprinting of Process Execution,” pp. 1580–1585, 2018.

[18] E. E. Schultz and D. Ph, “Where have the worms and viruses gone ?— new trends in malware Bots and Botnets : changes,” no.2, 2006.

[19] J. Gao, L. Li, P. Kong, T. F. Bissyande, and J. Klein, “Should You Consider Adware as Malware in Your Study?,” *SANER 2019 - Proc. 2019 IEEE 26th Int. Conf. Softw. Anal. Evol. Reengineering*, pp. 604–608, 2019.

[20] D. Javaheri, M. Hosseinzadeh, and A. M. Rahmani, “Detection and elimination of spyware and ransomware by intercepting kernel-level system routines,” *IEEE Access*, vol. 6, no. 3, pp. 78321–78332, 2018.

[21] M. Alazab, S. Venkatraman, P. Watters, M. Alazab, and A. Alazab,

"Cybercrime: The case of obfuscated malware," *Lect. Notes Inst. Comput. Sci. Soc. Telecommun. Eng.*, vol. 99, pp. 204–211, 2012.

[22] C. Moore, "Detecting ransomware with honeypot techniques," *Proc. - 2016 Cybersecurity Cyberforensics Conf. CCC 2016*, pp. 77–81, 2016.

[23] I. Nadir and T. Bakhshi, "Contemporary cybercrime: A taxonomy of ransomware threats & mitigation techniques," *2018 Int. Conf. Comput. Math. Eng. Technol. Inven. Innov. Integr. Socioecon. Dev. iCoMET 2018 - Proc.*, pp. 1–7, 2018.

[24] N. Hampton and Z. A. Baig, "Ransomware: Emergence of the cyber-extortion menace," *Proc. the13th Aust. Inf. Secur. Manag.*, pp. 47–56, 2015.

[25] K. P. Subedi, D. R. Budhathoki, and D. Dasgupta, "Forensic analysis of ransomware families using static and dynamic analysis," *Proc. - 2018 IEEE Symp. Secur. Priv. Work. SPW 2018*, pp. 180–185, 2018.

[26] A. Mitra, W. Najjar, and L. Bhuyan, "Compiling PCRE to FPGA for Accelerating SNORT IDS Categories and Subject Descriptors," pp. 127–135, 2007.

[27] H. Alnabulsi, "Detecting SQL Injection Attacks Using SNORT IDS.",2016

[28] S. Chakrabarti, "Study of Snort-Based IDS," , pp. 43–47, 2010.

[29] Almaspens, (2016.Apr.03). "Snort | Materi Kuliah,"[Online] Retrieved From Https://almaspens.wordpress.com /2016/04/03/snort.2016 pp.99, 2016.

[30] T. Informatika, F. I. Komputer, and U. B. Darma, "Analisis Aktivitas dan Pola Jaringan Terhadap Eternal Blue & Wannacry Ransomware," vol. 4, pp. 37–49, 2018.

[31] G. Varoquaux, L. Buitinck, G. Louppe, O. Grisel, F. Pedregosa, and A. Mueller, "Scikit-learn," *GetMobile Mob. Comput. Commun.*, vol. 19, no. 1, pp. 29–33, 2015.

[32] C. E. Rasmussen, “Gaussian Processes in machine learning,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 3176, pp. 63–71, 2004.

[33] J. Ma, “Supervised and semi-supervised twin parametric-margin regularized extreme learning machine,” *Pattern Anal. Appl.*, no.9, 2020.

[34] V. Ferrari, C. Sminchisescu, M. Hebert, and Y. Weiss, *Preface*, vol. 11218 LNCS. Springer International Publishing, 2018.

[35] Z. Wang, L. Qu, and J. Xin, “Regular Research Paper A unified distributed ELM framework with supervised , semi-supervised and unsupervised big data learning,” *Memetic Comput.*, 2018.

[36] J. Bagherzadeh and H. Asil, “A review of various semi-supervised learning models with a deep learning and memory approach,” *Iran J. Comput. Sci.*, vol. 2, no. 2, pp. 65–80, 2019.

[37] S. Learning, Q. Li, Z. Han, and X. Wu, “Deeper Insights into Graph Convolutional Networks.”,2017

[38] S. Learning, T. Miyato, S. Maeda, M. Koyama, and S. Ishii, “Virtual Adversarial Training : A Regularization Method for Supervised and,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 22, no. 3, pp. 1, 2018.

[39] “Garcia, Sebastian.(2018. Feb.21). Malware Capture Facility Project [Online]. Retrieved from https://stratosphereips.org,” p. 2018, 2018.

[40] Leyebiz, “Cara Kerja Bitcoin [Online],” Retrieved From Https://Steemit.com/crypto/@leebiz/miner-s-mining-and-trader-s-trading-altcoins-basic-1. 2018 p. 2018, 2018.

[41] M. E. Celebi, H. A. Kingravi, and P. A. Vela, “A comparative study of efficient initialization methods for the k-means clustering algorithm,” *Expert Syst. Appl.*, vol. 40, no. 1, pp. 200–210, 2013.

[42] G. K. Armah, G. Luo, and K. Qin, “A Deep Analysis of the Precision Formula for Imbalanced Class Distribution,” *Int. J. Mach. Learn. Comput.*,

vol. 4, no. 5, pp. 417–422, 2014.

[43] H. G. Lewis and M. Brown, “A generalized confusion matrix for assessing area estimates from remotely sensed data,” *Int. J. Remote Sens.*, vol. 22, no. 16, pp. 3223–3235, 2001.

[44] V. M. Patro and M. Ranjan Patra, “Augmenting Weighted Average with Confusion Matrix to Enhance Classification Accuracy,” *Trans. Mach. Learn. Artif. Intell.*, vol. 2, no. 4, 2014.