UIN IMAM BONJOL PADANG
MAP Journal
Mathematics & Applications
Web : ejournal.uinib.ac.id/jurnal/index.php/MAp
Email : map_journal@uinib.ac.id

# PEMODELAN MATEMATIKA PENYEBARAN VIRUS KOMPUTER MELALUI *FLASH DRIVE* DENGAN PERLINDUNGAN ANTIVIRUS

## *MATHEMATICAL MODELLING OF COMPUTER VIRUS SPREAD THROUGH FLASH DRIVE WITH ANTIVIRUS PROTECTION*

**La Ode Sabran[1§], Athisa Ratu Laura[2], Lathifah Annur[3]**

[1]Jurusan Matematika, Universitas Islam Negeri Imam Bonjol Padang, Indonesia [laodesabran@uinib.ac.id]
[2]Jurusan Matematika, Universitas Islam Negeri Imam Bonjol Padang, Indonesia [ratulauraathisa@gmail.com]
[3]Jurusan Matematika, Universitas Islam Negeri Imam Bonjol Padang, Indonesia [lathifahannur2003@gmail.com]
[§]*Corresponding Author*

Received 5th May 2024; Accepted 19th Jun 2024; Published 30th Jun 2024;

**Abstrak**

Peneltian ini membahas tentang model matematika penyebaran virus komputer. Media penyebaran virus yang ditinjau dalam penelitian ini adalah *flash drive*. Tujuan penelitian adalah menemukan model penyebaran virus dengan melibatkan antivirus untuk melindungi komputer. Model dikembangkan dengan membagi komputer ke dalam empat kompartemen yaitu kompartemen komputer rentan, komputer terinfeksi virus, komputer dengan antivirus, dan komputer tidak aktif. Sedangkan, *flash drive* dikelompokkan ke dalam dua kompartemen yaitu *flash drive* rentan dan terinfeksi. Analisis model menghasilkan dua titik ekuilibrium yaitu titik ekuilibrium bebas virus dan endemik virus. Kestabilan titik ekuilibrium bergantung pada bilangan reproduksi dasar ($R_0$). Hasil penelitian menunjukkan bahwa peningkatan laju penggunaan antivirus akan menurunkan nilai $R_0$. Hasil simulasi numerik memperlihatkan bahwa semakin besar nilai $R_0$ maka semakin banyak pula komputer yang terinfeksi virus. Namun sebaliknya, semakin kecil nilai $R_0$ maka semakin sedikit pula komputer yang terinfeksi virus. Nilai $R_0 < 1$ menandakan seluruh komputer bebas dari virus.

**Kata Kunci**: *Virus Komputer, Model Matematika, Flash Drive, Antivirus.*

***Abstract***

*This research discusses the mathematical model of the spread of computer viruses. The virus spreading media reviewed in this study is a flash drive. The aim of this study is to find a virus spread model that involves antivirus to protect computers. The model was developed by dividing computers into four compartments: susceptible computers, infected computers, computers with antivirus, and inactive computers. Meanwhile, flash drives are categorized into two compartments namely susceptible and infected flash drives. Analysis of the model resulted in two equilibrium points, namely virus-free and virus-endemic equilibrium points. The stability of the equilibrium points depends on the basic reproduction number* ($R_0$). *The results show that increasing the rate of antivirus usage will decrease the value of* $R_0$. *Numerical simulation results show that the larger the value of* $R_0$, *the more computers are infected with the virus. On the other hand, the smaller the* $R_0$ *value, the fewer computers are infected with the virus. The value of* $R_0 < 1$ *indicates that all computers are free from viruses.*

***Keywords****: Computer Virus, Mathematical Models, Flash Drive, Antivirus*

## 1. Pendahuluan

Teknologi Informasi dan Komputer (TIK) terus berkembang dengan pesat. Hampir seluruh aspek kehidupan manusia terkait dengan peralatan teknologi terutama komputer. Komputer sangat membantu manusia dalam bekerja, seperti untuk melakukan pekerjaan administrasi, terhubung dengan dunia luar melalui internet, melakukan perhitungan dan analisis dengan kapasitas jumlah data yang besar, melakukan kegiatan pemrograman dan simulasi, mendesain teknologi dan penemuan baru, dan lain sebagainya. Kemampuan canggih dari komputer sangat ditunjang oleh penemuan *software-software* atau aplikasi baru yang dapat dipasang pada komputer dan digunakan untuk bekerja.

Pada perkembangannya aplikasi yang dapat dipasang atau terpasang otomatis pada komputer bukan hanya aplikasi yang bermanfaat untuk kebutuhan pekerjaan. Namun, aplikasi yang justru merusak perangkat lunak komputer juga terus berkembang dan telah menyerang serta merusak ribuan bahkan jutaan komputer di dunia. Aplikasi ini dikenal dengan sebutan virus.

Virus merupakan *malware* atau program jahat yang memiliki fungsi untuk merusak sistem operasi, memperlambat kerja sistem operasi, menghapus data dan aplikasi penting milik pengguna, mengintip aktivitas pengguna komputer di internet, hingga merekam user dan *password* akun-akun internet milik pengguna [1].

Beberapa jenis virus komputer yang sangat berbahaya dan pernah menggegerkan Indonesia diantaranya adalah ***Ransomware Wanna Cry*** yang menyerang komputer dengan memblokir file dan meminta tebusan biaya bila pengguna ingin mengakses file tersebut, ***Gadis Mabuk*** yang menjadi spam pada facebook, ***Stuxnet*** yang merusak atau membuat *flash drive* dan *hard drive* komputer menjadi penuh, ***Win32*** yaitu *malware* yang dapat memperbanyak diri dan membuat penuh *hard drive* komputer, dan Virus ***Brontok*** yang membuat *windows* selalu *restart*.

Berdasarkan fakta yang terjadi, penyebaran virus dari satu komputer ke komputer lainnya terjadi melalui dua jalan yaitu jaringan internet dan media penyimpanan berbasis USB seperti *flash drive* dan *hard drive eksternal*. Bila suatu komputer yang terhubung ke jaringan internet mengakses atau mengunduh *link/URL* yang mengandung virus maka virus tersebut menginfeksi komputer tersebut. Sedangkan, penyebaran melalui *USB flash drive* terjadi saat *flash* yang mengandung virus terhubung ke *port USB* komputer. Akibatnya komputer tersebut terinfeksi virus. Demikian pula sebaliknya, suatu *flash derive* akan terinfeksi virus apabila terhubung ke komputer yang mengandung virus.

Proses transmisi virus pada komputer dan *flash derive* dapat dipandang sebagai model *host-vector* epidemi penyakit. Komputer merupakan *host* dan *flash derive* sebagai media perantara penyebaran virus atau *vector*. Model *host-vector* yang telah dikenal diantaranya adalah model epidemi SIR-SI. Model ini diantaranya digunakan untuk

menganalisis penyebaran penyakit demam berdarah *dengue* (DBD) seperti yang dilakukan oleh Esteva dan Vargas [2]. Demikian pula, Sabran [3] menggunakan model epidemi *host-vector* untuk menganalisis model penyebaran Covid-19 dengan manusia sebagai *host* dan gagang pintu sebagai *vector*.

Matematikawan yang telah melakukan penelitian dengan mengaplikasikan model epidemi penyakit untuk penyebaran virus komputer diantaranya adalah Coronel [4], Cohen [5] dan Muray [6]. Kelompok komputer dibedakan menjadi beberapa kompartemen seperti komputer rentan (S), terinfeksi virus (I), dan recovered (R). Selanjutnya, Upadhyay dan Singh [7] melakukan pemodelan penyebaran virus komputer dengan membagi komputer kedalam kelompok target infeksi dan kelompok komputer penginfeksi.

Penelitian ini mengembangkan model matematika penyebaran virus komputer dengan *flash drive* yang bertindak sebagai vektor atau perantara penyebaran virus. Melalui penelitian ini, perilaku penyebaran virus komputer dan tingkat penularannya dapat diketahui. Penggunaan antivirus menjadi subjek penting yang diamati. Hal ini dilakukan untuk mengetahui evektifitas penggunaan antivirus dalam mencegah infeksi virus komputer. Model yang dihasilkan diharapkan dapat digunakan dalam upaya preventif dan pengendalian berbagai jenis virus yang menyerang komputer, sehingga tindakan pengrusakan dan pencurian data serta akun-akun internet dan password dapat dihindari.

Model *host-vector* untuk penyebaran virus komputer secara langsung digambarkan oleh Al-Tuwairqi dan Bahashwan [1]. Mereka berdua menjadikan komputer sebagai *host* dan membaginya ke dalam tiga kelompok yaitu kelompok komputer yang dilengkapi antivirus dengan tingkat perlindungan lemah (*W*), komputer rentan tanpa perlindungan (*S*), dan komputer terinfeksi virus (*I*). Sedangkan, kelompok yang menjadi *vector* atau perantara penularan virus adalah USB *derive* seperti *flash drive* dan *hard drive*. USB *derive* dibagi kedalam dua kompartemen yaitu kelompok USB *derive* rentan $(R_s)$ dan USB *derive* terinfeksi $(R_i)$.

Pengembangan model penyebaran virus komputer yang dilakukan dalam penelitian ini adalah membagi komputer ke dalam empat kompartemen. Kompartemen yang ditambahkan adalah kompartemen $T_k$ untuk kelompok komputer yang tidak dapat dioperasikan karena tingkat serangan virus sudah cukup parah. Komputer yang dilengkapi anti virus diasumsikan kebal terhadap virus sampai masa aktif anti virusnya habis. Kompartemen *vektor* yaitu *flash drive* hanya dibagi kedalam dua kompartemen yaitu *flash drive* rentan $S_f$ dan terinfeksi $I_f$.

Berdasarkan arah pengembangan penelitian yang dilakukan maka permasalahan yang dibahas dalam artikel ini adalah:

1. Bagaimanakah model *host-vector* penyebaran virus komputer dengan perlindungan antivirus?
2. Bagaimana analisis titik kestabilan dan nilai *basic reproduction number* $(R_o)$ penyebaran virus komputer dengan antivirus?
3. Bagaimana hasil dari simulasi numerik model penyebaran virus komputer?

Adapun tujuan dari penelitian ini adalah:

1. Menemukan model matematika *host-vector* penyebaran virus komputer.
2. Melakukan analisis kestabilan titik kritis dan menemukan $R_o$.
3. Melakukan simulasi numerik untuk solusi model *host-vector* penyebaran virus komputer dengan perlindungan antivirus.

## 2. Landasan Teori

### 2.1. Persamaan Diferensial Linear dan Tak Linear

Persamaan diferensial adalah suatu pernyataan matematika berupa kalimat terbuka yang dihubungkan oleh tanda sama dengan dan memuat suatu fungsi yang belum diketahui beserta turunan-turunannya. Boyce dan DiPrima [8] menjelaskan bahwa persamaan diferensial dengan fungsi yang belum diketahui bergantung pada satu variable bebas disebut persamaan diferensial biasa dan persamaan diferensial dengan fungsi yang belum diketahui bergantung pada dua variable atau lebih serta mengandung turunan secara parsial disebut sebagai persamaan diferensial parsial.

Orde persamaan diferensial dilihat dari turunan tertinggi dari persamaan diferensial yang diberikan. Persamaan diferensial biasa orde *n* dengan variable independen *t* dan variabel dependen *y* dikatakan linear, jika berbentuk:

$$p_0(t)\frac{d^n y}{dt^n} + p_1(t)\frac{d^{n-1}y}{dt^{n-1}} + \cdots + p_{n-1}(t)\frac{dy}{dt} + p_n(t)y = G(t) \quad (1)$$

Apabila $G(t) = 0$ maka disebut sebagai persamaan diferensial biasa linear homogen. Sebaliknya, jika $G(t) \neq 0$ maka disebut persamaan diferensial biasa linear tak homogen. Persamaan diferensial biasa tak linear adalah persamaan diferensial biasa seperti bentuk (1), namun variabel tak bebasnya mengalami pemangkatan atau perkalian dengan turunan-turunannya atau perkalian antar sesama turunannya [8].

### 2.2. Sistem Persamaan Diferensial Linear dan Tak Linear

Sistem persamaan diferensial adalah suatu sistem yang komponen-komponennya terdiri lebih dari satu persamaan diferensial yang saling berkaitan satu dengan lainnya. Boyce dan DiPrima [8] menjelaskan bentuk umum sistem persamaan diferensial biasa linear orde pertama yaitu:

$$\begin{aligned} x_1' &= p_{11}(t)x_1 + \cdots + p_{1n}(t)x_n + g_1(t) \\ &\vdots \\ x_n' &= p_{n1}(t)x_1 + \cdots + p_{nn}(t)x_n + g_n(t) \end{aligned} \quad (2)$$

yang setara dengan sistem persamaan linear dengan *n* variabel. Jika $g(t) = 0$, maka sistem yang terbentuk disebut sebagai sistem persamaan diferensial linear homogen. Namun, sistem dengan $g(t) \neq 0$ maka disebut sistem tak homogen.

Sistem persamaan diferensial dikatakan linear apabila persamaan diferensial yang menjadi komponen penyusunnya merupakan persamaan diferensial linear. Sebaliknya, jika ada komponen penyusun sistem yang tak linear maka disebut sistem persamaan diferensial tak linear [8].

### 2.3. Kestabilan Sistem Persamaan Diferensial Linear Homogen

Sistem (2) dengan $g(t) = 0$ dapat dituliskan ke dalam bentuk:

$$\frac{dx}{dt} = Ax \quad (3)$$

dengan $A = \begin{pmatrix} p_{11} & \cdots & p_{1n} \\ \vdots & \ddots & \vdots \\ p_{n1} & \cdots & pnn \end{pmatrix}$ dan $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$

Titik kesetimbangan/equilibrium sistem (3) adalah $\tilde{x}$ dan tunggal (hanya satu-satunya titik kritis) jika *det (A)* $\neq 0$. Titik *x* dikatakan sebagai titik kesetimbangan jika memenuhi $A\tilde{x} = 0$ [9]. Sistem (3) juga dikenal dengan sebutan sistem autonomous.

Kestabilan lokal dari sistem (3) dapat diketahui dari nilai eigen yang diperoleh dari matriks *A*. Ada tiga jenis kestabilan dari bentuk $(A - \lambda I) = 0$ [10] yaitu:

(i) Titik kesetimbangan $\tilde{x}$ stabil asimtotik jika dan hanya jika bagian real dari nilai $\lambda_i < 0$ untuk setiap $i = 1, 2, \ldots, k$ dengan $k \leq n$.

(ii) Titik kesetimbangan $\tilde{x}$ stabil jika dan hanya jika bagian real dari nilai $\lambda_i < 0$ untuk setiap $i = 1, 2, \ldots, k$ dengan $k \leq n$ dan jika ada nilai eigen $\lambda_i$ yang terletak di sumbu imajiner maka multiplisitas aljabar harus sama dengan multiplisitas geometri untuk nilai eigen tersebut.

(iii) Titik kesetimbangan $\tilde{x}$ disebut tidak stabil jika dan hanya jika ada bagian real dari $\lambda_i > 0$ untuk $i = 1, 2, \ldots, k$ dengan $k \leq n$.

## 2.4. Kestabilan Sistem Persamaan Diferensial Tak Linear Homogen

Kestabilan sistem persamaan diferensial tak linear dapat diketahui dengan terlebih dahulu melakukan linearisasi terhadap sistem yang diberikan. Misalkan $x' = f(x)$ dengan $f(x) = (f_1(x), \ldots, f_n(x))$ dan $f(x)$ diferensiabel. Matriks

$$Jf(\tilde{x}) = \begin{bmatrix} \frac{\partial f_1(\tilde{x})}{\partial x_1} & \cdots & \frac{\partial f_1(\tilde{x})}{\partial x_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_n(\tilde{x})}{\partial x_1} & \cdots & \frac{\partial f_n(\tilde{x})}{\partial x_n} \end{bmatrix} \quad (4)$$

dinamakan matriks jacobian dari *f* di titik $\tilde{x}$. Sistem $x' = Jf(\tilde{x})(x - \tilde{x})$ merupakan linearisasi dari sistem tak linear $x' = f(x)$ di sekitar titik $\tilde{x}$ [9]. Berdasarkan teorema yang telah di jelaskan dalam Wiggins [10] bahwa jika diberikan matriks jacobian (4) yaitu $Jf(\tilde{x})$ dari suatu sistem persamaan diferensial yang tak linear $x' = f(x)$ dengan nilai eigen $\lambda$ sebagai hasil penjabaran dari polynomial karakteristik $|Jf(\tilde{x}) - \lambda I| = 0$, maka diperoleh dua keadaan yaitu:

(i) Stabil asimtotik lokal, jika semua bagian real nilai eigen ($\lambda$) dari matriks jacobian hasil linearisasi (matriks $Jf(\tilde{x})$) bernilai negatif.

(ii) Tidak stabil, jika terdapat paling sedikit satu nilai eigen ($\lambda$) dari matriks jacobian $Jf(\tilde{x})$ yang bagian realnya bernilai positif.

## 2.5. Next Generation Matrix (*NGM*) dan Bilangan Reproduksi Dasar ($R_0$)

Penyebaran virus komputer dapat dipandang sebagai penyebaran penyakit dalam model epidemiologi. Suatu parameter yang menggambarkan hilang atau tidaknya virus dalam himpunan/kumpulan komputer dapat disamakan dengan parameter yang disebut $R_0$ pada masalah epidemiologi. Bilangan reproduksi dasar ($R_0$) merupakan ekspektasi banyaknya kasus sekunder yang diakibatkan oleh satu kasus primer pada suatu populasi "*virgin*" selama periode infeksi [11]. Populasi "*virgin*" merupakan populasi yang di dalamnya tidak ada kasus infeksi.

Nilai ambang batas $R_0$ adalah 1. Jika $R_0 < 1$ maka rata-rata individu yang terinfeksi menghasilkan kurang dari satu individu baru yang terinfeksi selama masa penularan sehingga infeksi penyakit hilang dari populasi. Sedangkan, jika $R_0 > 1$ maka setiap individu yang terinfeksi rata-rata menghasilkan lebih dari satu infeksi baru, dan jumlah infeksi meningkat dalam populasi [12].

Salah satu cara untuk memperoleh bilangan reproduksi dasar ($R_0$) adalah melalui matriks *NGM* (*Next Generation Matriks*). Dalam hal ini $R_0$ merupakan nilai radius spektral atau nilai eigen terbesar dari matriks *NGM* tersebut. Cara memperoleh matriks *NGM* dari sistem tak linear adalah dengan melinearisasikan/membentuk matriks Jacobi dari komponen sistem yang merupakan populasi terpapar (*exposed*) dan terinfeksi (*infected*).

Misalkan persamaan kompartemen terpapar dan terinfeksi sebagai hasil linearisasi dari sistem persamaan diferensialnya di sekitar titik kesetimbangan bebas penyakit dinyatakan ke dalam bentuk:

$$x' = (F - V)x$$

dengan *F* adalah hasil linearisasi dari vektor yang menyatakan infeksi baru dan *V* adalah hasil linearisasi dari vektor yang menyatakan perpindahan individu antar kompartemen. Matriks *NGM* didefinisikan sebagai

$$NGM = FV^{-1}.$$

Selanjutnya, $R_0$ merupakan radius spektral dari matriks NGM [11] yang dinyatakan dengan

$$R_0 = \rho(FV^{-1}).$$

## 2.6. Virus Komputer dan Penyebarannya

Manusia dapat bekerja dengan komputer melalui *software* yang diintegrasikan dalam komputer. *Software* ini berjalan di atas sistem operasi pada komputer dan sangat berguna untuk membantu manusia dalam bekerja. Tidak semua *software* yang diciptakan bertujuan untuk memudahkan kerja pengguna komputer. Ada pula software yang dibuat untuk melakukan perusakan pada sistem operasi, merusak *software* lain yang berguna, atau untuk tindakan kejahatan. *Software* ini dikenal dengan sebutan *Malicous Software* atau *Malware* [13]. *Malware* merupakan perangkat lunak yang dirancang untuk tujuan merusak *software* lain. Contoh *malware* adalah *Trojan, Virus,* dan *Spyware* [14].

Yusianto dalam Pemungkas [15] menjelaskan bahwa virus komputer adalah suatu program yang mampu menjangkiti atau membuat salinan dari dirinya sendiri sehingga dapat menyebar dari satu komputer ke komputer lainnya tanpa diketahui oleh pengguna komputer. Proses penyebaran tersebut terjadi dengan cara virus mengubah program lain sehingga menjadi bagian dari virus tersebut. Akibatnya, setiap kali program tersebut dijalankan maka virus akan aktif menyerang komputer dan menginfeksi program lain lagi.

Penyebaran virus komputer serupa dengan penyebaran penyakit menular. Virus komputer dapat disebarkan melalui pesan email atau kiriman link yang kemudian diunduh dan mengandung file yang terinfeksi. Selain itu, menghubungkan komputer dengan *flash derive* atau *hard drive* dapat menjadi penyebab tersebarnya virus komputer [1]. Hal ini terjadi karena *hard derive/flash derive* yang mengandung virus akan

menginfeksi komputer yang sebelumnya bebas dari virus. Demikian pula, *hard derive/flash derive* yang terhubung dengan komputer yang mengandung virus akan mengakibatkan *hard derive/flash derive* yang sebelumnya bebas dari virus menjadi terinfeksi. Sehingga, *hard derive/flash derive* menjadi vektor peratara tersebarnya virus atau *malware*.

### 2.7. Antivirus Komputer

Antivirus merupakan suatu *software*/program yang bekerja untuk melindungi komputer dari serangan virus dengan mendeteksi, menghentikan kerja virus, membersihkan atau menghilangkan virus dan program berbahaya lainnya dari komputer [16]. Shadewa dalam Suci [16] menjelaskan ada tiga jenis program yang dapat melindungi komputer, yaitu:

(i) *Fix*, merupakan *software* yang melindungi komputer hanya dari satu jenis virus,

(ii) *Antidot*, merupakan *software* yang dapat melindungi komputer dari beberapa jenis virus dalam jumlah yang terbatas.

(iii) *Antivirus*, merupakan *software* yang dapat melindungi komputer dari serangan berbagai jenis virus dan otomatis langsung aktif ketika komputer dihidupkan.

## 3. Hasil Dan Pembahasan

### 3.1. Desain Model

Pemodelan penyebaran virus komputer dalam artikel ini dilakukan dengan menganggap komputer sebagai *host* yang menerima virus dan *flash derive* sebagai media perantara virus atau *vector*. Komputer dikelompokkan ke dalam 4 kompartemen yaitu kompartemen komputer rentan/*susceptible* ($S_k$) merupakan kelompok komputer yang bebas dari virus namun rentan untuk terinfeksi, kompartemen komputer yang terinfeksi virus/*infected* ($I_k$) merupakan kelompok komputer yang terjangkit virus/*malware* dan masih dapat dioperasikan, kompartemen komputer dengan anti virus ($A_k$) merupakan komputer yang terinstal antivirus dan diasumsikan kebal sampai masa aktiv antivirusnya habis, dan kompartemen komputer tidak aktif ($T_k$) merupakan kelompok komputer yang tidak dapat dioperasikan karena terinfeksi virus dengan parah sehingga harus diinstal/format ulang untuk dapat dioperasikan.

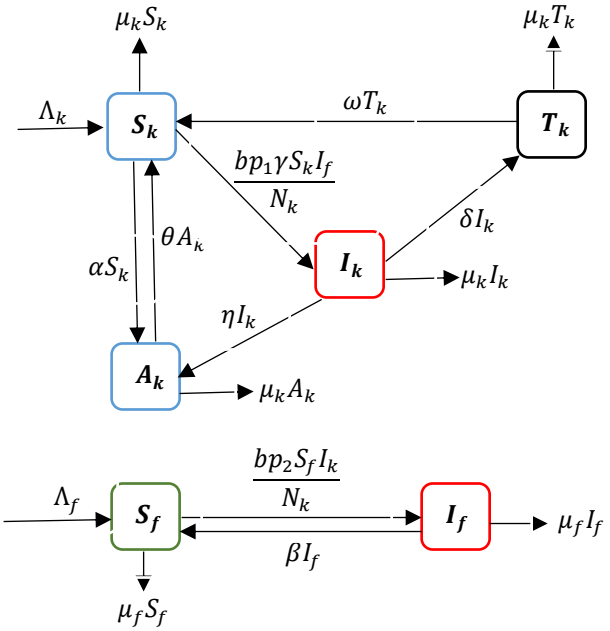
*Flash drive* dibagi ke dalam dua kompartemen yaitu kompartemen *flash drive susceptible*/rentan ($S_f$) merupakan kelompok *flash drive* yang bebas virus namun rentan untuk terinfeksi virus, dan kompartemen *flash drive infected* ($I_f$) merupakan kelompok *flash drive* yang terjangkit/mengandung virus.

Asumsi-asumsi yang digunakan untuk membangun model adalah:

1. Penambahan jumlah komputer dan *flash drive* bersifat konstan sepanjang waktu.
2. Laju kerusakan alami komputer dianggap sama untuk setiap kompartemen.
3. Laju kerusakan alami *flash drive* dianggap sama untuk setiap kompartemen
4. Transmisi virus hanya terjadi diantara komputer dan *flash drive* melalui kontak langsung. Tidak ada transmisi virus melalui jaringan internet.
5. Komputer yang dilengkapi anti virus diasumsikan kebal terhadap serangan virus

sampai masa aktif anti virusnya habis.

Penyebaran virus pada setiap kelompok komputer dan *flash drive* digambarkan dalam diagram transmisi berikut.




**Gambar 1.** Diagram transmisi virus komputer

Berdasarkan diagram transmisi seperti pada **Gambar 1** dan asumsi yang telah dijelaskan di atas, maka model matematika untuk penyebaran virus komputer melalui *flash drive* adala sebagai berikut:

$$\begin{aligned}
\frac{dS_k(t)}{dt} &= \Lambda_k - \frac{bp_1\gamma S_k(t)I_f(t)}{N_k} - \alpha S_k(t) + \theta A_k(t) + \\
&\quad \omega T_k(t) - \mu_k S_k(t) \\
\frac{dI_k(t)}{dt} &= \frac{bp_1\gamma S_k(t)I_f(t)}{N_k} - \delta I_k(t) - \eta I_k(t) - \mu_k I_k(t) \\
\frac{dA_k(t)}{dt} &= \alpha S_k(t) + \eta I_k(t) - \theta A_k(t) - \mu_k A_k(t) \qquad (5) \\
\frac{dT_k(t)}{dt} &= \delta I_k(t) - \omega T_k(t) - \mu_k T_k(t) \\
\frac{dS_f(t)}{dt} &= \Lambda_f - \frac{bp_2 S_f(t)I_k(t)}{N_k} + \beta I_f(t) - \mu_f S_f(t) \\
\frac{dI_f(t)}{dt} &= \frac{bp_2 S_f(t)I_k(t)}{N_k} - \beta I_f(t) - \mu_f I_f(t)
\end{aligned}$$

dengan jumlah komputer dan *flash drive* adalah konstan sepanjang waktu yaitu $N_k = S_k(t) + I_k(t) + A_k(t) + T_k(t)$ dan $N_f = S_f(t) + I_f(t)$.

Semua parameter dalam model bernilai positif yaitu $\Lambda_k > 0$, $b > 0$, $p_1 > 0$, $p_2 > 0$, $\gamma > 0$, $\alpha > 0$, $\theta > 0$, $\omega > 0$, $\mu_k > 0$, $\delta > 0$, $\eta > 0$, $\Lambda_f > 0$, $\beta > 0$, dan $\mu_f > 0$. Keterangan dari setiap parameter disajikan dalam **Tabel 1** berikut.

**Tabel 1.** Parameter dalam model

| Simbol | Keterangan (Satuan) |
|---|---|
| $\Lambda_k$ | Rata-rata jumlah produksi komputer *susceptible* (komputer/satuan waktu) |
| $\Lambda_f$ | Rata-rata jumlah produksi *flash drive susceptible* (*flash drive*/satuan waktu) |
| $b$ | Rata-rata banyak kali sebuah *flash* terhubung ke komputer (jumlah atau intensitas *flash drive* terhubung dengan komputer/satuan waktu) |
| $p_1$ | Peluang virus pada *flash drive* sukses menginfeksi komputer |
| $p_2$ | Peluang virus pada komputer sukses menginfeksi drive |
| $\gamma$ | Jumlah komputer yang terhubung dengan sebuah *flash drive* (komputer/*flash drive*) |
| $\alpha$ | Laju instalasi anti virus pada komputer *susceptible* (1/satuan waktu) |
| $\theta$ | Laju transisi dari $A_k$ menjadi $S_k$ karena masa aktif anti virus pada komputer telah habis (1/satuan waktu) |
| $\omega$ | Laju transisi komputer tidak aktif ($T_k$) menjadi komputer rentan ($S_k$) karena proses intalasi ulang telah dilakukan (1/satuan waktu) |
| $\delta$ | Laju transisi dari komputer terinfeksi virus menjadi komputer yang tidak aktif/tidak dapat dioperasikan (1/satuan waktu) |
| $\eta$ | Laju transisi komputer terinfeksi virus menjadi komputer $A_k$ (1/satuan waktu) |
| $\beta$ | Laju transisi *flash drive* terinfeksi menjadi *flash drive susceptible* (1/satuan waktu) |
| $\mu_k$ | Laju kerusakan alami komputer (1/satuan waktu) |
| $\mu_f$ | Laju kerusakan alami *flash drive* (1/satuan waktu) |
| $N_k$ | Jumlah total komputer |
| $N_f$ | Jumlah total *flash drive* |

### 3.2. Titik Ekuilibrium Bebas Virus dan Bilangan Reproduksi Dasar ($R_0$)

Model dinamik penyebaran virus komputer melalui *flash drive* yang digambarkan seperti pada

sistem persamaan (5), memiliki dua titik ekuilibrium yaitu titik ekuilibrium bebas virus ($E_0$) dan titik ekuilibrium endemik virus ($E_1$). Titik ekuilibrium $E_0$ diperoleh saat tidak ada komputer dan *flash drive* yang terinfeksi virus atau $I_k(t) = I_f(t) = 0$. Titik ekuilibrium $E_0$ dari Sistem (5) diberikan oleh

$$E_0 = \left\{S_k(t) = \frac{(\theta+\mu_k)\Lambda_k}{(\alpha+\theta+\mu_k)\mu_k}, A_k(t) = \frac{\alpha\Lambda_k}{(\alpha+\theta+\mu_k)\mu_k}, I_k(t) = 0, T_k(t) = 0, S_f(t) = \frac{\Lambda_f}{\mu_f}, I_f(t) = 0\right\}.$$

Selanjutnya, bilangan reproduksi dasar ($R_0$) diperoleh dengan cara membentuk matriks *NGM* yaitu mengambil kompartemen terinfeksi dari Sistem (5), sehingga diperoleh

$$\begin{pmatrix} \frac{dI_k(t)}{dt} \\ \frac{dI_f(t)}{dt} \end{pmatrix} = \begin{pmatrix} \frac{bp_1\gamma S_k(t)I_f(t)}{N_k} \\ \frac{bp_2 S_f(t)I_k(t)}{N_k} \end{pmatrix} - \begin{pmatrix} \delta I_k(t) + \eta I_k(t) + \mu_k I_k(t) \\ \beta I_f(t) + \mu_f I_f(t) \end{pmatrix} = M - N.$$

Linearisasi $M$ dan $N$ di sekitar titik ekuilibrium bebas virus ($E_0$) menghasilkan matriks infeksi baru $F$ dan matriks transisi $V$ yaitu

$$F = \begin{bmatrix} 0 & \frac{bp_1\gamma(\theta+\mu_k)\Lambda_k}{(\alpha+\theta+\mu_k)\mu_k N_k} \\ \frac{bp_2\Lambda_f}{\mu_f N_k} & 0 \end{bmatrix}, \text{ dan}$$

$$V = \begin{bmatrix} \delta+\eta+\mu_k & 0 \\ 0 & \mu_f+\beta \end{bmatrix}.$$

Matriks *NGM* dinyatakan oleh $NGM = FV^{-1}$ dan dituliskan

$$NGM = \begin{bmatrix} 0 & \frac{bp_1\gamma(\theta+\mu_k)\Lambda_k}{(\alpha+\theta+\mu_k)\mu_k N_k(\mu_f+\beta)} \\ \frac{bp_2\Lambda_f}{\mu_f N_k(\delta+\eta+\mu_k)} & 0 \end{bmatrix}$$

dengan polynomial karakteristik dari matriks *NGM* adalah $P(\lambda) = \lambda^2 N_k^2\mu_f\mu_k(\alpha+\theta+\mu_k)(\delta+\eta+\mu_k)(\mu_f+\beta) - \gamma b^2\Lambda_f\Lambda_k p_1 p_2(\theta+\mu_k)$. Nilai eigen terbesar dari polynomial ini merupakan bilangan reproduksi dasar yaitu

$$R_0 = \sqrt{\frac{\gamma b^2\Lambda_f\Lambda_k p_1 p_2(\theta+\mu_k)}{N_k^2\mu_f\mu_k(\alpha+\theta+\mu_k)(\delta+\eta+\mu_k)(\mu_f+\beta)}}. \quad (6)$$

### 3.3. Titik Ekuilibrium Endemik Virus

Titik ekuilibrium endemik virus ($E_1$) dari Sistem (5) akan eksis atau ada ketika nilai $R_0 > 1$ atau $I_k(t) > 0$ dan $I_f(t) > 0$. Titik ekuilibrium endemik virus dinyatakan sebagai $E_1 = \{S_k^*(t),\ I_k^*(t),\ A_k^*(t),\ T_k^*(t),\ S_f^*(t),\ I_f^*(t)\}$, dimana

$S_k^*(t) = \frac{X_1}{X_2}$,

$I_k^*(t) = \frac{(R_0^2-1)(\omega+\mu_k)X_3}{X_2}$,

$A_k^*(t) = \frac{X_4-X_5}{X_2}$,

$T_k^*(t) = \frac{(R_0^2-1)\delta X_3}{X_2}$,

$S_f^*(t) = \frac{X_6}{X_7}$,

$I_f^*(t) = \frac{(R_0^2-1)(\omega+\mu_k)X_3}{X_7}$,

dengan $R_0$ seperti pada Persamaan (6) dan

$X_1 = N_k\mu_f(\delta+\eta+\mu_k)(N_k(\mu_f+\beta)\mu_k^3 + ((\eta+\delta+\omega+\theta)(\mu_f+\beta)N_k + bp_2\Lambda_k)\mu_k^2 + ((\mu_f+\beta)((\eta+\theta)\omega+\delta\eta)N_k + bp_2\Lambda_k(\omega+\theta))\mu_k + b\omega\theta p_2\Lambda_k$ ,

$X_2 = bp_2(N_k\mu_f\mu_k^3 + \mu_f(\eta+\alpha+\delta+\omega+\theta)N_k + bp_1\Lambda_f\gamma)\mu_k^2 + (((\eta+\alpha+\delta+\theta)\omega+(\alpha+\theta)(\eta+\delta))N_k\mu_f + bp_1\Lambda_f\gamma(\eta+\delta+\omega+\theta))\mu_k + \omega\mu_f(\alpha+\theta)(\eta+\delta)N_k + b\Lambda_f\gamma((\eta+\theta)\omega+\delta\theta)p_1)\mu_k$ ,

$X_3 = N_k^2\mu_f\mu_k(\alpha+\theta+\mu_k)(\mu_f+\beta)(\delta+\eta+\mu_k)$ ,

$$X_4 = \mu_k \alpha N_k^2(\mu_k + \delta + \omega)(\delta + \eta + \mu_k)\mu_f^2 + \left(\mu_k \beta(\mu_k + \delta + \omega)N_k + bp_2\Lambda_k(\mu_k + \omega)\right)\alpha N_k(\delta + \eta + \mu_k)\mu_f + b^2 p_2 \Lambda_f \Lambda_k \eta\gamma p_1(\mu_k + \omega),$$

$$X_5 = \eta N_k^2 \mu_f \mu_k(\mu_k + \omega)\left(\mu_f + \beta\right)(\delta + \eta + \mu_k),$$

$$X_6 = N_k \mu_k\left(\mu_f + \beta\right)\left(N_k(\mu_k + \omega)(\alpha + \eta + \mu_k)(\delta + \eta + \mu_k)\mu_f + b\left(\mu_k^2 + (\eta + \delta + \omega + \theta)\mu_k + (\eta + \theta)\omega + \delta\theta\right)\Lambda_f \gamma p_1\right),$$

$$X_7 = \mu_f bp_1\gamma\left(N_k\left(\mu_f + \beta\right)\mu_k^3 + \left(\left(\mu_f + \beta\right)(\eta + \delta + \omega + \theta)N_k + b\Lambda_k p_2\right)\mu_k^2 + \left(\left(\mu_f + \beta\right)\left((\eta + \theta)\omega + \delta\theta\right)N_k + b\Lambda_k p_2(\omega + \theta)\right)\mu_k + b\omega\theta\Lambda_k p_2\right),$$

### 3.4. Kestabilan Titik Ekuilibrium

Kestabilan titik ekuilibrium bebas virus ($E_0$) diketahui melalui linearisasi Sistem (5) di sekitar titik $E_0$. Hasil linearisasi menghasilkan Matriks Jacobi $J(E_0)$ yaitu

$$J(E_0) = \begin{bmatrix} -\alpha - \mu_k & 0 & \theta & \omega & 0 & -\frac{bp_1\gamma\left(\theta + \mu_k\right)\Lambda_k}{\left(\alpha + \theta + \mu_k\right)\mu_k N_k} \\ 0 & -\eta - \delta - \mu_k & 0 & 0 & 0 & \frac{bp_1\gamma\left(\theta + \mu_k\right)\Lambda_k}{\left(\alpha + \theta + \mu_k\right)\mu_k N_k} \\ \alpha & \eta & -\theta - \mu_k & 0 & 0 & 0 \\ 0 & \delta & 0 & -\omega - \mu_k & 0 & 0 \\ 0 & -\frac{bp_2\Lambda_f}{\mu_f N_k} & 0 & 0 & -\mu_f & \beta \\ 0 & \frac{bp_2\Lambda_f}{\mu_f N_k} & 0 & 0 & 0 & -\beta - \mu_f \end{bmatrix}$$

Polinomial karakteristik dari Matrik $J(E_0)$ menghasilkan enam nilai eigen, dengan empat nilai eigen bernilai negatif yaitu $\lambda_1 = -(\mu_k + \omega)$, $\lambda_2 = -\mu_k$, $\lambda_3 = -\mu_f$, dan $\lambda_4 = -(\mu_k + \alpha + \theta)$. Selanjutnya nilai untuk $\lambda_5$ dan $\lambda_6$ ditentukan dari persamaan

$$a\lambda^2 + b\lambda + c = 0 \qquad (7)$$

dengan,

$a = -N_k^2 \mu_f \mu_k(\alpha + \theta + \mu_k)$,

$b = -N_k^2 \mu_f \mu_k(\alpha + \theta + \mu_k)\left(\eta + \beta + \delta + \mu_f + \mu_k\right)$, dan

$c = \gamma b^2 \Lambda_f \Lambda_k p_1 p_2(\theta + \mu_k) - N_k^2 \mu_f \mu_k(\alpha + \theta + \mu_k)(\delta + \eta + \mu_k)\left(\mu_f + \beta\right)$.

Berdasarkan Teorema Vieta, Persamaan (7) akan memiliki akar-akar negative ($\lambda_5 < 0$ dan $\lambda_6 < 0$), jika $c$ bernilai negatif ($c < 0$). Dengan demikian, Titik Ekuilibrium $E_0$ akan stabil asimtotik jika terpenuhi

$\gamma b^2 \Lambda_f \Lambda_k p_1 p_2(\theta + \mu_k) < N_k^2 \mu_f \mu_k(\alpha + \theta + \mu_k)(\delta + \eta + \mu_k)\left(\mu_f + \beta\right)$, atau

$\frac{\gamma b^2 \Lambda_f \Lambda_k p_1 p_2(\theta + \mu_k)}{N_k^2 \mu_f \mu_k(\alpha + \theta + \mu_k)(\delta + \eta + \mu_k)\left(\mu_f + \beta\right)} < 1.$

Dengan kata lain, jika $R_0^2 < 1$ serta $R_0^2 = \frac{\gamma b^2 \Lambda_f \Lambda_k p_1 p_2(\theta + \mu_k)}{N_k^2 \mu_f \mu_k(\alpha + \theta + \mu_k)(\delta + \eta + \mu_k)\left(\mu_f + \beta\right)}$ maka titik ekuilibrium bebas virus stabil asimtotik.

### 3.5. Simulasi Numerik

Simulasi numerik dilakukan untuk mengetahui dinamika perubahan jumlah komputer pada setiap kompartemen. Jumlah awal komputer di setiap kompartemen ditampilkan pada **Tabel 2**.

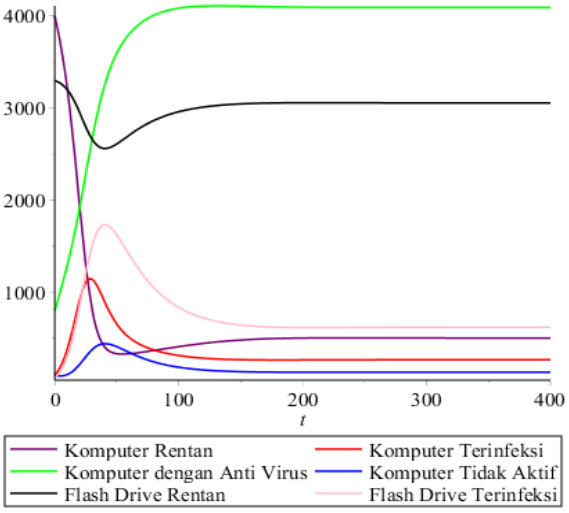
**Tabel 2.** Nilai awal

| $S_k(0)$ | $I_k(0)$ | $A_k(0)$ | $T_k(0)$ | $S_f(0)$ | $I_f(0)$ |
|---|---|---|---|---|---|
| 4000 | 100 | 800 | 100 | 9900 | 100 |

1. Simulasi dengan nilai $R_0 = 1{,}92$ ($R_0 > 1$)

   Nilai-nilai parameter yang digunakan dalam simulasi ini diasumsikan sebagai berikut: $\Lambda_k = \frac{5000}{15\times360}$, $\Lambda_f = \frac{10000}{5\times360}$, $b = \frac{1}{7}$,

$p_1 = \frac{9}{10}$, $p_2 = \frac{7}{10}$, $\gamma = \frac{5}{2}$, $\alpha = \frac{1}{90}$, $\theta = \frac{1}{180}$, $\omega = \frac{1}{15}$, $\delta = \frac{1}{30}$, $\eta = \frac{1}{15}$, $\beta = \frac{1}{17}$, $\mu_k = \frac{1}{15\times360}$, $\mu_f = \frac{1}{5\times360}$, , $N_k = 5000$, dan $N_f = 10000$. Hasil simulasi ditampilkan pada **Gambar 2**.

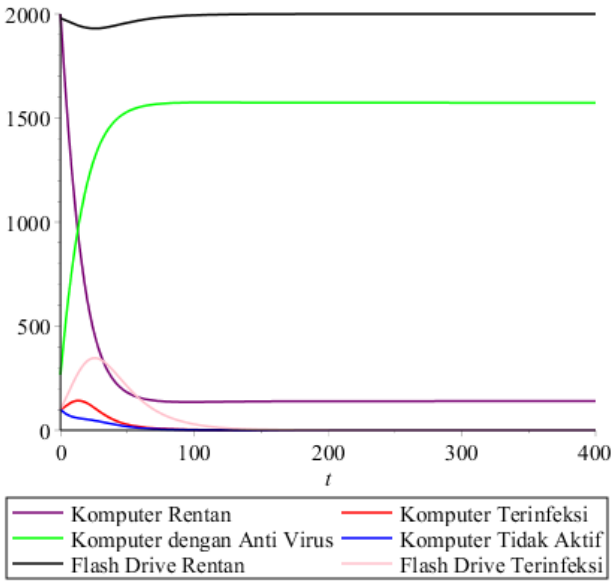



**Gambar 2.** Diagram perubahan jumlah komputer dari setiap kompartemen ($R_0 > 1$)

**Gambar 2** menunjukkan hasil simulasi numerik perubahan jumlah komputer pada setiap kompartemen. Simulasi ini dilakukan pada keadaan $R_0 = 1{,}92$ dengan laju penggunaan antivirus sangat rendah ($\alpha = \frac{1}{90}$ dan $\eta = \frac{1}{15}$). Berdasarkan hasil simulasi, terlihat bahwa komputer dan *flash drive* terinfeksi selalu ada di sepanjang waktu. Pada waktu $t$ > 200, jumlah komputer pada setiap kompartemen stabil. Hal ini berarti bahwa selalu ada komputer yang terinfeksi virus ketika tingkat penggunaan antivirus rendah.

2. Simulasi dengan nilai $R_0 = 0{,}51$ ($R_0 < 1$)

Nilai-nilai parameter yang digunakan dalam simulasi ini diasumsikan sebagai berikut: $\Lambda_k = \frac{5000}{15\times360}$, $\Lambda_f = \frac{10000}{5\times360}$, $b = \frac{1}{7}$, $p_1 = \frac{9}{10}$, $p_2 = \frac{7}{10}$, $\gamma = \frac{5}{2}$, $\alpha = \frac{1}{20}$, $\theta = \frac{1}{360}$, $\omega = \frac{1}{10}$, $\delta = \frac{1}{30}$, $\eta = \frac{1}{5}$, $\beta = \frac{1}{17}$, $\mu_k = \frac{1}{15\times360}$, $\mu_f = \frac{1}{5\times360}$, , $N_k = 5000$, dan $N_f = 10000$. Hasil simulasi ditampilkan pada **Gambar 3**.

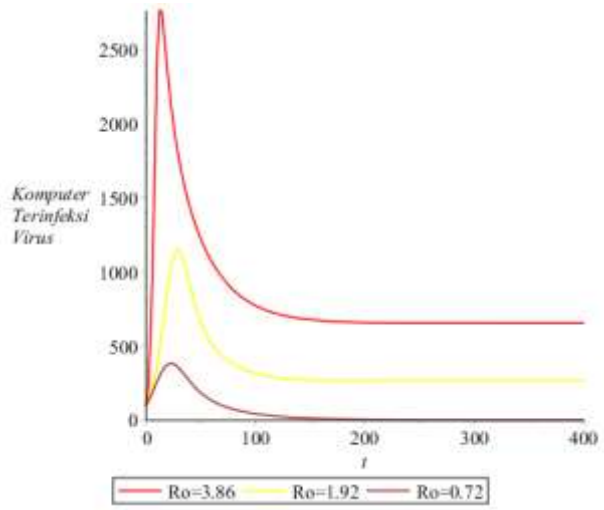



**Gambar 3.** Diagram perubahan jumlah komputer dari setiap kompartemen ($R_0 < 1$)

**Gambar 3** merupakan hasil simulasi numerik perubahan jumlah komputer pada setiap kompartemen dengan $R_0 = 0{,}51$. Pada simulasi ini laju penggunaan antivirus ditingkatkan menjadi $\alpha = \frac{1}{20}$ dan $\eta = \frac{1}{5}$, sehingga seiring berjalannya waktu seluruh komputer dan *flash drive* bebas dari virus. Hal ini sesuai dengan hasil simulasi dimana pada mulanya jumlah komputer dan *flash drive* terinfeksi meningkat lalu berkurang hingga nol dan stabil saat $t$ > 200.

3. Simulasi komputer terinfeksi virus ($I_k(t)$)

Simulasi untuk kompartemen komputer yang terinfeksi virus dilakukan untuk melihat perbandingan jumlah komputer terinfeksi virus pada nilai $R_0$ yang berbeda-beda. Hasil simulasi ditampilkan pada grafik berikut.

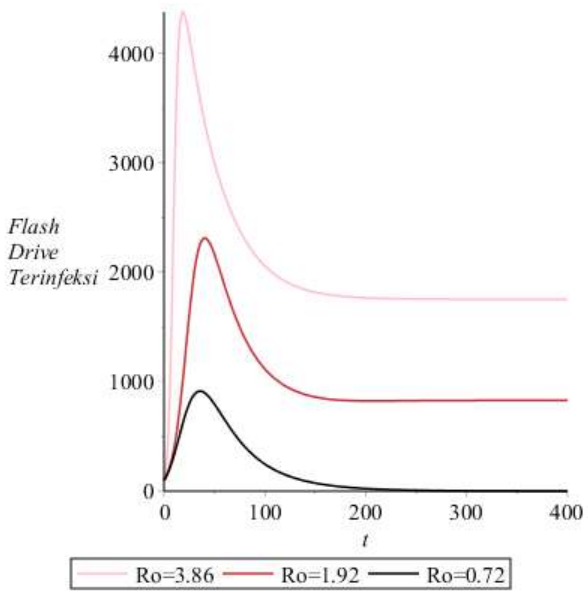



**Gambar 4.** Grafik perbandingan jumlah komputer terinfeksi virus pada nilai $R_0$ berbeda

Berdasarkan grafik yang ditampilkan pada **Gambar 4**, dapat kita ketahui bahwa jumlah komputer terinfeksi virus akan semakin banyak jika nilai $R_0$ semakin besar. Sebaliknya, semakin kecil nilai $R_0$ maka jumlah komputer terinfeksi virus akan semakin keci. Ketika $R_0 < 1$, maka jumlah komputer terinfeksi virus akan menuju nol. Pada grafik dalam **Gambar 4** terlihat bahwa $I_k(t) = 0$ saat $t > 200$, untuk $R_0 < 1$.

4. Simulasi kompartemen *flash drive* terinfeksi virus $(I_f(t))$

Simulasi untuk kompartemen *flash drive* yang terinfeksi virus dilakukan untuk melihat perbandingan jumlah *flash drive* terinfeksi virus pada nilai $R_0$ yang berbeda-beda. Hasil simulasi ditampilkan pada grafik berikut.




**Gambar 5.** Perbandingan jumlah *flash drive* terinfeksi pada nilai $R_0$ berbeda

Berdasarkan grafik yang ditampilkan pada **Gambar 5**, dapat kita ketahui bahwa jumlah *flash drive* terinfeksi virus akan semakin banyak jika nilai $R_0$ semakin besar. Sebaliknya, semakin kecil nilai $R_0$ maka jumlah *flash drive* terinfeksi virus akan semakin keci. Ketika $R_0 < 1$, maka jumlah *flash drive* terinfeksi virus akan menuju nol. Pada grafik dalam **Gambar 5** terlihat bahwa $I_f(t) = 0$ saat $t > 200$ untuk $R_0 < 1$.

## 4. Kesimpulan

Kesimpulan yang diperoleh dari hasil penelitian ini adalah:

1. Model penyebaran virus komputer melalui *flash drive* dengan perlindungan anti virus dalam penelitian ini memiliki dua titik ekuilibrium yaitu titik ekuilibrium bebas virus $(E_0)$ dan titik ekuilibrium endemik virus $(E_1)$.
2. Bilangan reproduksi dasar $(R_0)$ yang menunjukkan hilang atau tidaknya virus dalam populasi komputer dan *flash drive*

memiliki bentuk

$$R_0 = \sqrt{\frac{\gamma b^2 \Lambda_f \Lambda_k p_1 p_2 (\theta+\mu_k)}{N_k^2 \mu_f \mu_k (\alpha+\theta+\mu_k)(\delta+\eta+\mu_k)(\mu_f+\beta)}}.$$

3. Semakin besar nilai $R_0$ maka semakin banyak pula jumlah komputer dan *flash drive* yang terinfeksi virus/malware. Sebaliknya, semakin kecil nilai $R_0$ maka semakin sedikit pula komputer dan *flash drive* yang terinfeksi virus.
4. Virus/malware komputer pada akhirnya akan hilang dari populasi ketika nilai $R_0 < 1$. Kondisi ini dapat dicapai dengan meningkatkan penggunaan antivirus.

## 5. Ucapan Terima Kasih

Ucapan terimakasih tim peneliti sampaikan kepada keluarga, dan kepada seluruh pihak yang telah berpartisipasi dan mendukung pelaksanaan kegiatan penelitian ini.

## Daftar Pustaka

[1] S. M. Al-Tuwairqi and W. Bahashwan, "A dynamic model of viruses with the effect of removable media on a computer network with heterogeneous immunity," *Adv. Differ. Equations*, vol. 2020, no. 260, pp. 1–20, 2020, doi: 10.1186/s13662-020-02710-0.

[2] L. Esteva and C. Vargas, "Analysis of a dengue disease transmission model," *Math. Biosci.*, vol. 150, no. 2, pp. 131–151, 1998, doi: https://doi.org/10.1016/S0025-5564(98)10003-2.

[3] L. O. Sabran, I. D. Rianjaya, L. H. Hasibuan, and L. O. Nashar, "Analysis of Covid-19 Fomite Transmission Model With Disinfectant Spray," *BAREKENG J. Ilmu Mat. dan Terap.*, vol. 16, no. 3, pp. 1021–1030, 2022, doi: 10.30598/barekengvol16iss3pp1021-1030.

[4] A. Coronel, F. Huancas, I. Hess, E. Lozada, and F. Novoa-Muñoz, "Analysis of a SEIR-KS mathematical model for computer virus propagation in a periodic environment," *Mathematics*, vol. 8, no. 5, pp. 1–20, 2020, doi: 10.3390/MATH8050761.

[5] F. Cohen, "Computer viruses: Theory and experiments," *Comput. Secur.*, vol. 6, no. 1, pp. 22–35, 1987, doi: https://doi.org/10.1016/0167-4048(87)90122-2.

[6] W. H. Murray, "The application of epidemiology to computer viruses," *Comput. Secur.*, vol. 7, no. 2, pp. 139–145, 1988, doi: https://doi.org/10.1016/0167-4048(88)90327-6.

[7] R. K. Upadhyay and P. Singh, "Modeling and control of computer virus attack on a targeted network," *Phys. A Stat. Mech. its Appl.*, vol. 538, p. 122617, 2020, doi: https://doi.org/10.1016/j.physa.2019.122617.

[8] W. E. Boyce and R. C. Diprima, *Elementary Differential Equations and Boundary Value Problems*, Ninth Edit. John Wiley & Sons, Inc, 2009.

[9] L. Perko, *Differential Equations and Dynamical Systems*, Third Edit. New York: Springer, 2012.

[10] S. Wiggins, *Introduction to Applied Nonlinear Dynamical Systems and Chaos*, Second Edi. New York: Springer, 2006.

[11] O. Diekmann, J. A. P. Heesterbeek, and J. A. J. Metz, "On the definition and the computation of the basic reproduction ratio R0 in models for infectious diseases in heterogeneous populations," *J. Math. Biol.*, vol. 28, no. 4, pp. 365–382, 1990, doi: 10.1007/BF00178324.

[12] P. van den Driessche and J. Watmough, "Reproduction numbers and sub-threshold endemic equilibria for compartmental models of disease transmission," *Math. Biosci.*, vol. 180, no. 1, pp. 29–48, 2002, doi: https://doi.org/10.1016/S0025-5564(02)00108-6.

[13] T. A. Cahyanto, V. Wahanggara, and D. Ramadana, "Analisis dan deteksi malware menggunakan metode malware analisis dinamis dan malware analisis statis," *JUSTINDO (Jurnal Sist. dan Teknol. Inf. Indones.*, vol. 2, no. 1, pp. 19–30, 2017, doi: https://doi.org/10.32528/justindo.v2i1.1037.

[14] S. Kramer and J. C. Bradfield, "A general definition of malware," *J. Comput. Virol.*, vol. 6, no. 2, pp. 105–114, 2010, doi: 10.1007/s11416-009-0137-1.

[15] P. P. Pemungkas, S. Sutrisno, and S. Sunarsih, "Pengembangan Model Epidemik Sira Untuk Penyebaran Virus Pada Jaringan Komputer," *J. Fundam. Math. Appl.*, vol. 2, no. 1, pp. 13–21, 2019, doi: https://doi.org/10.14710/jfma.v2i1.26.

[16] Y. S. Suci, A. Aryanti, and A. Asriyadi, "Rancang bangun sistem keamanan data komputer pada antivirus vici menggunakan sistem realtime protector dan metode heuristic ganda," *IT J. Res. Dev.*, vol. 3, no. 1, pp. 84–94, 2018.