

## 1. Data Tren Virus

Data tren virus menampilkan gambaran tren virus yang didapatkan dari data yang dikumpulkan dan diproses sesuai dengan metodologi yang disampaikan pada dokumen ini. Pada sub bab pertama ini akan disampaikan metodologi yang sudah dipraktekan oleh peneliti.

### 1.1 Metode manual dengan cara sampling di tempat-tempat ramai:

Metodologi yang disampaikan berikut ini bukan merupakan satu-satunya metodologi yang dapat dilakukan di lapangan, akan tetapi merupakan metodologi yang dinilai oleh tim peneliti sebagai metodologi yang paling mungkin dan mudah untuk dilakukan, selain dari pada keinginan dari tim peneliti untuk dapat mengumpulkan data yang paling up-to-date atau mencerminkan keadaan nyata di masyarakat.

#### A. Pengumpulan Data

Pengumpulan data dilakukan berkala dengan menggunakan perangkat lunak antivirus ClamWin Portable Antivirus di warnet-warnet yang berada di lingkungan sekitar peneliti kerja dan tinggal.

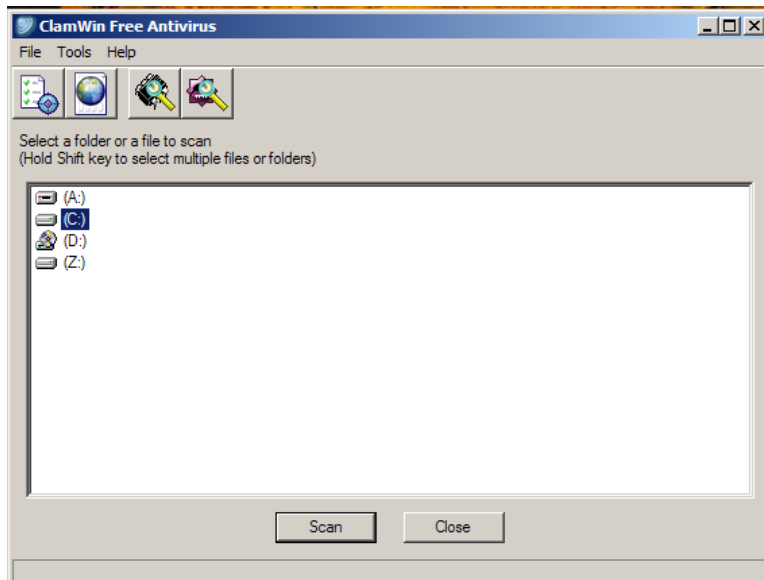
Metode yang dilakukan adalah sebagai berikut:

1. Mendatangi tempat-tempat yang diduga menjadi sumber penyebaran virus, seperti: warung internet (warnet), sekolah-sekolah, kantor-kantor, dll dengan menyiapkan sebuah usb flashdisk yang berisi software antivirus portable (peneliti menggunakan ClamWin Portable Antivirus) untuk dihubungkan dengan komputer-komputer yang akan dijadikan “target” pengumpulan data pada tempat-tempat tersebut.
2. Jalankan program aplikasi antivirus portable (ClamWin) dari flashdisk yang telah terhubung untuk mendapatkan file log yang berisi laporan scan virus pada komputer tersebut. ClamWin portable bisa didapatkan dari link: [http://portableapps.com/apps/utilities/ClamWin\\_portable](http://portableapps.com/apps/utilities/ClamWin_portable).

Cara menggunakan ClamWin Portable:

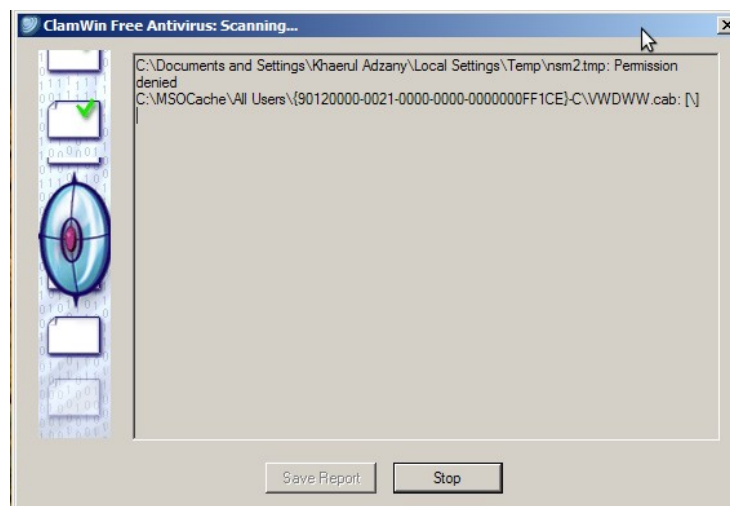
- a) Jalankan ClamWin Portable dari flashdisk. Apabila flashdisk kita terdeteksi sebagai drive D:\ maka jalankan ClamWinPortable.exe dari Drive D:\
- b) Setelah ClamWin portable jalan maka akan muncul jendela seperti pada gambar 1.1 dibawah. Mulai proses scan dengan menekan tombol **Scan** pada jendela utama ClamWin Portable.

Gambar 1.1 Tampilan Jendela Utama ClamWin Portable



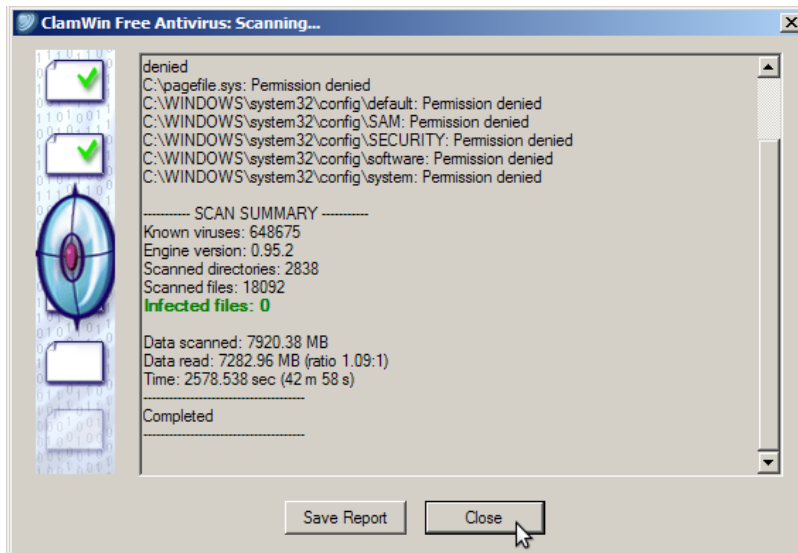
- c) Begitu proses scan sedang berjalan, kita dapat melihat file atau folder apa saja yang sedang melalui proses scanning oleh program ClamWin Portable seperti pada gambar 1.2 dibawah.

Gambar 1.2 Proses Scanning Oleh ClamWin Portable



- d) Jika proses scanning selesai, kita dapat menyimpan file hasil scan ke folder manapun yang kita kehendaki.

Gambar 1.3 Proses Scanning ClamWin Portable Selesai



- Setelah scan selesai, isikan hasil temuan ClamWin Portable pada berkas spreadsheet dengan format tabel seperti berikut:

Tabel 1.2 Hasil Virus Scan

Date	Name	Type	Jenis Sumber	Nama Sumber	Keterangan
2009-10-26	Trojan.Small-5	Trojan	Warnet	Multi Net	
2009-10-26	Trojan.Agent-6	Trojan	Warnet	Multi Net	
2009-10-26	Trojan.Agent-6	Trojan	Warnet	Multi Net	
2009-10-27	VBS:Malware-	Virus/Worm	Kantor	TMH	
2009-10-27	Win32:AutiUt-	Trojan	Kantor	TMH	
2009-10-27	Win32.Confi[W	Virus/Worm	Kantor	TMH	
2009-10-27	JS:Obfuscate	Trojan	Kantor	RHY	
2009-10-28	Worm.Autorun	Virus/Worm	Warnet	Boos Net	
2009-10-28	VBS.Hacksoft	Virus/Worm	Warnet	Boos Net	
2009-10-29	Trojan.Agent-1	Trojan	Warnet	Asanet	
2009-10-30	Virus found VE	Virus/Worm	Kantor	RHY	
2009-10-30	Trojan horse F	Virus/Worm	Kantor	RHY	

- Data yang didapatkan disimpan didalam dokumen dengan format CSV (Comma Separated Value). Opsi untuk menyimpan dokumen dengan menggunakan format CSV tersedia dalam perangkat lunak spreadsheet yang banyak digunakan di masyarakat, seperti Microsoft Office Excel dan OpenOffice Calc. Sebelum kita menyimpan data kedalam format CSV, bentuk tabel yang kita miliki harus kita betulkan sebelumnya, kolom yang bertumpuk seperti pada contoh diatas akan menyebabkan kesalahan pemrosesan ketika proses import data ke tabel database

dilakukan.

## B. Pemrosesan Data

Pemrosesan data virus dilakukan setelah data dengan menggunakan format CSV (Comma Separated Value) diperoleh menggunakan metode yang disampaikan pada sub bagian sebelumnya.

Data virus yang hendak diperoleh adalah data mengenai **berapa banyak kejadian serangan virus yang terjadi pada satu satuan waktu**. Untuk itu perlu dilakukan pemrosesan berdasarkan waktu yang tercatat.

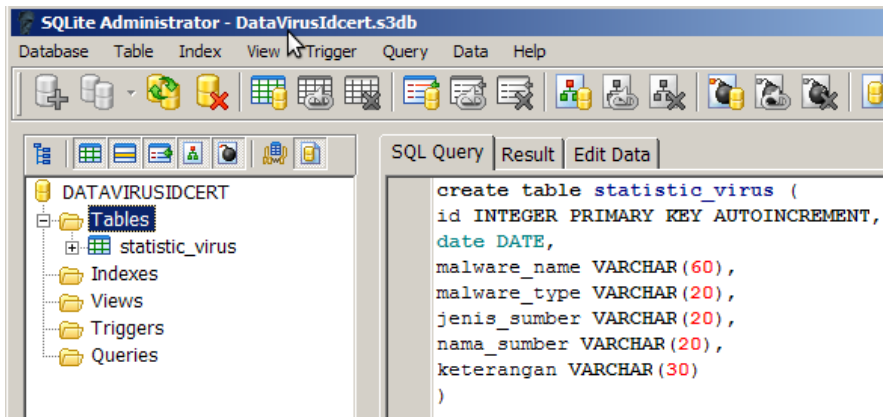
1. Data dengan format CSV akan dikonversi menjadi format tabel SQL yang dapat di query. Konversi data dengan format CSV menjadi tabel SQL dapat dilakukan dengan menggunakan bermacam perangkat lunak. Perangkat lunak yang digunakan untuk konversi data CSV menjadi SQL yang digunakan oleh peneliti adalah sqliteadmin yang dapat diperoleh melalui tautan berikut: <http://sqliteadmin.orbmu2k.de/>. Selain sqliteadmin, masih tersedia banyak perangkat lunak lainnya yang memiliki kemampuan untuk melakukan konversi data dari format CSV menjadi tabel database.

Petunjuk proses konversi data menggunakan sqliteadmin:

1. Jalankan program sqliteadmin dengan mengklik sqliteadmin.exe
2. Buka file database yang akan kita gunakan untuk menampung data yang akan kita proses, buka database dari menu **Database > Open**. Jika kita belum memiliki database sqlite yang akan kita gunakan, kita dapat membuat file database tersebut dari menu **Database > New**.
3. Buat tabel untuk menampung data yang akan kita proses, masukkan SQL Query kepada tab SQL Query pada sqlitadmin. Gunakan SQL query berikut:

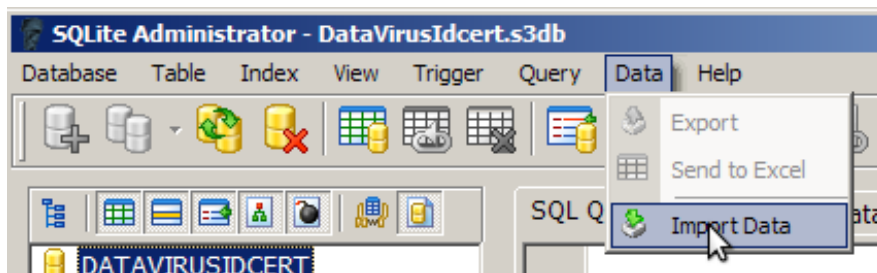
```
create table statistic_virus(  
id INTEGER PRIMARY KEY AUTOINCREMENT,  
date DATE,  
malware_name VARCHAR(60),  
malware_type VARCHAR(20),  
jenis_sumber VARCHAR(20),  
nama_sumber VARCHAR(20),  
keterangan VARCHAR(30))
```

Gambar 1.4 Tab SQL Query Untuk Memasukkan Sintaks SQL



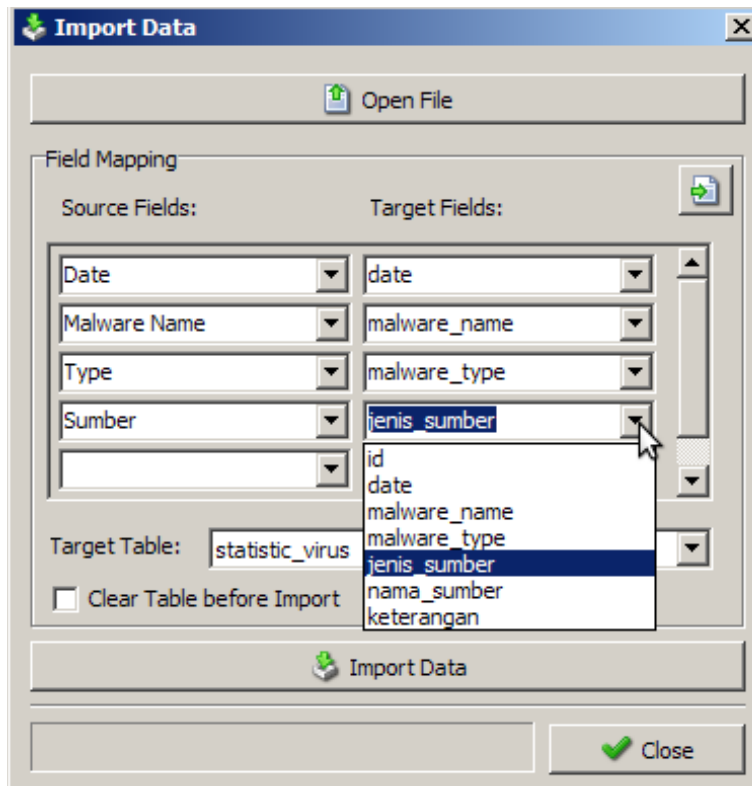
4. Lakukan import data dari file CSV ke tabel yang kita buat diatas dari menu **Data > Import Data**

Gambar 1.4 Menu Untuk Membuka Jendela Import Data



5. Proses import data menggunakan sqliteadmin merupakan pekerjaan yang mudah, karena sqliteadmin telah menyediakan jendela untuk import data dari berkas dengan format CSV.

Gambar 1.6 Jendela Import Data



Data yang telah berhasil dimasukkan kedalam tabel dapat segera diproses untuk didapatkan hasilnya.

2. Setelah data dimasukkan kedalam tabel database, kemudian data dapat diproses untuk mengetahui berapa jumlah virus yang masuk pada rentang waktu tertentu dengan query sebagai berikut:

```
select * from statistic_virus
where malware_name not in ('-', '')
and strftime('%m', date) = '10' --data untuk bulan oktober
```

3. Hasil query didapatkan dapat digunakan untuk visualisasi data. Contoh resultset yang dihasilkan adalah sebagai berikut:

Gambar 1.7 Contoh Resultset Hasil Query

id	date	malware_name	malware_type	jenis_sumber	nama_sumber	keterangan
78	10/20/2009	BV:AutoRun-S[Wrm]	Virus/Worm	Printing Center	-	
80	10/22/2009	Win32.Malware-gen	Virus/Worm	Portable Apps (Indow	-	
81	10/23/2009	BV:AutoRun-S[Wrm]	Virus/Worm	Sekolah	TB	
82	10/24/2009	Win32.Confi[Wrm]	Virus/Worm	Sekolah	TB	
85	10/26/2009	Trojan.Small-504	Trojan	Warnet	Multi Net	
86	10/26/2009	Trojan.Agent-62910	Trojan	Warnet	Multi Net	
87	10/26/2009	Trojan.Agent-62910	Trojan	Warnet	Multi Net	
88	10/27/2009	VBS:Malware-gen	Virus/Worm	Kantor	TMH	
89	10/27/2009	Win32:AutiUt-U[Trj]	Trojan	Kantor	TMH	
90	10/27/2009	Win32.Confi[Wrm]	Virus/Worm	Kantor	TMH	
91	10/27/2009	JS:Obfuscated-DA[Trj]	Trojan	Kantor	RHY	http://germankir
92	10/28/2009	Worm.Autorun-1838	Virus/Worm	Warnet	Boos Net	
93	10/28/2009	VBS.Hacksoft.NODfix	Virus/Worm	Warnet	Boos Net	
94	10/29/2009	Trojan.Agent-126462	Trojan	Warnet	Asanet	
95	10/30/2009	Virus found VBS/Worm	Virus/Worm	Kantor	RHY	
96	10/30/2009	Trojan horse PSW.OnlineGames	Virus/Worm	Kantor	RHY	
97	10/30/2009	Trojan horse Agent.ASXA	Virus/Worm	Kantor	RHY	
98	10/30/2009	Win32/Alman	Virus/Worm	Kantor	RHY	
99	10/30/2009	Worm/Generic_c.ZS	Virus/Worm	Kantor	RHY	
100	10/30/2009	Trojan horse Agent.ASXA	Virus/Worm	Kantor	RHY	
101	10/30/2009	Trojan horse Agent.ASLB	Virus/Worm	Kantor	RHY	

id	date	malware_name	malware_type	jenis_sumber	nama_sumber	keterangan
78	10/20/2009	BV:AutoRun-S[Wrm]	Virus/Worm	Printing Center	-	
80	10/22/2009	Win32.Malware-gen	Virus/Worm	Portable Apps (Indow	-	
81	10/23/2009	BV:AutoRun-S[Wrm]	Virus/Worm	Sekolah	TB	
82	10/24/2009	Win32.Confi[Wrm]	Virus/Worm	Sekolah	TB	
85	10/26/2009	Trojan.Small-504	Trojan	Warnet	Multi Net	
86	10/26/2009	Trojan.Agent-62910	Trojan	Warnet	Multi Net	
87	10/26/2009	Trojan.Agent-62910	Trojan	Warnet	Multi Net	
88	10/27/2009	VBS:Malware-gen	Virus/Worm	Kantor	TMH	
89	10/27/2009	Win32:AutiUt-U[Trj]	Trojan	Kantor	TMH	
90	10/27/2009	Win32.Confi[Wrm]	Virus/Worm	Kantor	TMH	
91	10/27/2009	JS:Obfuscated-DA[Trj]	Trojan	Kantor	RHY	http://germankir
92	10/28/2009	Worm.Autorun-1838	Virus/Worm	Warnet	Boos Net	
93	10/28/2009	VBS.Hacksoft.NODfix	Virus/Worm	Warnet	Boos Net	
94	10/29/2009	Trojan.Agent-126462	Trojan	Warnet	Asanet	
95	10/30/2009	Virus found VBS/Worm	Virus/Worm	Kantor	RHY	
96	10/30/2009	Trojan horse PSW.OnlineGames	Virus/Worm	Kantor	RHY	
97	10/30/2009	Trojan horse Agent.ASXA	Virus/Worm	Kantor	RHY	
98	10/30/2009	Win32/Alman	Virus/Worm	Kantor	RHY	
99	10/30/2009	Worm/Generic_c.ZS	Virus/Worm	Kantor	RHY	
100	10/30/2009	Trojan horse Agent.ASXA	Virus/Worm	Kantor	RHY	
101	10/30/2009	Trojan horse Agent.ASLB	Virus/Worm	Kantor	RHY	

Dari hasil query pertama ini kita dapat mengambil data yang kita inginkan sejak awal metode ini yaitu untuk mengetahui berapa banyak kejadian serangan virus yang terjadi pada satu satuan waktu. Maka untuk mendapatkan data tersebut kita ubah query kita menjadi:

```
select count(1), strftime('%m', date) from statistic_virus
where malware_name not in ('-', '')
and strftime('%m', date) = '10' --data untuk bulan oktober
```

atau

```
select count(1), strftime('%m', date) from statistic_virus
where malware_name not in ('-', '')
and strftime('%m', date) = '10' -- untuk data per bulan
(dengan -- catatan semua data berada pada tahun yang sama)
```

### C. Visualisasi Data

Visualisasi data dilakukan setelah informasi yang diinginkan berhasil didapatkan, visualisasi data yang digunakan peneliti adalah grafik batang (bar graph).

1. Grafik batang dapat dibuat dengan menggunakan aplikasi-aplikasi spreadsheet seperti Microsoft Excel atau OpenOffice Calc.
2. Spesifikasi grafik batang yang dijadikan sebagai laporan untuk tren virus di Indonesia adalah sebagai berikut:
  1. Kordinat x digunakan sebagai grouping berdasarkan waktu
  2. Kordinat y digunakan sebagai representasi nilai jumlah virus yang muncul
3. Contoh grafik batang yang dihasilkan adalah sebagai berikut dibawah:

Gambar 1.8 Grafik Batang

