

Membersihkan Virus, Malware, dan Spyware

Tim EMS

Membersihkan Virus, Malware, dan Spyware

pustaka-indo.blogspot.com

Sanksi Pelanggaran Pasal 113

Undang-Undang Nomor 28 Tahun 2014

tentang Hak Cipta

1. Setiap Orang yang dengan tanpa hak melakukan pelanggaran hak ekonomi sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf i untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 1 (satu) tahun dan/atau pidana denda paling banyak Rp100.000.000 (seratus juta rupiah).
2. Setiap Orang yang dengan tanpa hak dan/atau tanpa izin Pencipta atau pemegang Hak Cipta melakukan pelanggaran hak ekonomi Pencipta sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf c, huruf d, huruf f, dan/atau huruf h untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 3 (tiga) tahun dan/atau pidana denda paling banyak Rp500.000.000,00 (lima ratus juta rupiah).
3. Setiap Orang yang dengan tanpa hak dan/atau tanpa izin Pencipta atau pemegang Hak Cipta melakukan pelanggaran hak ekonomi Pencipta sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf a, huruf b, huruf e, dan/atau huruf g untuk Penggunaan Secara Komersial dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/atau pidana denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).
4. Setiap Orang yang memenuhi unsur sebagaimana dimaksud pada ayat (3) yang dilakukan dalam bentuk pembajakan, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau pidana denda paling banyak Rp4.000.000.000,00 (empat miliar rupiah).

Membersihkan Virus, Malware, dan Spyware

Tim EMS

PENERBIT PT ELEX MEDIA KOMPUTINDO



Membersihkan Virus, Malware, dan Spyware

Tim EMS

© 2015, PT Elex Media Komputindo, Jakarta

Hak cipta dilindungi undang-undang

Diterbitkan pertama kali oleh

Penerbit PT Elex Media Komputindo

Kelompok Gramedia, Anggota IKAPI, Jakarta 2015

12115xxxx

ISBN: 978-602-02-xxxx-x

[eEp]

Dilarang keras menerjemahkan, memfotokopi, atau memperbanyak sebagian atau seluruh isi buku ini tanpa izin tertulis dari penerbit.

Dicetak oleh Percetakan PT Gramedia, Jakarta

Isi di luar tanggung jawab percetakan

KATA PENGANTAR

Apakah Anda sering mengalami komputer terasa berat ketika digunakan? Atau malah komputer hang atau macet sehingga harus reboot? Itulah beberapa contoh bahwa komputer Anda mengalami gangguan. Bisa terjangkiti virus, atau terkena gangguan lainnya. Terlebih-lebih, ketika Anda terhubung ke internet, komputer langsung terasa berat ketika menjalankan program apa saja.

Mengapa komputer kita bisa seperti ini? Padahal bisa dikatakan jarang menggunakan flash disk yang bisa menyebabkan penularan virus.

Buku ini akan memberikan banyak solusi dalam membersihkan berbagai virus, spayware, mailware atau pengganggu lainnya yang menyebabkan komputer Anda menjadi bermasalah dan kurang nyaman digunakan. Materi yang akan dibahas meliputi:

- Anti Virus
- Anti Spyware
- Pengamanan Internet
- Teknik Lainnya.

Diharapkan dengan menguasai teknik dalam membersihkan berbagai gangguan virus, malware, atau spayware, komputer Anda semakin kuat dan sehat sehingga nyaman digunakan.

Semoga bermanfaat.

DAFTAR ISI

KATA PENGANTAR.....	V
DAFTAR ISI	VII
BAB 1 ANTIVIRUS.....	1
1.1 AVAST.....	1
1.1.1 Instalasi AVAST	2
1.1.2 Pemindaian Cepat.....	5
1.1.3 Pembersihan Browser	8
1.1.4 Pemindaian Jaringan Keamanan Rumah.....	10
1.1.5 VPN Secure Line	12
1.1.6 Fitur Lainnya.....	13
1.1.7 Pengaturan AVAST	16
1.2 CLAM Win AV.....	35
1.2.1 Menginstal Clam Win AV	35
1.2.2 Scan Drive dan Folder.....	40
1.2.3 Scan Memory.....	43
1.2.4 Scan File Tertentu.....	44
1.2.5 Pengaturan ClamWin	45
1.3 Hidden File Tool.....	53
1.4 Little Registry Cleaner.....	55
1.5 Windows Defender	65
BAB 2 ANTISPYWARE.....	71
2.1 SPY BOT.....	71
2.1.1 Instalsi SpyBot	72
2.1.2 Memindai Spyware System Scan	77
2.1.3 File Scan	80
2.1.4 Immunisasi	82
2.1.5 Melihat Karantina	83

2.1.6	Statistik Data.....	85
2.1.7	Pengaturan Program.....	86
2.1.8	Tools Startup	90
2.1.9	Rootkit Scan	93
2.2	Bazooka	94
2.3	Nixory.....	99
2.3.1	Menginstal Nixory.....	99
2.3.2	Menggunakan Nixory.....	102
BAB 3	PENGAMANAN INTERNET.....	109
3.1	Web Of Trust.....	109
3.1.1	Menambahkan dan Menggunakan WOT	110
3.2	Password Maker	112
3.2.1	Download dan Instalasi	113
3.2.2	Menggunakan PasswordMaker	115
3.3	KeePass	116
3.3.1	Mendownload dan Mengakses KeePass.....	117
3.3.2	Menggunakan KeePass	118
3.4	Password Safe.....	126
3.4.1	Download dan Install Password Safe	127
3.4.2	Menggunakan Password Safe.....	130
3.4.3	Membuka File Password.....	135
BAB 4	TEKNIK LAINNYA.....	137
4.1	WireShark	137
4.1.1	Menginstal WireShark.....	137
4.1.2	Menggunakan WireShark	143
4.2	Windows Firewall.....	151
4.3	BitLocker	158
4.4	Alternatif Penyelamatan Terakhir dengan Rescue CD	163
4.4.1	System Rescue CD.....	163
4.4.2	AVG Rescue CD	173
4.4.3	Kaspersky Rescue Disk	176
4.4.4	Antivir Rescue	185
4.4.5	F-Secure Rescue CD	189
4.4.6	Membakar File ISO ke CD.....	193

1 ANTIVIRUS

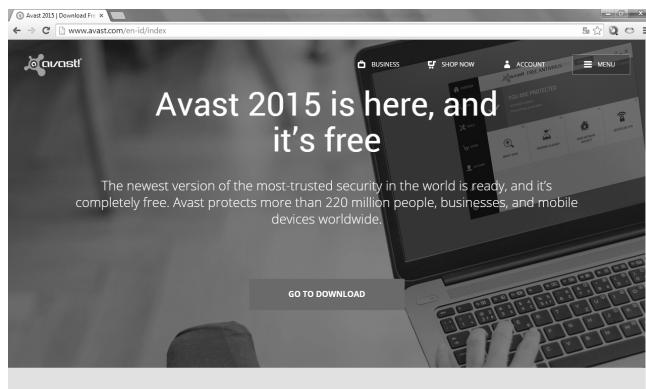
Virus adalah program di komputer yang bisa melakukan operasi yang tidak terotorisasi. Seperti menghapus data, menyalin data, padahal tidak diinginkan oleh user, serta memiliki kecenderungan untuk menyebar ke komputer lain. Virus umumnya mengakibatkan kerugian ke user seperti file dokumen hilang, atau sistem operasi rusak. Agar komputer tidak terkena virus, Anda bisa menggunakan antivirus. Windows pun menyarankan untuk menginstal anti virus guna memproteksi komputer Anda.

1.1 AVAST

AVAST adalah salah satu anti virus unggulan yang dapat di-download dari situs avast.com. Anda bisa mendownload boot strapper-nya, nanti saat proses download, Anda akan men-download file-file definisi virus secara terpisah.

Antivirus Avast ini perlu dipertimbangkan, karena memiliki banyak kelebihan. Beberapa kelebihan tersebut diantaranya: pemindaian secara cepat, mampu membersihkan browser yang terjangkiti virus, pemindaian di dalam jaringan sehingga bisa memaindai komputer lain yang terhubung di dalam jaringan, dan lain-lain.

Untuk pemanfaatan antivirus Avast ini akan dijelaskan mulai dari instalasi hingga cara penggunaannya.

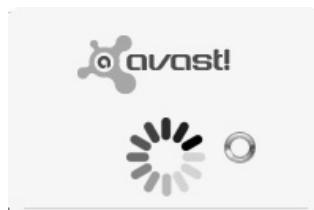


Gambar 1.1 Halaman avast.com

1.1.1 Instalasi AVAST

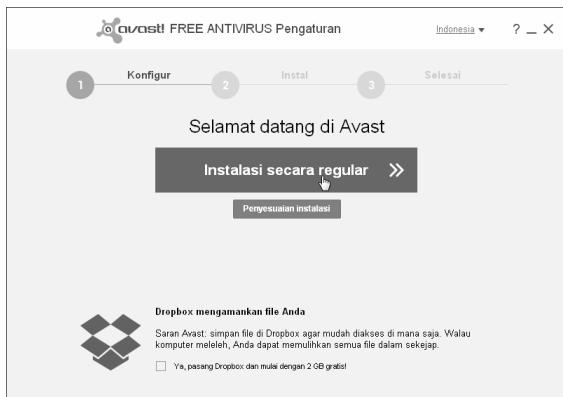
Berikut ini cara menginstal AVAST ke komputer Anda:

1. Klik 2x pada installer Avast bootstrapper yang sudah di-download. Muncul splash screen seperti gambar berikut ini:



Gambar 1.2 Tampilan splash screen AVAST

2. Muncul halaman Selamat Datang di Avast yang masuk tahap konfigurasi. Klik pada tombol **Instalasi Secara Reguler**. Atau kalau menentukan fitur-fitur khusus yang ingin diinstal, Anda bisa mengklik pada **Penyesuaian Instalasi**.



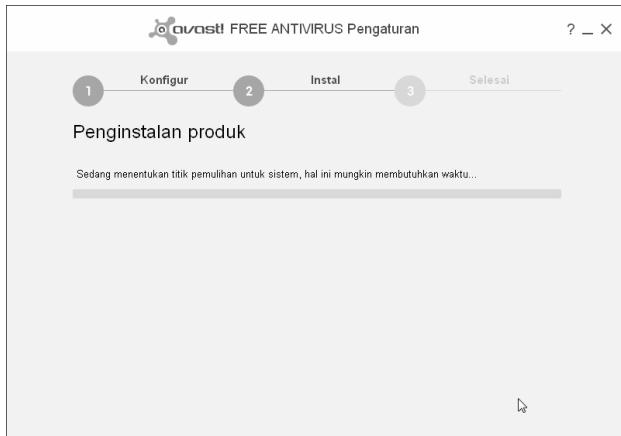
Gambar 1.3 Klik Instalasi secara reguler

3. Di halaman lisensi pengguna, klik tombol **Lanjutkan**.



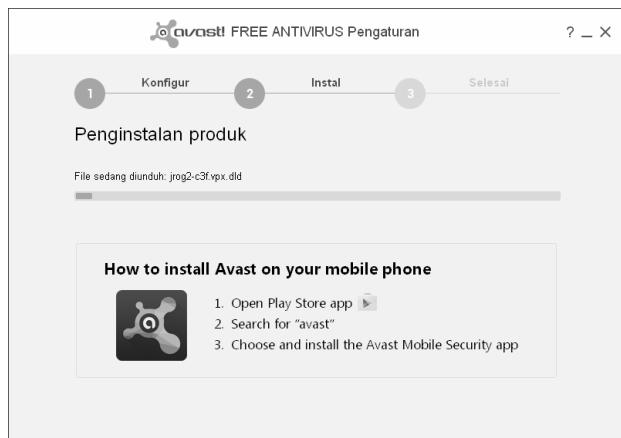
Gambar 1.4 Halaman lisensi pengguna

4. Selanjutnya instalasi akan masuk ke tahapan **Instal**.



Gambar 1.5 Instalasi masuk ke tahapan Install

5. File-file definisi virus langsung di-download secara langsung. Anda butuh koneksi yang cukup kencang kalau ingin proses tahapan ini berjalan dengan cepat.



Gambar 1.6 Proses download definisi

6. Kalau sudah selesai, muncul konfirmasi bahwa instalasi sudah selesai.

1.1.2 Pemindaian Cepat

Apabila avast sudah terinstal, Anda dapat menggunakan fasilitas Pemindaian Cepat untuk melihat kondisi awal komputer Anda berikut ini:

1. Jalankan avast, di halaman Sekilas Info, Anda bisa melihat beberapa fungsi utama antivirus avast, antara lain pemindaian cepat, bersihkan browser dan jaringan keamanan rumah.



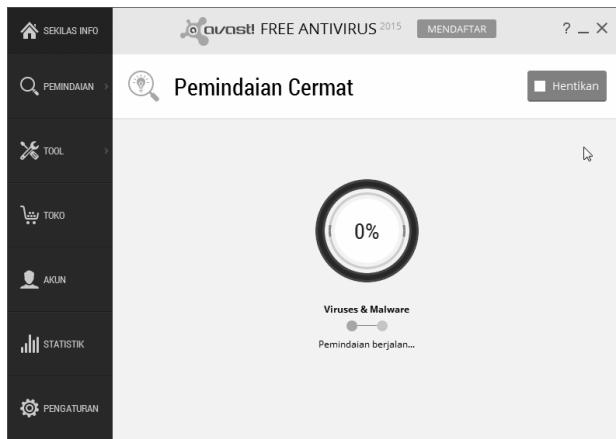
Gambar 1.7 Halaman Sekilas info

2. Untuk memindai komputer pertama, klik pada link **Pemindaian Cepat**.



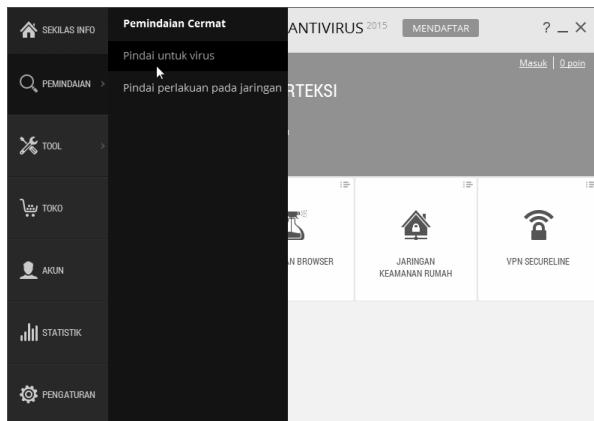
Gambar 1.8 Klik pada Sekilas Info > Pemindaian Cepat

3. Maka proses pemindaian akan berlangsung dan hasilnya langsung ditampilkan di akhir pemindaian cepat, apakah ada virus atau malware di komputernya.



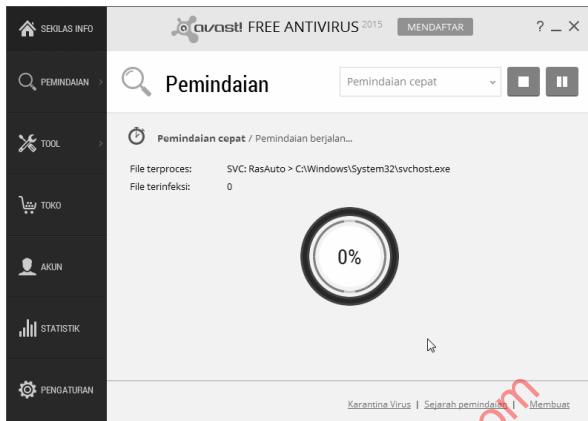
Gambar 1.9 Proses pemindaian berlangsung

4. Ada juga pemindaian lain yang lebih advanced, misalnya khusus untuk virus, klik pada **Pemindaian > Pindai untuk virus**.



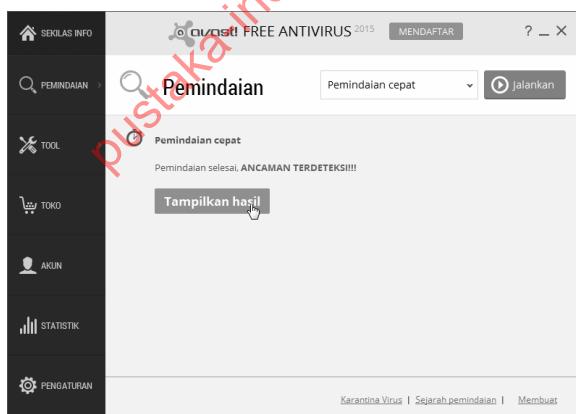
Gambar 1.10 Klik Pindai untuk virus

5. Maka file-file akan dicek apakah mengandung virus, file-file yang sedang dicek terlihat path-nya di **File terproses**.



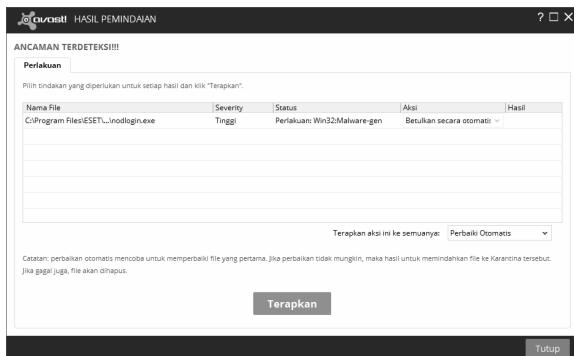
Gambar 1.11 Proses pemindaian file apakah ada virusnya

6. Kalau ada ancaman, muncul tulisan “Ancaman Terdeteksi”. Klik pada tombol Tampilkan hasil untuk melihat detil ancaman yang terdeteksi.



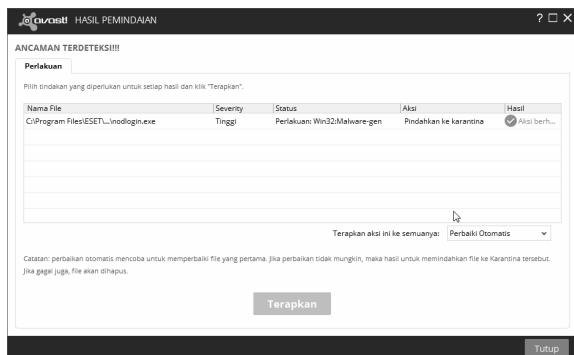
Gambar 1.12 Ada pemberitahuan “Ancaman Terdeteksi”

7. Daftar file yang mengancam beserta jenisnya terlihat di jendela yang muncul.



Gambar 1.13 Ancaman yang muncul dan terdeteksi oleh AVAST

8. Klik **Terapkan**, Anda bisa melihat file tersebut dinetralkan agar tidak membahayakan lagi.

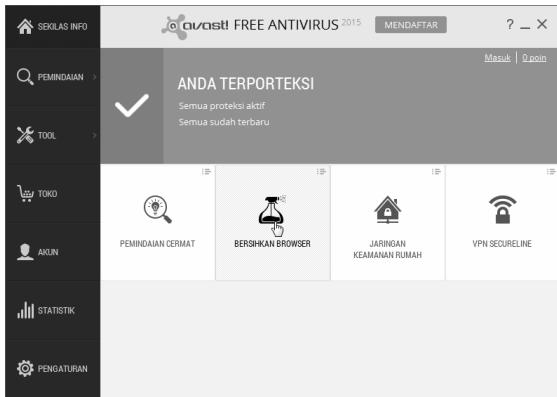


Gambar 1.14 Penetralan file yang menjadi ancaman

1.1.3 Pembersihan Browser

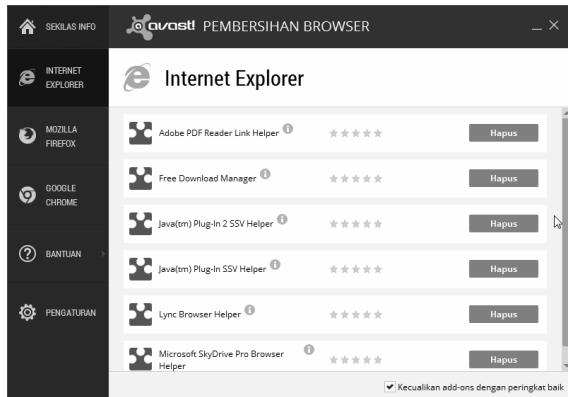
Salah satu jalur masuk virus ke dalam komputer adalah browser, ini juga berlaku untuk spyware. AVAST memiliki fasilitas pembersihan browser yang membersihkan browser dari kemungkinan ditunggangi virus. Berikut ini cara menggunakan fasilitas pembersihan browser dari AVAST:

1. Klik pada **Sekilas Info > Bersihkan Browser**.



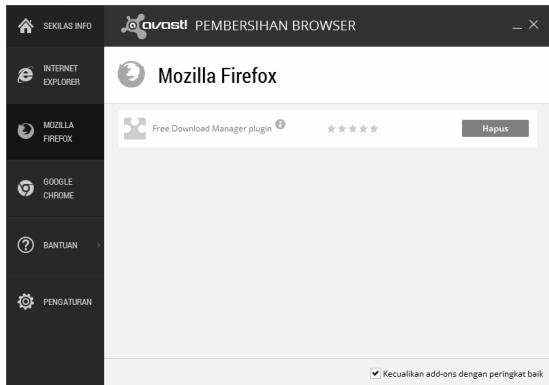
Gambar 1.15 Klik pada Bersihkan Browser

2. Muncul halaman yang menampilkan berbagai browser yang terinstal di komputer. Anda bisa mengklik IE untuk menampilkan komponen-komponen dan plugin yang terpasang di IE yang ingin dihapus. Klik pada tombol Hapus untuk menginstal.



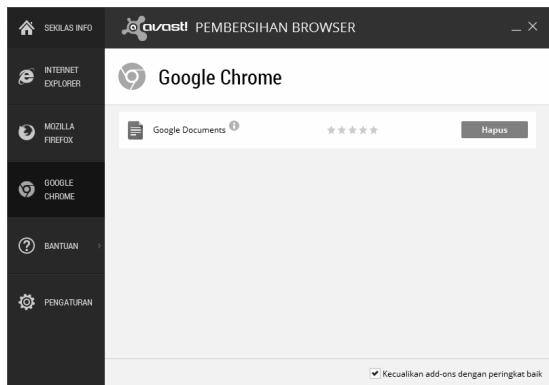
Gambar 1.16 Pembersihan di IE

3. Klik pada Mozilla Firefox untuk menghapus komponen-komponen yang tidak diperlukan di Firefox.



Gambar 1.17 Penghapusan Mozilla Firefox

4. Di Google Chrome, Anda bisa membersihkan browser Google Chrome. Apabila ada browser lain di komputer Anda, semuanya akan ditampilkan di jendela **Pembersihan Browser** ini.



Gambar 1.18 Pembersihan browser Google Chrome

1.1.4 Pemindaian Jaringan Keamanan Rumah

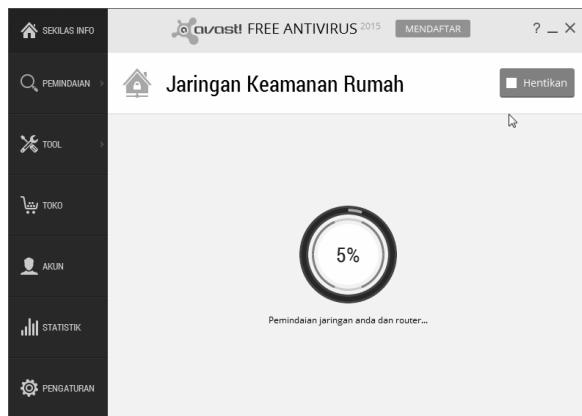
Salah satu modus virus menyebar adalah melalui jaringan atau networking. Karena itu Anda bisa memindai jaringan di komputer Anda untuk memastikan bebas virus. AVAST memiliki fasilitas pemindaian jaringan yang dilakukan dengan cara seperti ini:

1. Klik pada Sekilas Info > Jaringan Keamanan Rumah.



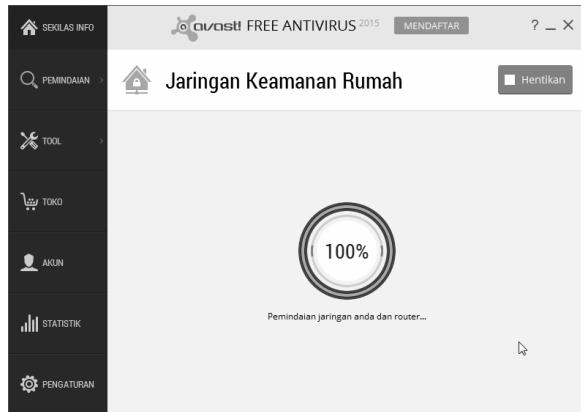
Gambar 1.19 Klik tombol untuk mengakses jaringan keamanan rumah

2. Muncul jendela Jaringan Keamanan Rumah yang memindai jaringan dan router yang dipakai untuk terhubung ke internet atau di jaringan.



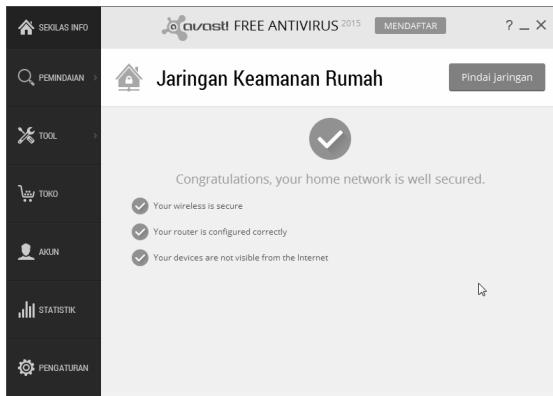
Gambar 1.20 Jaringan Keamanan Rumah

3. Kalau sudah selesai, maka 100% komponen jaringan sudah terpindai semuanya.



Gambar 1.21 100% komponen sudah terpindai semuanya

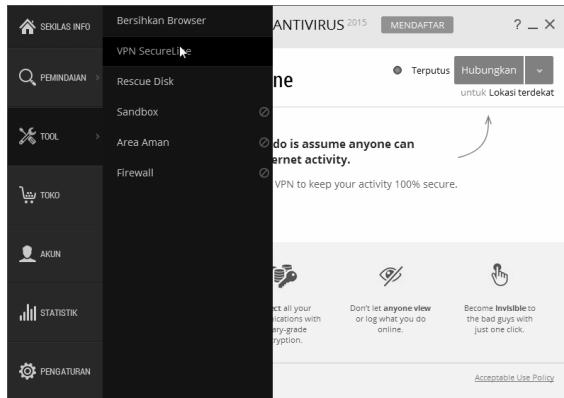
4. Apabila tidak ditemukan ancaman, muncul konfirmasi **Home network well secured**.



Gambar 1.22 Jaringan sudah aman

1.1.5 VPN Secure Line

Anda bisa menghubungkan vpn (virtual private network) secara mana dengan menggunakan VPN SecureLine dari AVAST yang bisa diakses dari Tool > VPN Secure Line.



Gambar 1.23 *VPN Secure Line*

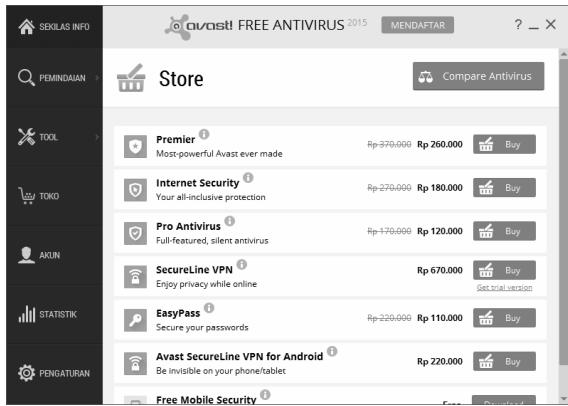
Kemudian klik Hubungkan untuk menghubungkan ke server menggunakan VPN secure.



Gambar 1.24 *VPN Secure Line*

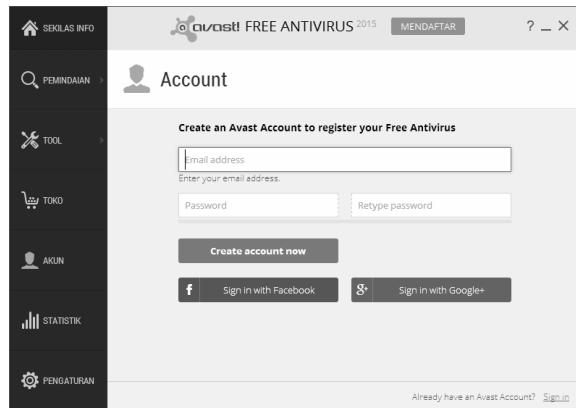
1.1.6 Fitur Lainnya

Ada banyak fitur lainnya yang bisa dipakai untuk meningkatkan kemampuan AVAST. Bagian Store digunakan untuk membeli komponen-komponen tambahan untuk meningkatkan keamanan pc. Dari mulai anti virus pro, sampai Easy pass untuk mengamankan password Anda.



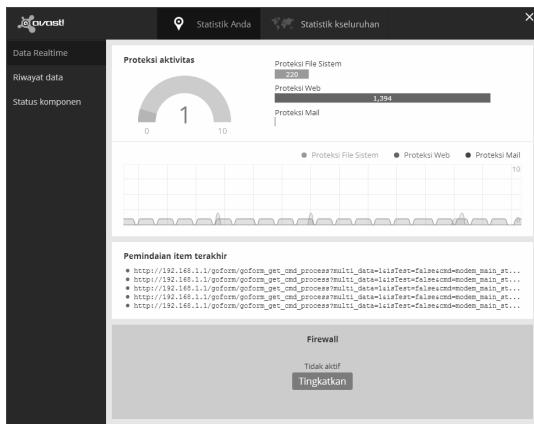
Gambar 1.25 *Store untuk membeli komponen baru*

Di Akun, Anda bisa membuat akun baru untuk me-register-kan sebagai pengguna AVAST Free AV.



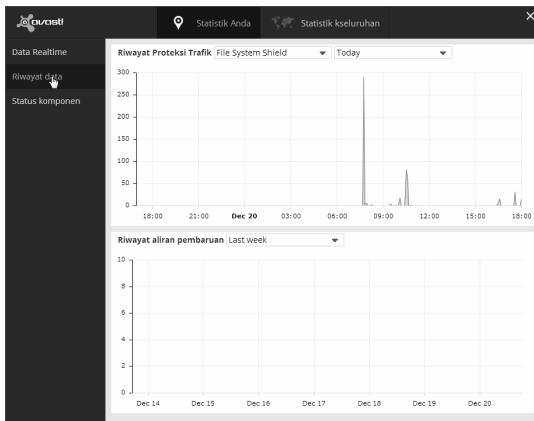
Gambar 1.26 *Halaman Akun*

Di Statistik, Anda bisa melihat data statistik pemindaian dan virus yang ada di komputer. Caranya klik Statistik.



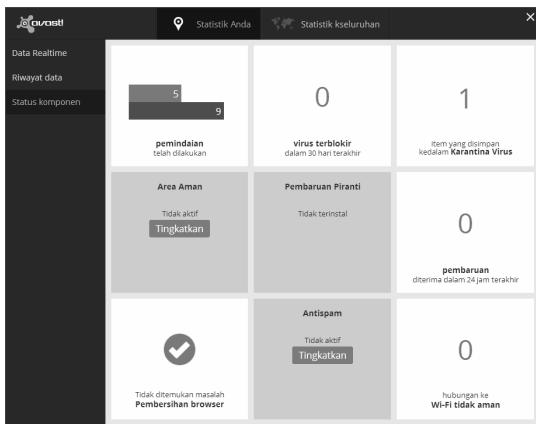
Gambar 1.27 Halaman Statistik

Kalau diklik Tingkatkan, Anda bisa melihat statistik tambahan yang menjelaskan sejarah pemindaian.



Gambar 1.28 Halaman sejarah pemindaian

Di **Statistik > Status Komponen**, Anda bisa melihat status komponen-komponen yang ada, termasuk bagaimana meningkatkan status komponen ke pro yang bersifat komersil.



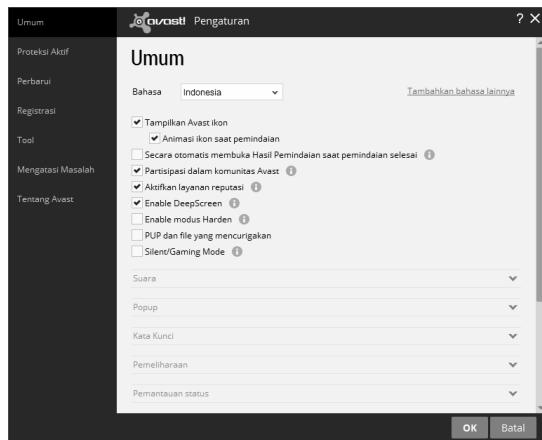
Gambar 1.29 Status komponen

1.1.7 Pengaturan AVAST

Agar pemindaian berjalan efektif, Anda perlu mengatur dan mengkonfigurasi AVAST terlebih dahulu. AVAST menyediakan menu Pengaturan yang cukup kompleks yang memudahkan Anda mengefektifkan proses pemindaian virus di komputer.

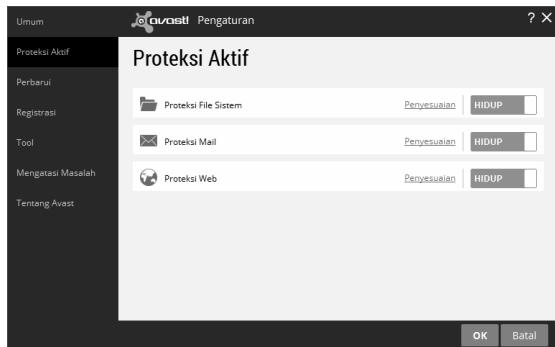
Dari halaman utama klik tab Pengaturan, muncul banyak sekali menu pengaturan di situ Anda bisa mengatur dengan langkah-langkah seperti berikut ini:

1. Di tab Umum, Anda bisa mengatur pengaturan umum dari mulai bahasa, ikon, aktifkan layanan Reputasi, mengaktifkan DeepScreen atau tidak. Anda juga bisa mengeset agar program ini berjalan di background dengan memilih **Silent/Gaming Mode**.



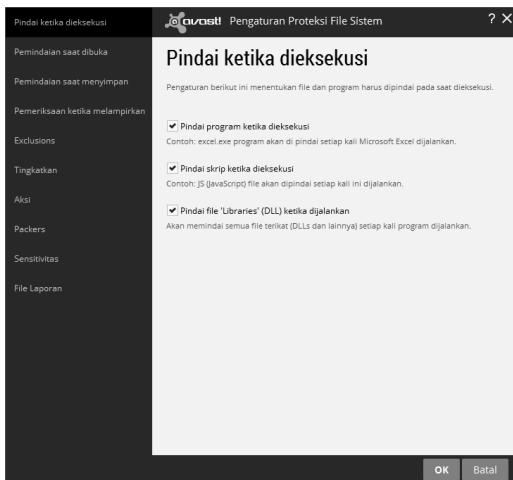
Gambar 1.30 Pengaturan umum di tab Umum

2. Di tab Proteksi aktif, ada tiga pengaturan, Anda bisa mengeset Proteksi sistem file, mail dan web serta melihat status apakah proteksi-proteksi tersebut aktif atau tidak.



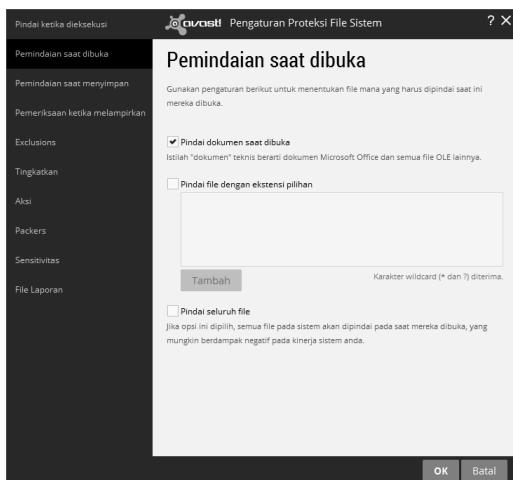
Gambar 1.31 Tab Proteksi Aktif

3. Klik **Penyesuaian** di bagian Proteksi file sistem untuk mengatur penyesuaian bagi AVAST ketika memindai sistem file. Muncul tab Pindai ketika dieksekusi, Anda bisa mengeset apakah file-file executable, script seperti javascript dan file .dll otomatis dieksekusi ketika file tersebut dibuka.



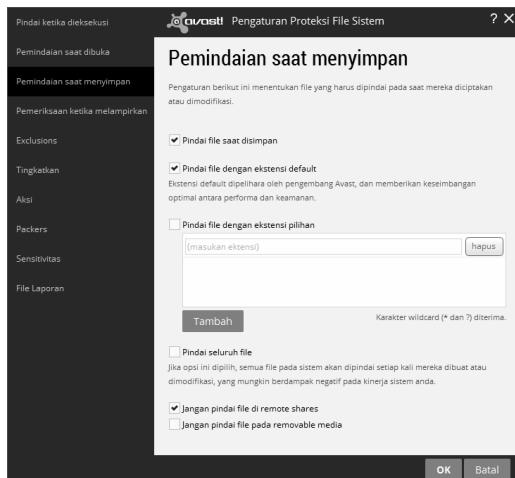
Gambar 1.32 Pengaturan pemindaian ketika dieksekusi

4. Di **Pemindaian Saat Dibuka**, Anda bisa mengatur apakah dokumen seperti MS Office dan OLE (object linking and embedded) otomatis dipindai saat dibuka. Anda juga bisa mengeset apakah file-file ekstensi tertentu bisa ditambahkan saat dibuka.



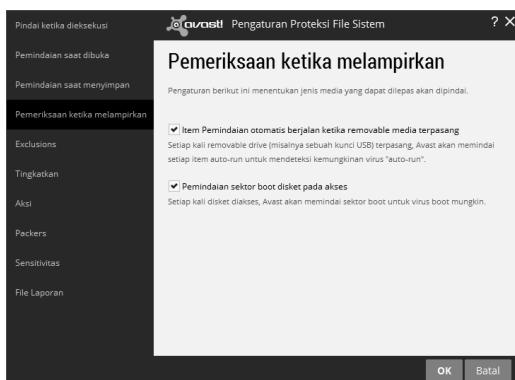
Gambar 1.33 File-file saat dibuka

5. Di Pemidnaian saat disimpan, Anda bisa menentukan tipe-tipe file yang akan dipindai lagi saat akan disimpan untuk melihat apakah ada virus atau tidak.



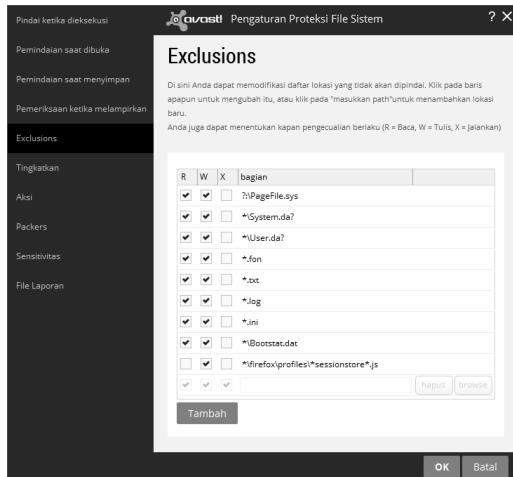
Gambar 1.34 Pengaturan Pemindaian saat menyimpan

6. Di Pemeriksaan ketika melampirkan, Anda bisa mengaktifkan apakah file di media removable, seperti usb flash disk atau memori card langsung dipindai ketika dimasukkan atau tidak?



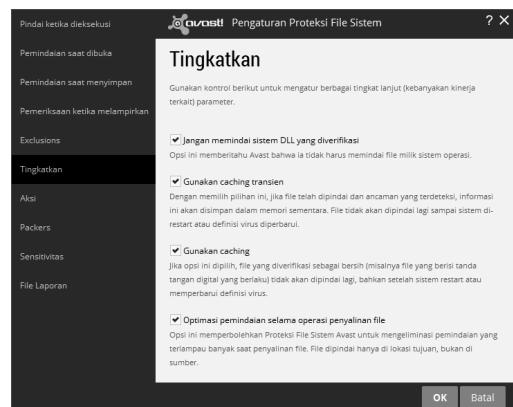
Gambar 1.35 Pengaturan Pemeriksaan ketika Melampirkan

7. Anda bisa menentukan tipe-tipe file yang tidak akan ikut dipindai di bagian **Exclusions**.



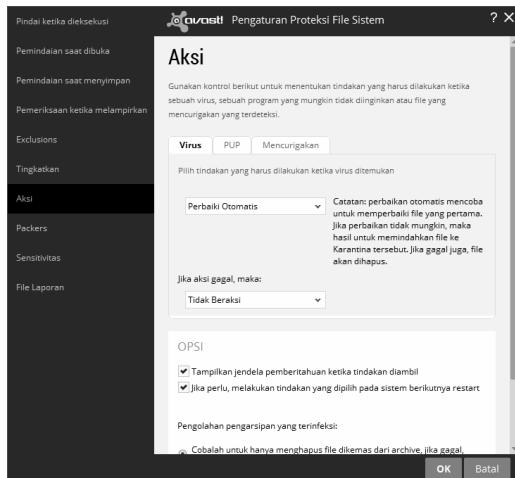
Gambar 1.36 Pengaturan Exclusions

8. Di Tingkatkan, Anda bisa mengatur kontrol lanjutan untuk pemindaian tingkat lanjut, seperti apakah akan memindai file dll yang terverifikasi, menggunakan cache transien, menggunakan cache atau optimasi pemindaian selama penyalinan file.



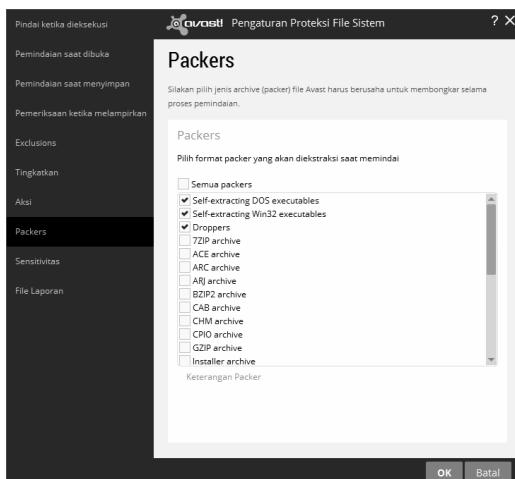
Gambar 1.37 Pengaturan di tab Tingkatkan

9. Di tab Aksi, Anda bisa mengatur opsi action apa yang mau diambil untuk virus, PUP, dan file-file mencurigakan.



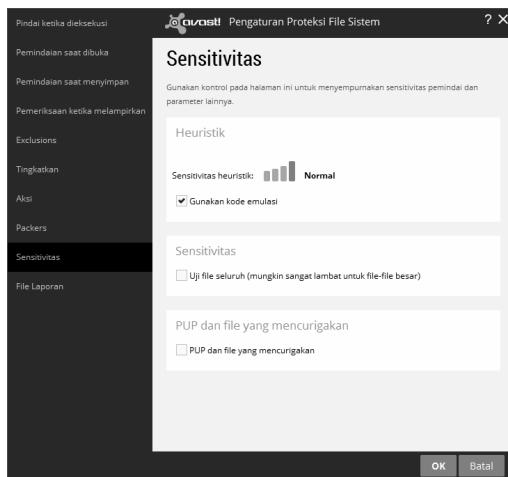
Gambar 1.38 Pengaturan tab Aksi untuk sistem file

10. Di Packers, Anda dapat menentukan format file pengarsip yang akan dibongkar selama proses pemindaian.



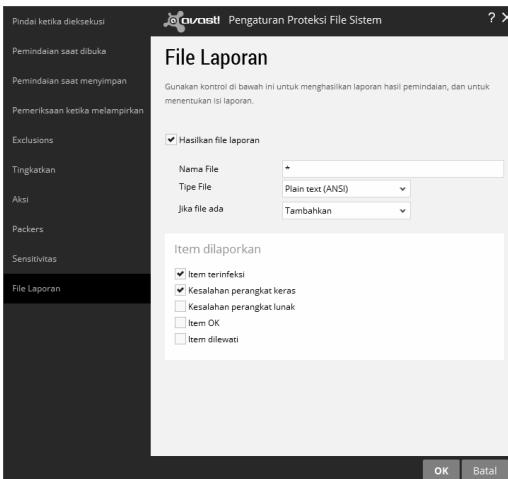
Gambar 1.39 Packers

11. Di **Sensitivitas**, Anda bisa mengatur sensitivitas heuristik saat memindai sistem file.



Gambar 1.40 Sensitivitas heuristik

12. Di **File Laporan**, Anda bisa mengeset apakah akan membuat laporan setelah pemindaian dan mengatur format laporan.



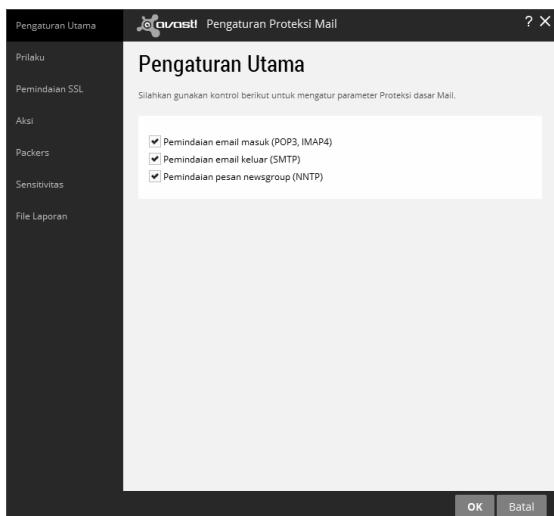
Gambar 1.41 File Laporan

- Kembali ke proteksi aktif, Anda bisa mengesuaikan untuk pengaturan email dengan klik **Penyesuaian** pada **Proteksi email**.



Gambar 1.42 Proteksi aktif pada email

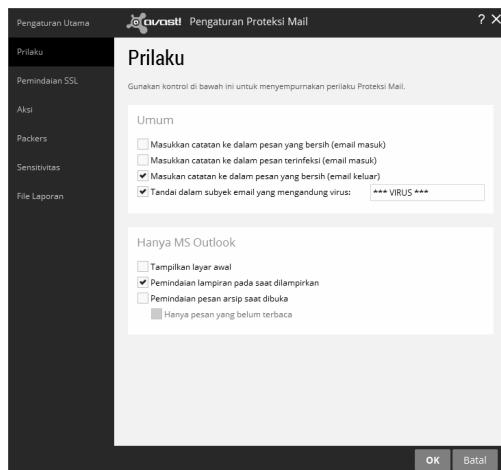
- Di Pengaturan Utama untuk email, Anda bisa mengeset apa sajakah protokol email yang akan dipindai, seperti POP3, IMAP4, SMTP, NNTP.



Gambar 1.43 Pengaturan protokol

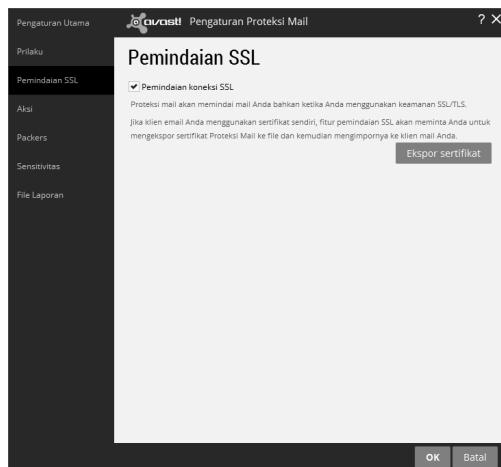
- Di tab Perilaku, Anda bisa mengeset perilaku pemindaian email, seperti apakah memasukkan catatan yang sudah dipindai ke Email masuk, dan menandai email yang terkena virus dengan mengganti subjek dengan tambahan ****VIRUS***.

16. Di bagian Outlook, Anda dapat mengatur perilaku khusus untuk email client **MS Outlook**.



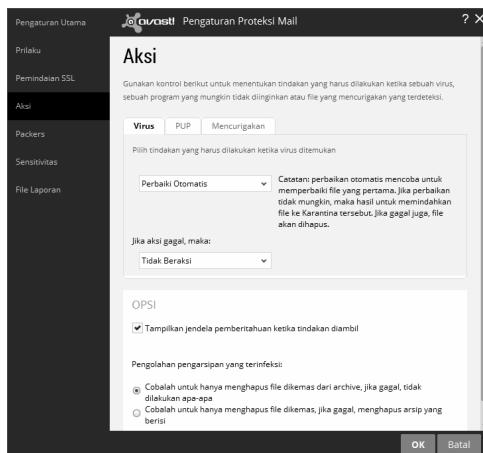
Gambar 1.44 Pengaturan Perilaku

17. Di Pemindaian SSL, Anda bisa mengecek apakah akan memindai koneksi SSL dari email atau tidak.



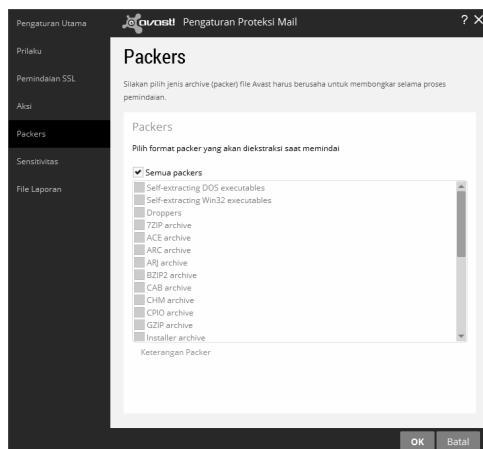
Gambar 1.45 Pengaturan Pemindaian SSL untuk email

18. Di **Aksi**, Anda bisa mengatur apa action yang akan dilakukan jika ditemukan Virus, PUP dan file mencurigakan di email Anda.



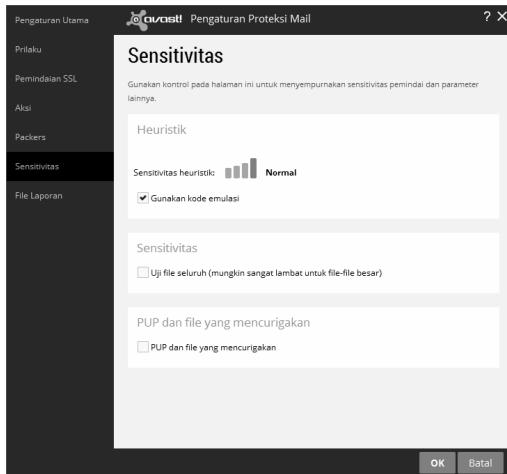
Gambar 1.46 Pengaturan Aksi untuk pemindaian email

19. Di **Packers**, Anda bisa mengeset file-file arsip di email yang akan dipindai.



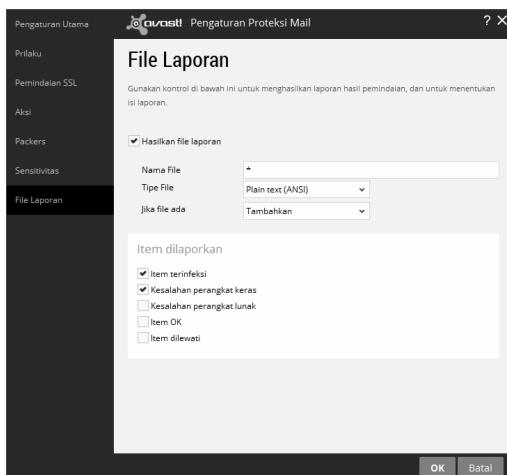
Gambar 1.47 Pengaturan Packers

20. Di Sensitivitas, Anda dapat mengatur sensitivitas pada pemindaian virus di email.



Gambar 1.48 Pengaturan sensitivitas di email

21. Di File Laporan, Anda bisa mengeset format dan nama file laporan untuk pemindaian email.



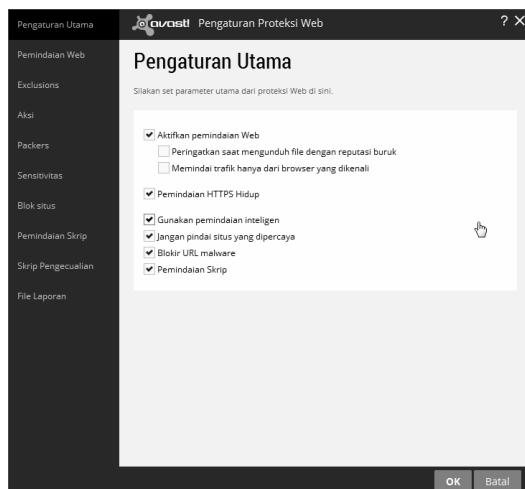
Gambar 1.49 Pembuatan File laporan untuk pemindaian email

22. Kembali ke halaman sebelumnya, klik Penyesuaian untuk proteksi web. Ini adalah pemindaian virus di browser.



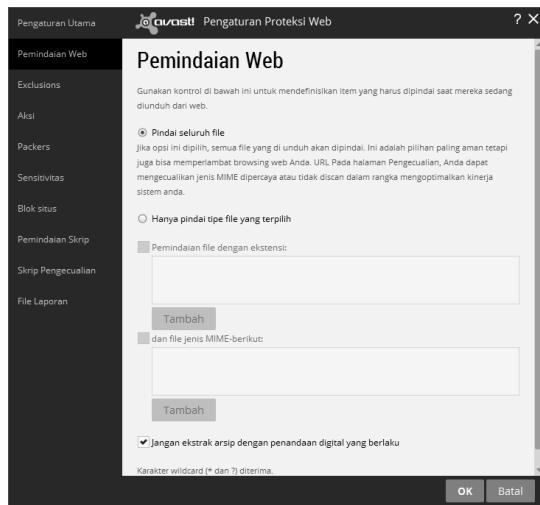
Gambar 1.50 Penyesuaian untuk Proteksi Web

23. Di Pengaturan Utama, Anda bisa mengeset apakah pemindaian untuk web diaktifkan. Begitu pula dengan pemindaian HTTPS, lalu pemindaian inteligen, dan apakah url malware diblokir agar tidak bisa diakses.



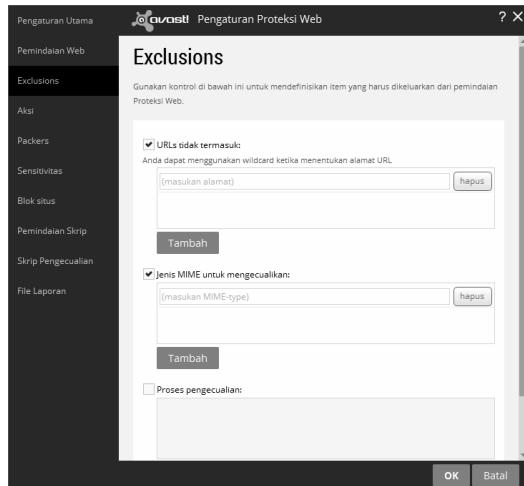
Gambar 1.51 Pengaturan utama s

24. Di Pemindaian Web, Anda bisa mengatur apakah semua file akan dipindai, atau file-file tertentu saja.



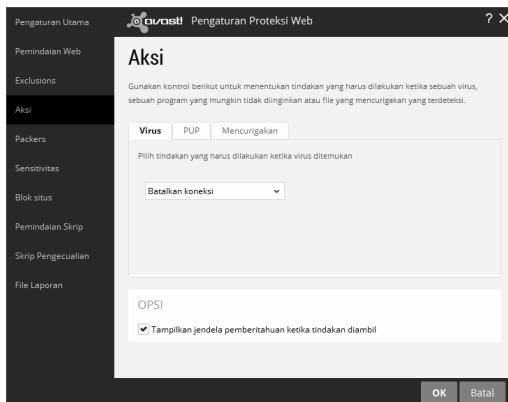
Gambar 1.52 Pengaturan pemindaian web pada seluruh file atau file tertentu saja

25. Di Exclusions, Anda bisa mengecualikan url yang tidak akan dipindai, atau jenis MIME yang akan dikecualikan.



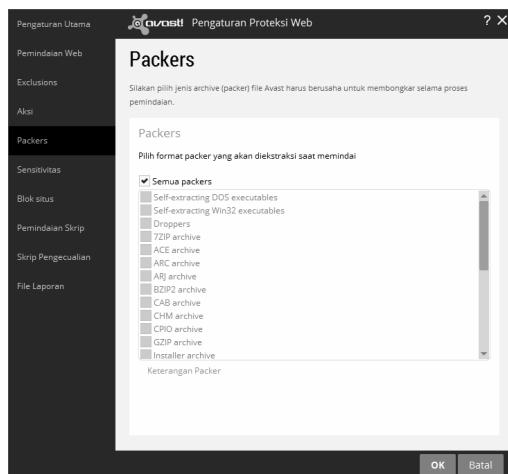
Gambar 1.53 Pengaturan Exclusions untuk mengecualikan file tertentu dari pemindaian

26. Di Aksi, Anda bisa menentukan apa action yang dilakukan jika ada virus, PUP dan file yang mencurigakan. Default-nya adalah membatalkan atau memutuskan koneksi.



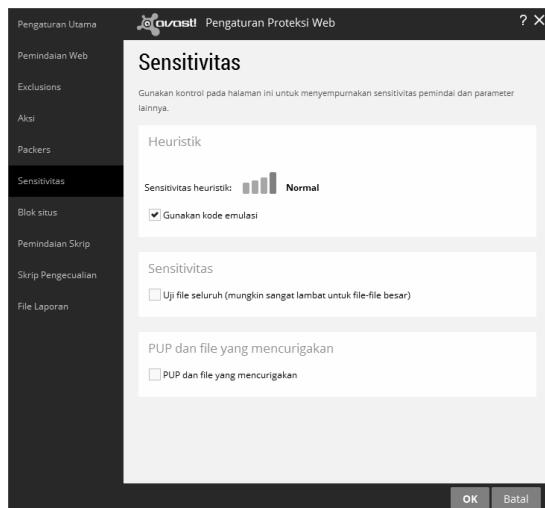
Gambar 1.54 Pengaturan action default untuk Aksi standar

27. Di Packers, Anda dapat menentukan tipe file arsip di web yang akan dipindai, apakah semuanya atau tertentu saja.



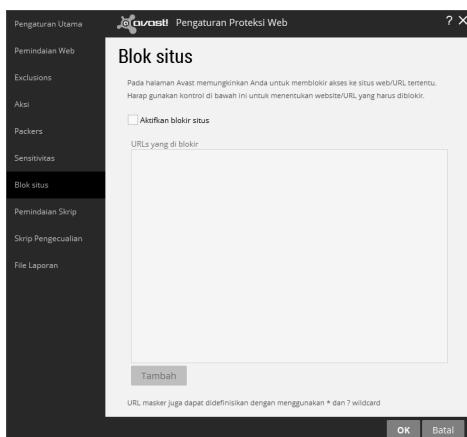
Gambar 1.55 Pengaturan Packers

28. Di Sensitivitas, Anda bisa mengatur sensitivitas pemindaian untuk web, apakah normal atau ekstra sensitif.



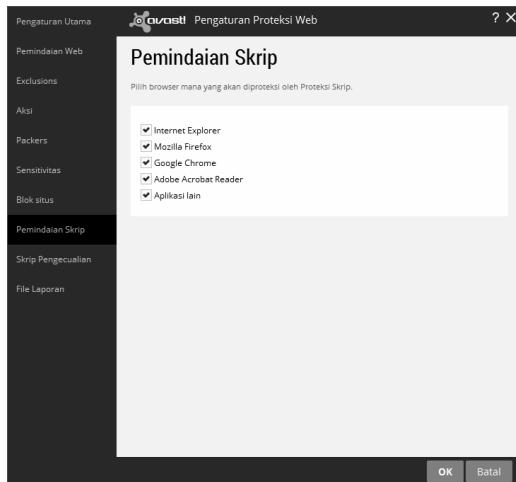
Gambar 1.56 Pengaturan sensitivitas pemindaian web

29. Di Blok Situs, Anda bisa mengeset pemblokiran situs tertentu berdasarkan url yang dimasukkan.



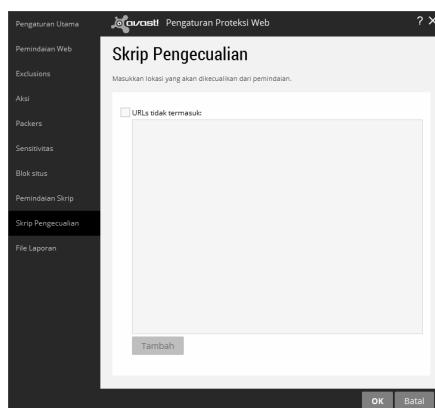
Gambar 1.57 Memasukkan Blok situs

30. Di Pemindaian Skrip, Anda bisa memilih browser yang akan diproteksi ketika memindai skrip.



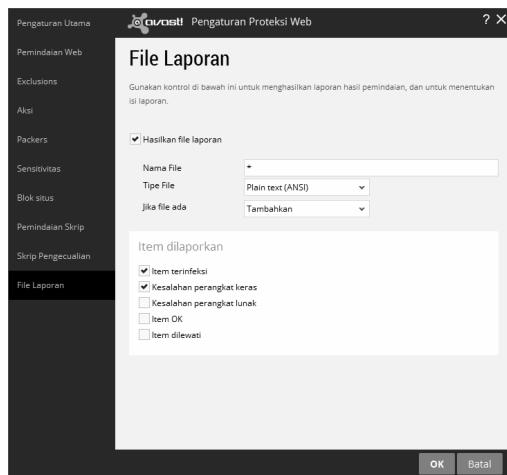
Gambar 1.58 Pemilihan browser yang diproteksi dari pemindaian skrip

31. Di Skrip Pengecualian, Anda bisa menentukan url dari skrip yang tidak ingin dilihat apakah ada virus-nya atau tidak.



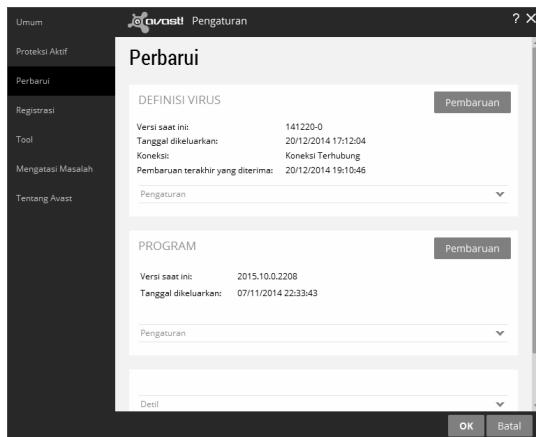
Gambar 1.59 Pengecualian untuk pemindaian skrip

32. Di File Laporan, Anda bisa mengeset apakah akan membuat laporan atau tidak untuk pemindaian web.



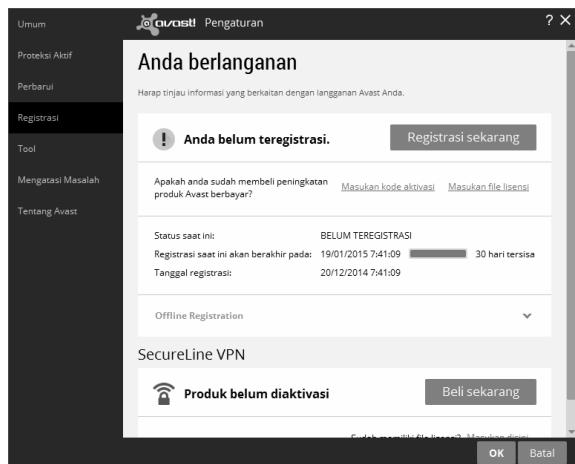
Gambar 1.60 Pemindaian web

33. Kembali ke halaman Pengaturan, klik Perbarui untuk memperbarui file definisi virus agar pemindaian menjadi presisi.



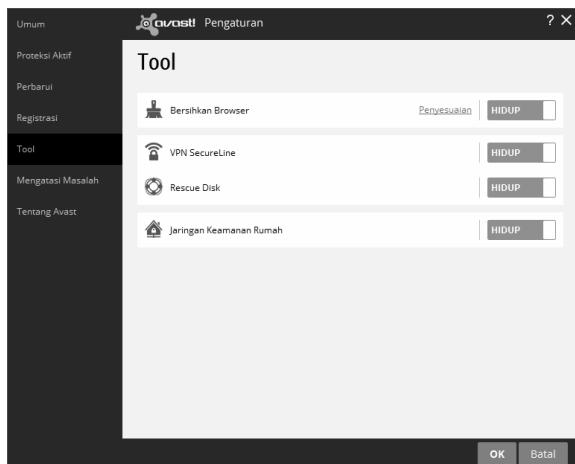
Gambar 1.61 Pemindaian menjadi presisi dengan update definisi virus

34. Di Registrasi, Anda bisa me-registrasi akun untuk mengaktifkan fitur-fitur komersil.



Gambar 1.62 Halaman Registrasi dari pengaturan AVAST

35. Di Tool, Anda bisa melihat tool-tool yang tersedia, dan apakah tool tersebut hidup/aktif atau tidak.



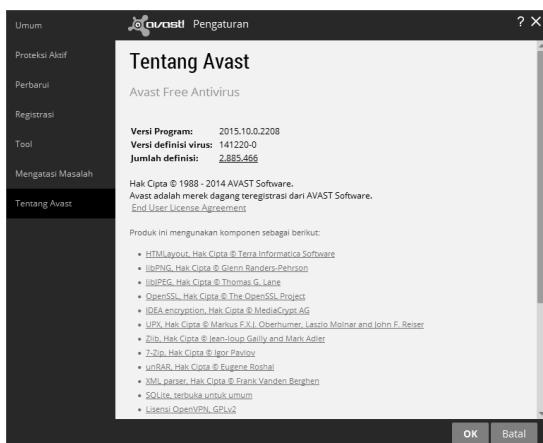
Gambar 1.63 Pengaturan Tool di AVAST

36. Di Mengatasi Masalah, Anda bisa mengatur kontrol-kontrol, seperti apakah akan mengaktifkan pemindaian rootkit di startup sistem, mengaktifkan akses disk, dan mengaktifkan modul Self-defense pada AVAST.



Gambar 1.64 Bagian Mengatasi masalah

37. Di Tentang AVAST, Anda bisa melihat informasi mengenai produk AVAST ini, termasuk versi definisi virus dan jumlah virus yang dikenali di Jumlah Definisi.



Gambar 1.65 Halaman Tentang AVAST

1.2 CLAM Win AV

Anti virus kedua untuk membasmi virus dengan definisi virus yang terus di-update sampai sekarang adalah CLAMWIN. Ini adalah software open source yang sudah dikembangkan sejak dulu secara open source, dan definisi virusnya tetap up to date. Anda bisa men-download CLAM WIN AV ini dari url <http://www.clamwin.com/content/view/18/46/>.



Gambar 1.66 Halaman utama untuk CLAMWIN AV

1.2.1 Menginstal Clam Win AV

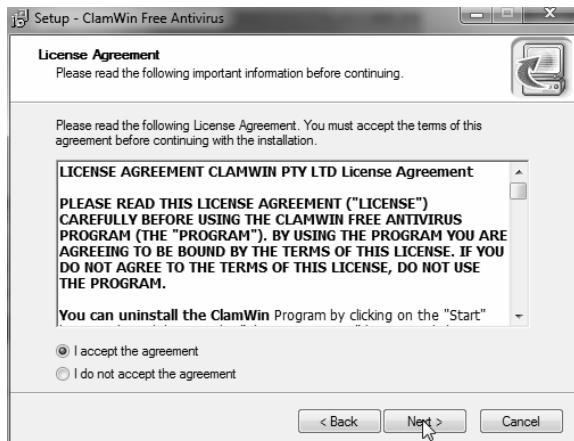
Setelah di-download, Anda perlu menginstalnya terlebih dahulu karena sifat AV ini harus diinstal, dan bukan aplikasi portabel. Tahapan instalasinya seperti ini:

1. Eksekusi file installer ClamWin Free AV.
2. Pertama muncul halaman Welcome to the CLAMWINFree AV Setup Wizard, klik Next.



Gambar 1.67 Welcome to the Clam Win Free AV

3. Muncul License Agreement, klik I accept the Agreement, kemudian klik Next.



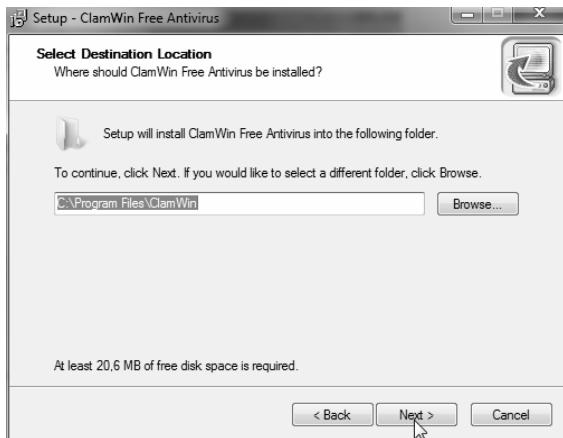
Gambar 1.68 Jendela License Agreement

4. Di **Select Installation Options**, Anda bisa memilih opsi **Anyone who uses this computer (all users)** agar semua user yang bisa memakai program ini.



Gambar 1.69 Select Installation Options

5. Pilih lokasi instalasi di Select Destination Location, klik Next.



Gambar 1.70 Pemilihan lokasi instalasi di Select Destination Location

6. Pilih komponen yang akan diinstal di **Select Components**.



Gambar 1.71 Pilih komponen Select Components

7. Di Select Start Menu Folder, pilih nama folder untuk start menu.



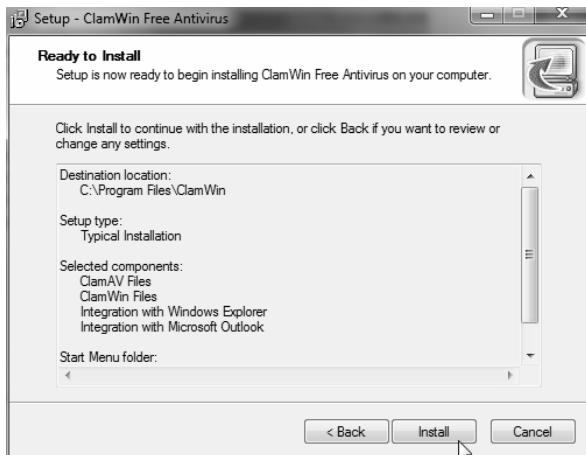
Gambar 1.72 Pemilihan nama folder untuk start menu

8. Kalau mau membuat shortcut di desktop, cek pada Additional Icons pada Create a desktop icon, klik **Next** kemudian.



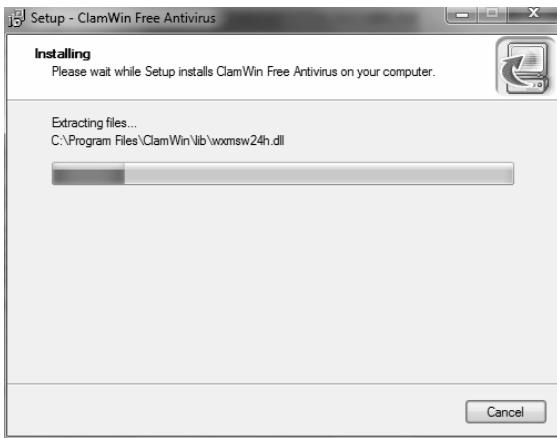
Gambar 1.73 Select Additional Tasks

9. Di Ready to Install, Anda bisa melihat rekap instalasi, klik Install untuk memulai menginstal.



Gambar 1.74 Ready to install

10. Tunggu hingga proses instalasi selesai.



Gambar 1.75 Proses instalasi tengah berlangsung

11. Setelah proses selesai, klik Finish untuk menutup proses instalasi.



Gambar 1.76 Akhir proses instalasi

1.2.2 Scan Drive dan Folder

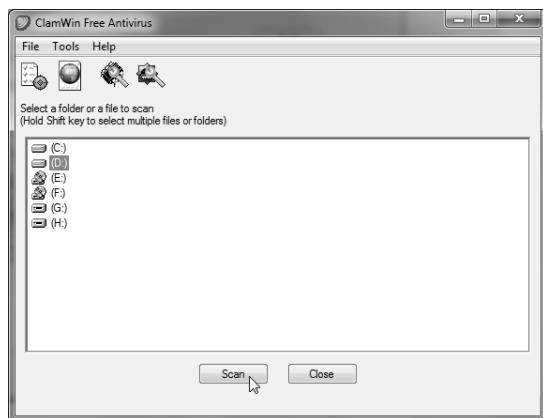
Setelah terinstal, Anda bisa langsung memakai Clam Win AV untuk memindai virus di komputer Anda. Untuk memindai ada beberapa variasi. Yang pertama adalah memindai drive, caranya seperti berikut ini:

1. Jalankan ClamWin AV, terlihat jendela utama seperti berikut:



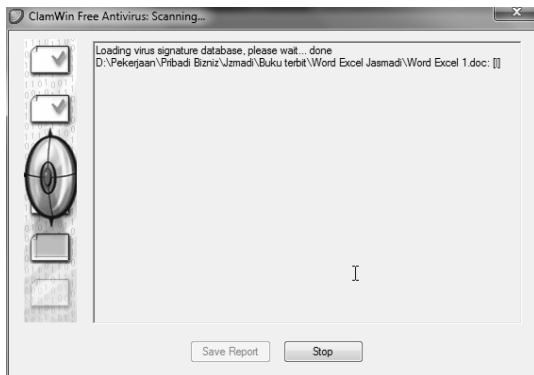
Gambar 1.77 Jendela utama ClamWin AV

2. Anda bisa memindai drive dengan klik pada drive yang akan dipindai untuk mengecek apakah ada virusnya atau tidak, kemudian klik Scan.



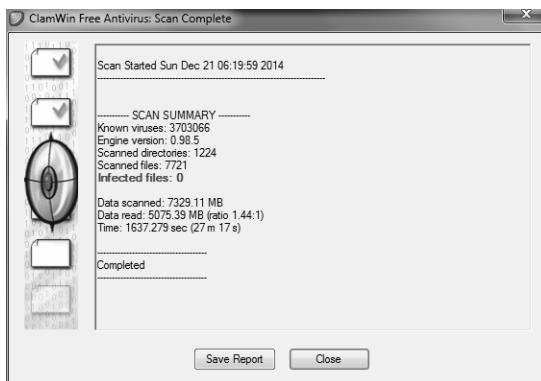
Gambar 1.78 Klik Scan setelah dipilih drive D

3. Tunggu hingga semua isi drive akan dipindai.



Gambar 1.79 Semua drive dipindai

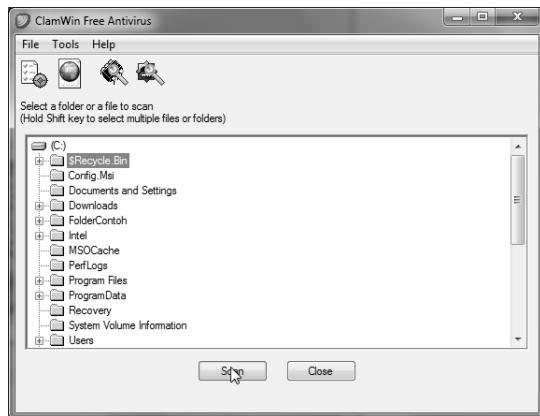
- Hasilnya terlihat seperti berikut, kalau ada yang terinfeksi virus, Anda bisa melihatnya di **Infected files**.



Gambar 1.80 Memilih di Infected Files

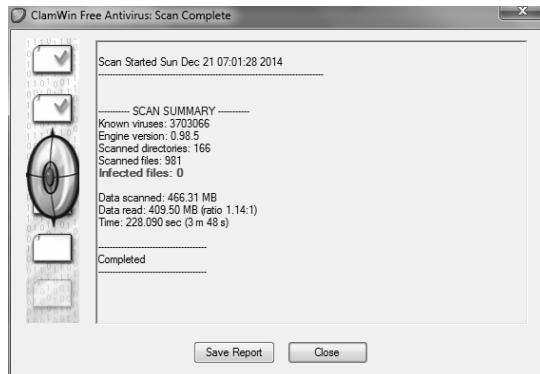
Untuk memindai folder, caranya seperti berikut:

- Klik pada drive yang menampung folder, maka drive tersebut akan menampilkan isi folder-folder di dalamnya.
- Klik pada salah satu folder yang akan dipindai.



Gambar 1.81 Klik pada salah satu folder

3. Hasil pemindaian folder nanti ditampilkan di halaman Scan Complete.

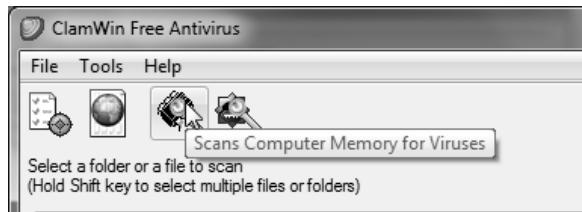


Gambar 1.82 Hasil pemindaian folder

1.2.3 Scan Memory

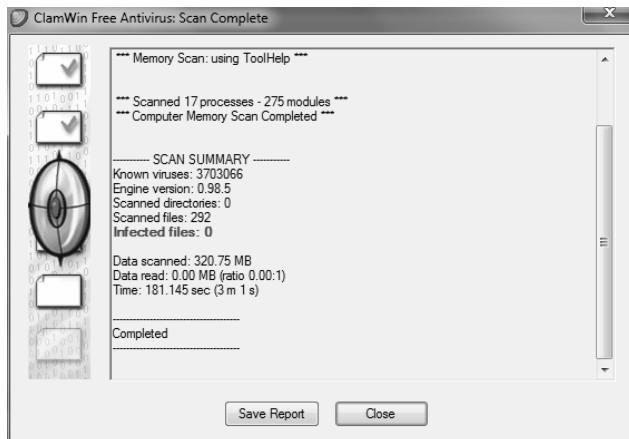
Virus kadang bercokol di memory, Clam Win AV memiliki fasilitas pemindaian memori untuk melihat apakah ada virus di memori. Caranya seperti ini:

1. Klik pada tombol Scans Computer Memory for viruses seperti di gambar berikut ini:



Gambar 1.83 Klik pada tombol Scan Computer Memory for viruses

2. Tunggu hingga semua bagian di memori diinstal, hasilnya muncul di halaman Scan Complete.

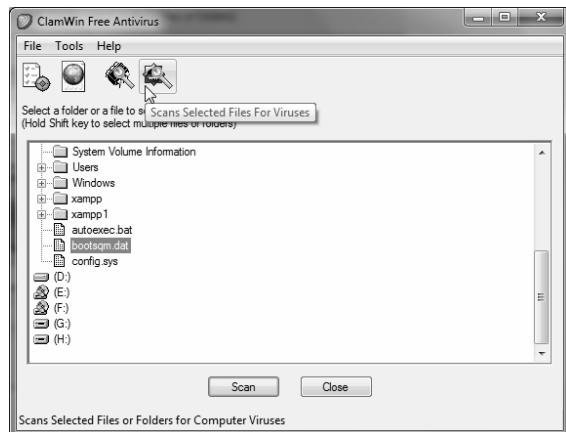


Gambar 1.84 Klik di Scan Complete

1.2.4 Scan File Tertentu

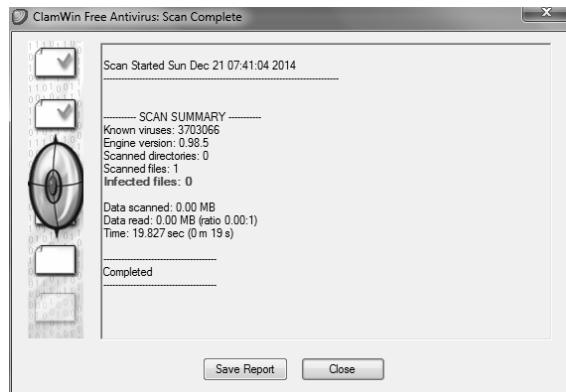
File tertentu saja bisa dipindai dengan cara seperti berikut:

1. Pilih file yang akan dipindai di explorer. Pilih drive, folder sampai file-nya terlihat.



Gambar 1.85 Pemilihan file di explorer

2. Kalau file sudah dipindai, Anda bisa melihat hasilnya apakah terinfeksi atau tidak.

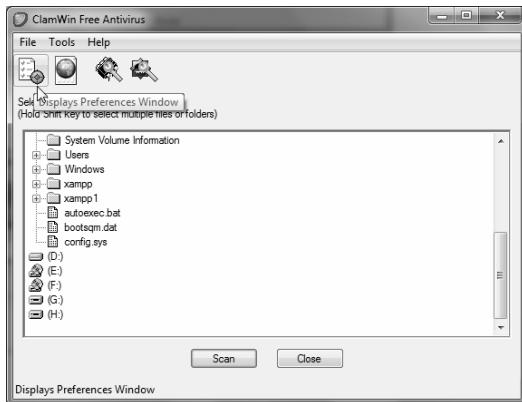


Gambar 1.86 Laporan hasil pemindaian

1.2.5 Pengaturan ClamWin

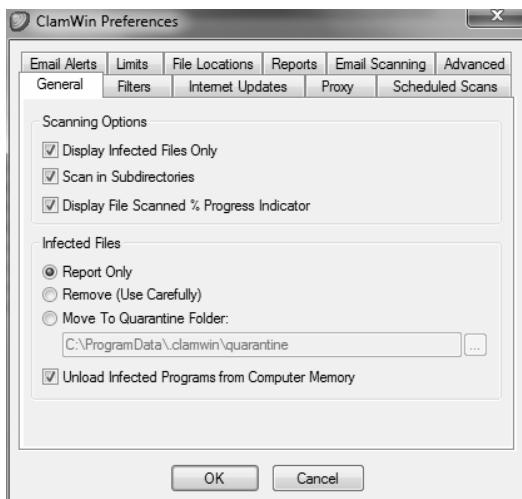
Agar pemindaian optimal dan efektif sesuai kebutuhan, Anda bisa mengkostumisasi clamWin dengan mengutak atik jendela Preferenes. Caranya seperti ini:

1. Klik pada tombol Display Preferences Window.



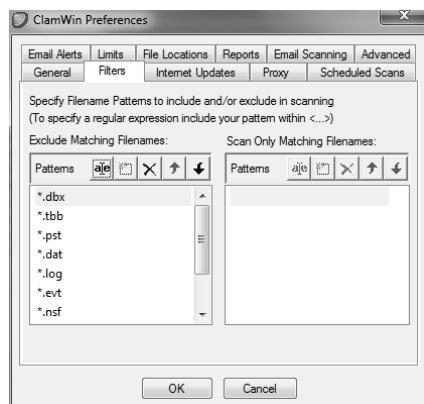
Gambar 1.87 Klik pada Display Preferences Window

2. Muncul jendela ClamWin Preferences. Klik tab General untuk melakukan pengaturan umum, Anda bisa mengatur opsi pemindaian di Scanning Options, dan action apa yang akan diambil untuk file yang terinfeksi di Infected Files.



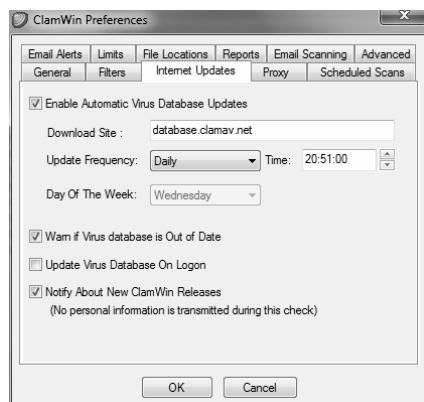
Gambar 1.88 Pengaturan General

3. Di tab Filters, Anda bisa mengatur tipe file yang akan dipindai, apakah semuanya atau ada yang dikecualikan di bagian **Exclude matching filenames**.



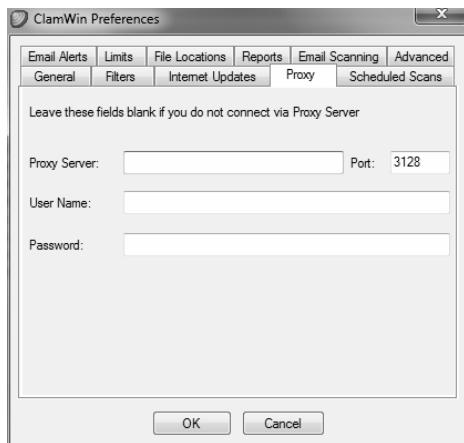
Gambar 1.89 Tab Filters untuk menyaring pemindaian virus di clam AV

4. Di **Internet Updates**, Anda bisa menentukan kapan meng-update database virus. Agar clam AV optimal, Anda harus meng-update terus definisi virus, tapi pastikan koneksi Anda mencukupi, misalnya kalau menggunakan koneksi unlimited, Anda bisa meng-update definisi virus harian dengan memilih Daily di **Update Frequency**.



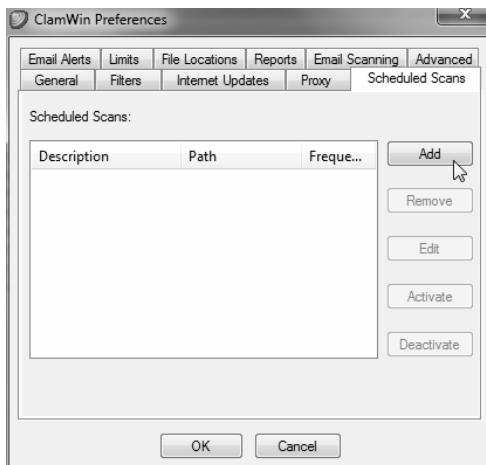
Gambar 1.90 Pengaturan update

5. Di **Proxy**, Anda bisa memasukkan proxy untuk terhubung ke internet. Dikosongkan jika Anda tidak menggunakan proxy.



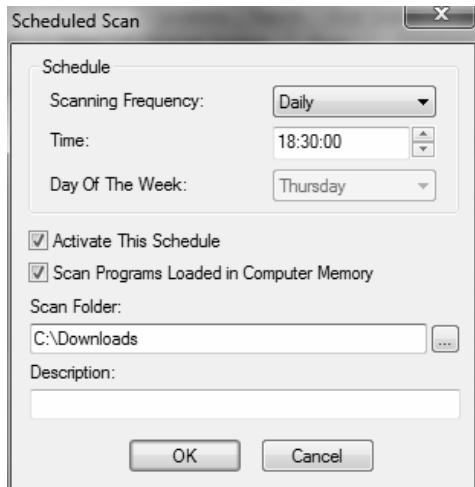
Gambar 1.91 Pengisian proxy server

6. Di **Scheduled Scans**, Anda bisa menambahkan pemindaian terjadwal. Klik **Add** untuk menambahkan jadwal pemindaian yang akan dieksekusi sesuai jadwal.



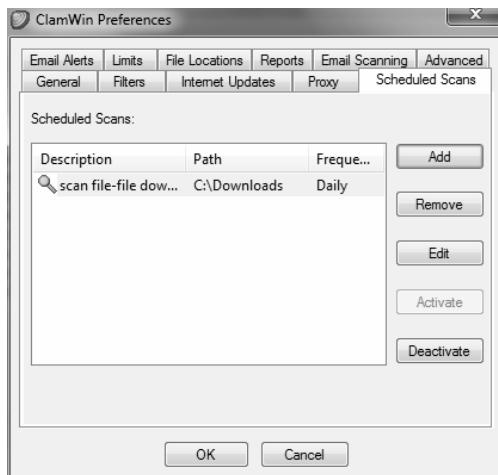
Gambar 1.92 Klik Add untuk menambahkan pemindaian terjadwal

7. Tentukan frekuensi pemindaian, dan waktu serta folder yang akan dipindai pada jendela **Scheduled Scan**.



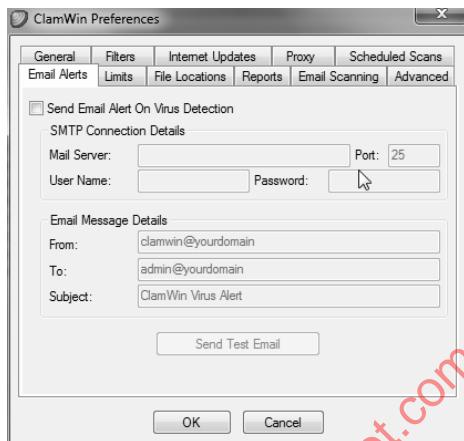
Gambar 1.93 Pemindaian folder

8. Klik OK maka jadwal pemindaian muncul di **Scheduled Scans**.



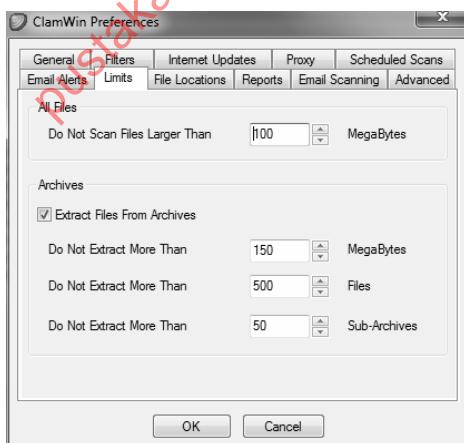
Gambar 1.94 Jadwal pemindaian ada di Scheduled Scans

9. Di Email Alerts, Anda bisa menentukan apakah mau mengirimkan email tiap kali ada pendekripsi virus. Anda bisa menentukan detil mail server yang dipakai, serta subject dan pengirimnya.



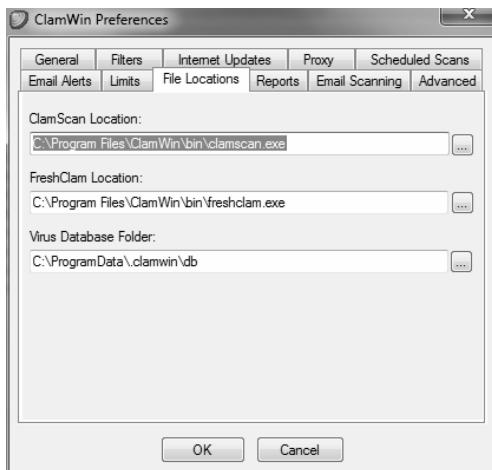
Gambar 1.95 Pengisian informasi di Email Alerts

10. Di Limits, Anda bisa menentukan ukuran maksimal file yang tidak dipindai untuk mempercepat proses pemindaiannya, serta ukuran untuk tidak mengekstrak arsip dengan ukuran tertentu.



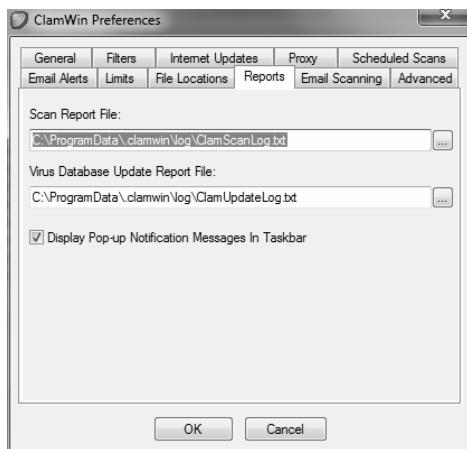
Gambar 1.96 Limits untuk membatasi pemindaian

11. Di File Location, Anda bisa melihat lokasi dari komponen-komponen software ini. Kalau tidak diubah, tidak perlu diganti.



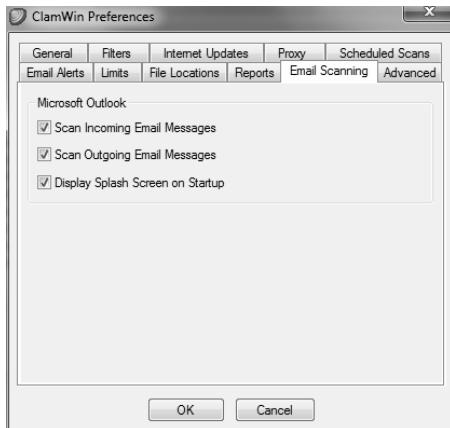
Gambar 1.97 Pengaturan lokasi komponen pemindaian

12. Di Reports Anda bisa menentukan dimana akan menyimpan laporan hasil pemindaian virus.



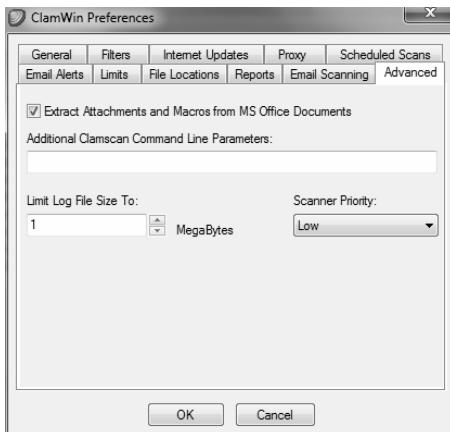
Gambar 1.98 Menentukan lokasi laporan pemindaian virus

13. Di Email Scanning, Anda bisa melihat software mail client yang akan dipindai, beserta bagian-bagiannya yang akan dipindai.



Gambar 1.99 Email scanning

14. Di Advanced, Anda bisa melihat pengaturan tambahan, seperti apakah akan mengekstrak attachment dan macro dari dokumen MS Office ketika hendak memindai dokumen tersebut untuk melihat apakah ada virusnya atau tidak.



Gambar 1.100 Pengaturan Advanced

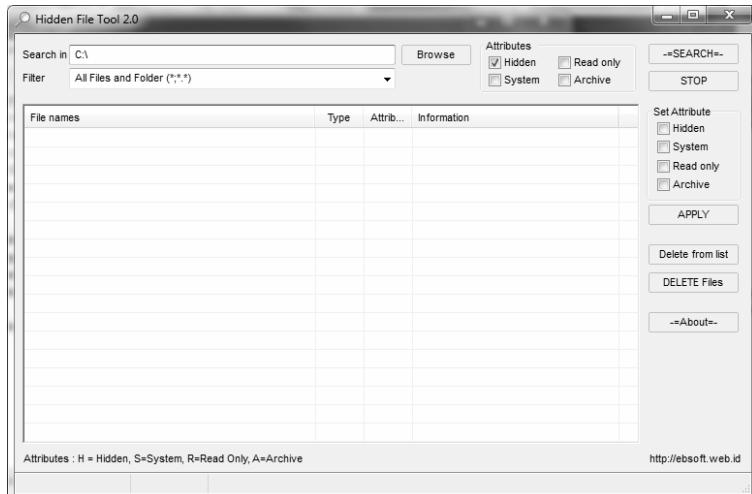
1.3 Hidden File Tool

Virus atau malware, kadang bersembunyi menggunakan atribut file hidden, sehingga tidak terlihat di Explorer. Karena itu Anda perlu menggunakan Hidden file tool adalah tool gratisan untuk mendeteksi dan mengedit file yang tersembunyi.

Hebatnya software ini dibuat oleh programmer Indonesia dari Jogjakarta yang bernama mas Ebta. Untuk memperoleh software ini, Anda bisa memperolehnya dari <http://ebsoft.web.id/download/hidden-file-tool/>

Cara menggunakan hidden file tool buatan ebsoft.web.id ini adalah seperti berikut:

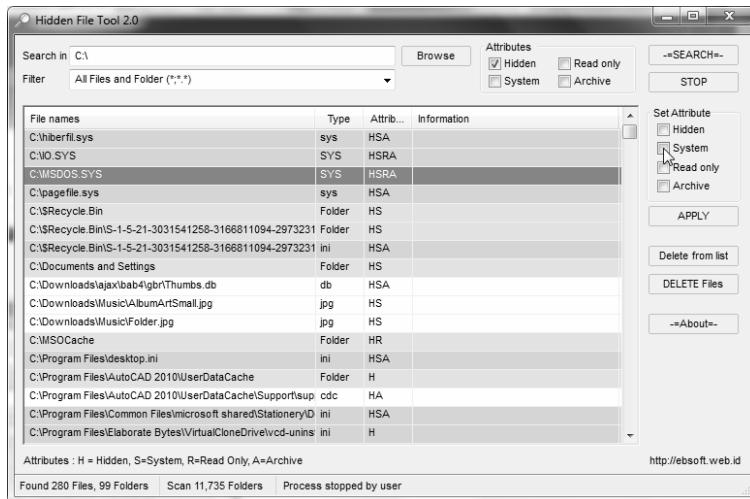
1. Setelah terdownload, langsung ekstrak file exe yang ada di dalamnya. File ini adalah file portable sehingga bisa langsung dipakai tanpa menginstal.
2. Tentukan drive yang akan menjadi tempat pencarian di **Search in**. Kalau mau mengubah, klik di **Search in**.



Gambar 1.101 Tampilan awal Hidden file tool 2.0

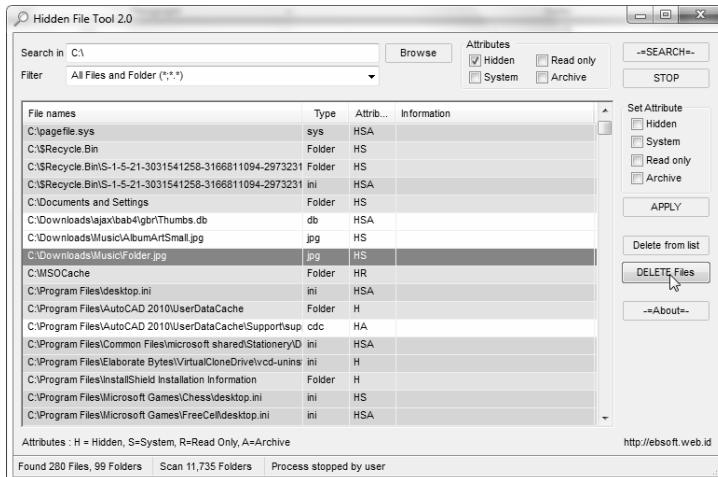
3. Klik **Search** untuk memulai pencarian.
4. Anda bisa klik **Stop** kalau mau menghentikan pencarian.

5. Anda bisa membuat atribut baru untuk file hidden ini di **Set attribute**.



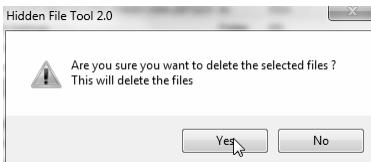
Gambar 1.102 Set attribute untuk mengubah atribut hasil pencarian

6. Anda bisa menghapus file dengan klik **Delete files** setelah memilih file tersebut.



Gambar 1.103 Menghapus file hidden dengan klik Delete files

7. Sebelum terhapus, ada konfirmasi **Are you sure you want to delete the selected files**, klik **Yes**.



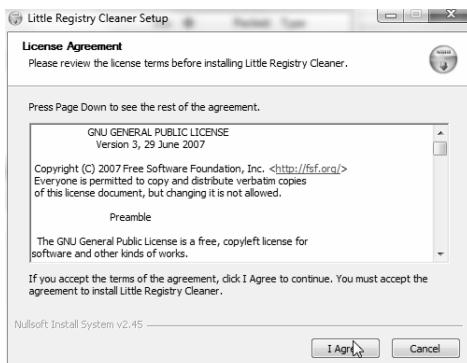
Gambar 1.104 Konfirmasi penghapusan file

1.4 Little Registry Cleaner

Registry juga dapat menjadi ancaman keamanan karena bisa menjadi tempat pendukung persembunyian virus, karena file-file virus biasanya juga melibatkan registry di dalamnya. Untuk itu Anda bisa mengecek registry Anda menggunakan Little Cleaner, yang merupakan software ringkas dan kecil untuk pembersihan registry.

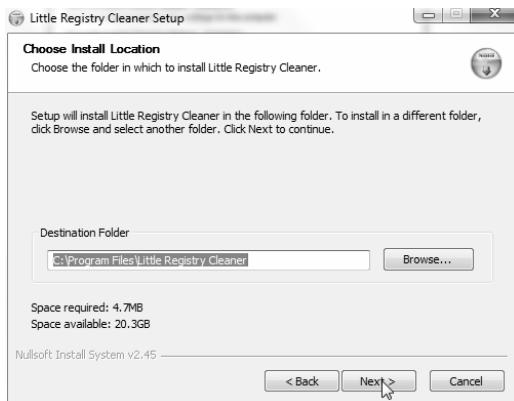
Software ini bisa didapat dari <http://sourceforge.net/projects/littlecleaner>, dimana menginstal dan memakainya seperti berikut:

1. Klik 2x pada installer Little Cleaner. Software ini open source, sehingga license agreementnya memakai GNU GPL. Klik **I agree** untuk melanjutkan ke langkah selanjutnya.



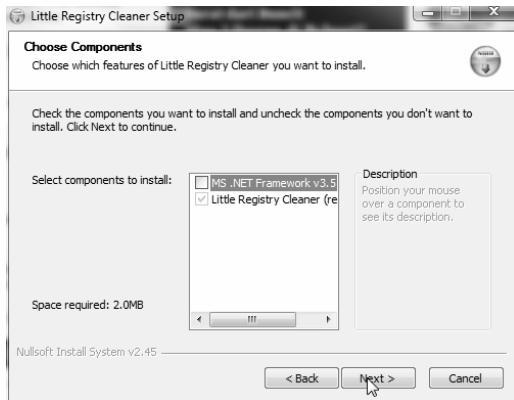
Gambar 1.105 License agreement dari Little cleaner

2. Lokasi instalasi ditentukan di **Choose install location**. Klik Next.



Gambar 1.106 Penentuan lokasi instalasi di Choose install location

3. Jika Anda belum memiliki net framework di komputer, cek pada MS Net framework di **components**. Kalau sudah, cek bisa dilepas, klik **Next** kemudian.



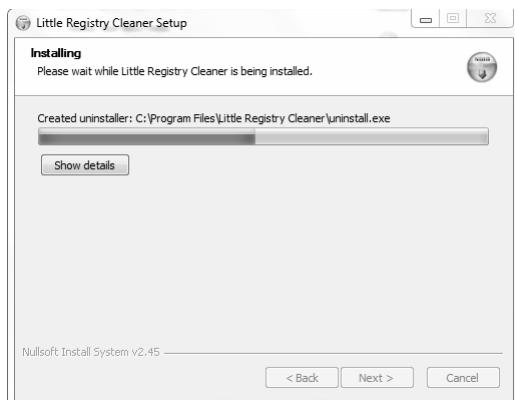
Gambar 1.107 Pemilihan komponen untuk instalasi

4. Tentukan nama untuk start menu di **Choose start menu folder**. Klik Next.



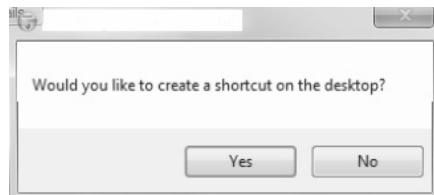
Gambar 1.108 Choose start menu folder

5. Installing untuk memindahkan file **Little Cleaner** ke hard disk.



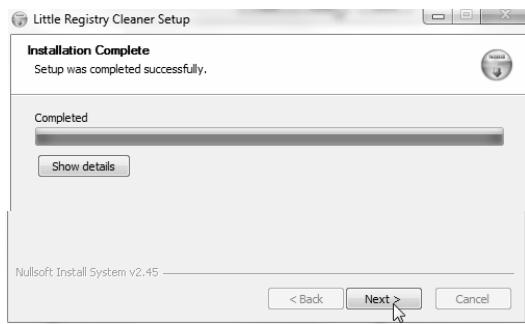
Gambar 1.109 Little cleaner ke hard disk

6. Tentukan apakah Anda ingin membuat shortcut di desktop dengan klik **Yes** di kotak konfirmasi **Would you like to create a shortcut on the desktop?**.



Gambar 1.110 Would you like to create a shortcut on the desktop

7. Tunggu hingga selesai instalasi, kalau sudah complete, klik **Next**.



Gambar 1.111 Instalasi sudah lengkap

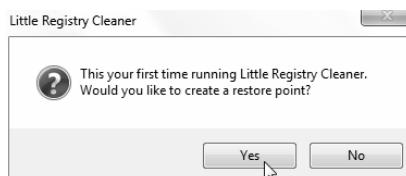
8. Klik **Finish** di **Completing the little registry cleaner setup wizard**.



Gambar 1.112 Akhir proses instalasi

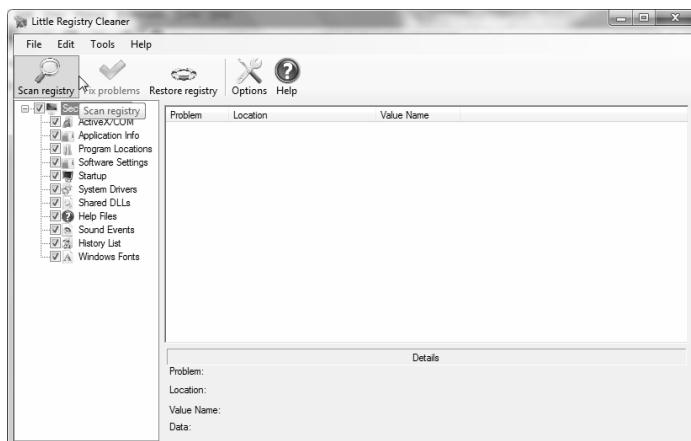
Kalau sudah terinstal gunakan Little Registry Cleaner untuk membetulkan registry di komputer Anda:

1. Jalankan Little Registry cleaner dari start menu. Kalau pakai Windows 8 langsung cari Little registry Cleaner dari ikon di Start Screen.
2. Ketika pertama kali dijalankan, ada pemberitahuan **This is your first time running LRC, would you like to create a restore point**. Klik **Yes** untuk membuat restore point. Ini penting untuk mengembalikan kondisi setelah di-restore.



Gambar 1.113 Konfirmasi pembuatan restore point

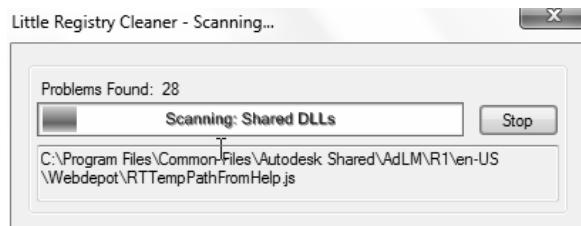
3. Tampilan utama halaman Little registry cleaner seperti berikut, klik **Scan registry** untuk memindai registry.



Gambar 1.114 Scan registry untuk memindai registry

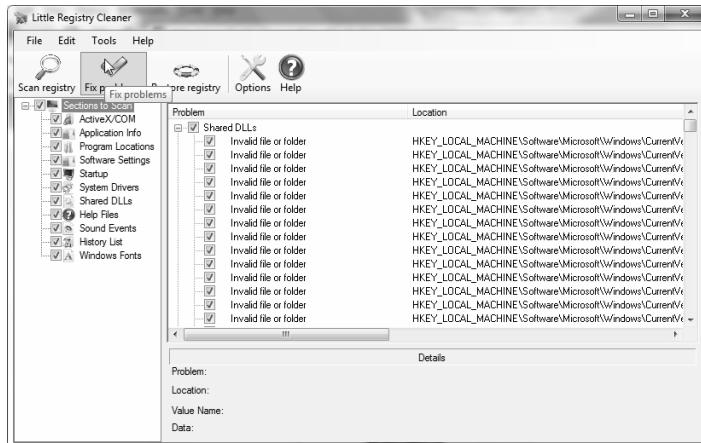
4. Klik **Scan** untuk memindai.

5. Proses scanning akan berlangsung.



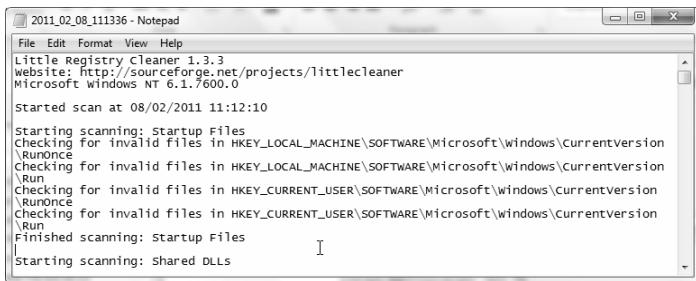
Gambar 1.115 Proses scanning akan berlangsung

6. Semua ancaman di registry akan ditampilkan, klik pada **Fix problems** untuk memperbaiki semua masalah.



Gambar 1.116 Klik pada **Fix problems** untuk membetulkan masalah di registry

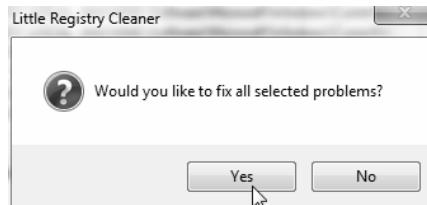
7. Muncul tampilan notepad membuka file log yang berkaitan dengan item-item di registry yang telah dicek.



2011_02_08_111336 - Notepad
File Edit Format View Help
Little Registry Cleaner 1.3.3
website: http://sourceforge.net/projects/littlecleaner
Microsoft Windows NT 6.1.7600.0
Started scan at 08/02/2011 11:12:10
Starting scanning: Startup Files
Checking for invalid files in HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Checking for invalid files in HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
Checking for invalid files in HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
Finished scanning: startup Files
Starting scanning: Shared DLLs

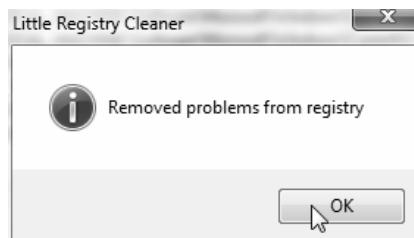
Gambar 1.117 Item-item di registry yang sudah dicek di pemindaian pertama

8. Muncul konfirmasi, **Would you like to fix all selected problems**, klik **Yes**.



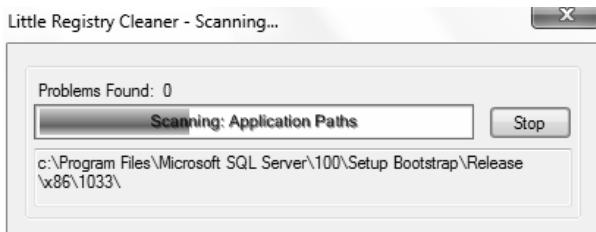
Gambar 1.118 Konfirmasi untuk membetulkan semua masalah di registry

9. Kalau semua masalah sudah beres, muncul kotak notifikasi seperti berikut. Klik **OK**.



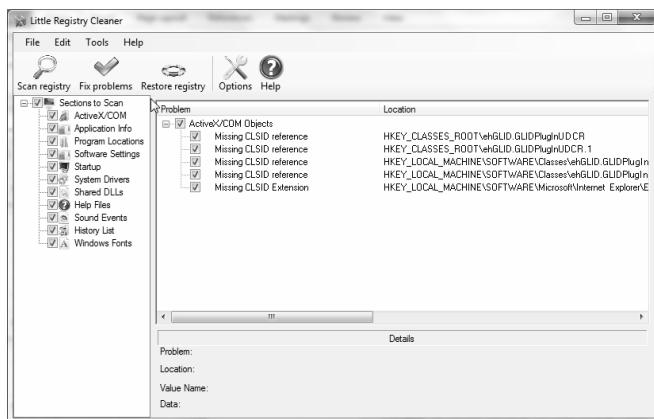
Gambar 1.119 Semua masalah sudah beres

10. Berikutnya little registry cleaner akan memindai lagi, untuk melihat adanya masalah lain di item lain.



Gambar 1.120 Pemindaian kedua

11. Dengan cara yang sama, Anda bisa melakukan pembersihan terus menerus. Karena itu masalah tidak langsung beres dalam satu pemindaian, tapi bisa beberapa kali pemindaian.



Gambar 1.121 Hasil pemindaian kedua

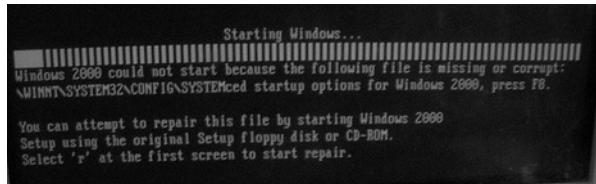
12. Kalau sudah klik Exit, ketika muncul konfirmasi, klik Yes.



Gambar 1.122 Are you sure want to exit

Jika komputer Anda tidak bisa restart, maka registry kemungkinan korup. Ada beberapa pesan error yang muncul. Beberapa contohnya seperti berikut:

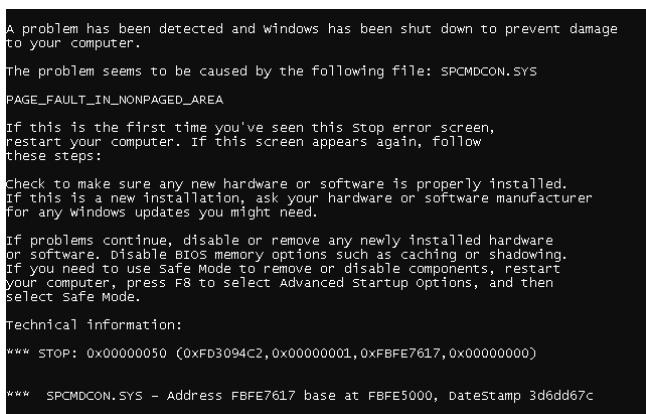
- Windows could not start because the following file is missing or corrupt:\WINNT\SYSTEM32\CONFIG\SYSTEM.ced



Gambar 1.123 Pesan kesalahan ketika gagal restart

- Windows could not start because the following file is missing or corrupt:\WINNT\SYSTEM32\CONFIG\SYSTEM
- Windows could not start because the following file is missing or corrupt:\WINNT\SYSTEM32\CONFIG\SOFTWARE

Dan juga kesalahan lainnya di blue screen of death



Gambar 1.124 Pesan kesalahan di Blue screen of death

- Stop 0xc0000218 (0xe11a30e8, 0x00000000, 0x00000000, 0x00000000) UNKNOWN_HARD_ERROR

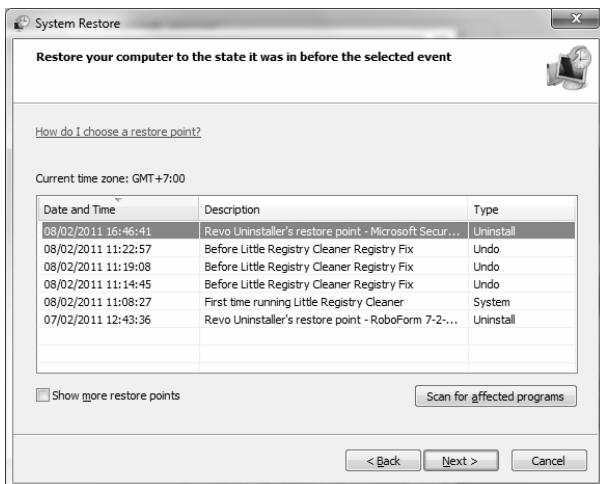
- Stop: 0xc0000218 {Registry File Failure} The registry cannot load the hive (file): \SystemRoot\System32\Config\CorruptHive or its log or alternate. It is corrupt, absent, or not writable.

Ada banyak sebab yang bisa menyebabkan registry bisa korup selain karena adanya virus. Kebanyakan kejadian korup ini terjadi ketika komputer sedang dimatikan. Dan Anda tidak bisa melacak penyebabnya karena komputer melakukan unload pada proses dan driver selama shutdown.

Jadi lazimnya sulit untuk melacak penyebab korupnya registry. Bagian ini menjelaskan beberapa penyebab dari korupnya file registry, dan langkah-langkah untuk menegahnya.

1. Kegagalan Listrik: Ini akan menyebabkan shutdown yang tidak diinginkan yang menyebabkan registry menjadi korup. Ini nantinya bisa dilihat di Event ID 6008 yang mengindikasikan bahwa ada shutdown yang tidak diinginkan. Biasanya ada proses di komputer yang memodifikasi registry, tapi proses modifikasi ini belum selesai, komputer sudah mati mendadak. Ini akan menyebabkan bagian registry akan kacau. Karena penyimpanan registry belum berjalan sempurna. Saat restart, komputer akan mencari registry tersebut, tapi karena penyimpanan belum sempurna, akan muncul pesan error berkaitan dengan registry tersebut.
2. File Korup dan Hardware Gagal: Korup kadang tidak hanya berkaitan dengan registry saja, tapi juga bisa berkaitan dengan file dan hardware. Kegagalan hardware bisa menyebabkan kegagalan registry. Biasanya hardware yang berkaitan dengan penulisan file ke disk, seperti
 - Random access memory (RAM)
 - Cache
 - Prosesor
 - Disk controller
3. Penulisan registry di shutdown: Jika ada satu atau dua registry yang korup terus menerus, maka kemungkinan masalahnya di shutdown. Jadi ada proses yang error di shutdown. Coba cek apakah Anda menginstal software baru-san.

- Untuk troubleshooting, caranya hanya me-restore komputer menggunakan fasilitas system restore. Restore akan mengembalikan kondisi ke sebelum error.



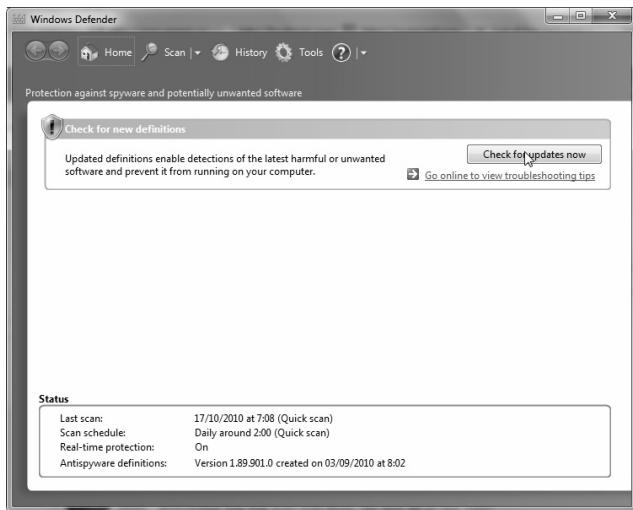
Gambar 1.125 Tampilan system restore di Windows

1.5 Windows Defender

Mulai versi Windows Vista ke atas, termasuk Windows 7 dan Windows 8 memiliki fasilitas Windows Defender yang merupakan tool inheren di Windows yang digunakan untuk memindai virus dan spyware. Windows defender ini bisa diupdate database signature-nya secara online untuk menghasilkan hasil pemindaian yang valid.

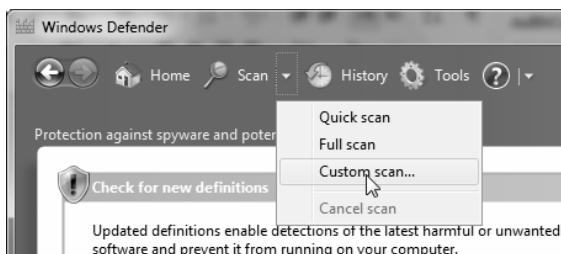
Cara menggunakan Windows Defender adalah:

- Buka **Start** kemudian ketikkan “Windows defender” di kotak teks pencarian yang ada.



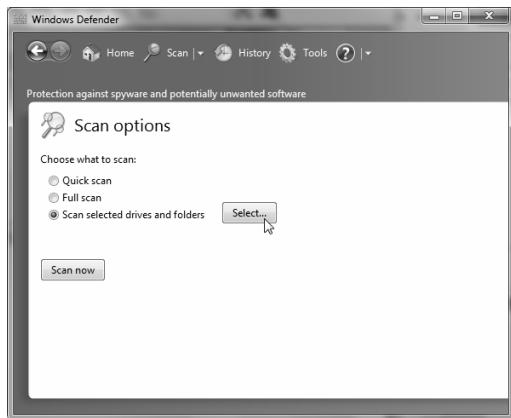
Gambar 1.126 Windows defender

2. Klik pada Tools > Custom Scan.



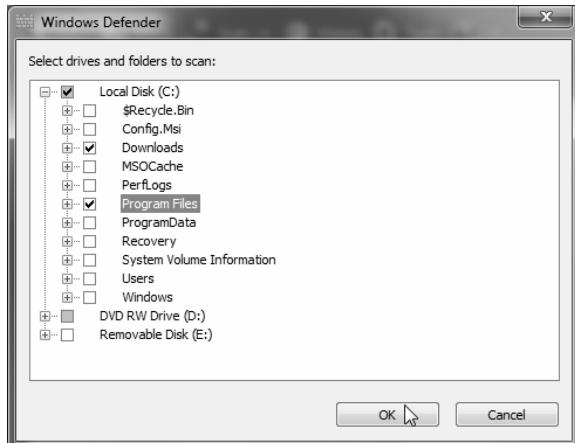
Gambar 1.127 Custom scan untuk melakukan scanning kustom

3. Anda dapat memilih drive dan folder tertentu untuk discan dengan klik pada radio button **Scan selected drives and folders**. Kemudian klik tombol **Select** di samping kanannya.



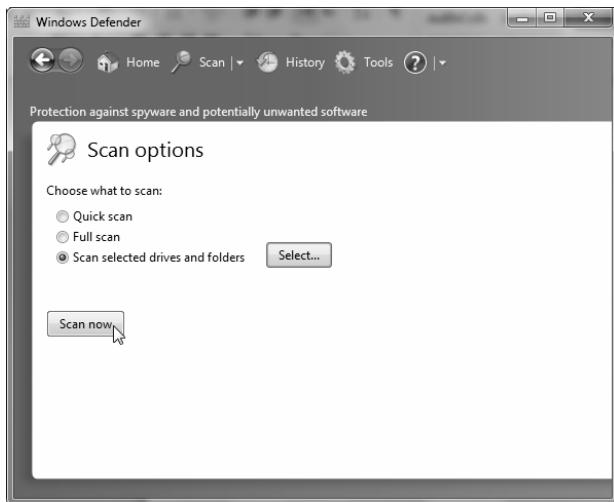
Gambar 1.128 Select untuk memilih bagian yang akan discan

4. Muncul kotak **Select drives and folders to scan**. Kemudian cek pada drive atau folder yang akan dipindai. Klik **OK**.



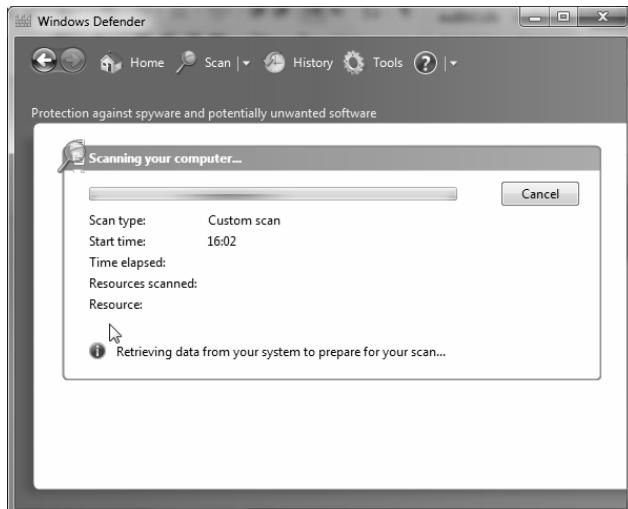
Gambar 1.129 Windows defender

5. Kembali ke **Scan options**, klik **Scan now**.



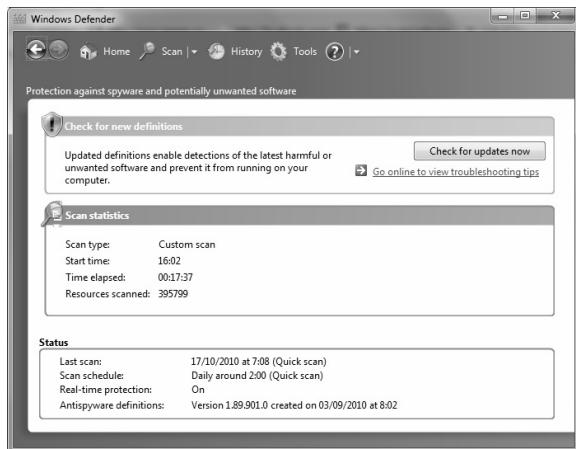
Gambar 1.130 Pengaturan scan options

6. Tunggu hingga proses scanning selesai.



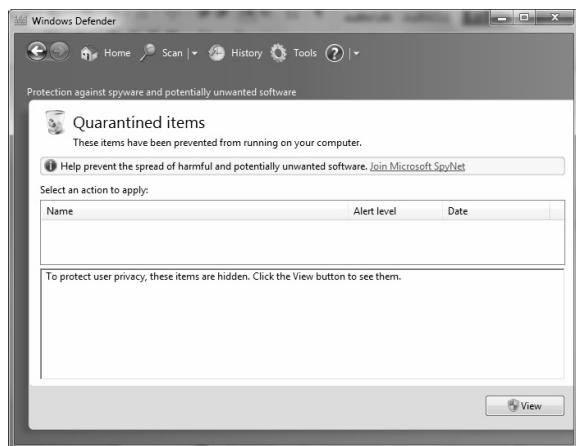
Gambar 1.131 Proses scanning sedang berlangsung

7. Hasilnya ditampilkan di **Scan statistics**.



Gambar 1.132 Hasil scan statistics

8. Jika ada hal yang mencurigakan, Anda bisa mengkarantina hal-hal tersebut. Untuk melihat item-item yang dikarantina, Anda bisa mengklik Tools > Quarantine Items.



Gambar 1.133 Quarantine items

2 ANTI SPYWARE

Spyware adalah program yang bisa mencuri informasi berharga di komputer Anda. Umumnya program ini berkaitan erat dengan internet karena memata-matai komputer Anda untuk mencari username dan password yang Anda masukkan ketika menggunakan email, atau bertransaksi di internet.

Spyware sangat berbahaya, karena itu Anda perlu beberapa tool yang akan dijelaskan di bab ini untuk menghilangkan spyware dari komputer.

2.1 SPY BOT

Spybot adalah software yang akan memindai dan menghilangkan spyware dari komputer Anda. Software ini beralamatkan di <http://www.safer-networking.org/> dan bisa di-download dari <http://www.safer-networking.org/dl/>. Anda bisa memilih salah satu mirror yang dipakai untuk men-download.

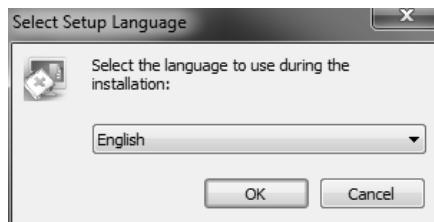


Gambar 2.1 Memilih salah satu mirror untuk men-download

2.1.1 Instalsi SpyBot

Setelah file di-download, Anda perlu meng-instal dengan menggunakan cara seperti berikut ini:

1. Eksekusi installer Spy Bot.
2. Pilih bahasa English pada tahapan Select Setup Language.



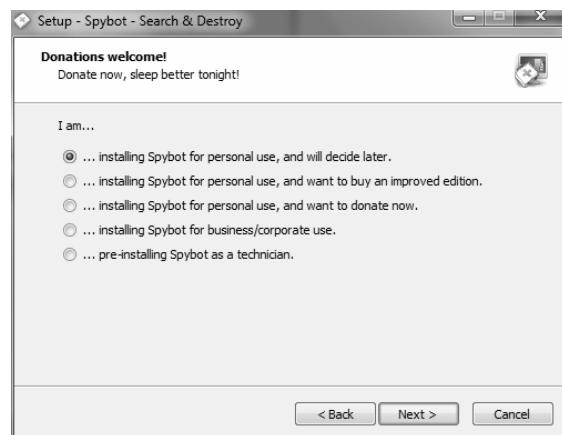
Gambar 2.2 Pemilihan bahasa untuk instalasi ke English

3. Muncul Welcome to the Spybot Setup Wizard, klik **Next**.



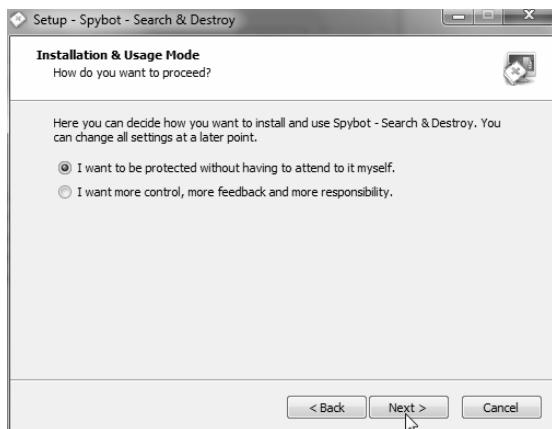
Gambar 2.3 Welcome to the SpyBot Setup Wizard

4. Pilih opsi pertama, Installing spybot for personal use, klik Next.



Gambar 2.4 Installing Spybot for personal use

5. Pilih proteksi tipe pertama di jendela Installation & Usage Mode. Kemudian klik Next.



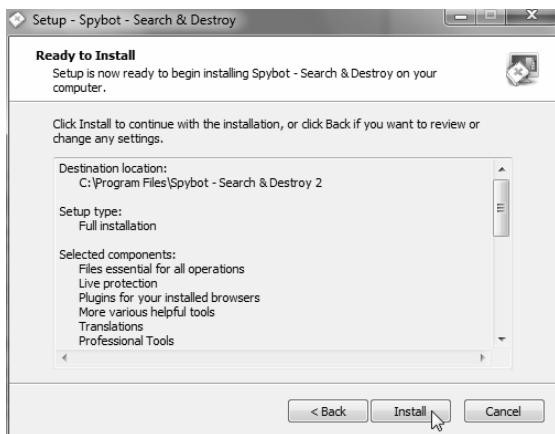
Gambar 2.5 Pemilihan mode instalasi dan penggunaan

6. Di License Agreement, klik pada I accept the agreement dan klik Next.



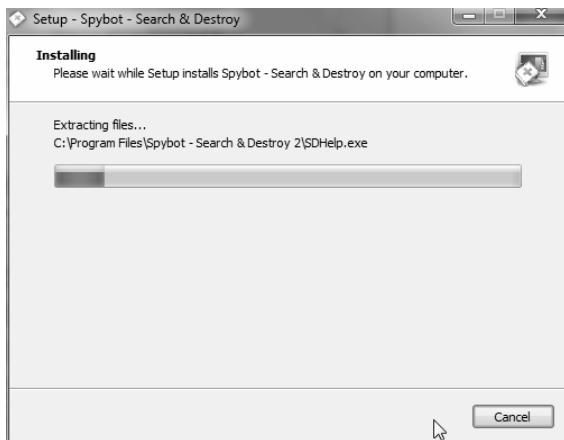
Gambar 2.6 Halaman License Agreement

7. Rekap info instalasi muncul di jendela Ready to install, klik Install untuk memulai instalasi.



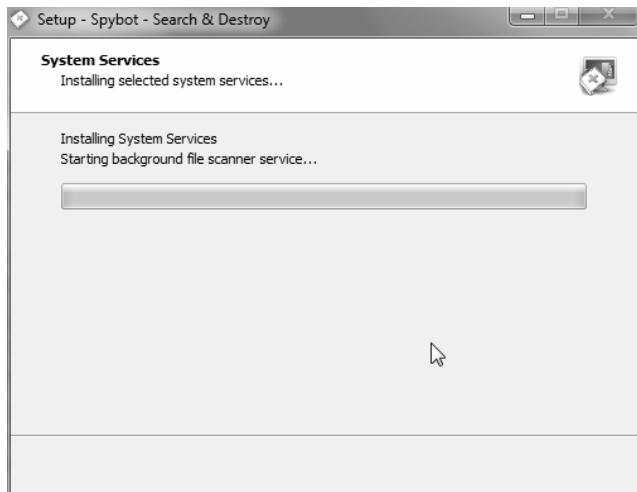
Gambar 2.7 Klik Ready to install untuk memulai instalasi

8. Tunggu hingga instalasi selesai.



Gambar 2.8 Proses instalasi berlangsung

9. Berikutnya System Service akan diinstal.



Gambar 2.9 System Service diinstal

10. Terakhir di Completing the Spybot Setup wizard, klik Finish untuk mengakhiri proses instalasi SpyBot ini.

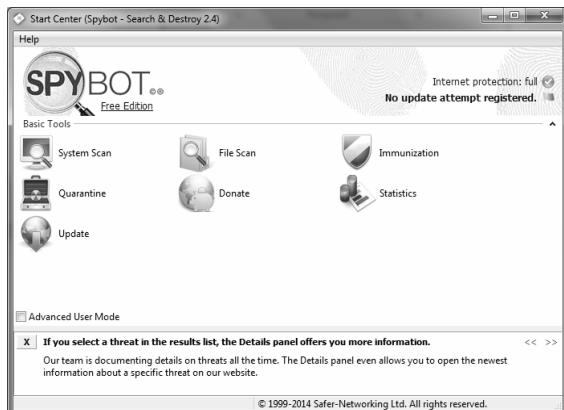


Gambar 2.10 Proses instalasi Spybot selesai

2.1.2 Memindai Spyware System Scan

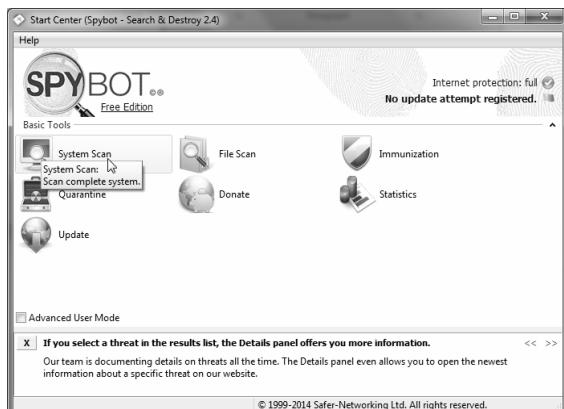
Setelah terinstal, Anda bisa memindai spyware di komputer dengan menggunakan spybot. Ada beberapa metode pertama adalah System Scan untuk memindai sistem secara keseluruhan. Caranya seperti ini:

1. Jalankan Spybot, terlihat ada tujuh tombol utama dari spybot.



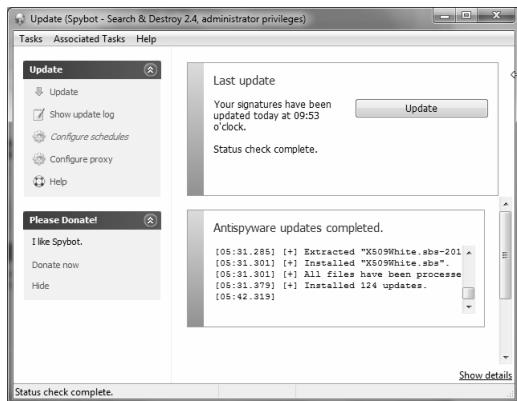
Gambar 2.11 Tujuh tombol utama spybot

2. Klik pada tombol pertama **System Scan**.



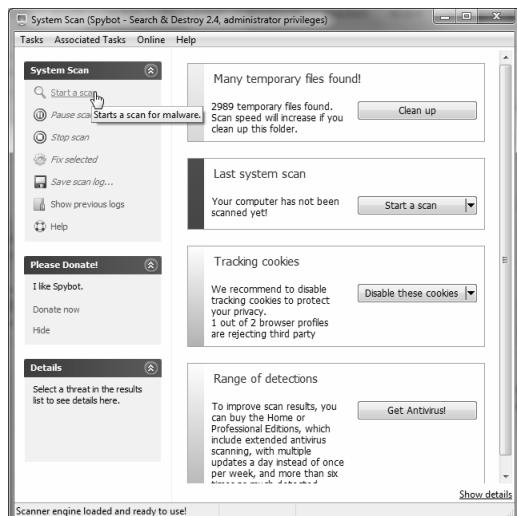
Gambar 2.12 Klik System scan

3. Muncul tampilan jendela seperti berikut. Anda klik Update dulu untuk meng-update definisi spyware supaya bisa memulai pemindaian. Kalau sudah, baru tombol **System scan** muncul.



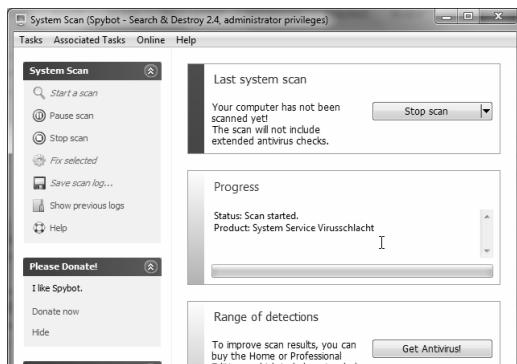
Gambar 2.13 Tampilan setelah update definisi spyware

4. Klik Start a scan untuk memulai pemindaian.



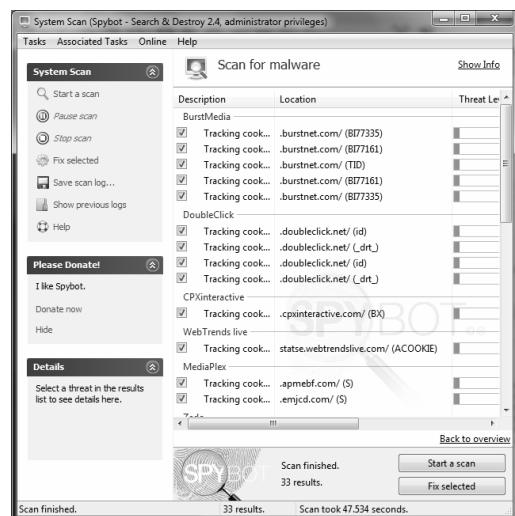
Gambar 2.14 Klik start a scan di kiri atas untuk memulai pemindaian

- Di bagian kanan tengah muncul progress bar di kotak Progress yang menjelaskan kemajuan proses pemindaian sistem untuk melihat apakah ada spyware atau tidak.



Gambar 2.15 Progress bar sistem

- Kalau sudah selesai pemindaian, hasil file-file spyware dan yang berpotensi spyware akan terlihat. Untuk menangani spyware, klik **Fix selected**.

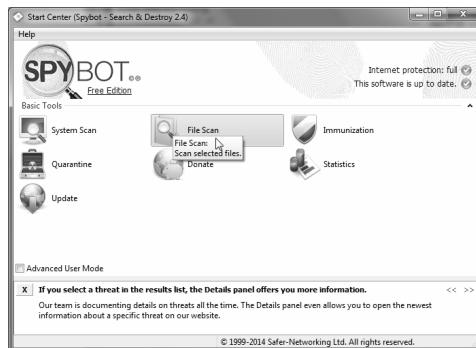


Gambar 2.16 File-file terlihat

2.1.3 File Scan

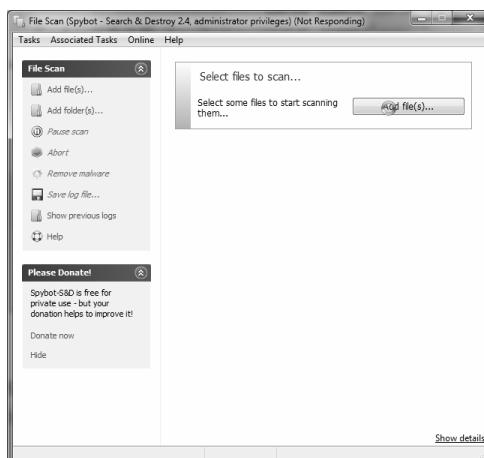
Anda juga bisa memindai file tertentu saja untuk melihat apakah ada spyware atau tidak. Caranya seperti ini:

1. Klik pada tombol File Scan di halaman utama SpyBot.



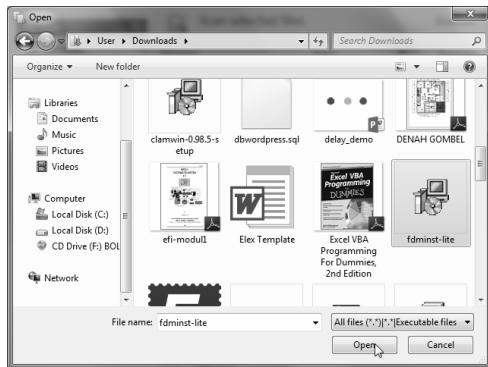
Gambar 2.17 Klik pada tombol File Scan di SpyBot

2. Muncul jendela File Scan, pilih file yang akan dipindai untuk melihat apakah file tersebut ada spyware-nya atau tidak dengan klik tombol Add File(s).



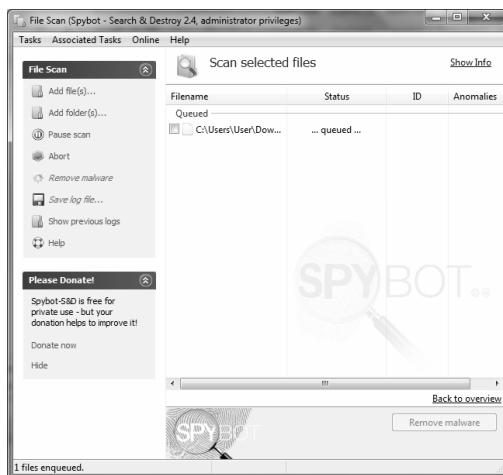
Gambar 2.18 Klik Add file(s)

- Pilih file yang akan dipindai di jendela Open, Anda bisa memilih lebih dari satu file.



Gambar 2.19 Memilih file yang akan dipindai

- Maka file tersebut akan di-queue dan tunggu sebentar untuk dipindai.



Gambar 2.20 File sedang diantrikan untuk dipindai oleh spybot

- Kalau sudah, Anda bisa melihat apakah file tersebut clean (bersih dan bebas spyware) atau ada spyware-nya.

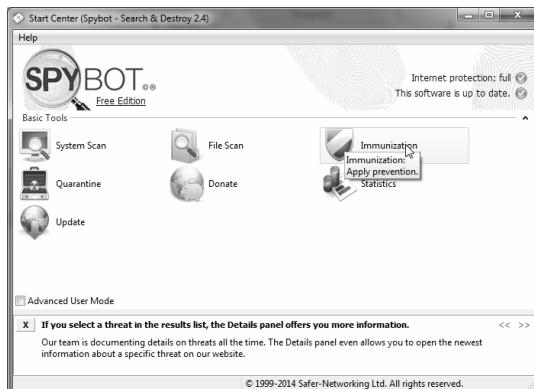


Gambar 2.21 Hasil pemindaian file

2.1.4 Immunisasi

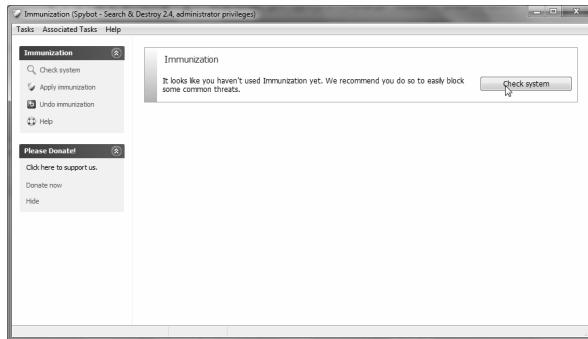
Agar sistem lebih kuat terhadap ancaman spyware, SpyBot punya fitur imunisasi yang mengubah setting komputer agar tidak mudah terinfeksi spyware. Berikut ini cara mengaktifkan fitur imunisasi:

1. Dari halaman utama SpyBot, klik Immunization.



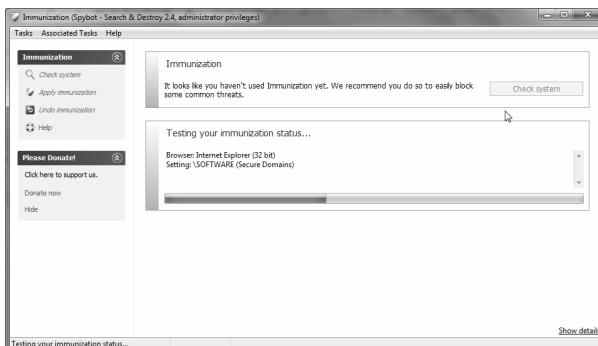
Gambar 2.22 Klik Immunization

2. Muncul jendela Immunization seperti berikut, kemudian klik tombol Check System di kanan atas.



Gambar 2.23 Klik Check System di kanan atas

3. Tunggu hingga sistem dites dan diset agar lebih imun.

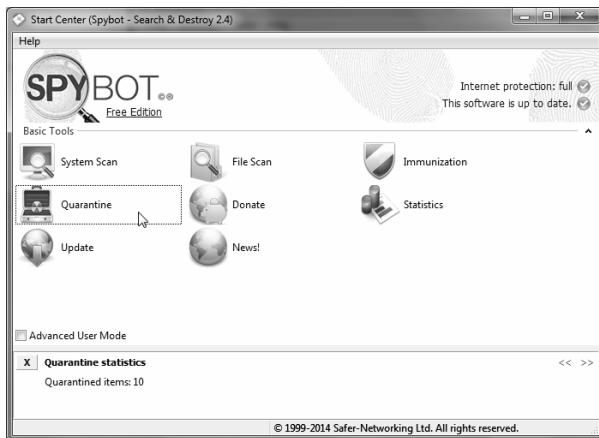


Gambar 2.24 Pengetesan dan setting komputer agar lebih imun

2.1.5 Melihat Karantina

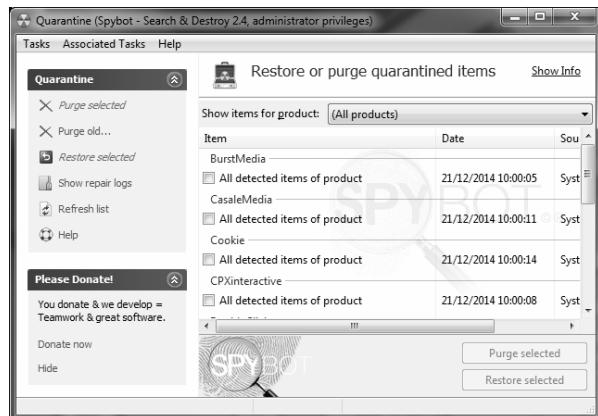
Spyware yang sudah ditangkap akan dikarantina agar tidak bisa menjalankan aksinya lagi. Untuk melihat file-file spyware yang dikarantina, caranya seperti ini:

1. Klik pada tombol Quarantine di halaman awal.



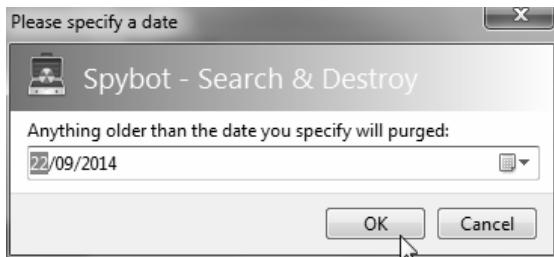
Gambar 2.25 Klik Quarantine

2. Muncul file-file yang dikarantina di bagian kanan.



Gambar 2.26 File-file yang dikarantina

3. Anda bisa menghapus file dengan mengklik **Purge Old**. Tentukan tanggal yang ingin dihapus.

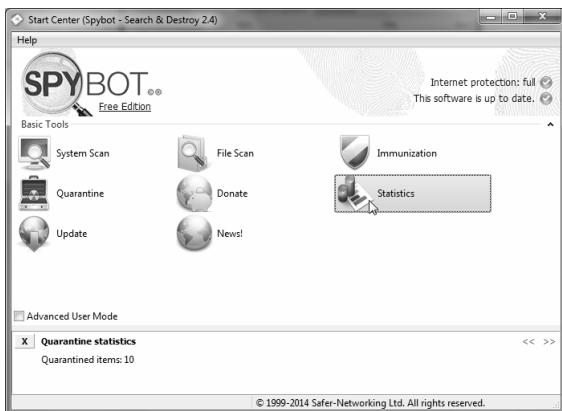


Gambar 2.27 Purge Old

2.1.6 Statistik Data

Anda bisa melihat statistik pemindaian dan action yang sudah dilakukan di spybot dengan cara seperti berikut ini:

1. Klik menu Statistics.



Gambar 2.28 Klik menu Statistics di SpyBot

2. Terlihat tampilan statistik data yang sudah dilakukan, dari mulai pemindaian sistem, pemindaian file, scan rootkit dan pemindah PhoneApp.

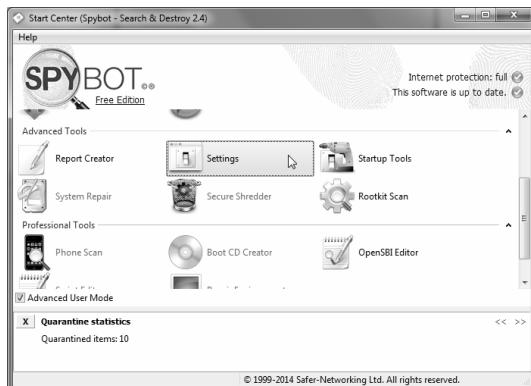
Statistics (Spybot - Search & Destroy 2.4.40.0)		
Item	Data	Details
System Scans		
Last scan	9:59	
Number of scans	1	
Detected items	33	
File Scans		
Last scan	unknown	
Number of scans	1	
Detected malware items	0	
Detected heuristic items	0	
Rootkit Scans		
Last quick scan	unknown	
Last deep scan	unknown	
Number of scans	0	
Last detected entry	n/a	
Phone App Scans		

Gambar 2.29 Statistik data

2.1.7 Pengaturan Program

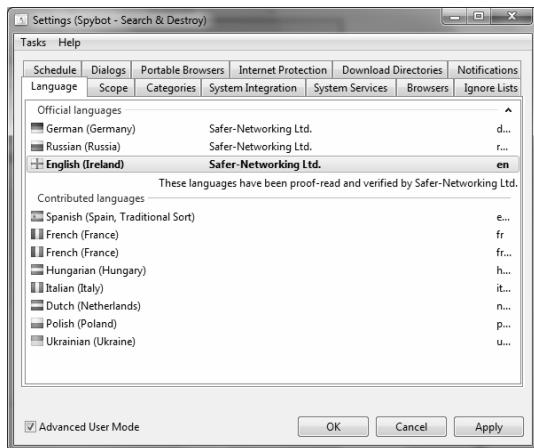
Agar pemindaian spyware optimal, Anda dapat mengatur setting program dengan cara seperti berikut ini:

1. Klik pada Settings di Spybot.



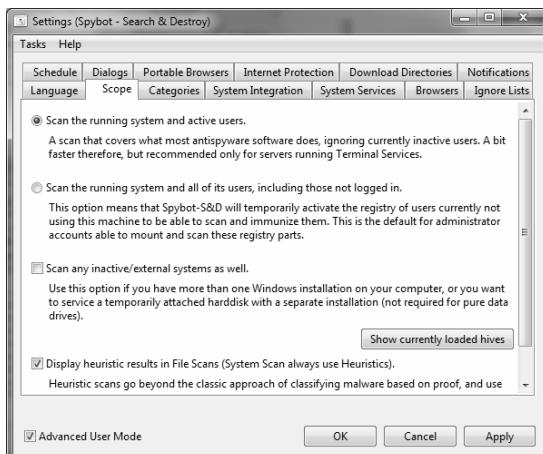
Gambar 2.30 Klik Settings di Spybot

2. Di Language, Anda bisa memilih bahasa yang akan dipakai di program SpyBot ini. Default-nya adalah English.



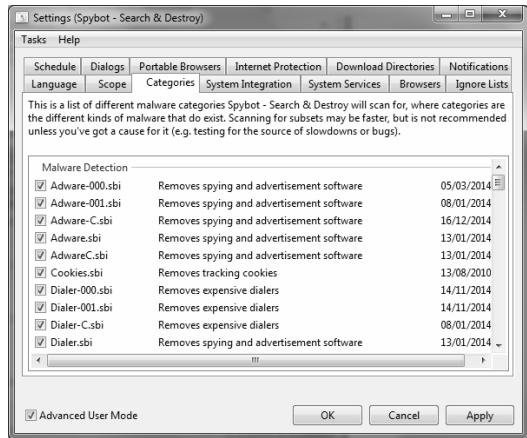
Gambar 2.31 Pemilihan bahasa di Language

3. Di **Scope**, Anda bisa mengatur ruang lingkup pemindaian spybot, apakah sistem dan user yang aktif saja, ataupun termasuk user yang sedang tidak aktif.



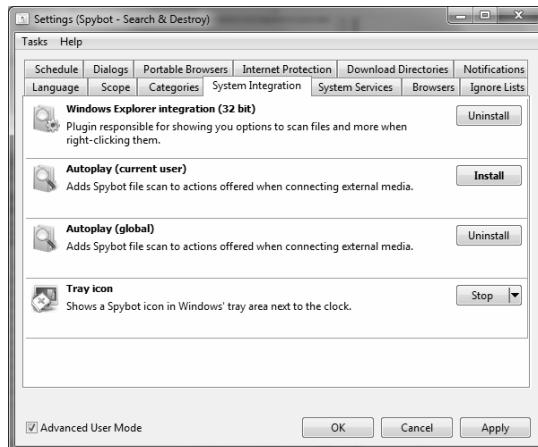
Gambar 2.32 Pengaturan ruang lingkup pemindaian

4. Di **Categories**, Anda bisa mengecek kategori spyware yang akan dipindai ada, dari mulai adware, cookies, dialer, dan lain sebagainya.



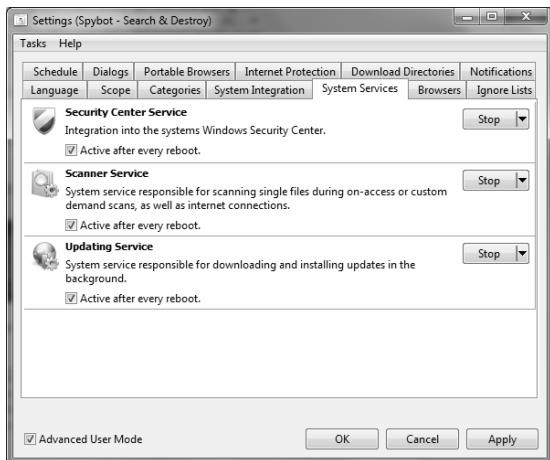
Gambar 2.33 Pengaturan kategori dari dialer

5. Di **System Integeration**, Anda bisa memasang modul integrasi agar mengintegrasikan spybot ke Explorer, AutoPLAY, atau Tray Icon.



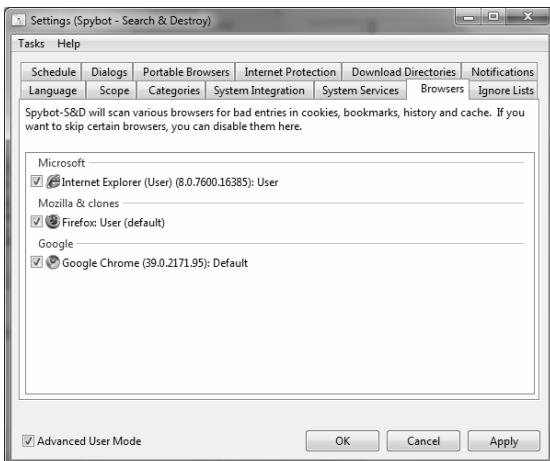
Gambar 2.34 Modul integerasi Spybot ke Windows

6. Di **System Services**, andab isa menyetop service-service yang berkaitan dengan spybot apabila dibutuhkan. Kondisi default-nya, service-service ini selalu berjalan.



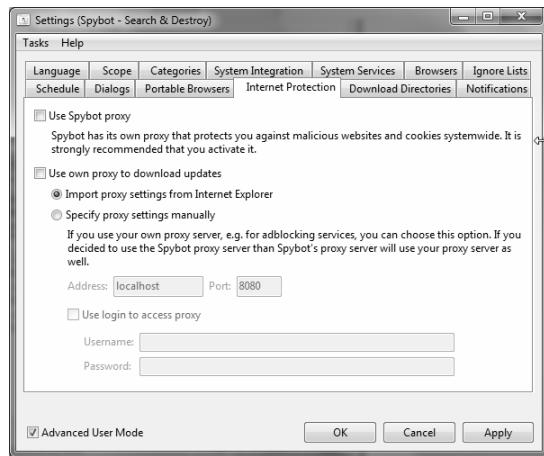
Gambar 2.35 Kondisi service spybot sedang berjalan

7. Di Browsers, Anda bisa melihat browser yang akan dicek apakah ada spyware di cookies, bokomark, history dan cache-nya.



Gambar 2.36 Pemilihan browser yang akan dicek

8. Di tab **Internet Protection**, Anda bisa mengatur cara spybot terkoneksi ke internet, apakah lewat proxy atau tidak.

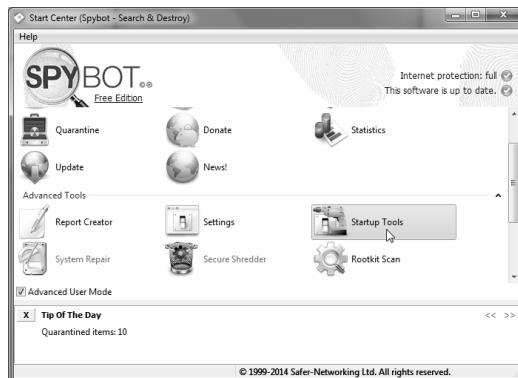


Gambar 2.37 Tab Internet Protection

2.1.8 Tools Startup

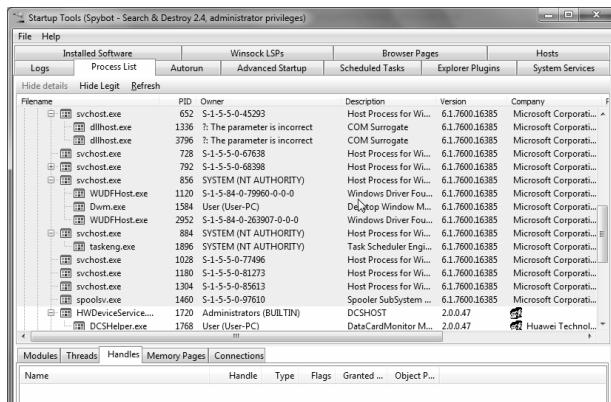
Spyware bisa menyebar saat startup, untuk itu Spybot menyediakan fasilitas Startup Tools yang bisa digunakan untuk mengeset pengamanan saat proses startup. Caranya seperti berikut:

1. Klik Advanced Tools hingga muncul beberapa menu tambahan yang awalnya tidak ada, kemudian klik pada link Startup Tools.



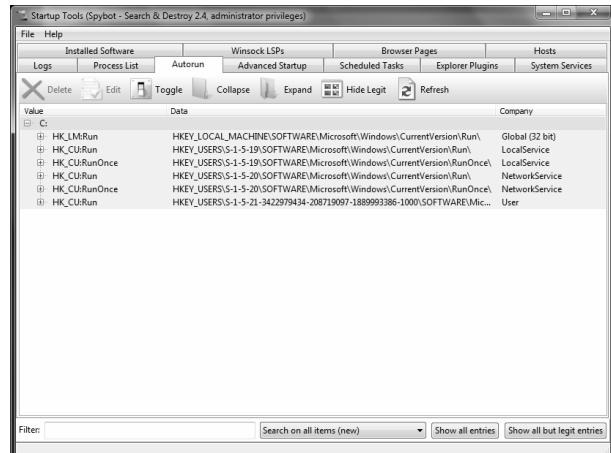
Gambar 2.38 Klik Startup Tools

2. Ada beberapa tab yang bisa diakses, pertama adalah Process List yang memungkinkan Anda melihat list proses yang berjalan. Anda melihat modul, thread, handle dan memory pages yang dikonsumsi oleh proses tersebut.



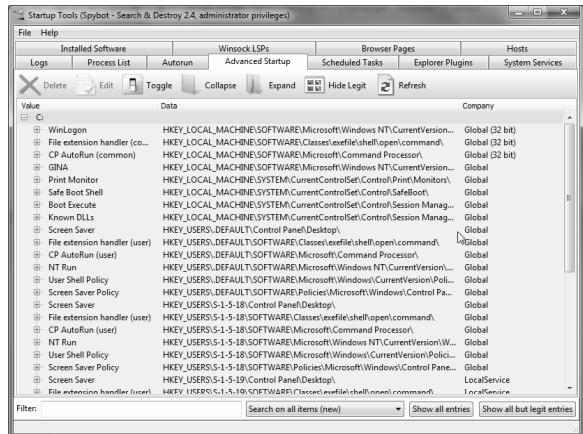
Gambar 2.39 Process List

3. Di tab AutoRun, terdapat file-file program yang dijalankan saat startup. Anda bisa menghapus salah satu program yang diinginkan.



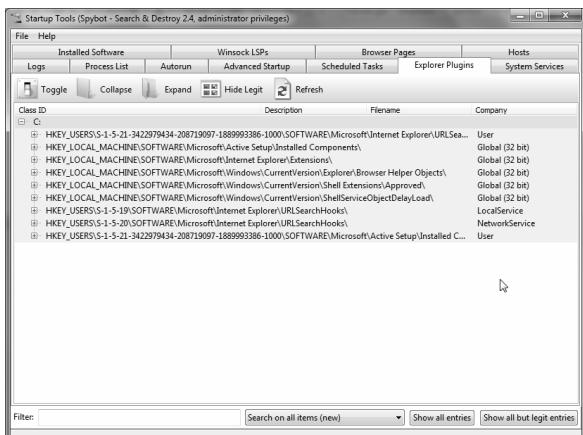
Gambar 2.40 Tab AutoRun

4. Di **Advanced Startup**, Anda bisa melihat lebih jelas apa yang dijalankan saat startup di registry editor.



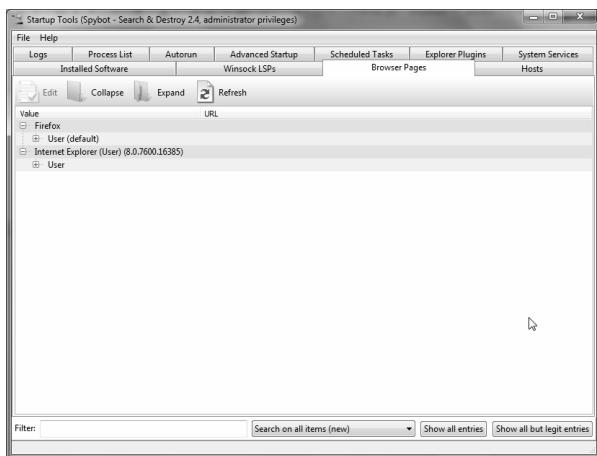
Gambar 2.41 Entry registry yang dijalankan saat startup

5. Di **Explorer Plugins**, Anda bisa melihat plugin yang dikaitkan dengan explorer. Anda bisa mengecek apakah ada spyware di situ.



Gambar 2.42 Pengecekan plugin yang ada di spyware

6. Di **Browser Pages**, Anda bisa melihat daftar browser yang ada.

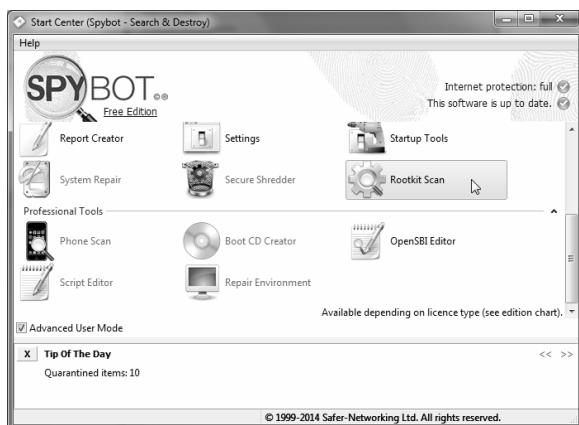


Gambar 2.43 Daftar browser yang didukung saat startup

2.1.9 Rootkit Scan

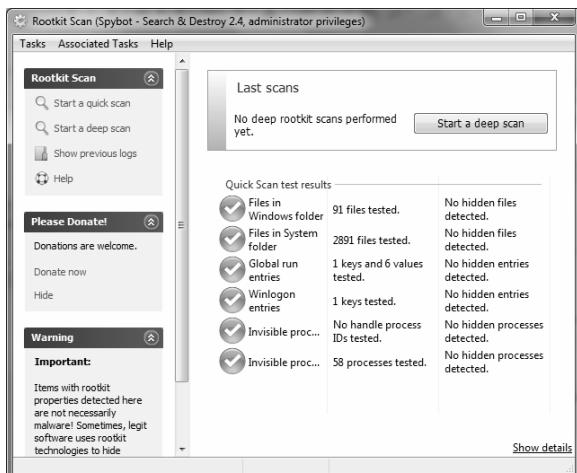
Rootkit scan berguna memindai komputer untuk melihat apakah ada spyware di sistem windows, system logon dan win logon. Caranya seperti ini:

1. Klik pada Rootkit Scan.



Gambar 2.44 Klik RootKit Scan

2. Klik pada tombol **Start a deep scan**.
3. Hasilnya, maka terlihat apakah ada file hidden yang dideteksi atau tidak.



Gambar 2.45 Hasil pemindai rootkit

2.2 Bazooka

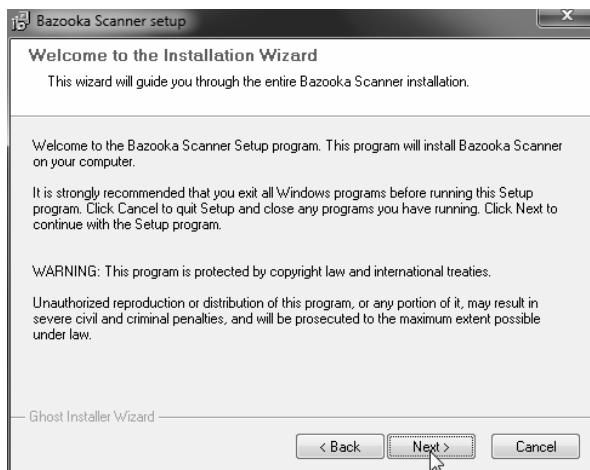
Bazooka adalah software mini yang digunakan untuk memindai spyware di komputer. Fiturnya tidak terlalu banyak dan dapat di-download dari <http://www.kephyr.com/spywarescanner/supportus.phtml>. Berikut ini cara menginstal dan menggunakan Bazooka:

1. Eksekusi file installer Bazooka dan pilih bahasa **English** di **Choose Installation Language**.



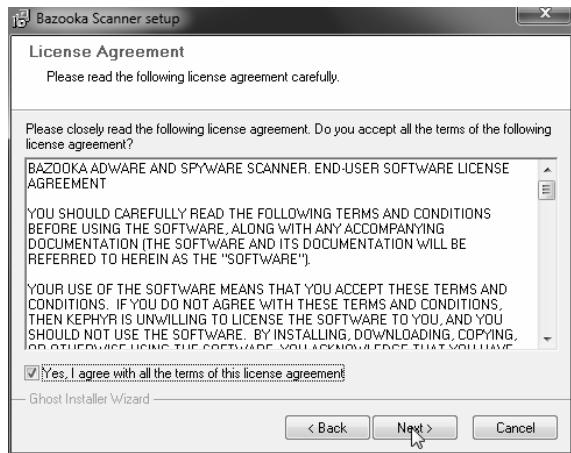
Gambar 2.46 Pemilihan bahasa

2. Muncul jendela Welcome to the Installation Wizard, klik Next.



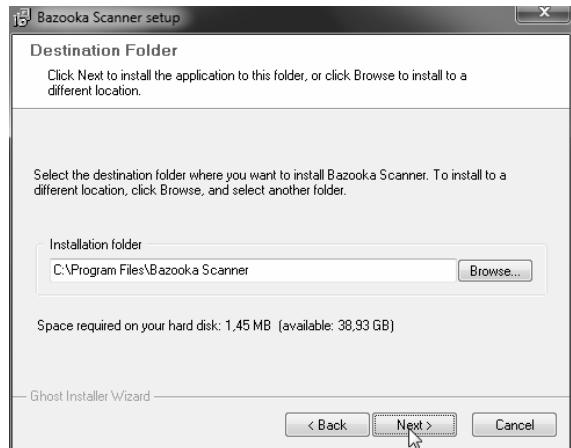
Gambar 2.47 Jendela Welcome to the Installation Wizard

3. Muncul endela License Agreement, cek pada combobox I agree with all the terms of this license agreement, dan klik Next.



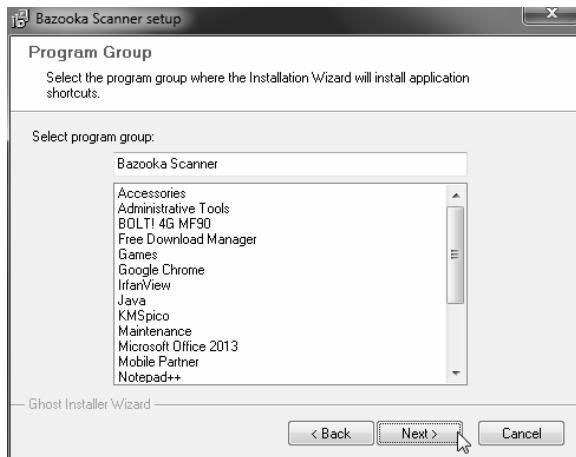
Gambar 2.48 Jendela License Agreement dari Bazooka

4. Pilih lokasi pemasangan di **Installation Folder**.



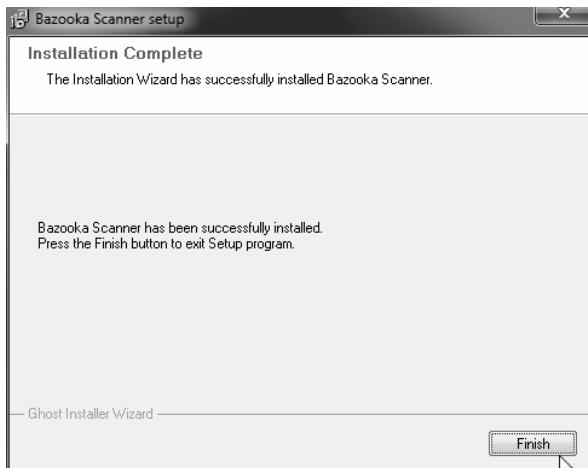
Gambar 2.49 Pemilihan lokasi di Installation Folder

5. Pilih nama program di Program Group. Kalau pakai Windows 8, ini bebas karena tidak ada Program menu di Windows 8.



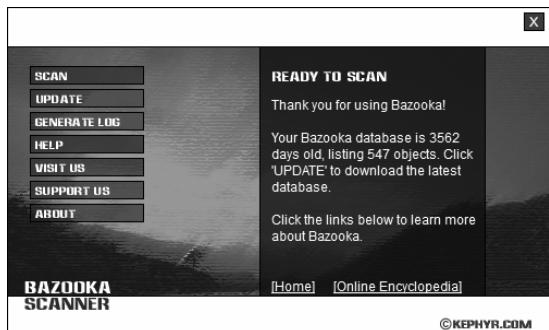
Gambar 2.50 Program Group

6. Kalau instalasi sudah selesai, muncul jendela **Installation Complete**, klik **Finish**.



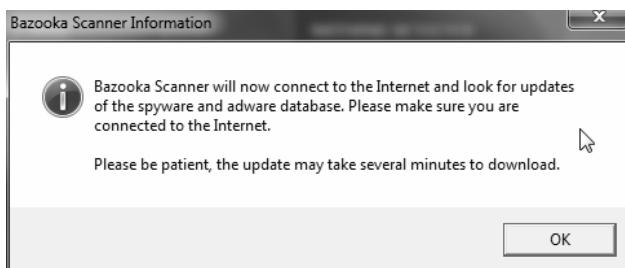
Gambar 2.51 Jendela Installation Complete, instalasi sudah selesai

7. Untuk memindai, Anda tinggal jalankan program hingga muncul jendela seperti berikut ini:



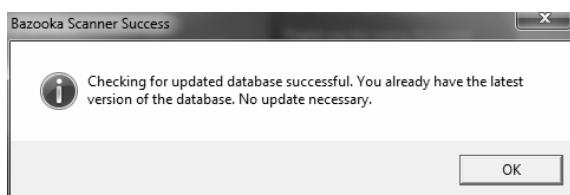
Gambar 2.52 Program dijalankan

8. Klik Update terlebih dahulu untuk memutakhirkan definisi spyware.



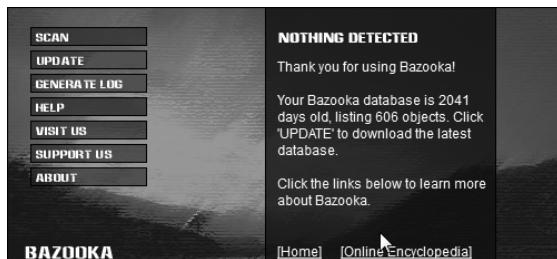
Gambar 2.53 Proses update

9. Kalau update sudah diproses Anda siap memindai.



Gambar 2.54 Pengecekan database sudah selesai

10. Klik **Scan** untuk memindai, kalau ada spyware terdeteksi Anda akan melihat hasilnya dan akan dikarantina, kalau tidak, maka muncul tulisan Nothing detected yang menunjukkan kondisi aman.



Gambar 2.55 Scan sudah selesai

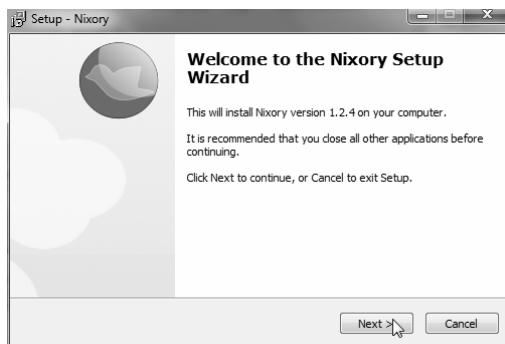
2.3 Nixory

Nixory bisa berintegrasi dengan firewall dan software anti virus yang ada untuk menghilangkan ancaman software spyware dan data-mining yang mencuri informasi di komputer Anda.

2.3.1 Menginstal Nixory

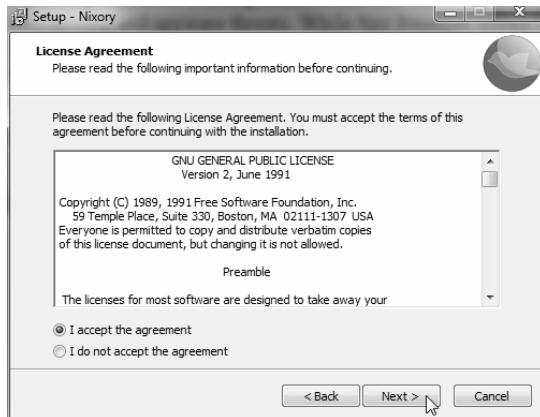
Anda bisa memperoleh Nixory ini dari situs <http://nixory.sourceforge.net/>. Setelah ter-download, Anda dapat menginstal Nixory dengan langkah-langkah seperti ini:

1. Eksekusi file installer Nixory, di **Welcome to the Nixory Setup Wizard**, klik **Next**.



Gambar 2.56 Welcome to the Nixory Setup Wizard

2. Di jendela License Agreement, klik I accept the agreement, kemudian klik Next.



Gambar 2.57 Persetujuan lisensi License Agreement

3. Pilih lokasi instalasi di jendela Select Destination Location, klik Next kemudian.



Gambar 2.58 Pemilihan lokasi instalasi Nixory

4. Pilih nama start menu folder, untuk windows 8 ke atas, biarkan default dan klik Next.



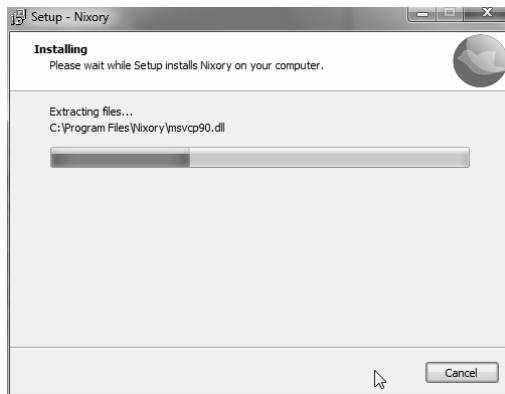
Gambar 2.59 Pemilihan start menu folder

5. Di Ready To install, ada info rekap instalasi, klik Install untuk memulai instalasi.



Gambar 2.60 Rekap instalasi

6. Ketika proses instalasi berlangsung, Anda bisa melihat kemajuan di progress bar yang ada.



Gambar 2.61 Proses instalasi tengah berlangsung

7. Terakhir, klik **Finish** di jendela Completing the Nixory setup wizard. Artinya proses instalasi sudah berlangsung.



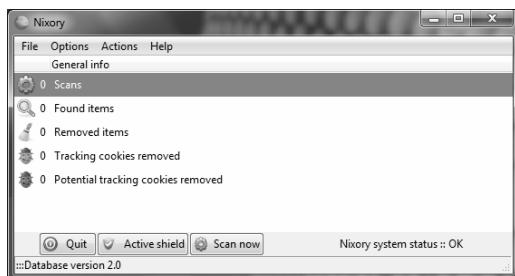
Gambar 2.62 Completing the Nixory setup wizard

2.3.2 Menggunakan Nixory

Setelah terinstal, Anda bisa memanfaatkan Nixory untuk memindai dan mendeteksi spyware. Fiturnya simpel, tidak sekompleks spybot. Berikut ini langkah-langkah menggunakan Nixory:

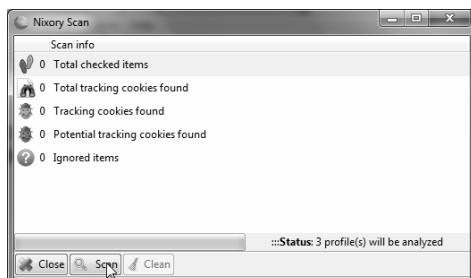
1. Jalankan Nixory.

2. Tampilan awal seperti berikut:



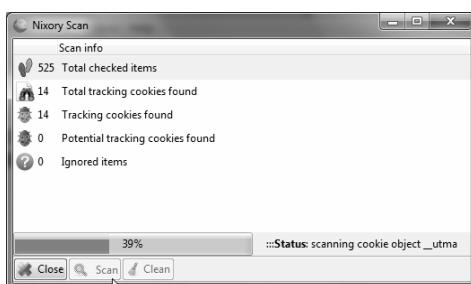
Gambar 2.63 Tampilan awal Nixory

3. Klik pada tombol Scan di bawah untuk memulai pemindaian.



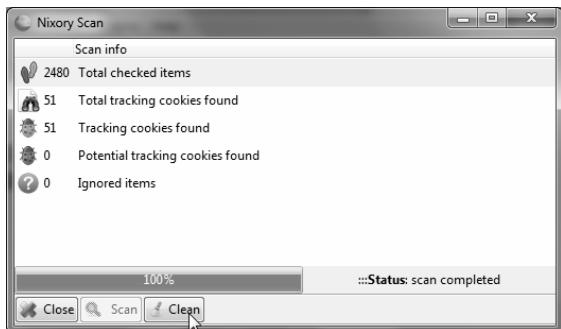
Gambar 2.64 Klik tombol Scan

4. Tunggu hingga pemindaian selesai dilakukan.



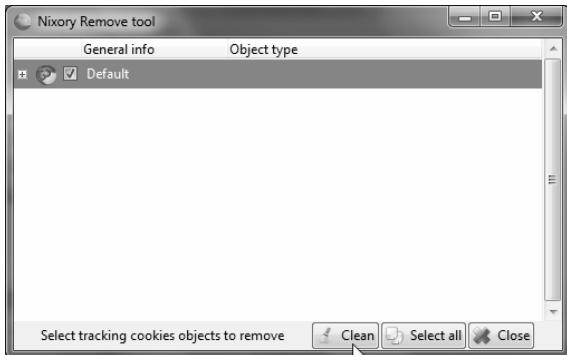
Gambar 2.65 Pemindaian sedang dilakukan

- Kalau status san complet, Anda bisa melihat item yang dipindai dan apakah ada spyware di situ.
- Klik Clean untuk membersihkan.



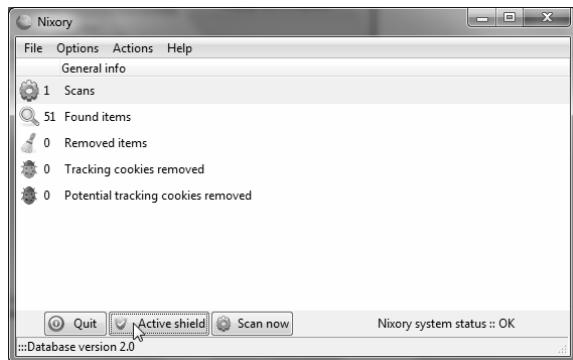
Gambar 2.66 Klik Clean untuk membersihkan

- Muncul di browser apa yang akan di-remove, klik Clean.



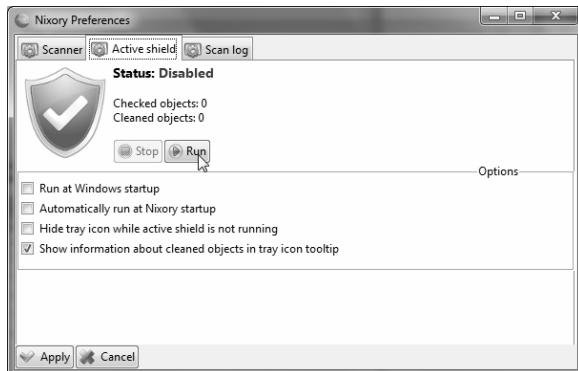
Gambar 2.67 Info yang akan dihapus

- Untuk aktif melindungi komputer dari spyware, klik pada tombol Active Shield.



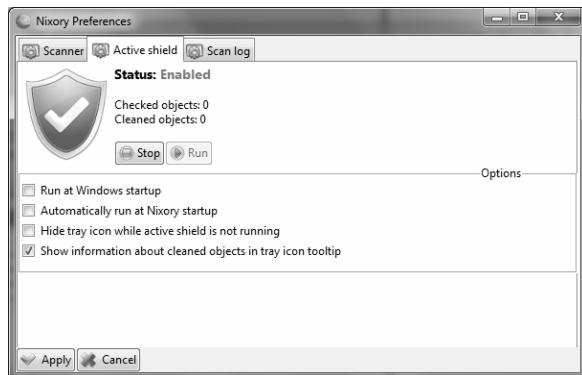
Gambar 2.68 Klik Active Shield

9. Muncul tab Active Shield, terlihat shield belum aktif. Anda bisa mengeset active shield ini untuk dijalankan di startup windows, atau menyembunyikan ikon ketika tidak dijalankan.



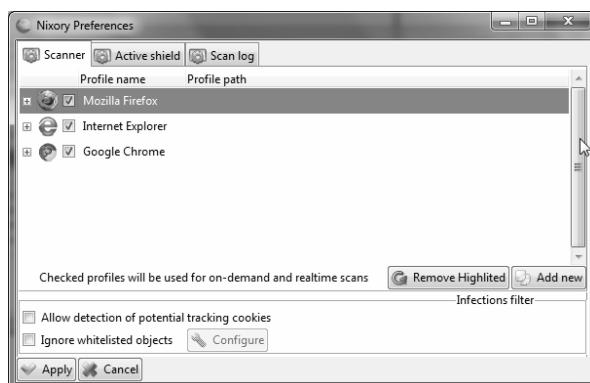
Gambar 2.69 Active Shield

10. Klik Run untuk menjalankan Active Shield ini, kalau sudah diaktifkan, Anda bisa melihat status menjadi Enabled.



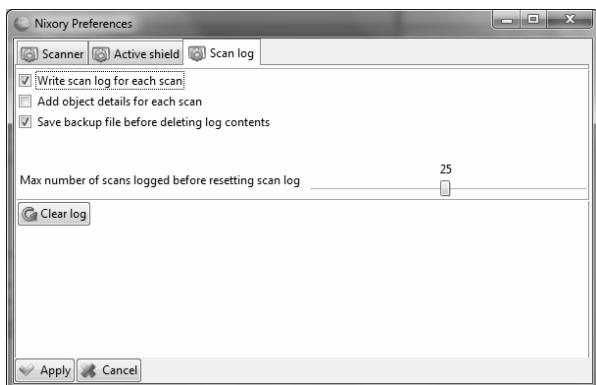
Gambar 2.70 Status menjadi enabled

11. Di tab Scanner, Anda bisa menyesuaikan pemindaian untuk tiap-tiap browser.



Gambar 2.71 Penyesuaian pemindaian untuk tiap-tiap browser

12. Di Scan log, Anda bisa menyesuaikan pencatatan untuk pemindaian.



Gambar 2.72 Scan log

3

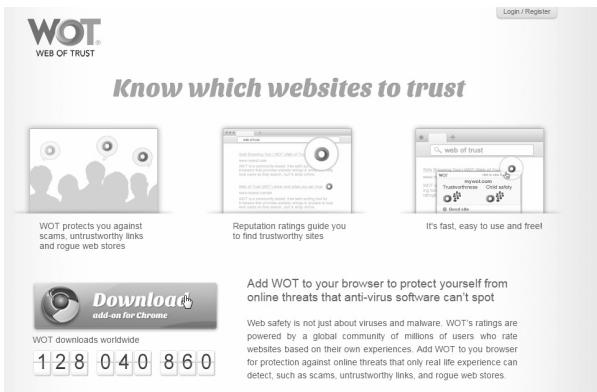
PENGAMANAN INTERNET

Dalam berinternet, Anda sering terekspos dengan berbagai ancaman. Ancaman ini ada yang sangat ringan tingkat bahayanya dan ada pula yang sangat berbahaya. Ada beberapa tool yang cukup penting yang membantu Anda, dari mulai tool untuk melihat kredibilitas situs-situs internet, hingga enkripsi untuk mengamankan data Anda yang akan dikirim via internet, misalnya menggunakan email atau aplikasi seperti BBM, WhatsApp dan LINE.

3.1 Web Of Trust

Di internet, banyak sekali website yang mencurigakan. Dari mulai website penyebar spyware, malware, virus dan lain sebagainya. Untuk itu Anda perlu alat WOT ini yang fungsinya mengecek berdasarkan inputan dari user apakah sebuah situs terpercaya atau tidak.

WOT yang bisa diambil dari <https://www.mywot.com/> menggunakan data yang bersumber dari inputan penggunanya. Jadi datanya valid, selain itu WOT tidak memperlambat proses browsing Anda.

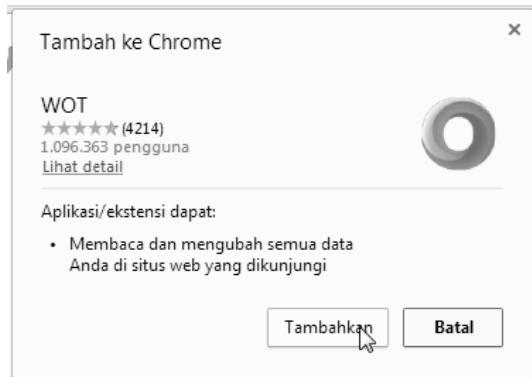


Gambar 3.1 Download

WOT memproteksi Anda dari scam, link yang meragukan dan webstore penipu dan situs-situs lainnya yang membahayakan. Rating dari WOT sangat bisa dipercaya, mudah digunakan dan gratis.

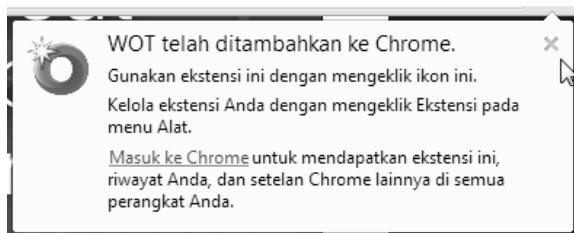
3.1.1 Menambahkan dan Menggunakan WOT

Untuk menambahkan WOT, caranya cukup mudah. Yaitu dengan mendownload dari situs WOT di atas, hingga muncul konfirmasi untuk menginstal WOT sesuai dengan browser yang dipakai.



Gambar 3.2 Konfirmasi menambahkan WOT sebagai ekstensi

Kalau sudah dipasang ke browser, muncul notifikasi bahwa WOT sudah dimasukkan ke browser.



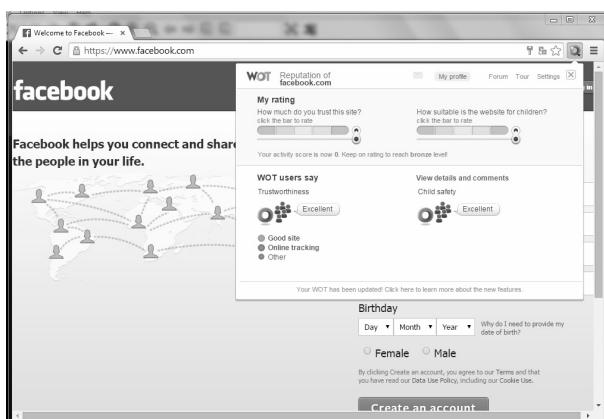
Gambar 3.3 Notifikasi bahwa WOT sudah dimasukkan

Ketika Anda mengakses situs tertentu, maka di kanan atas ada ikon pada plugin WOT.



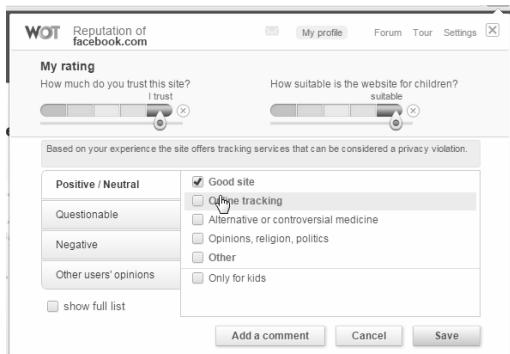
Gambar 3.4 Ikon pada plugin WOT

Anda bisa klik pada plugin tersebut untuk memberikan rating.



Gambar 3.5 Kotak dialog untuk memberikan rating

Rating ada dua, yaitu rating umum dan apakah situs tersebut aman untuk anak-anak. Klik save untuk menyimpannya.



Gambar 3.6 Klik Save untuk menyimpan

Maka hasil rating akan dimasukkan dan ini berguna untuk orang lain.

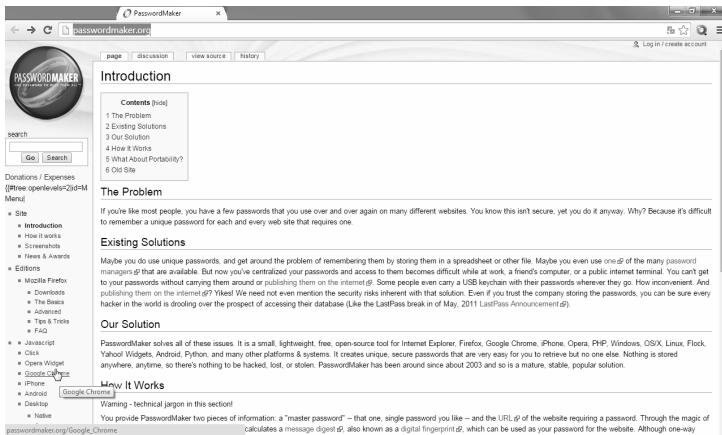


Gambar 3.7 Hasil rating dimasukkan

3.2 Password Maker

Salah satu penyebab website sering diretas adalah pembuatan password yang kurang aman. Untuk membantu membuat password yang aman, ada salah satu tool populer yaitu Passwordmaker yang bisa diambil dari

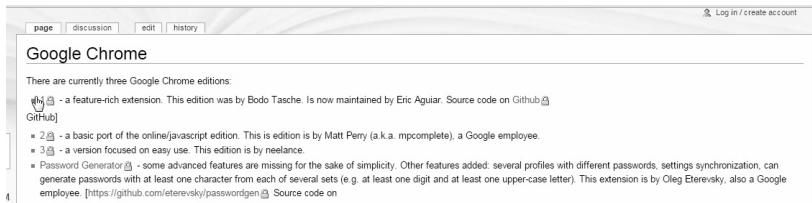
<http://passwordmaker.org/>. Ini adalah plugin untuk berbagai browser yang memudahkan Anda dalam membuat password yang aman.



Gambar 3.8 Halaman Password maker

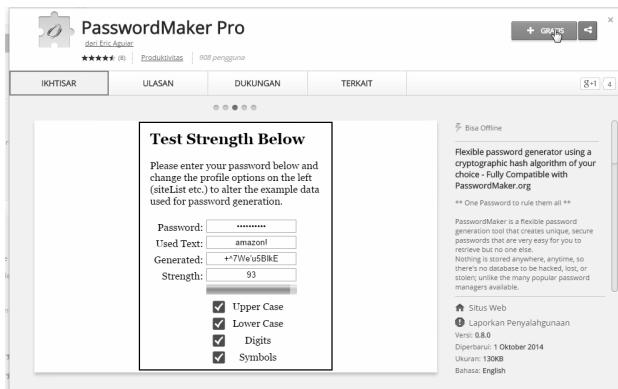
3.2.1 Download dan Instalasi

Anda bisa mendownload PasswordMaker ini sesuai dengan browser Anda. setelah itu mendownload plugin password maker.



Gambar 3.9 Download plugin passwordmaker

Muncul konfirmasi untuk memasang plugin ini, klik pada link Plus untuk menambahkan plugins ini.



Gambar 3.10 Klik untuk menambahkan plugin PasswordMaker Pro

Di notifikasi, klik Tambahkan.



Gambar 3.11 Klik Tambahkan untuk menambahkan ekstensi

Kalau sudah dimasukkan, Anda bisa melihat notifikasi kedua bahwa PasswordMaker Pro sudah ditambahkan.

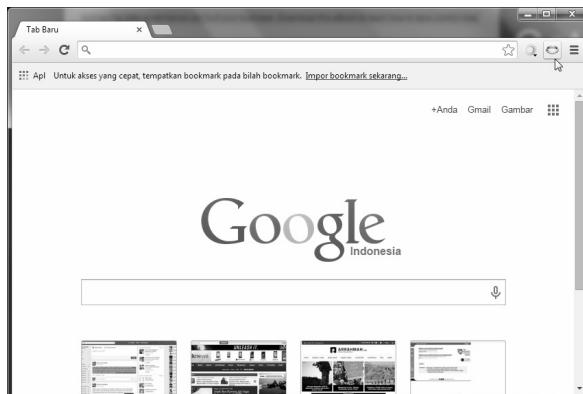


Gambar 3.12 PasswordMaker Pro sudah ditambahkan

3.2.2 Menggunakan PasswordMaker

Untuk meng-generate password aman dengan PasswordMaker Pro, caranya seperti ini:

1. Buka browser.
2. Klik pada ikon cincin dari PasswordMaker Pro.



Gambar 3.13 Klik ikon cincin dari PasswordMaker Pro

3. Awalnya ada teks standar, ini perlu diubah.



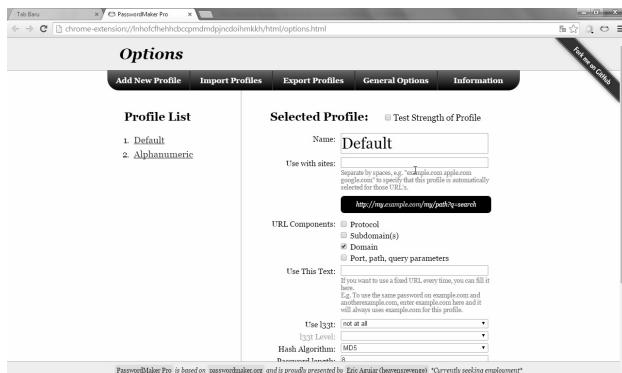
Gambar 3.14 Teks standar

- Isikan password awal yang ingin dijadikan inputan di Password dan Confirm Password. Kemudain isikan kata kunci untuk enkripsi di Used text.



Gambar 3.15 Pengisian teks inputan dan enkripsi

- Password yang dihasilkan terlihat di Generated Password, Anda bisa menyalinnya dengan klik pada tombol Copy. Di Options, Anda bisa mengatur profil lainnya.



Gambar 3.16 Pengaturan options

3.3 KeePass

Password yang baik adalah password yang susah dihapal, karena itu untuk menangani ini, Anda perlu software manajemen password yang

memungkinkan password disimpan dengan aman. Salah satu software untuk manajemen password saat berinternet adalah KeePass yang bisa diambil dari <http://keepass.info/>. Dengan KeePass, Anda bisa

3.3.1 Mendownload dan Mengakses KeePass

Program KeePass harus diinstal didownload terlebih dahulu. Anda bisa memilih versi portable agar tidak perlu menginstal dan file-nya bisa ditaruh di perangkat portabel seperti usb flash disk. Caranya seperti ini:

1. Buka Keepass.info.
2. Klik pada link Downloads.



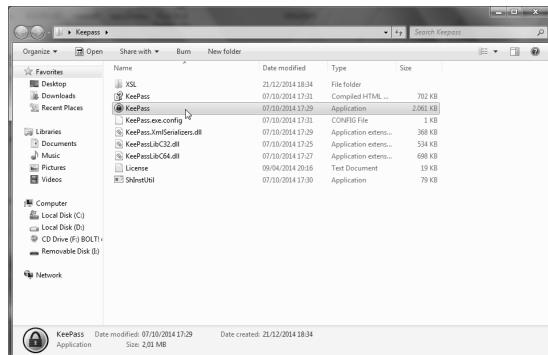
Gambar 3.17 Klik link Downloads di situs KeePass.info

3. Download versi Portable dari Professional Edition.



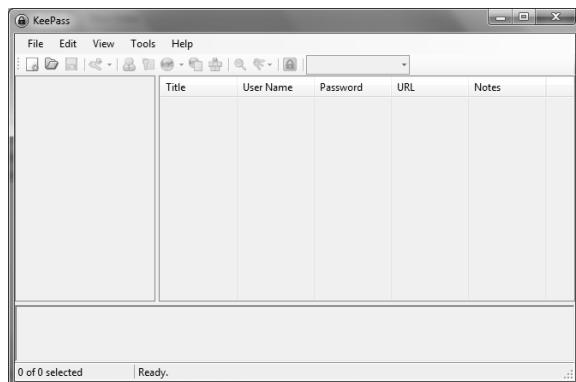
Gambar 3.18 Download versi Portable

4. Untuk menjalankan, klik pada file KeePass.exe dari folder hasil download.



Gambar 3.19 Klik pada file KeePass.exe untuk menjalankan

5. Maka tampilan keepass saat masih kosong terlihat seperti berikut ini:

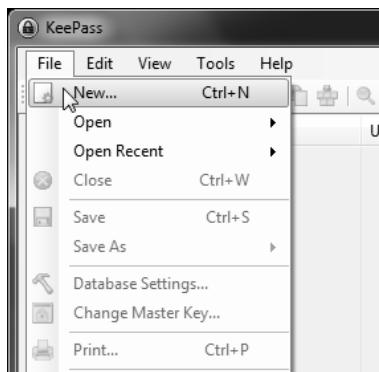


Gambar 3.20 Tampilan KeePass saat masih kosong

3.3.2 Menggunakan KeePass

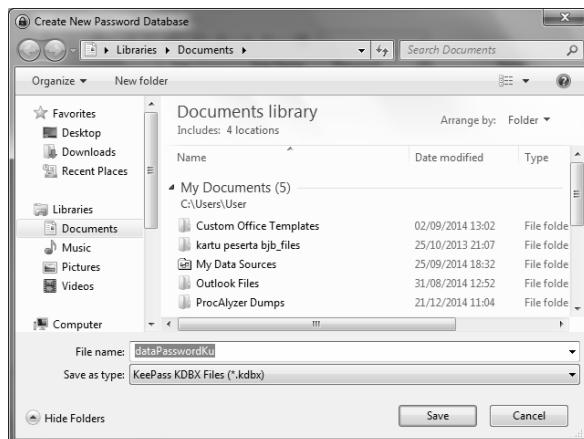
Setelah bisa dijalankan, berikut ini langkah-langkah manajemen password untuk berinternet menggunakan KeePass:

1. Klik **File > New** di menu utama KeePass.



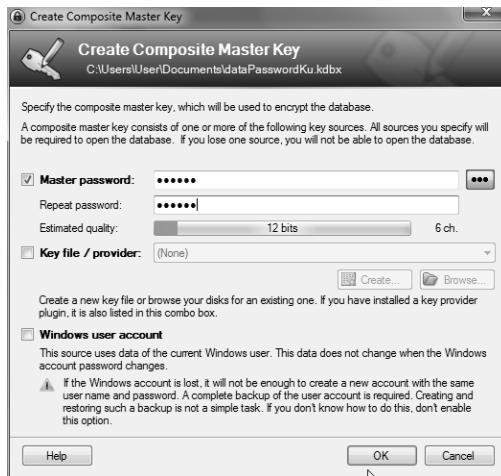
Gambar 3.21 Klik File > New

2. Muncul jendela **Create New Password Database**, masukkan nama database yang akan dipakai untuk menyimpan semua data ini, dan klik **Save**.



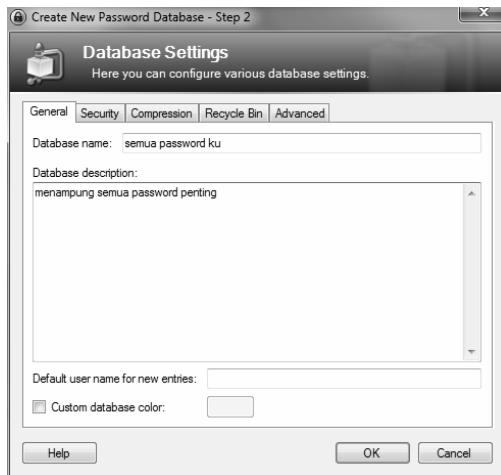
Gambar 3.22 Create New Password Database

3. Tentukan password utama untuk mengakess semua password di database ini.



Gambar 3.23 Pembuatan Master key atau password utama

4. Di Database Settings, isikan setting-setting database yang ada. Di tab General, tentukan penjelasan di **Database Description**.



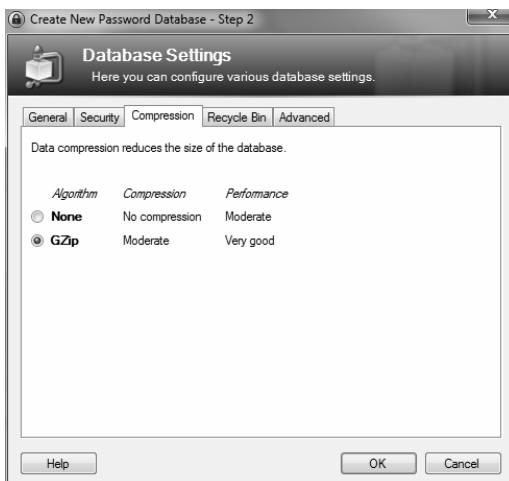
Gambar 3.24 Pengisian database settings

5. Di Security, tentukan jenis algoritma enkripsi yang digunakan.



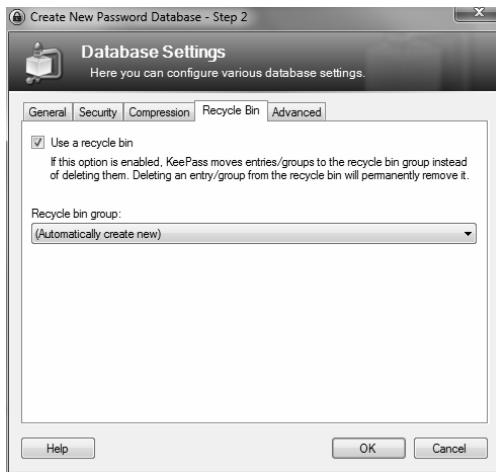
Gambar 3.25 Pemilihan algoritma enkripsi

6. Di Compression, tentukan metode kompresi yang diinginkan.



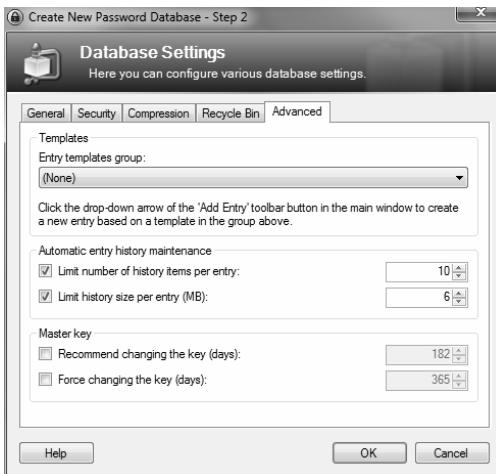
Gambar 3.26 Penentuan metode kompresi

7. Di Recycle Bin, Anda bisa menentukan apakah langsung menghapus password yang di-delete atau menggunakan Recycle bin dulu untuk menampung sementara.



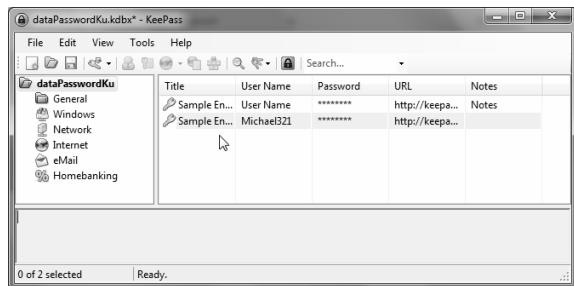
Gambar 3.27 Pengaturan Recycle bin

8. Di Advanced, Anda bisa mengeset jumlah entri history, dan template untuk mengatur database ini. Lebih baik dibiarkan default saja.



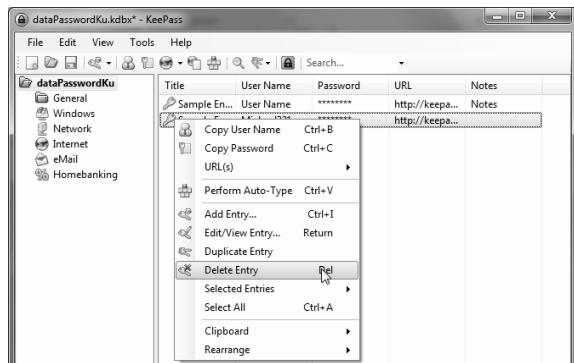
Gambar 3.28 Tampilan Advanced

9. Saat database baru dibuat, ada beberapa kategori password dan contoh password di dalamnya.



Gambar 3.29 Tampilan awal database

10. Hapus password default dengan cara klik kanan pada sample kemudian klik menu Delete Entry.



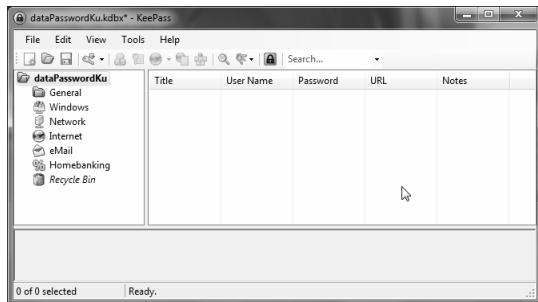
Gambar 3.30 Klik Delete Entry untuk menghapus entry yang ada

11. Muncul konfirmasi untuk menghapus entri tersebut ke recycle bin. Klik Yes untuk menghapusnya.



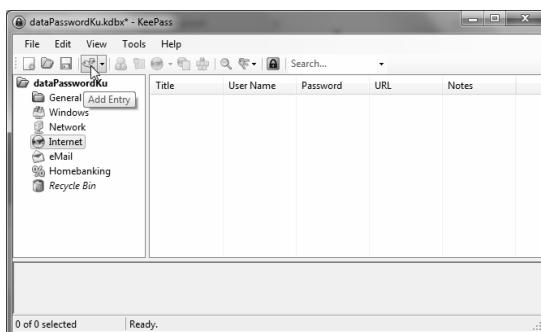
Gambar 3.31 Memindahkan entri ke recycle bin

12. Maka entri password akan kosong.



Gambar 3.32 Entri password menjadi kosong

13. Untuk memasukkan entri baru, klik pada kategori password, misalnya Internet, kemudian klik tombol **Add Entry**.



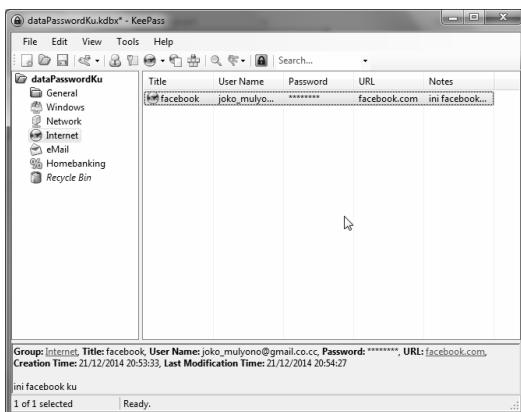
Gambar 3.33 Klik Add Entry untuk menambahkan entri

14. Muncul jendela Add Entry, di tab Entry, Anda bisa memasukkan judul password di Title.
15. Isikan username yang akan disimpan di **User name**.
16. Isikan password dua kali di **Password** dan **Repeat**, pengisian 2x ini untuk menghindari kesalahan dalam pemasukan password.
17. Masukkan url untuk memasukkan password ini di **URL**.
18. Isikan penjelasan di **Notes**.



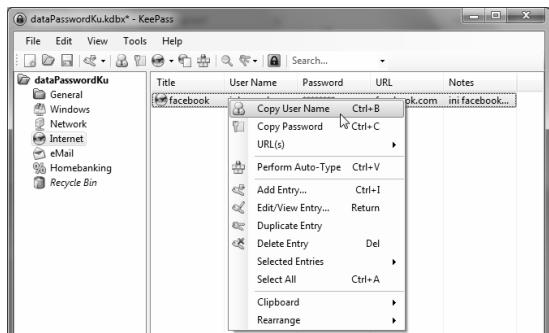
Gambar 3.34 Pengisian 2x untuk password

17. Klik **OK** untuk menyimpan
18. Data password tersebut langsung tersimpan.



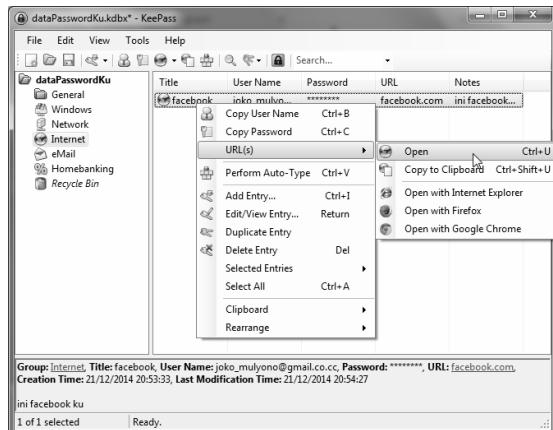
Gambar 3.35 Data password tersimpan

19. Untuk mengambil username dan password, Anda tidak perlu membuka entri tersebut, tinggal klik kanan dan pilih menu **Copy Username** atau **Copy password**.



Gambar 3.36 Menyalin Username

20. Anda juga bisa membuka url dari situs yang menampung password tersebut secara langsung dengan klik kanan pada url dan pilih menu **Open**.



Gambar 3.37 Klik menu URL > Open untuk membuka url

3.4 Password Safe

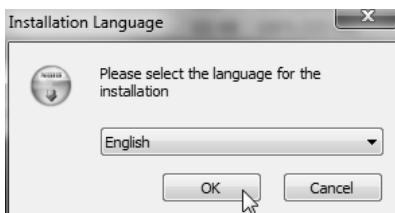
Software kedua untuk password management adalah password safe. Software ini fungsinya adalah mengatur password sehingga mudah diingat dan tidak mudah lupa.

3.4.1 Download dan Install Password Safe

Password Safe adalah kotak aman untuk menyimpan password-password Anda. Sifat program ini open source dan juga bisa diambil secara gratis dari internet.

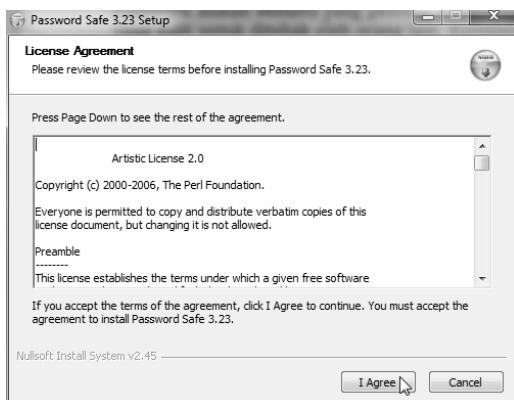
Berikut ini caranya:

1. Buka <http://passwordsafe.sourceforge.net/>. Klik link download yang ada. Tunggu hingga download selesai.
2. Klik 2x pada file installer yang sudah didownload.
3. Pilih bahasa English di **Please select the language for the installation**. Klik OK.



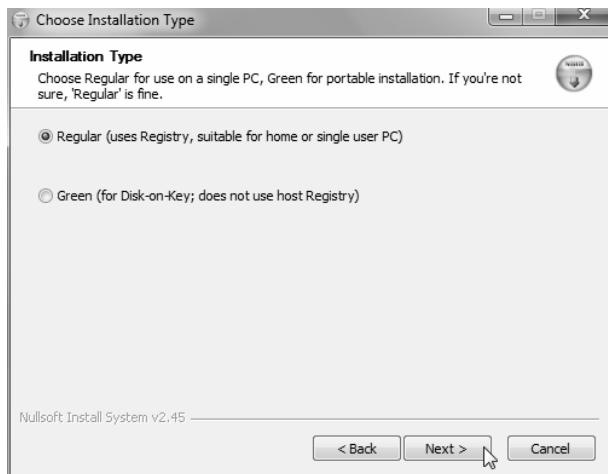
Gambar 3.38 Installation language

4. Klik I agree untuk menyetujui perjanjian lisensi.



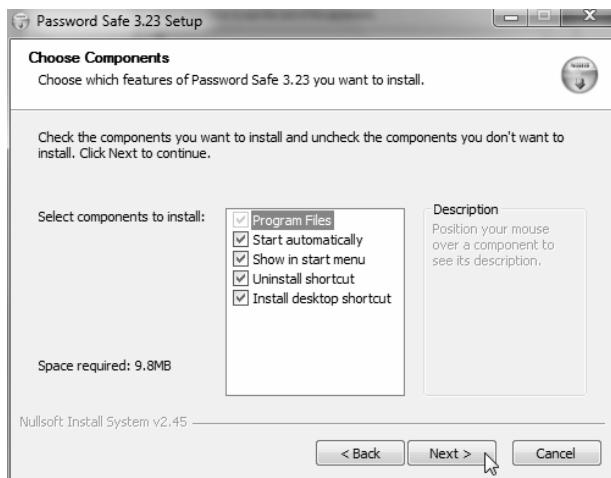
Gambar 3.39 License agreement

5. Tentukan tipe instalasi **Regular**, lalu klik **Next**.



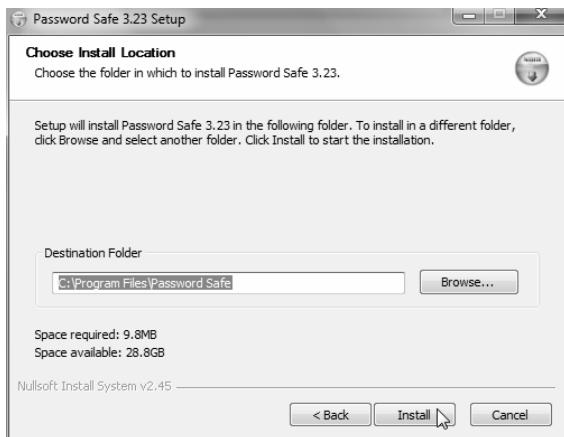
Gambar 3.40 Pemilihan tipe instalasi Regular

6. Cek pada semua komponen di **Select components to install**. Kemudian klik **Next**.



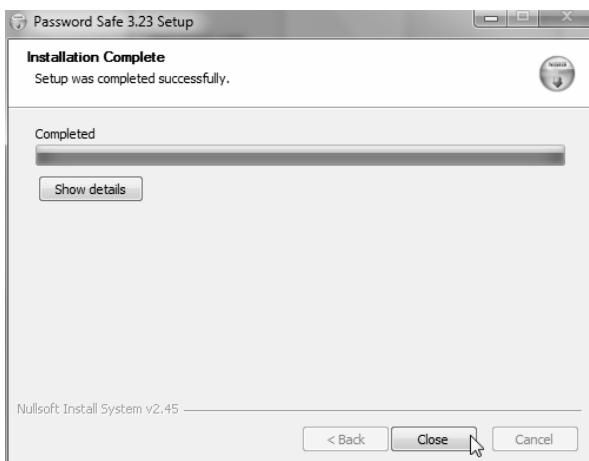
Gambar 3.41 Memilih komponen yang akan diinstal

7. Tentukan lokasi instalasi di **Choose install location**. Klik **Install** kalau sudah, kalau ingin mengganti lokasi instalasi, klik **Browse**.



Gambar 3.42 Choose install location

8. Kalau instalasi sudah selesai, klik **Close** untuk mengakhiri instalasi.



Gambar 3.43 Akhir instalasi Password Safe

3.4.2 Menggunakan Password Safe

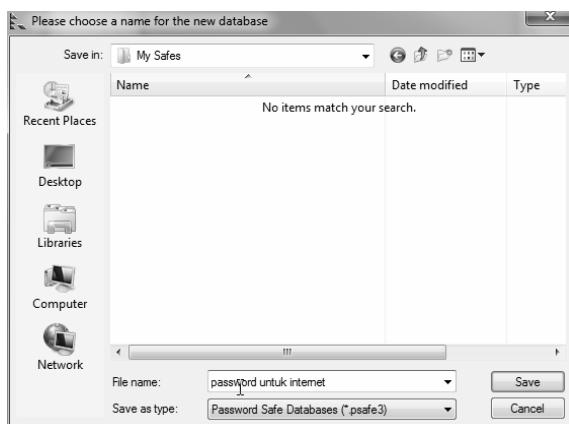
Password safe yang sudah terinstal dapat dijalankan dari Start menu menggunakan kotak **Search result**. Atau kalau menggunakan Windows 8 langsung akses di Start Screen. Setelah aktif, berikut ini penggunaan Password safe untuk menyimpan password dengan aman.

1. Buat dahulu database dengan klik **New database** di jendela utama dari **Password Safe**.



Gambar 3.44 Password Safe

2. Isikan nama file di **File Name**, kemudian klik **Save**.



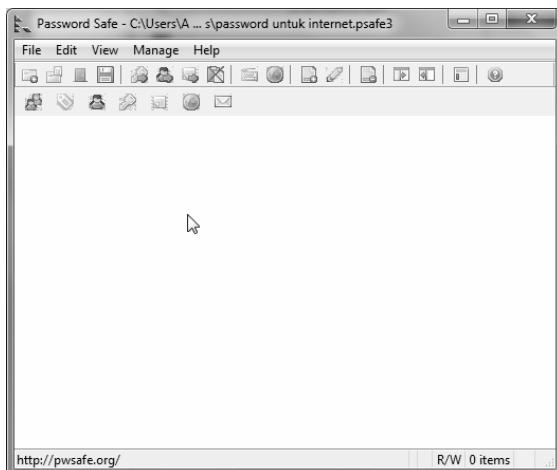
Gambar 3.45 Pengisian nama file di kotak Please choose a name for the new database

3. Tenukan password kombinasi untuk membuka file database ini, jadi file database ini sebenarnya terenkripsi sehingga password di dalamnya aman. Password kombinasi diisikan 2x untuk menghindari kesalahan. Klik **OK**.



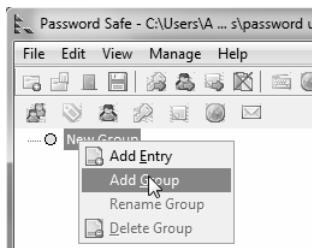
Gambar 3.46 Pengisian password kombinasi

4. Muncul jendela kosong seperti berikut dimana Anda bisa memasukkan semua password di dalamnya.



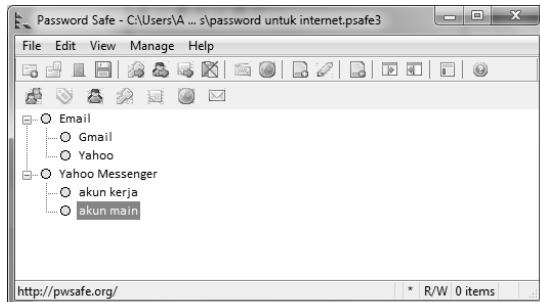
Gambar 3.47 Jendela kosong sebelum file dikirim

5. Anda bisa menambahkan group untuk mengelompokkan kategori password Anda dengan klik kanan kemudian pilih **Add group**.



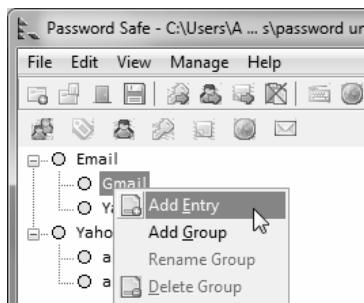
Gambar 3.48 *Menu untuk menambahkan group*

6. Kemudian Anda bisa menambahkan group di dalam group sehingga terlihat ada tingkatan.



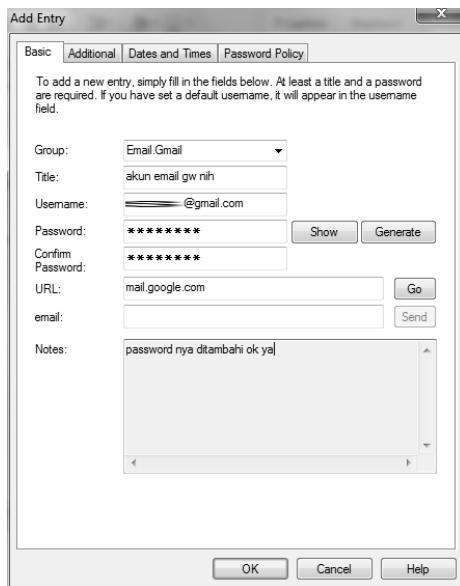
Gambar 3.49 *Tingkatan untuk mengelompokkan password*

7. Tambahkan entry password dengan klik kanan pada salah satu group kemudian klik **Add entry**.



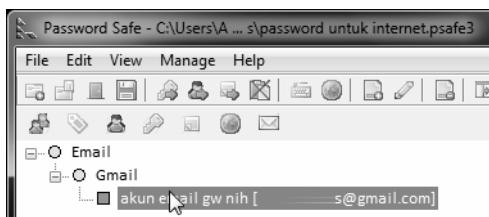
Gambar 3.50 *Menambahkan entry password dengan klik Add entry*

- Isikan judul di title.
- Isikan username dan password untuk entry ini. Lainnya bisa melengkapi.



Gambar 3.51 Pengisian username dan password yang akan disimpan pada entry database

- Klik OK, maka entry password tersebut akan diciptakan.



Gambar 3.52 Entry baru sudah diciptakan

- Untuk menyalin password, klik 2x pada entry maka langsung clipboard akan disiapkan.



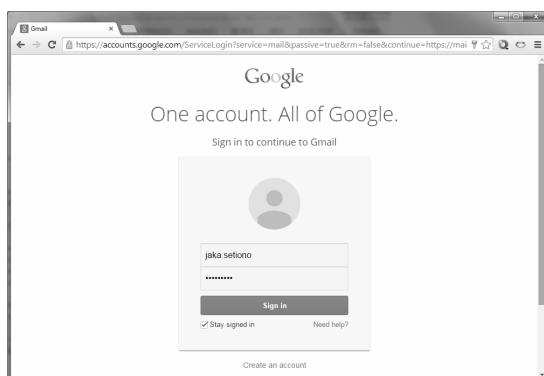
Gambar 3.53 Clipboard berisi salinan password

12. Jika Anda mengisikan alamat web saat membuat entry, Anda juga bisa membuka web tersebut dengan klik **Browse to URL**.



Gambar 3.54 Browse to URL untuk membuka web dengan url berkaitan dengan entry

13. Browser langsung membuka web yang dispesifikasikan.



Gambar 3.55 Web dibuka langsung dari Password Safe

3.4.3 Membuka File Password

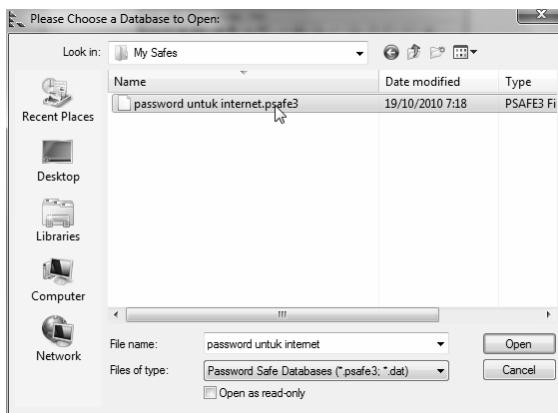
Anda bisa membuka file password baru yang sudah terbuat menggunakan password safe menggunakan cara berikut ini:

1. Klik tombol elipsis di sebelah kanan kotak teks **Open password database**.



Gambar 3.56 Open password database

2. Pilih pada file yang sudah dibuat sebelumnya kemudian klik **Open**.



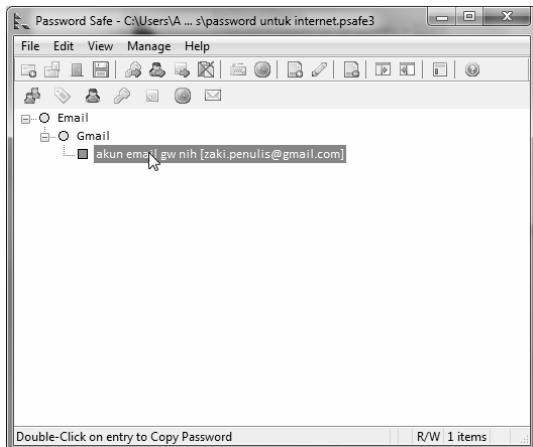
Gambar 3.57 Memilih file database password yang akan dibuka

3. Isikan password kombinasi untuk membuka enkripsi.



Gambar 3.58 Pengisian password untuk membuka enkripsi

4. Hasilnya, file database password terbuka, dan Anda bisa mengakses password yang diinginkan dengan klik 2x.



Gambar 3.59 File database password sudah terbuka

4

TEKNIK LAINNYA

Masih ada banyak teknik lainnya yang bisa dipakai untuk mengamankan komputer Anda dari virus spyware dan malware. Di sini dijelaskan beragam tool dari mulai tool untuk melihat paket jaringan, firewall dan lain sebagainya.

4.1 WireShark

Wireshark adalah software package sniffing yang digunakan untuk melihat paket-paket apa saja yang melewati jaringan, baik jaringan wireless atau biasa. Apabila ada spyware atau malware, biasanya di jaringan ada transfer data yang tidak diinginkan.

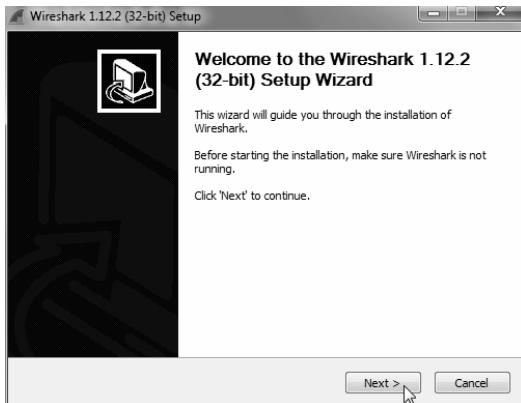
Anda dapat melihatnya menggunakan WireShark ini. Anda bisa mendownload dari url <https://www.wireshark.org/download.html>

Tool ini sebenarnya adalah tool administrator jaringan, sehingga informasinya mungkin tidak terlalu dimengerti oleh orang awam, tapi paling tidak Anda bisa melihat apakah ada transfer data atau tidak menggunakan alat ini, dimana jika tanpa alat ini susah mengetahui apakah ada transfer data atau tidak.

4.1.1 Menginstal WireShark

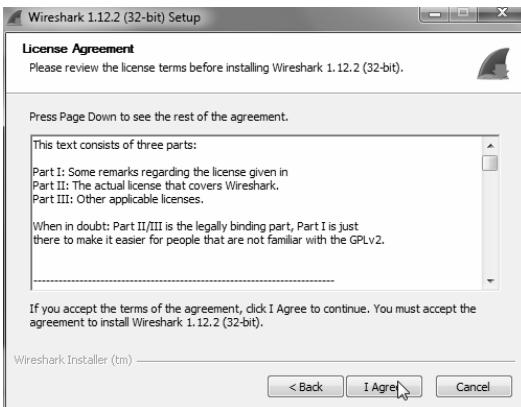
WireShark harus didownload dan diinstal dahulu sebelum bisa dipakai. Caranya menginstal WireShark seperti berikut ini:

1. Klik 2x pada installer Wireshark untuk menjalankan WireShark ini.
2. Di Welcome to the Wireshark setup wizard, klik **Next**.



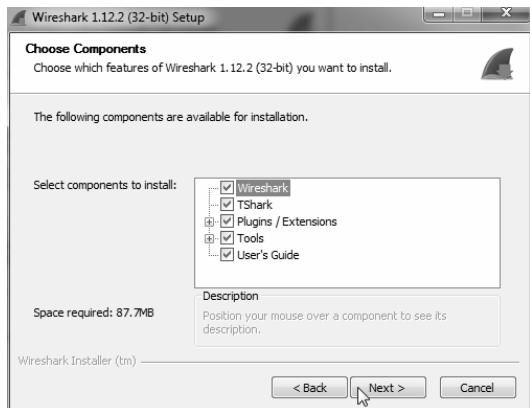
Gambar 4.1 Welcome to the Wireshark setup Wizard

3. Muncul jendela License Agreement, klik pada tombol I agree untuk menyetujui.



Gambar 4.2 Klik I Agree untuk menyetujui

4. Di Choose Components, pilih semua komponen dan klik Next.



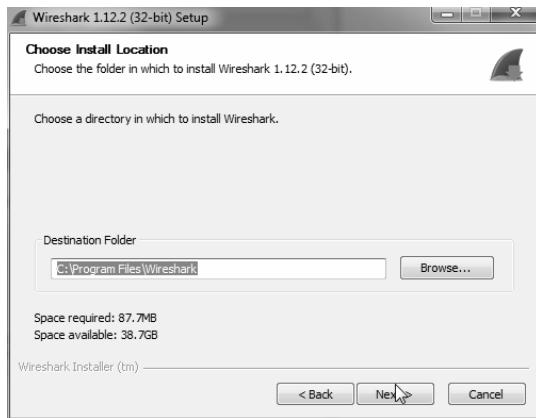
Gambar 4.3 Choose Components

5. Di Select Additional Tasks, cek pada Associate trace file extensions to Wireshark.



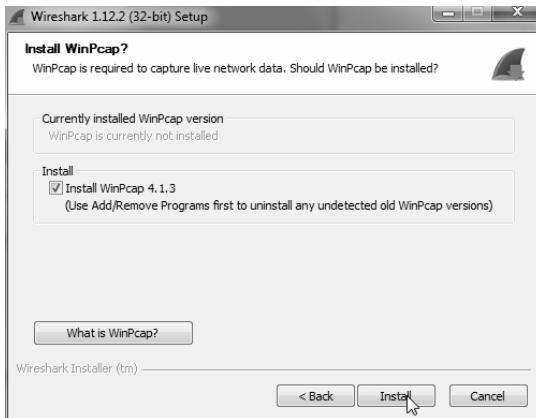
Gambar 4.4 Megnasosiasiakan tipe file untuk wire shark

6. Pilih lokasi instalasi di Choose Install Location.



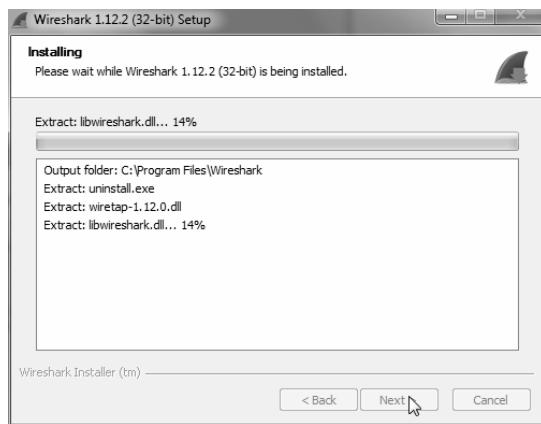
Gambar 4.5 Pemilihan lokasi instalasi

7. Kalau Anda belum menginstal WinPcap, Anda harus menginstalnya di jendela Install WinPCap. Klik Install untuk memulai instalasi.



Gambar 4.6 Jendela InstallWinPcap

8. Tunggu saat instalasi dilakukan.



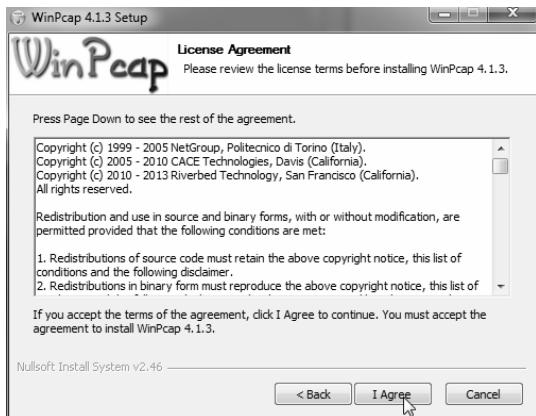
Gambar 4.7 Instalasi tengah berlangsung

9. Di tengah instalasi Wire Shark, muncul instalasi WinPcap. Klik **Next** di **Welcome to the WinPCap Setup Wizard**.



Gambar 4.8 Welcome to the WinPCap Setup Wizard

10. Klik I agree di **License Agreement** WinPcap.



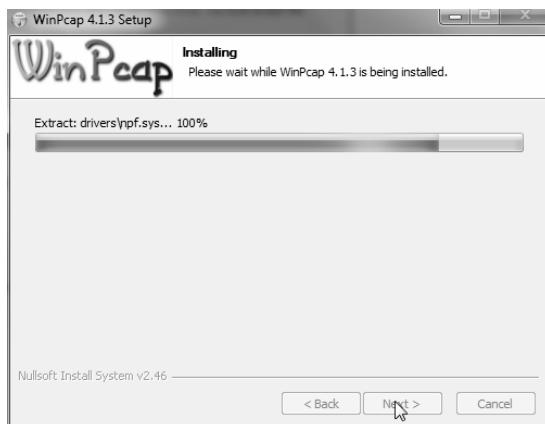
Gambar 4.9 Jendela License Agreement pada WinPcap

11. Di Installation Options, cek pada checkbox **Automatically start the WinPCap driver at boot time**.



Gambar 4.10 Automatically start the WinPCap driver at boot time agar winpcap selalu diaktifkan saat booting

12. Tunggu hingga proses instalasi WinPcap dijalankan.



Gambar 4.11 Instalasi WinPcap dijalankan

13. Di Completing the WinPcap Setup wizard, klik **Finish**.

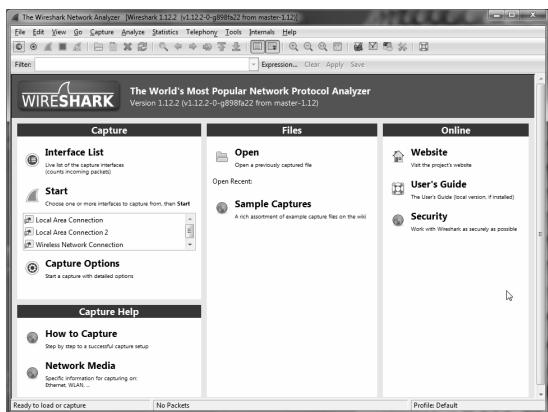


Gambar 4.12 Klik Finish di WinPcap setup wizard

4.1.2 Menggunakan Wireshark

Setelah diinstal, Anda dapat menggunakan Wireshark seperti berikut ini:

1. Jalankan Wireshark dengan antarmuka seperti berikut ini:



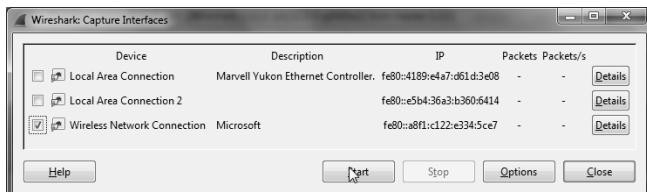
Gambar 4.13 WireShark

2. Klik pada Interface List untuk memilih antarmuka yang akan digunakan.



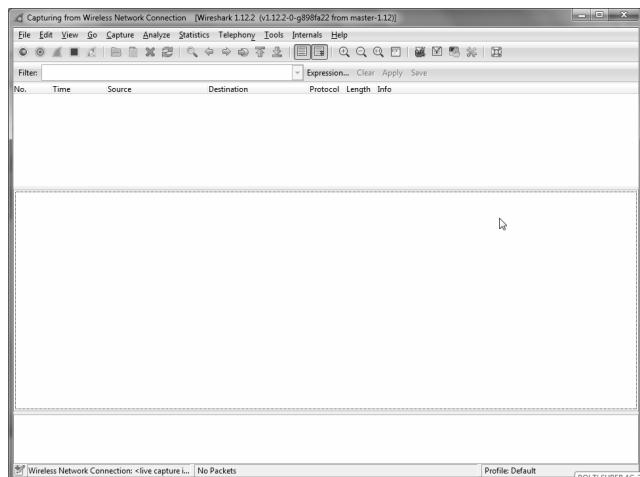
Gambar 4.14 Interface List

3. Beberapa koneksi yang ada di komputer ditampilkan. Pilih pada koneksi yang akan diintai dengan memberi tanda cek kemudian klik Start.



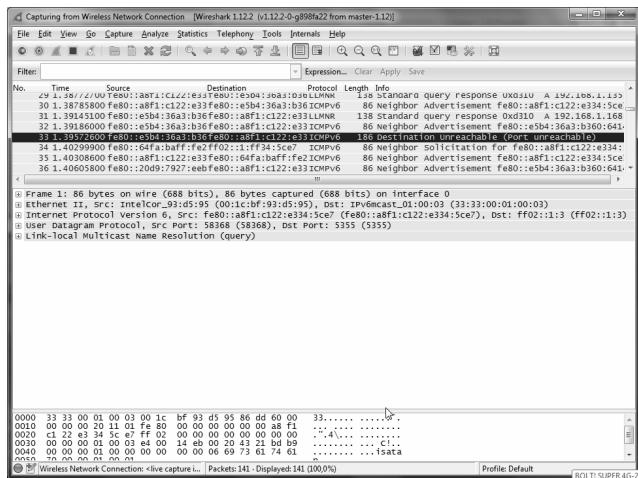
Gambar 4.15 Klik Start untuk memindai koneksi

4. Anda bisa melihat alat Wire Shark ini tidak menampilkan apa-apa ketika tidak ada transfer data di internet (contoh di sini menggunakan wireless network yang merupakan koneksi ke modem HSDPA).



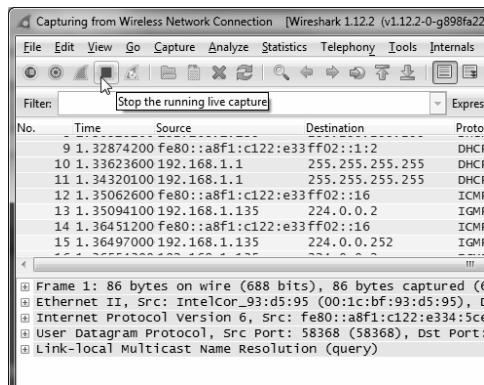
Gambar 4.16 Wire Shark

5. Ketika Anda memulai browsing atau ketika ada transfer data, maka muncul data-data yang ditransfer, beserta protokol, port, dan lainnya secara detil.



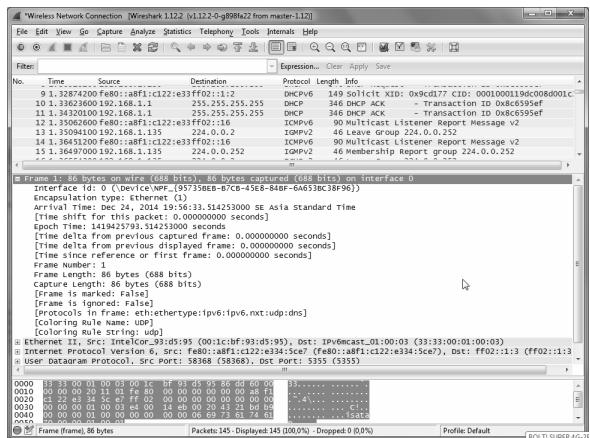
Gambar 4.17 Tampilan sniffing

- Untuk menghentikan sniffing, klik pada tombol **Stop** seperti tombol berikut ini:



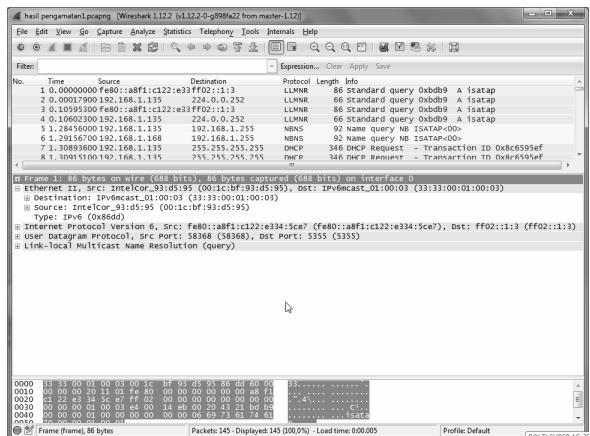
Gambar 4.18 Klik Stop untuk menghentikan capture data

- Data-data yang sudah di-capture bisa dianalisa lebih lanjut. Misalnya Frame menampilkan informasi data jumlah frame, panjang frame dan protokol yang terlibat dalam frame data tertentu.



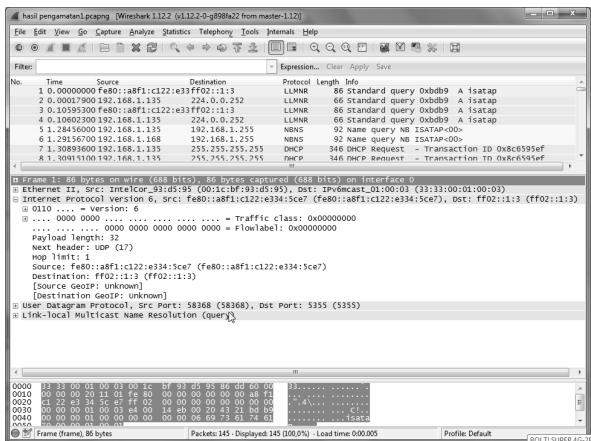
Gambar 4.19 Frame data

8. Tampilan data di Ethernet menampilkan tujuan, source dan jenis protokol.



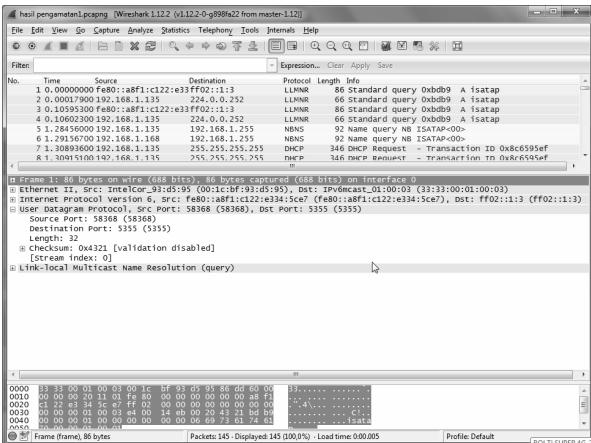
Gambar 4.20 Tampilan data di ethernet

9. Anda bisa mem-breakdown lagi alamat tujuan dan alamat sumber dari data.



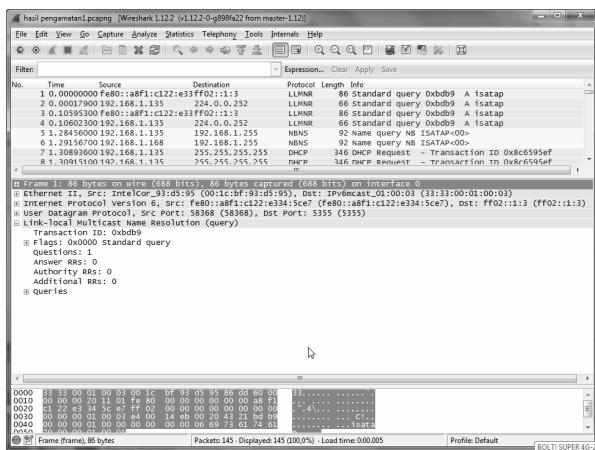
Gambar 4.21 Alamat tujuan dan alamat sumber dari data

- Di UDP, Anda bisa melihat diagram data protocol, seperti sumber, tujuan, panjang, checksum dan lain sebagainya.



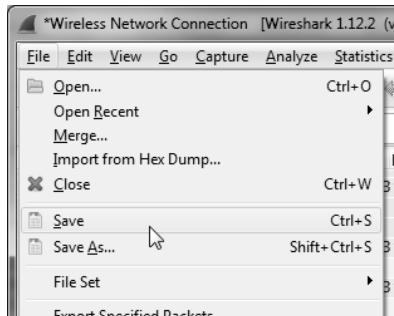
Gambar 4.22 Tujuan UDP

- Di Link Local Multicast, Anda bisa melihat informasi multicast, seperti id transaksi, questions, answer RSS dan RSS tambahan.



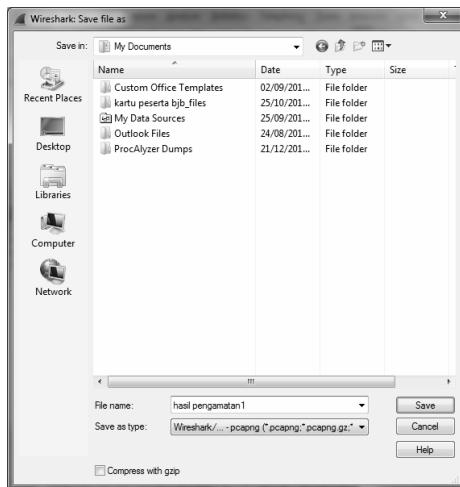
Gambar 4.23 Link Local Multicast

12. Untuk menyimpan data, klik tombol **File > Save**.



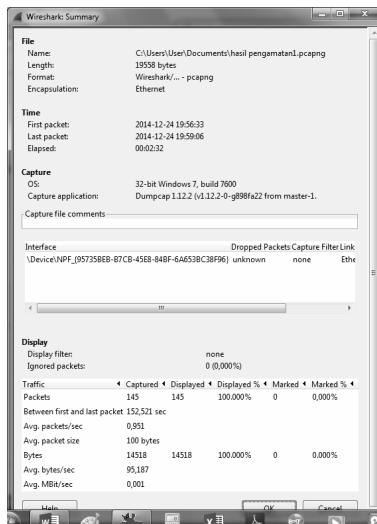
Gambar 4.24 Klik pada File > Save

13. Isikan nama file yang akan menyimpan data wireshark.



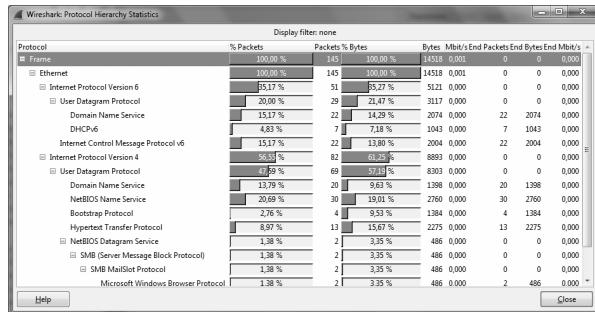
Gambar 4.25 Mengisikan nama file untuk menyimpan data

14. Klik **Statistics Summary** untuk melihat ringkasan data, termasuk sistem operasi yang dipakai untuk meng-capture.



Gambar 4.26 Summary sistem

15. Klik **Statistics > Protocol Hierarchy** untuk melihat hierarki protokol yang digunakan.



Gambar 4.27 Hierarki protokol yang diambil data

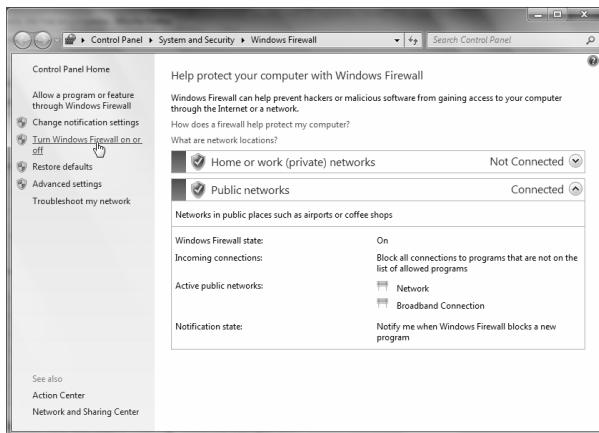
4.2 Windows Firewall

Dalam sistem komputer yang terkoneksi ke internet atau jaringan, komputer sebenarnya menjadi rentan terhadap virus dan spyware. Ini karena komputer terbuka dengan lingkungannya.

Untuk mengamankan komputer dalam jaringan lokal atau internet, Anda lebih baik menggunakan firewall. Firewall adalah benteng antara komputer Anda dengan lingkungan sekitarnya.

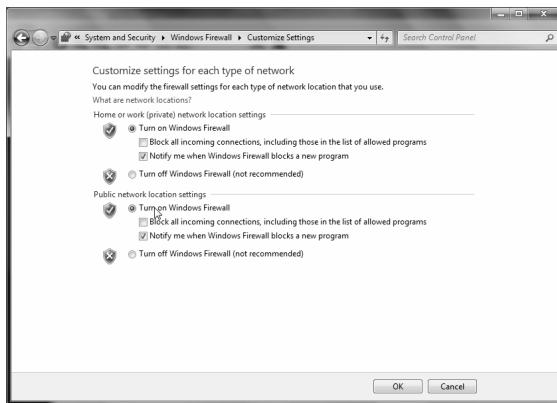
Windows sendiri sudah memiliki fasilitas firewall yang memungkinkan Anda mengamankan komputer dari lingkungan sekitarnya, baik jaringan lokal atau internet.

1. Di **Windows**, aktifkan **Control Panel > System and security > Windows Firewall**.



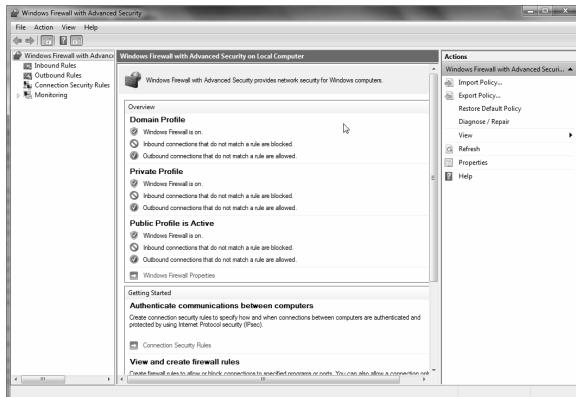
Gambar 4.28 Windows Firewall

2. Anda bisa menentukan apakah jaringan terhubung untuk jaringan lokal atau internet (public network).
3. Untuk mengaktifkan atau menonaktifkan firewall untuk komputer lokal, Anda bisa memilihnya di **Home or work (private) network location settings**.



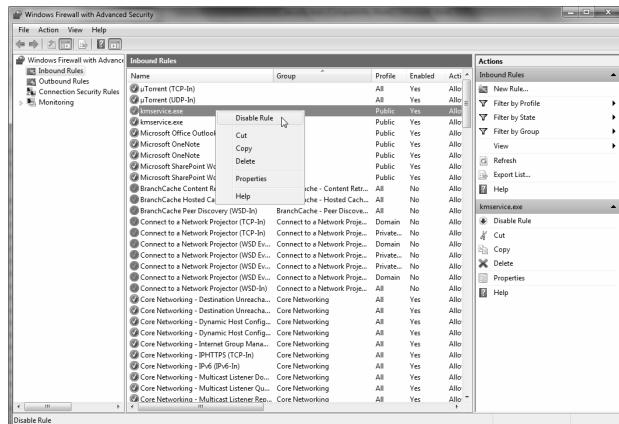
Gambar 4.29 Kostumisasi windows firewall

4. Klik **Advanced Settings**, Anda bisa melihat setting advanced untuk firewall.



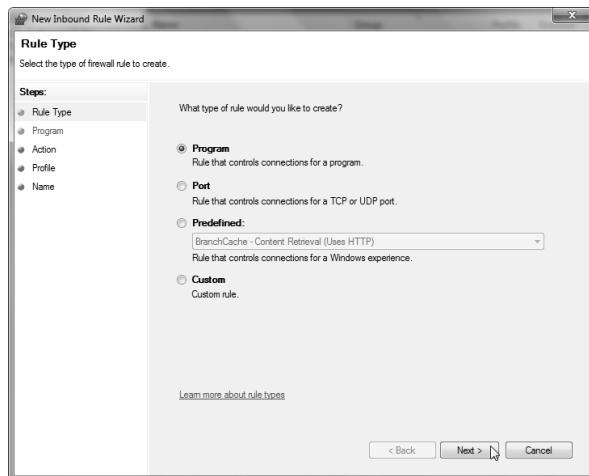
Gambar 4.30 Advanced settings

5. Anda dapat mengaktifkan dan menonaktifkan rule. Untuk menonaktifkan rule, klik kanan pada rule dan pilih **Disable rule**.



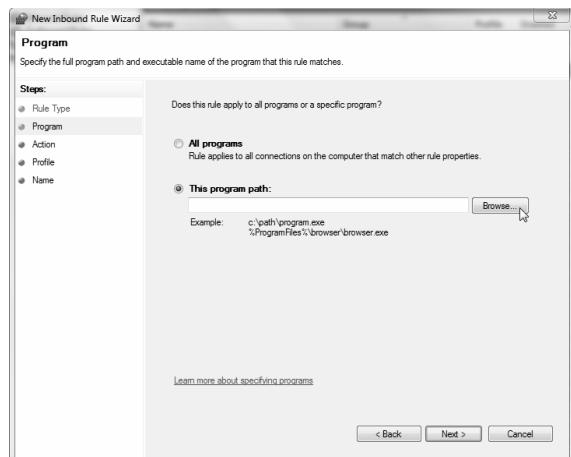
Gambar 4.31 Menu untuk disable rule

6. Anda bisa menambahkan rule sendiri dengan klik pada **New Rule**.



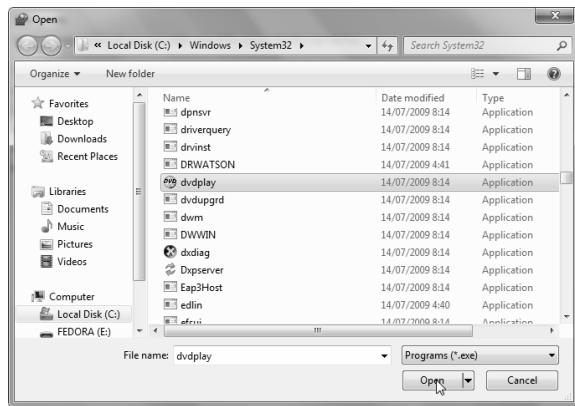
Gambar 4.32 Menambahkan dengan new rule

7. Tentukan apakah rule tersebut hendak dikenakan pada program, port atau lainnya. Misalnya penulis hendak memberikan pada program.
8. Pilih programnya di **The program path** dengan klik **Browse**.



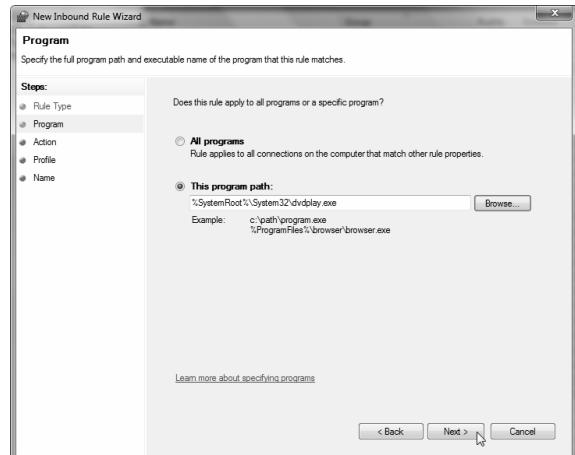
Gambar 4.33 Memilih program untuk diterapkan rule

9. Pilih program di jendela **Open**.



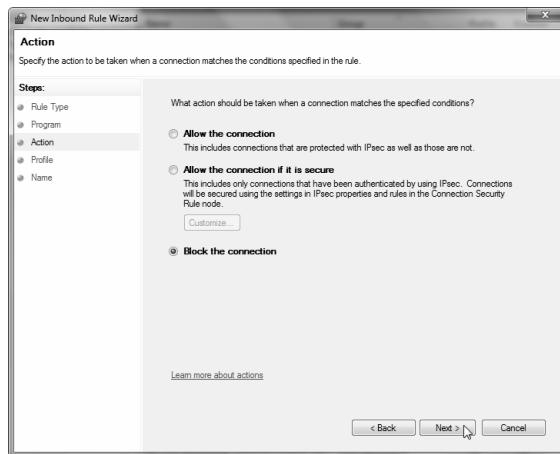
Gambar 4.34 Pemilihan program di jendela Open

10. Kembali ke pemilihan program, path dari program terlihat di **This program path**. Klik **Next**.



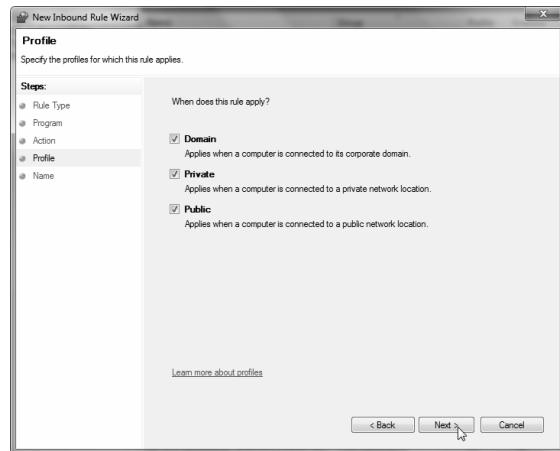
Gambar 4.35 This program path

11. Anda bisa menentukan rule untuk program ini, apakah membolehkan/allow atau menghalangi/block. Klik **Next** kemudian.



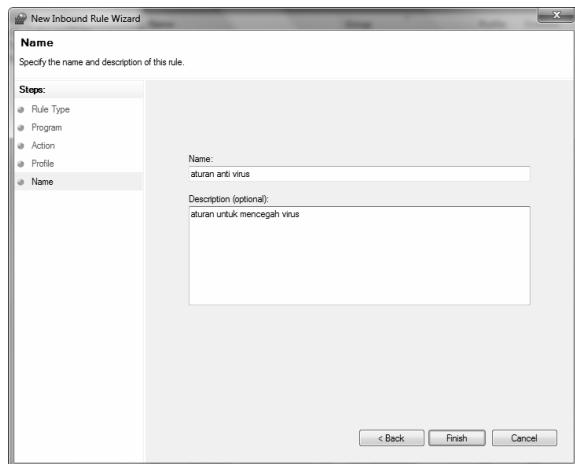
Gambar 4.36 Menentukan apakah Anda ingin allow atau block

12. Anda bisa menentukan apakah rule ini akan diterapkan ke domain, private atau publik. Klik **Next**.



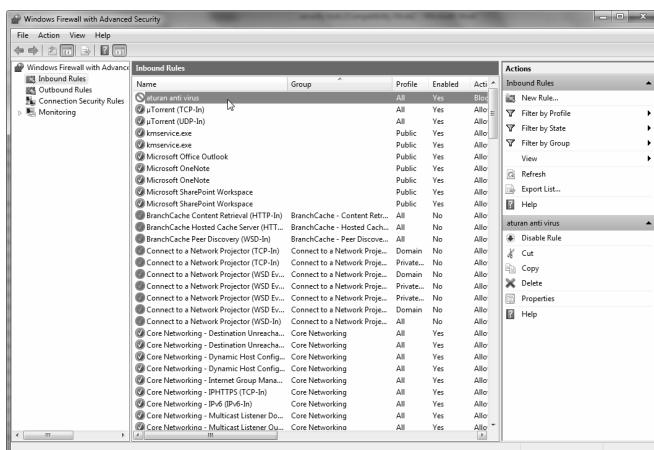
Gambar 4.37 Menentukan ruang lingkup rule

13. Tentukan nama rule di **Name** dan deskripsi rule di **Description (optional)**. Klik **Finish**.



Gambar 4.38 Nama dan deskripsi rule di Optional

14. Maka rule akan diperlihatkan di jendela Advanced settings.



Gambar 4.39 Rule baru sudah dibuat

15. Rule akan langsung diterapkan ketika sudah terbuat. Dengan cara yang sama, Anda juga bisa memblok port tertentu di komputer Anda untuk menonaktifkan download torrent, dan lainnya yang relatif berbahaya terhadap susunan spyware.

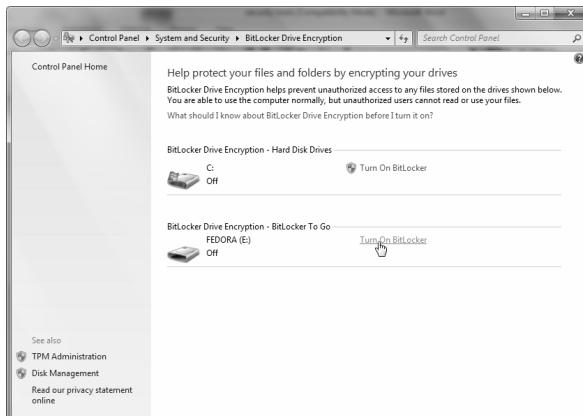
4.3 BitLocker

Untuk menyimpan data berharga dari serangan virus, spyware atau malware, Anda dapat mengenkripsi dan menyimpan file menggunakan software Bitlocker.

Bitlocker ini adalah fasilitas bawaan dari windows yang tugasnya mengenkripsi disk atau volume portabel. Berbeda dengan software lainnya, bit locker tidak perlu didownload, karena sudah ada secara asli di Win Vista, 7 dan Windows 8.

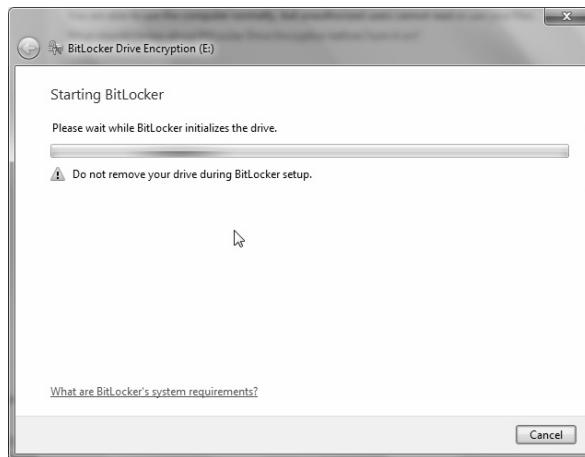
Cara menggunakan bitlocker adalah:

1. Klik **Start** kemudian ketikkan bit locker di **Search**.
2. Ketikkan bitlocker untuk mencari aplikasi ini, kemudian klik **Enter** untuk menjalankan bitlocker. Atau kalau memakai Windows 8, cari BitLocker di start screen.
3. Muncul jendela **BitLocker disk encryption**. Untuk mengaktifkan, klik pada **Turn on bitlocker** pada volume yang ingin Anda proteksi.



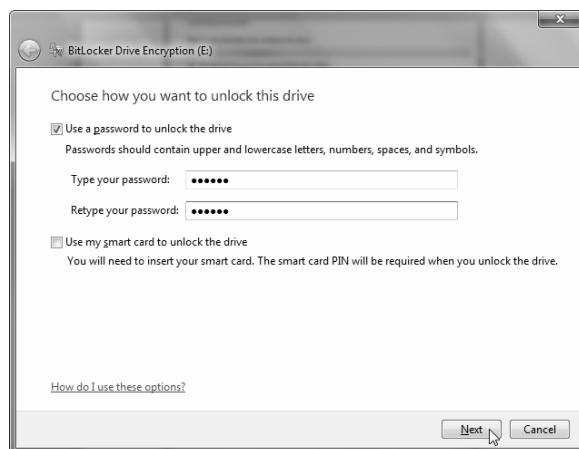
Gambar 4.40 Mengaktifkan proteksi pada volume tertentu

4. Maka muncul jendela **Starting BitLocker**, proses pengaktifan enkripsi sedang dimulai.



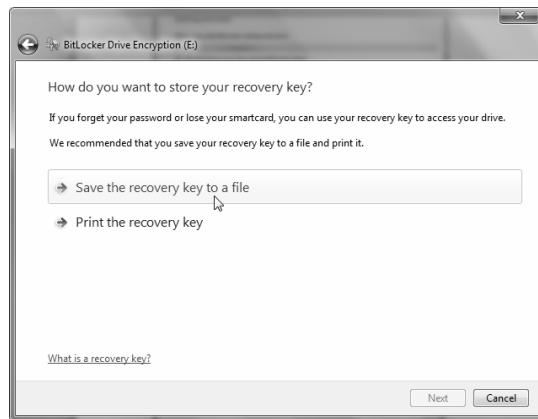
Gambar 4.41 Bitlocker sedang mengaktifkan enkripsi untuk volume tertentu

5. Isikan password 2x di **Type your password**, dan **Retype your password**. Klik **Next** kemudian.



Gambar 4.42 Choose how you want to unlock this drive

6. Berikutnya, Anda bisa memilih apakah membuat recovery keyfile. Klik **Save the recovery key to a file**.



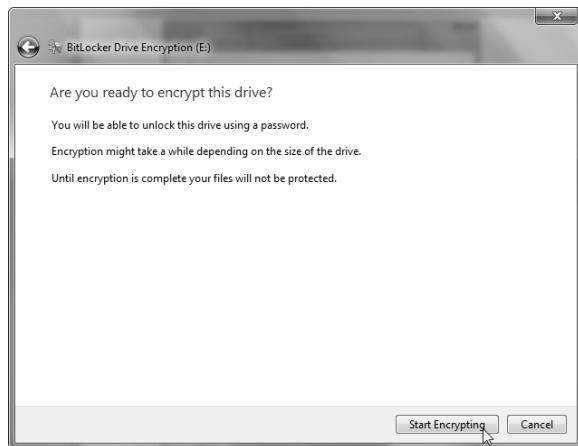
Gambar 4.43 Save the recovery key to file

7. Tentukan nama file untuk menyimpan recovery file. Kemudian klik **Save**.



Gambar 4.44 Pemilihan file untuk keyfile recovery

8. Ketika muncul pertanyaan **Are you ready to encrypt this drive**, klik **Start Encrypting**.



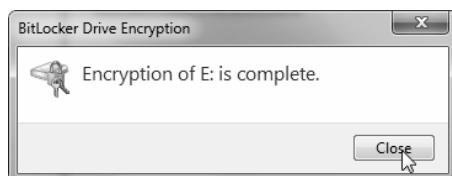
Gambar 4.45 Start encrypting

9. Proses enkripsi akan dijalankan.



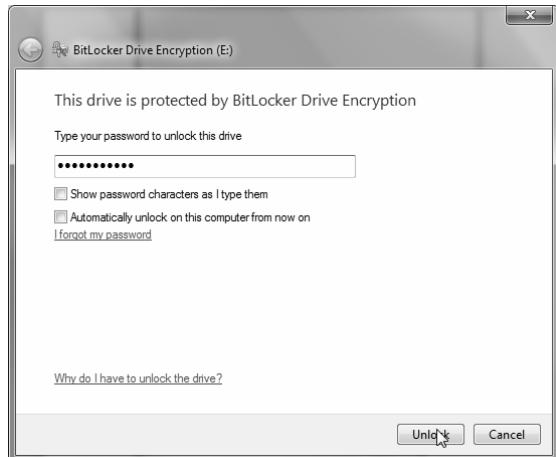
Gambar 4.46 Proses enkripsi sedang dijalankan

10. Ketika enkripsi sudah lengkap, klik **Encryption is complete**.



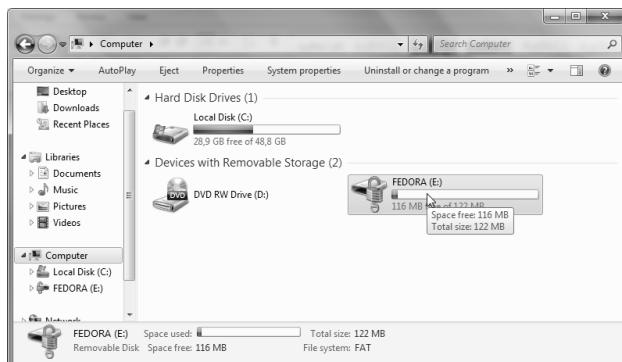
Gambar 4.47 Enkripsi sudah lengkap

11. Ketika Anda hendak mengakses drive, muncul kotak pemberitahuan bahwa drive dilindungi oleh **Bitlocker drive encryption**.
12. Masukkan password kemudian klik **Unlock**.



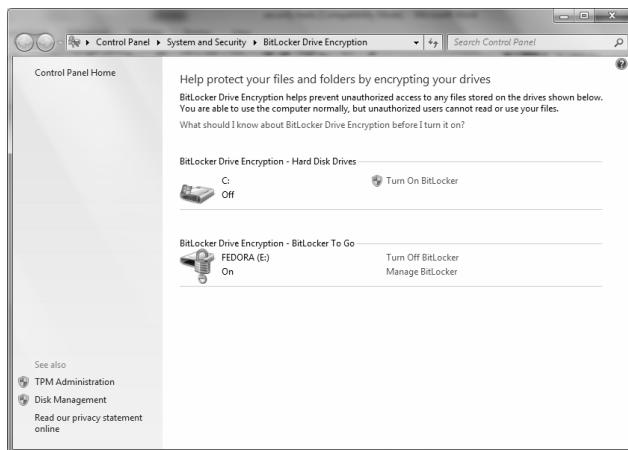
Gambar 4.48 Memasukkan password untuk unlock

13. Ketika password sudah benar, di Windows Explorer muncul ikon dari drive. Tapi ikon drive sedikit berbeda, yaitu ada ikon kunci.



Gambar 4.49 Ikon kunci menandakan drive adalah drive yang terenkripsi oleh bitlocker

14. Anda juga bisa menonaktifkan bitlocker dengan membuka Bitlocker Drive encryption kemudian klik **Turn off bitlocker**.



Gambar 4.50 Turn off bitlocker untuk mengaktifkan

4.4 Alternatif Penyelamatan Terakhir dengan Rescue CD

Bagaimana jika virus, hacker atau spyware sudah mengacak-acak komputer Anda? Dan komputer tidak bisa booting dan menjalankan sistem operasi. Apa yang akan Anda lakukan? Alternatif penyelamatan terakhir adalah dengan menggunakan sebuah rescue CD. Sebuah software yang bisa mengecek komputer yang sedang pingsan. Rescue Cd memiliki sistem operasi sendiri yang nanti mem-booting dan bisa menyelamatkan data dari komputer, sekaligus memindai apakah ada virus atau spyware di situ.

4.4.1 System Rescue CD

System rescue cd adalah sebuah cd bootable yang bisa dibooting tanpa menggunakan sistem operasi karena memiliki sistem operasi Linux liveCD sendiri.

SystemRescueCD memungkinkan penyelamatan komputer yang sudah sakit, atau bahkan yang mati total dimana sistem operasi standarnya tidak bisa dijalankan.

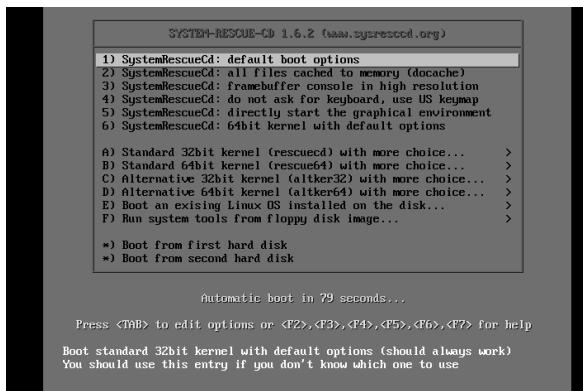
Beberapa tool yang tersedia di System rescue CD adalah:

- GNU Parted dan GParted untuk mempartisi disk dan mengatur ulang ukuran partisi. Banyak format disk yang didukung, antara lain FAT32 dan NTFS.
- Ranish Partition Manager.
- fdisk untuk mengedit tabel partisi disk.
- PartImage, software disk imaging untuk menyalin sektor yang dipakai.
- TestDisk untuk me-recovery file, data dan partisi. Juga pasangannya PhotoRec untuk me-recovery data hilang.
- CD dan DVD burner, yang bisa digunakan untuk membakar data ke cd dan dvd.
- Dua buah bootloader: GRUB dan SYSLINUX
- Web browser seperti Mozilla Firefox, Lynx, Links, dan Dillo.
- Software mirip MS Explorer, yaitu Midnight Commander
- Software untuk membuat file arsip dan ekstrak.
- Tool file system tool: untuk membuat sistem file, delete dan resize.
- Mendukung banyak sistem file seperti NTFS read/write access dan juga FAT32 serta Mac OS HFS.
- Mendukung arsitektur komputer Intel x86 dan PowerPC, termasuk Mac.
- Bisa membuat boot disk untuk berbagai sistem operasi.
- Mendukung editing registry Windows dan mampu mengubah password dari Linux.
- Bisa memboot FreeDOS, Memtest86+, software dianostik hardware dan boot disk lain dari satu CD saja.

Tidak semua fitur dari system rescue cd dijelaskan, tapi penulis akan menjelaskan prinsip dasar cara menggunakan system rescue CD ini. Pertama Anda harus mendownloadnya baru kemudian bisa dipakai.

Langkah-langkah penggunaannya seperti berikut ini:

1. Buka halaman download untuk system rescue CD di <http://www.sysresccd.org/Download>.
2. Di pemilihan tipe booting, set **default boot options**.



Gambar 4.51 Pemilihan default boot options

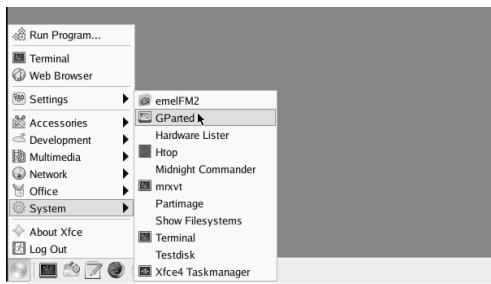
3. Default tampilan adalah teks, tanpa adanya xWindow. Untuk menjalankan xWindows/tampilan grafis, ketikkan “startx” di command line.

```
* Doing udev cleanups
=====
SystemRescue-Cd ----- 1.6.2 ===== tty1/6 ==
http://www.sysresccd.org/
* You should stop the Network-Manager service if you want to configure
  the network by hand. Just run this command: /etc/init.d/NetworkManager stop
* Type net-setup eth0 to specify ethernet configuration.
* If your PC is on an ethernet local network, you can configure by hand:
  - ifconfig eth0 192.168.x.a (your static IP address)
  - route add default gw 192.168.x.b (IP address of the gateway)
* To be sure there is an ssh server running, type /etc/init.d/sshd start.
  You will need to create an user or to change the root password with passwd.
* Available console text editors: nano, vim, gemacs, joe.
* Web browser in the console: elinks www.web-site.org.
* Ntfs-3g : If you need a full Read-Write NTFS access, use Ntfs-3g.
  Mount the disk: ntfs-3g /dev/sdal /mnt/windows
* Graphical environment : use either Xorg or Xfbdev.
  Type wizard to run the graphical environment (or startx but it may fail)
  X.Org comes with the Xfce environment and several graphical tools:
    - Partition manager:..gparted
    - Web browsers:.....firefox-3.6
    - Text editors:.....gvim and geany
root@localhost /root % startx_

```

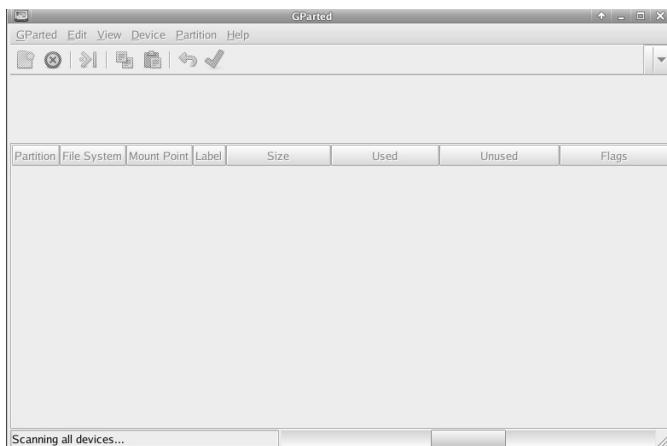
Gambar 4.52 Mengisikan startx di command line

- Untuk mengedit partisi, klik pada tombol **menu** > **System** > **Gparted**. Gparted adalah software untuk editing partisi hard disk. Anda bisa mengubah partisi-partisi hard disk di komputer yang sedang rusak atau terjangkiti penyakit.



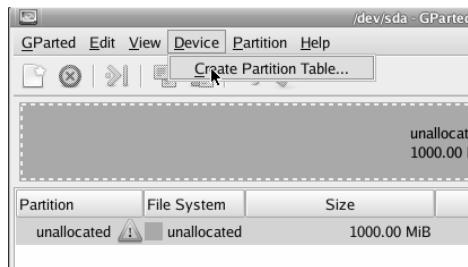
Gambar 4.53 Menu untuk menjalankan Gparted

- Pertama kali diaktifkan, Gparted akan menyelidiki kondisi hard disk di komputer Anda.



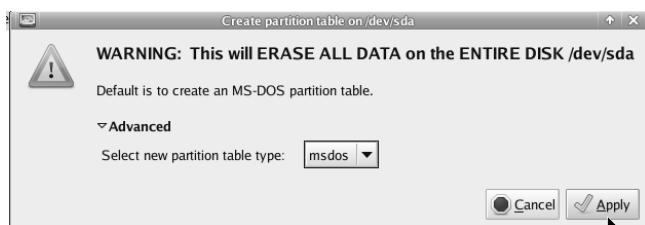
Gambar 4.54 Gparted menyelidikan kondisi hard disk di komputer Anda

- Untuk hard disk yang belum pernah disentuh sama sekali, Anda bisa membuat tabel partisi terlebih dahulu dengan klik menu **Device** > **Create partition table**.



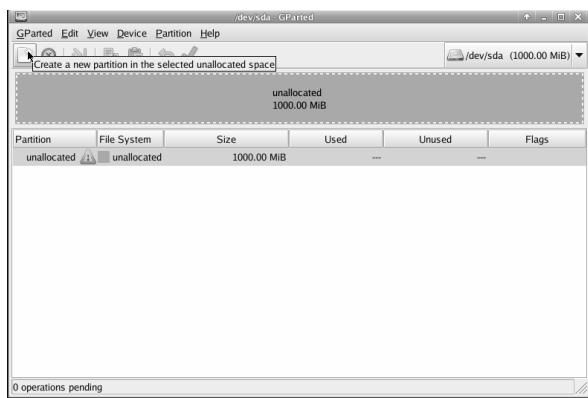
Gambar 4.55 Create partition table

7. Tentukan tipe tabel partisi, dan klik **Apply**.



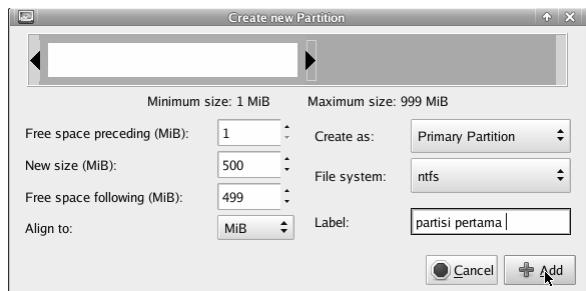
Gambar 4.56 Penentuan tabel partisi dan klik Apply

8. Ketika tabel partisi sudah ada, Anda baru bisa membuat partisi baru. Caranya klik **Create new**.



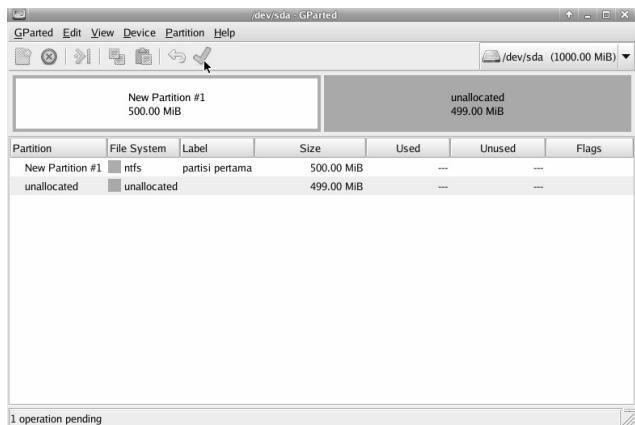
Gambar 4.57 Create new untuk membuat partisi baru

9. Tentukan ukuran partisi di **New Size (MB)**.



Gambar 4.58 Penentuan properti dari partisi baru

10. Tentukan tipe partisi apakah **Primary** atau **Secondary**.
11. Tentukan label di **Label**.
12. Untuk mengeksekusi partisi, klik tanda **Centang**.



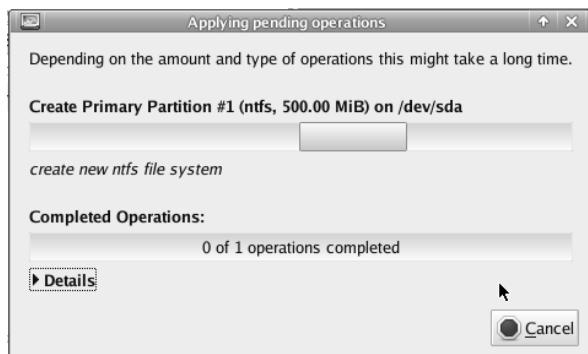
Gambar 4.59 Partisi sebelum dieksekusi

13. Saat muncul konfirmasi apakah Anda ingin mengeksekusi operasi. Klik **Apply**.



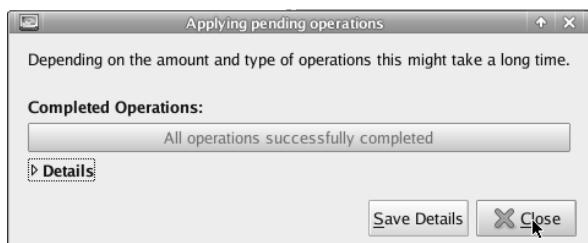
Gambar 4.60 Konfirmasi apakah ingin mengeksekusi operasi

14. Proses pengeditan partisi akan dijalankan.



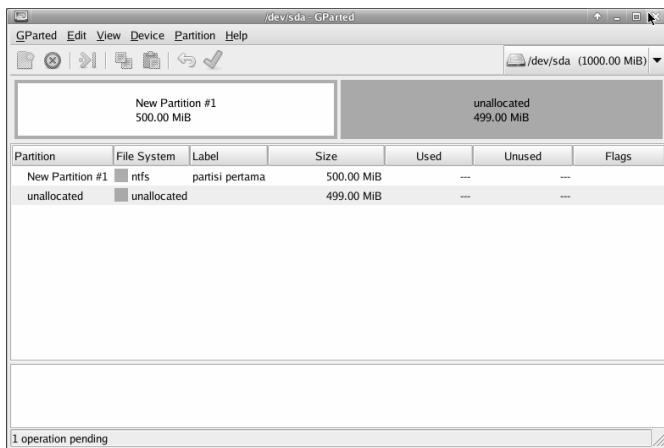
Gambar 4.61 Proses pengeditan partisi akan dijalankan

15. Kalau operasi sudah selesai, muncul pemberitahuan **All Operations successfully completed**. Klik Close.



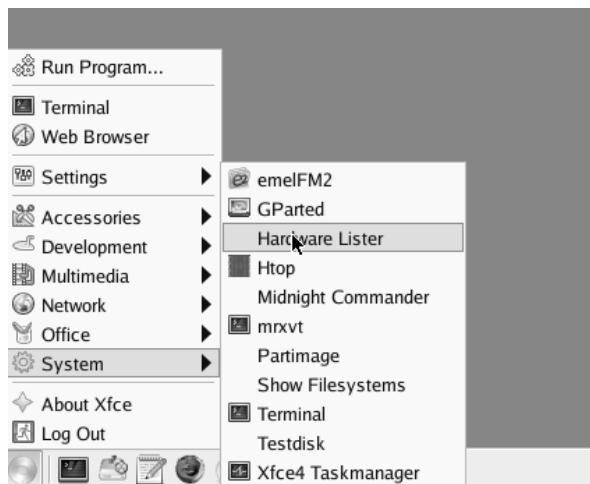
Gambar 4.62 Semua operasi sudah diselesaikan

16. Setelah tereksekusi, partisi akan terbuat dengan sempurna.



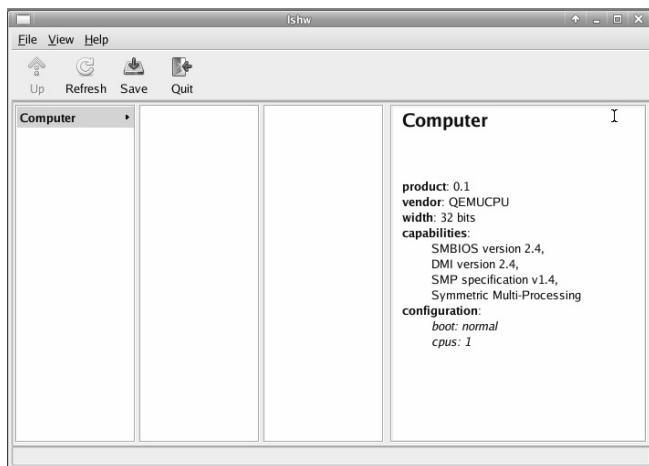
Gambar 4.63 Partisi terbuat dengan sempurna

17. Anda juga bisa melihat spek hardware dengan klik pada **Menu > System > Hardware Lister**.



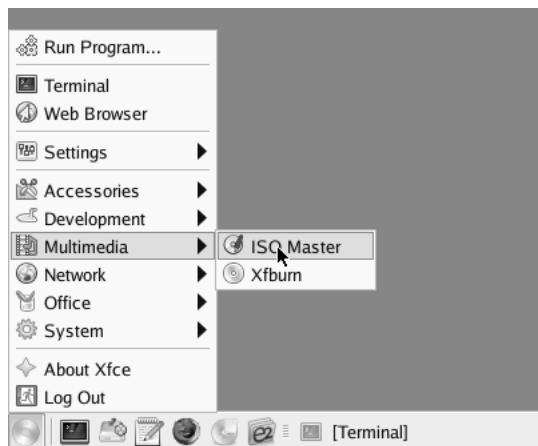
Gambar 4.64 Menu untuk mengetahui spek hardware komputer yang rusak

18. Spek hardware akan terlihat di jendela yang muncul.



Gambar 4.65 Spek hardware

19. Misalnya Anda ingin menyelamatkan data dari komputer yang rusak, caranya bisa dengan membakarnya ke CD atau DVD. Ada tool **Multimedia > ISO Master** untuk melakukan hal ini.



Gambar 4.66 Multimedia > Iso Master untuk menjalankan program ini

20. Di jendela **ISO master**, Anda bisa mendrag file yang akan dibakar ke CD dengan menggesernya ke bawah. Anda juga bisa membuat folder dengan membuat **Create new directory**.



Gambar 4.67 Pembuatan folder

21. Untuk mematikan sysrescue ini, klik pada tombol **Menu > Log off**.

```
Build Operating System: Linux 2.6.32-23-fd10.fc13.x86_64 i686 Gentoo
Current Operating System: Linux localhost.localdomain 2.6.35-std162-i386 #9 SMP
Mon Oct 11 18:00:53 UTC 2010 i686
Kernel command line: scandelay=1 initrd=initram.img BOOT_IMAGE=rescuecd
Build Date: 10 October 2010 10:05:02PM

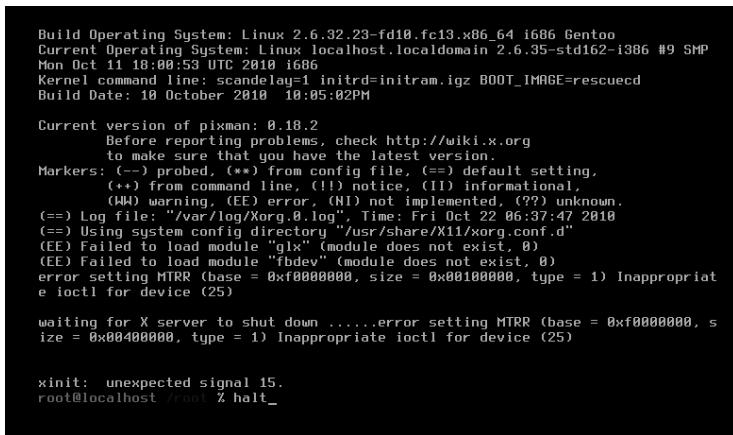
Current version of pixman: 0.18.2
Before reporting problems, check http://wiki.x.org
to make sure that you have the latest version.
Markers: (--) probed, (**) from config file, (==) default setting,
(++) from command line, (!!) notice, (II) informational,
(WW) warning, (EE) error, (NI) not implemented, (??) unknown.
(==) Log file: "/var/log/Xorg.0.log", Time: Fri Oct 22 06:37:47 2010
(==) Using system config directory "/usr/share/X11/xorg.conf.d"
(EE) Failed to load module "glx" (module does not exist, 0)
(EE) Failed to load module "fbdev" (module does not exist, 0)
error setting MTTR (base = 0xf0000000, size = 0x00100000, type = 1) Inappropriate ioctl for device (25)

waiting for X server to shut down .....error setting MTTR (base = 0xf0000000, size = 0x00400000, type = 1) Inappropriate ioctl for device (25)

xinit: unexpected signal 15.
-
```

Gambar 4.68 System rescue CD akan dimatikan

22. Untuk mematikan total, ketikkan “halt” di bagian command line.



```
Build Operating System: Linux 2.6.32.23-fd10.fc13.x86_64 i686 Gentoo
Current Operating System: Linux localhost.localdomain 2.6.35-std162-1386 #9 SMP
Mon Oct 11 10:00:53 UTC 2010 i686
Kernel command line: scandelay=1 initrd=initram.igz BOOT_IMAGE=rescuecd
Build Date: 10 October 2010 10:05:02PM

Current version of pixman: 0.18.2
Before reporting problems, check http://wiki.x.org
to make sure that you have the latest version.

Markers: (--) probed, (**) from config file, (=) default setting,
(++) from command line, (!!) notice, (II) informational,
(WW) warning, (EE) error, (NI) not implemented, (??) unknown.

Log file: "/var/log/Xorg.0.log", Time: Fri Oct 22 06:37:47 2010
Using system config directory "/usr/share/X11/xorg.conf.d"
(FE) Failed to load module "glx" (module does not exist, 0)
(FE) Failed to load module "fbdev" (module does not exist, 0)
error setting MTRR (base = 0xf0000000, size = 0x00100000, type = 1) Inappropriate ioctl for device (25)

Waiting for X server to shut down .....error setting MTRR (base = 0xf0000000, size = 0x00400000, type = 1) Inappropriate ioctl for device (25)

xinit: unexpected signal 15.
root@localhost ~% halt
```

Gambar 4.69 Mengetikkan “halt” di command line

23. Setelah komputer mati dengan aman, Anda bisa mendapatkan data-data Anda yang penting di CD atau mempartisi. Selain itu Anda juga bisa me-recovery data untuk kemudian dibackup.

4.4.2 AVG Rescue CD

Tool lain untuk rescue CD, namun dalam bentuk tekstual adalah AVG Rescue CD. Tool ini buatan AVG namun disebarluarkan secara gratis. Anda bisa mendownloadnya dari <http://www.avg.com/us-en/download-file-cd-arm-iso>

Kemudian file iso tersebut bisa dibakar ke CD sama seperti System Rescue CD menggunakan software CD burner. Boot komputer ke drive optik CD/DVD untuk mengakses fasilitas ini.

Menggunakan AVG Rescue CD

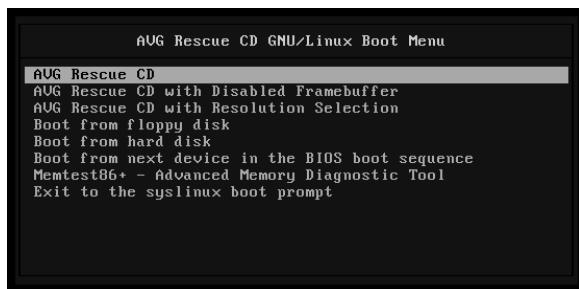
Saat cd berisi AVG rescue cd di-boot, maka muncul beberapa menu. Berikut ini beberapa arti dari menu-menu yang ada:

- Scan: Melakukan scan secara langsung
- Scan Result: Menampilkan laporan hasil scan

- Update: Melakukan update AVG Rescue CD, bisa update online, manual (file update di copykan ke komputer dulu) atau download
- Vault: Untuk melihat virus/malware yang disimpan di AVG virus vault, dan me-restore jika mungkin itu hanya kesalahan mendeteksi
- Mount: Untuk memulai mounting (menampilkan/melihat) drive seperti media berbasis USB.
- Network: Untuk mengatur koneksi jaringan
- USB: Untuk membuat bootable USB Flash drive yang berisi AVG Rescue CD
- Utilities: Beberapa tool bermanfaat seperti File manager, registry editor, Ping dan Test Disk
- Eject: Membuka/menutup CD/DVD-ROM Drive
- Reboot: untuk me-restart komputer
- Shutdown – Untuk mematikan komputer
- About: Menampilkan informasi tentang AVG Rescue CD

Berikut ini cara penggunaan AVG Rescue CD:

1. Ketika Anda menjalankan booting dari CD, tampilan yang Anda hadapi seperti berikut ini:



Gambar 4.70 Pilihan awal booting

2. Tunggu hingga semua library AVG ter-load.

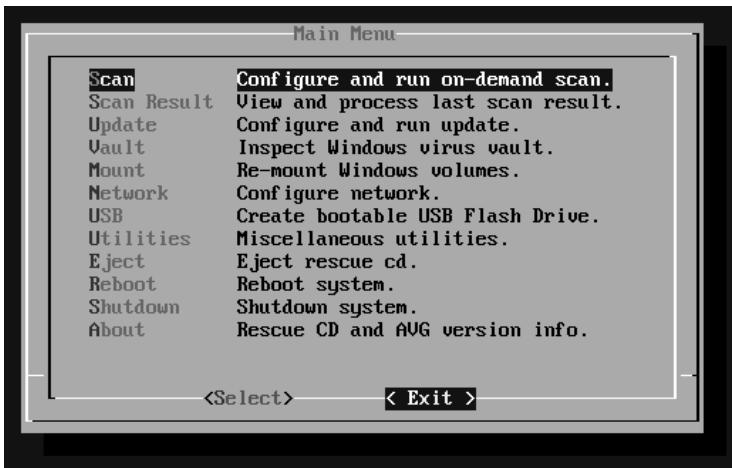
```

scsi0 : ata_pmix
scsi1 : ata_pmix
ata0: PATA max UDMA/2 cmd 0x1f0 ctl 0x3f6 bdma 0xc000 irq 14
ata1: PATA max UDMA/2 cmd 0x170 ctl 0x376 bdma 0xc008 irq 15
ata2: ATAPI max 128 sectors, multi 1.0, max UDMA/100
ata3: ATAPI max 128 sectors, multi 1.1, max UDMA/100
ata4: configured for UDMA/100
ata1.00: 2048000 sectors, multi 16: LBA48
ata1.00: configured for UDMA/2
scsi0 0:0:0:0: Direct-access ATA QEMU HARDDISK 0.11 PQ: 0 ANSI: 5
sd 0:0:0:0: attached scsi generic sg1 type 5
sd 0:0:0:0: (sda) Attached SCSI disk
B139cp: B1390+ Fast Ethernet driver v0.9.28
B139cp: B1390+ Fast Ethernet driver v0.9.28 (Oct 2002)
B139cp: B1390+ 10/100 PCI Ethernet driver v1.3 (Mar 22, 2004)
PCI: PCI Interrupt Link [LNKC1] enabled at IRQ 11
B139cp 0000:00:00:03:0: PCI INT A -> Link[LNKC1] -> GSI 11 (level, low) -> IRQ 11
B139cp 0000:00:03:0: eth0: RTL-B139C at 0x0b8c000, 52:54:00:1b:ae:5f, IRQ 11
Initializing random number generator... done.
Setting up DM-MD devices...
no valid drivers found
Starting network...
dhcpc (v1.16.1) started
Sending discover...
Sending select for 10.0.2.15...
Received lease of 10.0.2.15 obtained, lease time 86400
selected routers
route: SIGHUP:RT: No such process
adding dns 10.0.2.3
ip: RTNETLINK answers: File exists
Starting sshd: OK
kernel.shmax = 134217728

```

Gambar 4.71 Loading library AVG

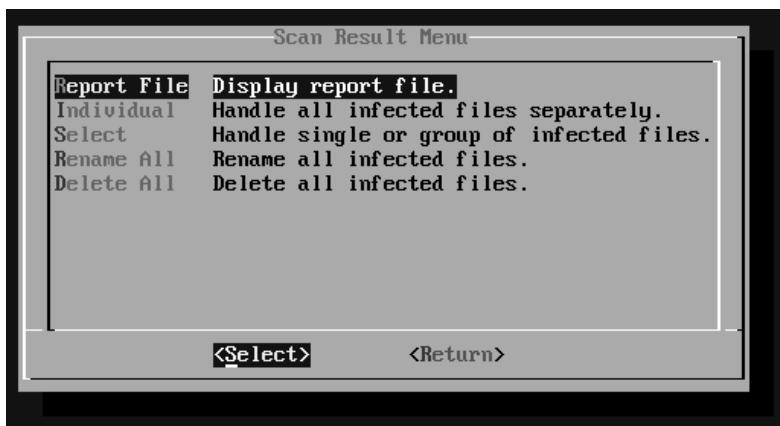
- Ada berbagai menu, Anda bisa memilih dengan klik **Enter**.



Gambar 4.72 Berbagai menu

- Salah satunya, Anda bisa melakukan **Scan** dengan menggunakan database dari virus AVG. Anda juga bisa update antivirus, baik secara online, download atau offline (manual)

5. Ada juga fasilitas **System Recovery** dari infeksi virus dan spyware
6. AVG System recovery ini cocok untuk me-recovery Microsoft Windows (baik file sistem FAT atau NTFS) dan Linux.
7. Bisa dibuat bootable dari CD-ROM atau USB Flashdisk
8. Disediakan tool-tool seperti File Manager, Registry Editor, Test disk dan Ping.
9. Untuk melakukan Scan komputer, pilih menu Scan dari tampilan di atas, yang selanjutnya kita bisa memilih opsi yang tersedia, seperti scan volume (semua file di drive yang ada) atau directory/folder tertentu saja. Saat prosesscan, dapat dihentikan dengan menekan tombol Ctrl+C.



Gambar 4.73 Scan Result

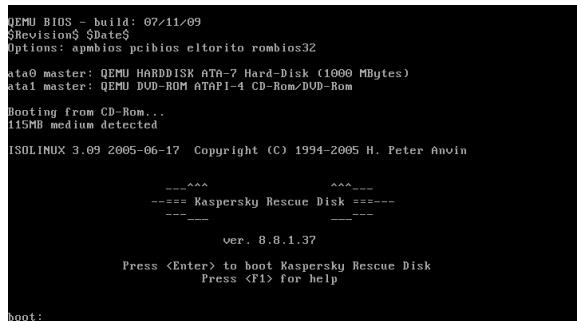
4.4.3 Kaspersky Rescue Disk

Kaspersky, produsen antivirus kelas dunia juga membuat distro live cd untuk keperluan rescue disk. Cd ini bisa diperoleh dari <http://devbuilds.kaspersky-labs.com/devbuilds/RescueDisk/>

Cara menggunakan kaspersky rescue CD seperti berikut:

1. Booting komputer ke CD/DVD kemudian masukkan CD ke dalamnya.

2. Ada tulisan **Press Enter to boot kaspersky rescue disk**, klik Enter tersebut.



Gambar 4.74 Klik Enter untuk booting dari Kaspersky rescue disk

3. Muncul pengecekan file-file dari distro Linux yang dipakai sebagai platform untuk kaspersky ini.

```
- Populating /dev with existing devices through uevents ... ok  
- Letting udev process events ... ok  
- Finalizing udev configuration ... ok  
- Mounting devpts at /dev/pts ... ok  
- Mounting local filesystems ... ok  
- Mounting USB device filesystem (usbfs) ... ok  
- Activating (possible) swap ... ok  
- Setting system clock using the hardware clock [UTC] ... ok  
- Configuring Kernel parameters ... ok  
- Updating environment ... ok  
- Cleaning /var/lock, /var/run ... ok  
- Updating initram ... ok  
- Caching service dependencies ... ok  
- Setting hostname to karescue ... ok  
- Loading key mappings ... ok  
- Setting terminal encoding to UTF-8 ... ok  
- Setting user font ... ok  
- Starting lo ... ok  
* Bringing up lo ... ok  
*      127.0.0.1/8 ... ok  
*      Adding routes ... ok  
*      127.0.0.0/8 ... ok  
* Initializing random number generator ... ok  
[!!] Entering runlevel: 3
```

Gambar 4.75 Pengecekan file-file untuk booting dari distro linux yang dipakai oleh Kaspersky rescue CD

4. Di tab Scan, cek pada item yang mau dipindai.
5. Anda bisa menambahkan lagi dengan klik **Add new item**.



Gambar 4.76 Tab scan untuk memindai komputer untuk mengetahui apakah ada masalah

6. Anda bisa menambahkan objek di **Select object to scan**. Kemudian klik **OK** jika ada berbagai hard disk di komputer Anda.



Gambar 4.77 Select object to scan

7. Atur terlebih dahulu level keamanan untuk pemindaian di **Security level**. Semakin tinggi, semakin detil pencarian.



Gambar 4.78 Pengaturan security level

8. Set pula bagaimana action yang harus dilakukan jika terdeteksi ada ancaman terhadap komputer di **On threat detection**.



Gambar 4.79 On threat detection sedang diatur

9. Kemudian klik **Start scan** untuk memulai pemindaian.



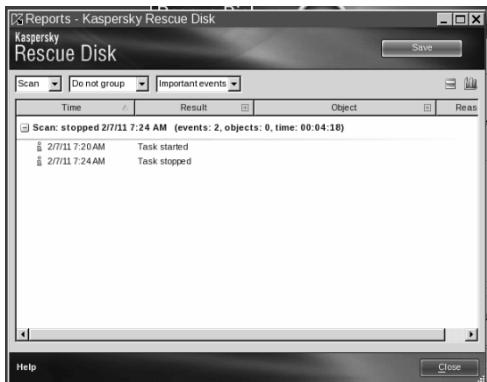
Gambar 4.80 Start scan untuk memulai pemindaian

10. Tunggu hingga scan selesai, untuk menghentikan scan, klik Stop scan.



Gambar 4.81 Scan sedang dilakukan

- Hasilnya langsung muncul report. Jika ada masalah, nanti akan terlihat di sini.



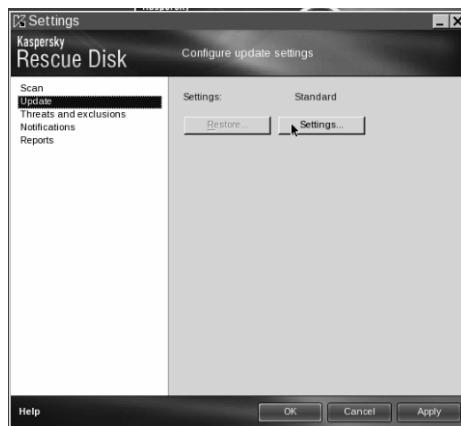
Gambar 4.82 Report scanning dari Kaspersky

- Klik pada **settings** untuk mengatur setting dari kaspersky rescue disk ini.
- Di **Scan**, Anda bisa mengatur opsi pemindaian yang sudah dilakukan.



Gambar 4.83 Opsi pemindaian yang sudah dilakukan

14. Di **Update**, Anda bisa mengatur setting untuk melakukan update database. Ini penting agar kualitas pemindaian baik.



Gambar 4.84 Pemindaian untuk melihat kualitas pemindaian

15. Cek pada source untuk database, Anda bisa menambahkan mirror jika tahu dengan klik **Add**.



Gambar 4.85 Update settings

16. Di **Threats and exclusions**, Anda bisa menentukan bagaimana mengecualikan kategori software tertentu untuk tidak usah dipindai. Klik Settings untuk melihat detilnya.



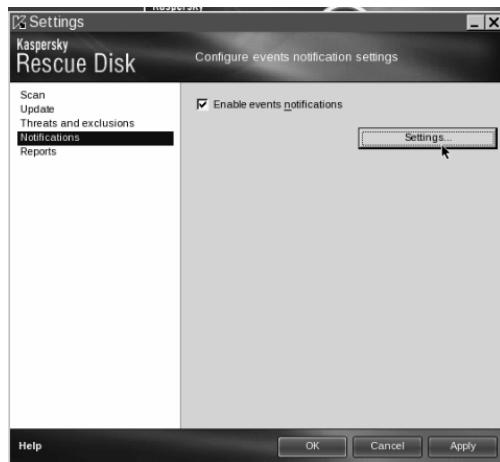
Gambar 4.86 Pengetikan setting untuk Threats and exclusions

17. Hilangkan cek pada kategori program yang tidak ingin dipindai.



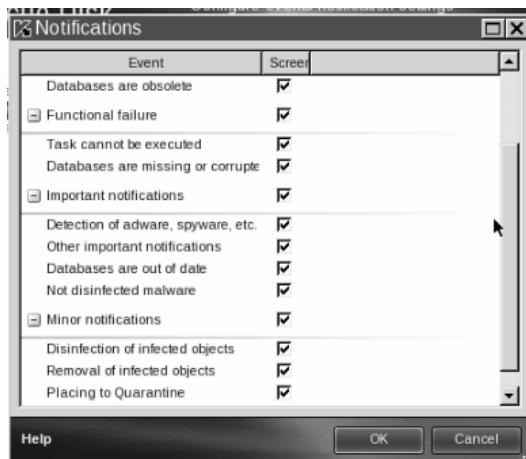
Gambar 4.87 Penghilangan cek pada item yang ingin dipindai

18. Di **Notifications**, Anda bisa menentukan untuk mengaktifkan pemberitahuan/notifikasi atau tidak. Klik Settings untuk mengurnanya.



Gambar 4.88 Pengaturan notifications

19. Cek pada notifikasi yang tidak ingin ditampilkan.



Gambar 4.89 cek pada notifikasi yang tidak ingin ditampilkan

20. Di **Reports**, Anda bisa mengatur bagaimana report ditampilkan.



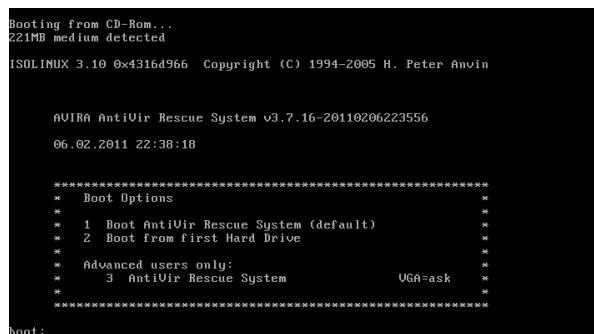
Gambar 4.90 Pengaturan report

4.4.4 Antivir Rescue

Antivir yang merupakan software anti virus juga mengeluarkan layanan rescue CD yang cocok digunakan jika komputer Anda macet karena adanya virus atau malware. Avira antivir rescue ini bisa didapat dari <http://www.avira.com/en/support-download-avira-antivir-rescue-system>.

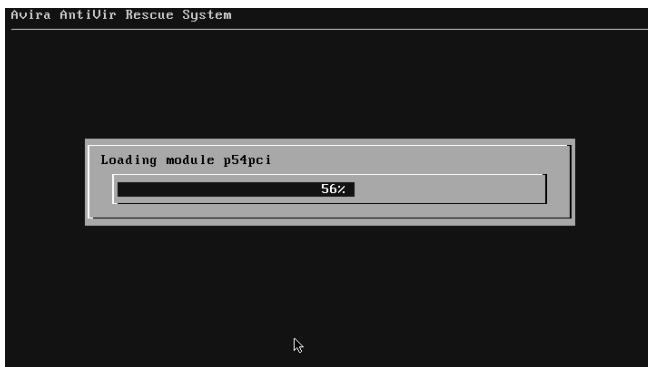
Cara penggunaannya adalah:

1. Boot-lah dari CD yang Anda inginkan.
2. Kalau muncul opsi boting, klik *Enter* langsung untuk menuju ke opsi standar dari **Antivir Rescue system**.



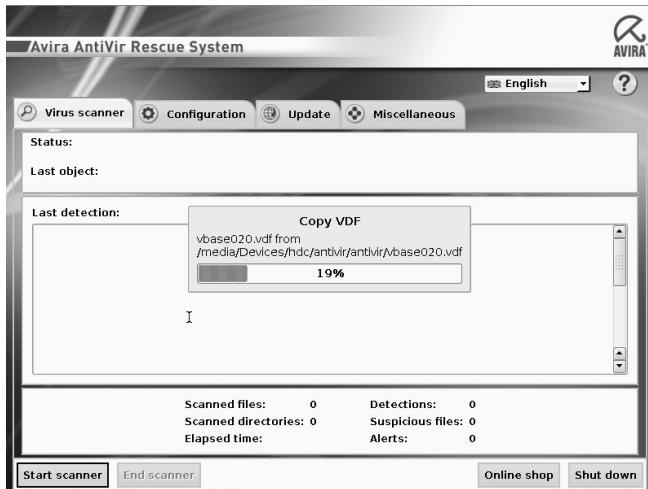
Gambar 4.91 Antivir rescue system

3. Antivir akan loading modul-modul yang ada.



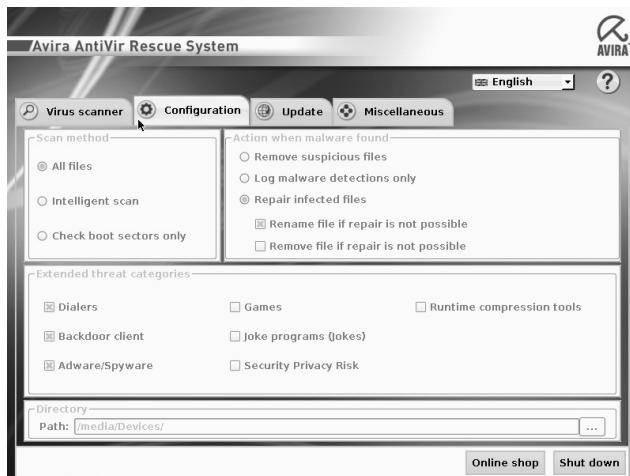
Gambar 4.92 Loading modul-modul yang ada

4. Klik tab **Virus scanner** untuk memulai scanning virus.



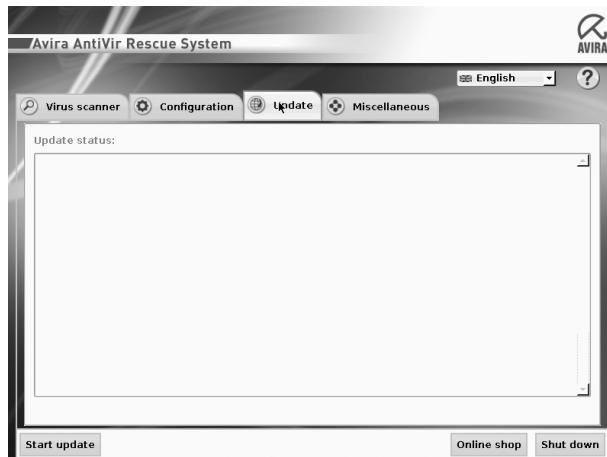
Gambar 4.93 Tab Virus scanner

5. Tab **Configuration** digunakan untuk mengkonfigurasikan berbagai opsi dari **Avira Antivir Rescue CD**.



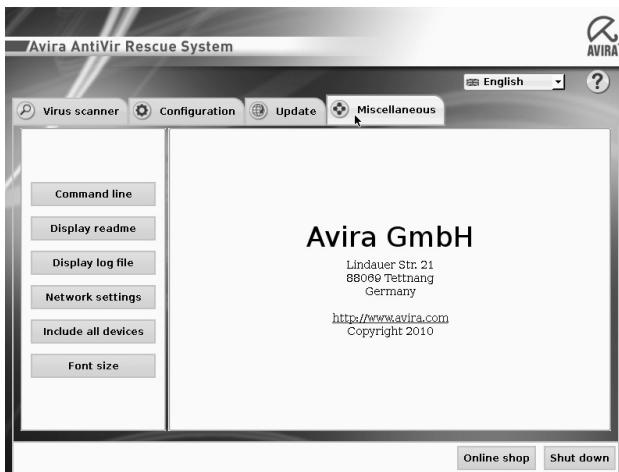
Gambar 4.94 Avira Antivir rescue CD

6. Di tab **Update**, Anda dapat mengatur status update (jika ada).



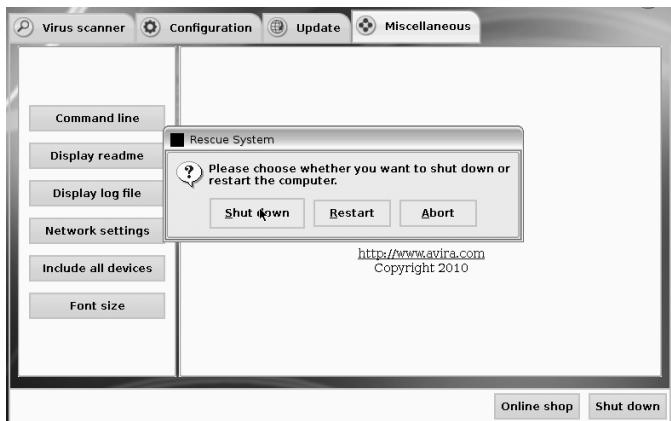
Gambar 4.95 Tab Update

7. Di tab **Miscellaneous**, Anda bisa menentukan berbagai informasi seputar program Avira antivir rescue system ini. Seperti command line, display readme dan sebagainya.



Gambar 4.96 Avira antivirus rescue system

8. Untuk menutup, avira antivir rescue system punya tombol Shut down untuk mematikan komputer. Klik **Shutdown** jika muncul kotak konfirmasi.



Gambar 4.97 Klik konfirmasi untuk Shutdown

9. Tunggu hingga proses shutdown selesai.

```
Avira AntiVir Rescue System
Druecken Sie Alt-F7 um in die grafische Oberfläche zurückzukehren
Press Alt-F7 to return to the graphical User Interface

start X... done
start icewm... done
start rs_gui... done
AVIRA AntiVir Rescue System is going down....
Stop running processes...
stop X... Killed
```

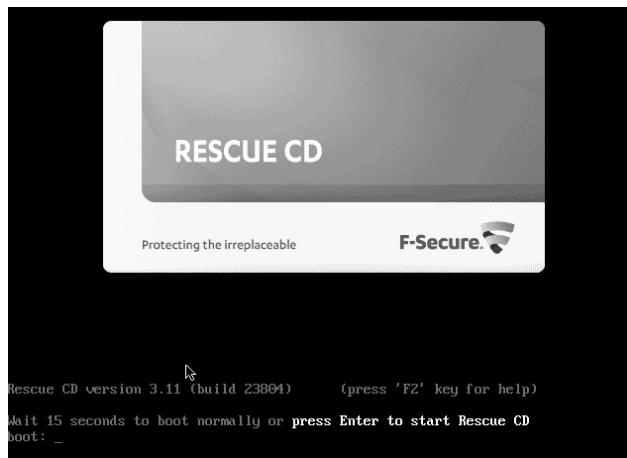
Gambar 4.98 Proses shutdown sedang dilakukan

4.4.5 F-Secure Rescue CD

F secure, salah satu produsen antivirus juga tak ketinggalan dengan pesaingnya untuk membuat distro rescue CD yang bisa dihandalkan jika komputer Anda sedang error. File iso-nya bisa didapat dari http://www.f-secure.com/en_EMEA-Labs/security-threats/tools/rescue-cd/.

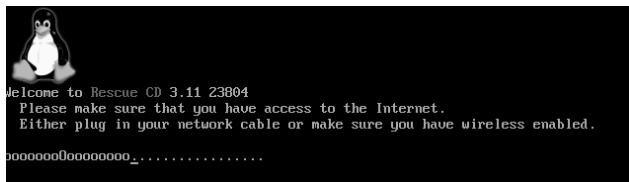
Cara menggunakannya seperti berikut:

1. Booting lah dari disk rescue cd yang sudah didownload.
2. Muncul tampilan seperti berikut, klik **Enter** untuk memulai F-Secure rescue CD.



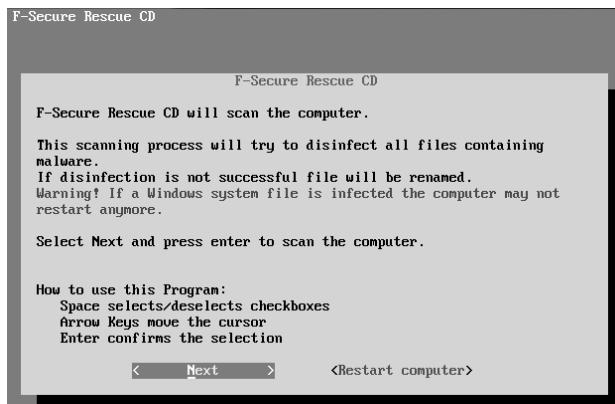
Gambar 4.99 Tampilan rescue cd

3. Jika Anda terkoneksi ke internet, F secure akan mengupdate database-nya.



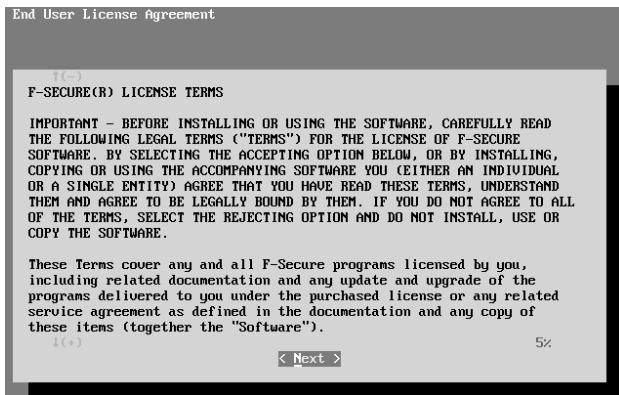
Gambar 4.100 F secure sedang mengecek apakah ada internet atau tidak

4. Kalau sudah muncul tampilan utama **F-Secure Rescue CD**, klik **Next** menggunakan keyboard, karena antarmukanya teks yang tidak bisa menggunakan mouse.



Gambar 4.101 Tampilan utama F-Secure rescue CD

5. Muncul license terms sebelum bisa menggunakan software ini, klik **Next**.



Gambar 4.102 License terms untuk menggunakan F-Secure

6. Pilih item-item yang akan dipindai di **Select what to scan**.
7. Kemudian klik **Start scan** untuk memulai pemindaian.



Gambar 4.103 Start scan untuk memulai pemindaian

8. Saat sedang scanning, tampilannya seperti berikut:

```
Scanning

Alt-F1 This screen.
Alt-F5 To see details of files being scanned.
Alt-F6 To see any malware found.
Ctrl-C To cancel scanning.

Scan started at Mon Feb  7 08:52:07 UTC 2011
with Database version: 2009-09-13_01.

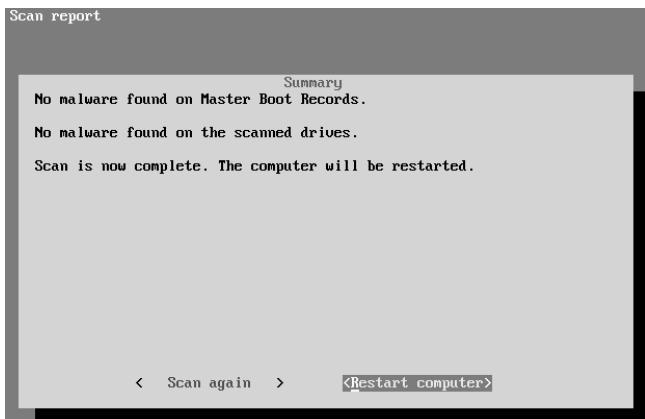
No malware found on Master Boot Records.

Scanned  Malware  Done  Progress
          0        0    100%.

Scan completed. Press Enter to see report.
```

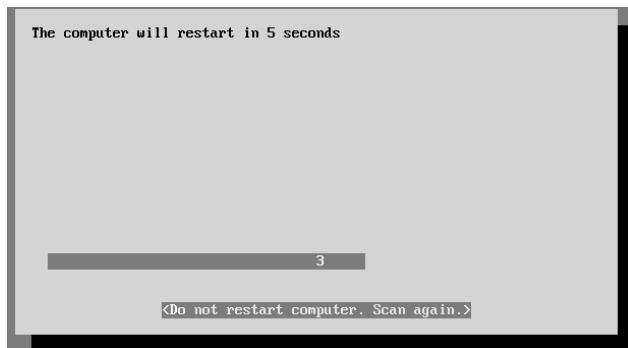
Gambar 4.104 Tampilan saat sedang scanning

9. Kalau sudah scanning, hasil akhirnya diganti di summary.



Gambar 4.105 Tampilan summary

10. Kalau sudah, Anda bisa me-restart komputer dengan klik pada **Restart computer**.



Gambar 4.106 Restart computer

4.4.6 Membakar File ISO ke CD

File-file rescue cd di atas, didownload dalam bentuk file image ISO, yaitu file yang mirip dengan CD/DVD tapi masih dalam bentuk soft copy yang harus dibakar ke dalam cd atau dvd.

Anda bisa menggunakan alat bantu berupa software cd burner, seperti Nero, Ashampoo, dan sebagainya. Tapi sebenarnya ada juga software yang bagus yang gratis, yaitu Infrarecorder yang bisa diambil dari <http://infrarecorder.org>.

Instal dahulu program ini sebelum bisa dipakai:

1. Klik 2x pada installer Infrarecorder.
2. Set bahasa ke Indonesia di **Please select a language**.



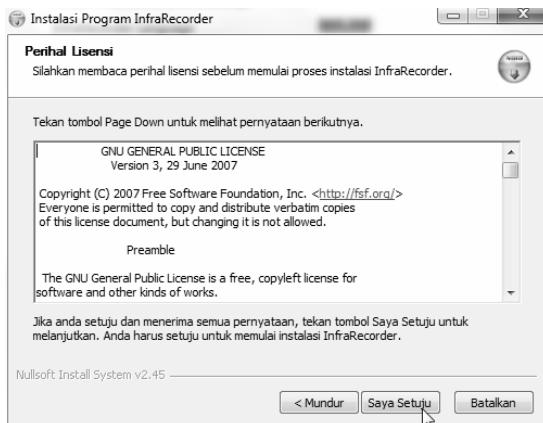
Gambar 4.107 Pemilihan bahasa Indonesia di please select a language

3. Jendela pertama adalah **Selamat datang di program instalasi infra recorder**, klik **Lanjut**.



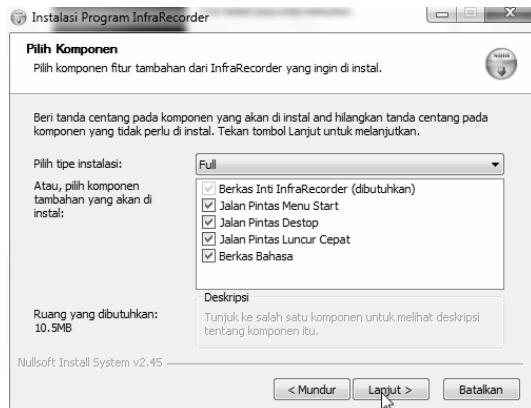
Gambar 4.108 Selamat datang di program instalasi infra recorder

4. Di **Lisensi**, klik pada **Saya setuju**.



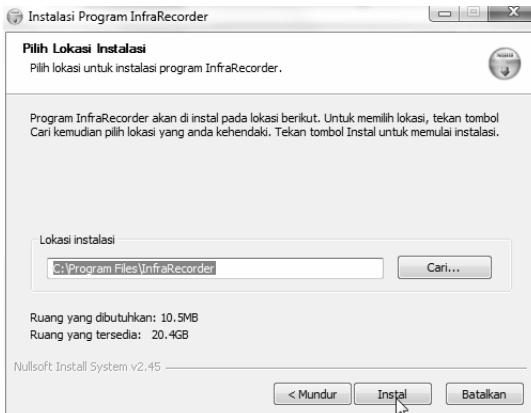
Gambar 4.109 Saya setuju di License agreement

5. Pilih komponen yang akan Anda gunakan di **Pilih komponen**. Kemudian klik **Lanjut**.



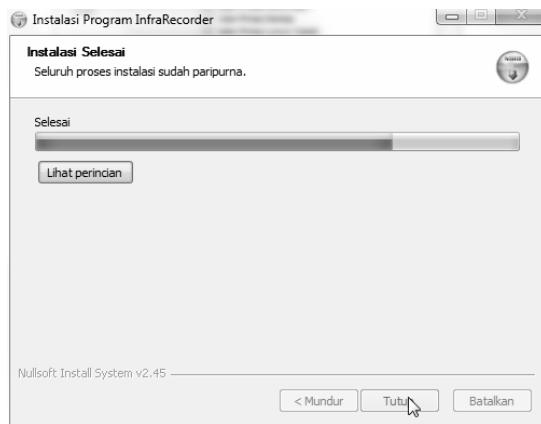
Gambar 4.110 Pilih komponen

6. Pilih lokasi instalasi di jendela **Pilih Lokasi Instalasi**. Kalau mau ganti lokasi, klik Cari, tapi kalau tidak, langsung klik **Install** untuk menginstal program ini ke hard disk.



Gambar 4.111 Pilih lokasi instalasi

7. Tunggu hingga instalasi selesai. Kalau sudah selesai, klik **Tutup**.



Gambar 4.112 Proses instalasi sedang berlangsung

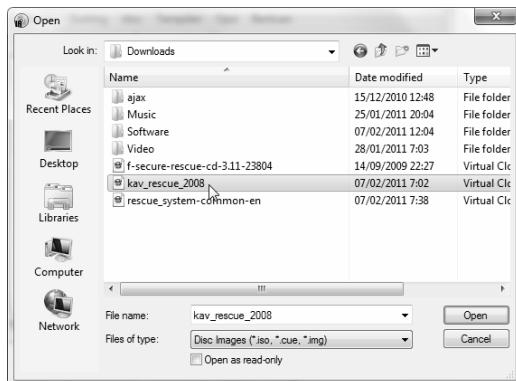
Adapun cara untuk membakarnya adalah:

1. Jalankan InfraRecorder, klik tombol **Write**.



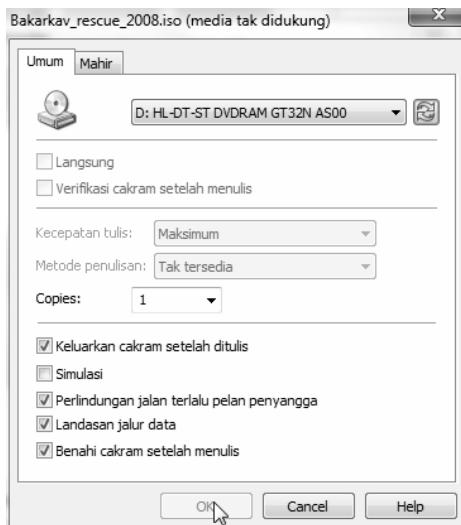
Gambar 4.113 Klik tombol Write untuk menuliskan image ke disk/membakarnya

2. Pilih file image yang akan dibakar di jendela Open.



Gambar 4.114 Pemilihan file image yang akan dibakar

3. Kemudian masukkan cd kosong atau dvd kosong yang akan dibakar di drive optik PC atau laptop Anda, kemudian klik **OK**.



Gambar 4.115 Tampilan sebelum membakar, dan sebelum cd dimasukkan ke drive optik

TENTANG PENULIS

Tim EMS

E-Media Solusindo adalah lembaga yang bergerak di bidang IT dengan layanannya: internet services, software development dan publishing. Bekerja sama dengan penerbit PT. Elex Media Komputindo menerbitkan buku-buku komputer. Email: publisher@e-mediasolusindo.com.



Ketika komputer/laptop Anda masih baru, rasanya nyaman, lancar, cepat, dan enak digunakan. Sejalan dengan waktu, komputer menjadi berat ketika dinyalakan, sering hang ketika sedang online, dan berbagai masalah lainnya yang membuat Anda BéTe dan kurang produktif bekerja. Mengapa bisa seperti itu?

Virus, malware, dan spyware adalah biang keladinya. Solusinya? Baca buku ini agar komputer tetap sehat dan enak digunakan.

Materi yang akan dibahas meliputi:

- ▶ Anti Virus
- ▶ Anti Spyware
- ▶ Pengamanan Internet
- ▶ Teknik Lainnya

Kelompok
Utility
Keterampilan
<input checked="" type="checkbox"/> Tingkat Pemula
<input checked="" type="checkbox"/> Tingkat Menengah
<input type="checkbox"/> Tingkat Mahir
Jenis Buku
<input checked="" type="checkbox"/> Referensi
<input checked="" type="checkbox"/> Tutorial
<input type="checkbox"/> Latihan

