

# TIS13534P KOMUNIKASI DAN KEAMANAN DATA

Minggu 5 – Alat Keamanan



# Sub Tema

- Firewall
- Virtual Private Network
- Anti Virus
- Anti Malware

# Apa Itu Firewall?

- Dinding Api?
- Lebih tepatnya:
  - Sebuah hardware/software yang gunanya buat menyaring paket data yang masuk/keluar.
  - Firewall berisi daftar peraturan “rules” untuk memfilter paket yang masuk/keluar
  - Bisa berbentuk Hardware/Software



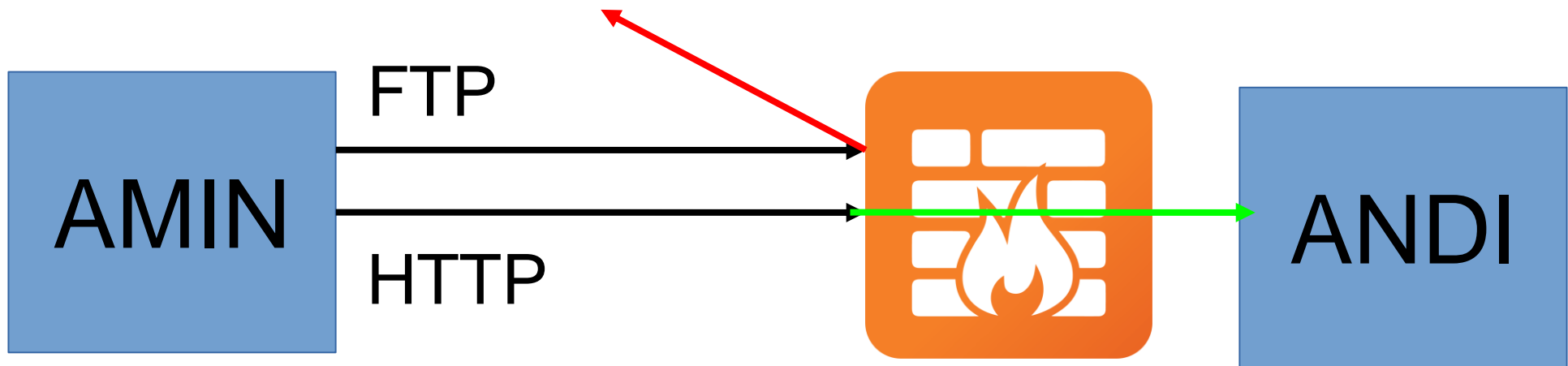
# Contoh Peraturan Firewall

Protokol	Masuk/Keluar	Sumber	Tujuan
TCP	Keluar	192.168.1.2	192.168.1.4
IP	Masuk	192.168.3.5	192.168.3.7
UDP	Keluar	10.0.0.1	10.0.0.2
HTTP	Masuk	10.0.10.5	10.0.10.8

**Warna Hijau:** Firewall mengizinkan paket data

**Warna Merah:** Firewall menolak paket data

# Ilustrasi



Protokol	Masuk/Keluar	Sumber	Tujuan
<b>FTP</b>	<b>Masuk</b>	<b>Amin</b>	<b>Andi</b>
<b>HTTP</b>	<b>Masuk</b>	<b>Amin</b>	<b>Andi</b>

# Penjelasan

- Jika sebuah paket masuk **daftar hitam (blacklist)**, paket tersebut akan di-drop (berhenti di Firewall)
- Namun, jika sebuah paket masuk **daftar putih (whitelist)** maka paket tersebut akan diteruskan hingga tuntas.

# Lebih Kurang Firewall

- Alat pertahanan dari serangan jaringan +
- Sebagai alat pengontrol keamanan ketika daring +
- Konfigurasi mudah dengan pengetahuan dasar +
- Firewall terkadang memblokir port yang kita gunakan, contoh Game LAN -

# Di Mana Firewall Berada?

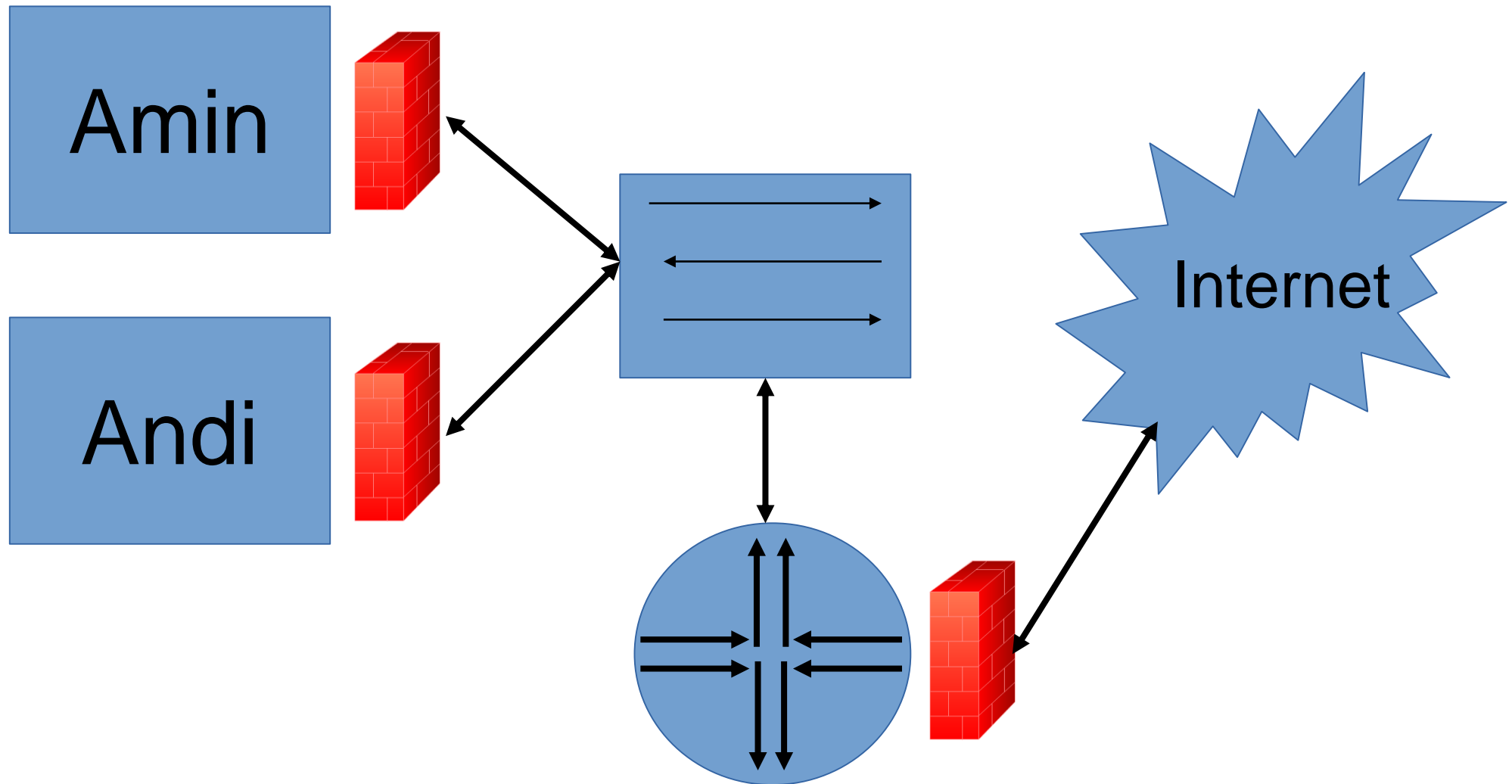
- Komputer
  - Semua Sistem Operasi pasti memiliki jenis software Firewall mereka sendiri. Dengan prinsip yang sama
- Smartphone
- Router
  - Router Cisco memiliki Sistem Operasi CISCO IOS yang salah satu fiturnya adalah Firewall



# Perbedaan Firewall

- Apa bedanya Firewall Software VS Hardware berbasis Firewall?
  - Software: Dia sudah tersedia sebagai **perangkat lunak** yang bisa berjalan di semua hardware, dan menjadi bagian dari sistem operasi.
  - Hardware: Dia adalah sebuah **perangkat keras khusus** yang berguna untuk menyaring paket-paket data di jaringan. Contoh: CISCO Router.

# Lokasi Firewall



# Zonasi Firewall

Firewall memberlakukan Zonasi untuk mempermudah keamanan. Pada dasarnya ada TIGA zona yang sudah tersedia secara default

Zona Rumah (Home)

Zona Kantor (Office)

Zona Umum (Public)

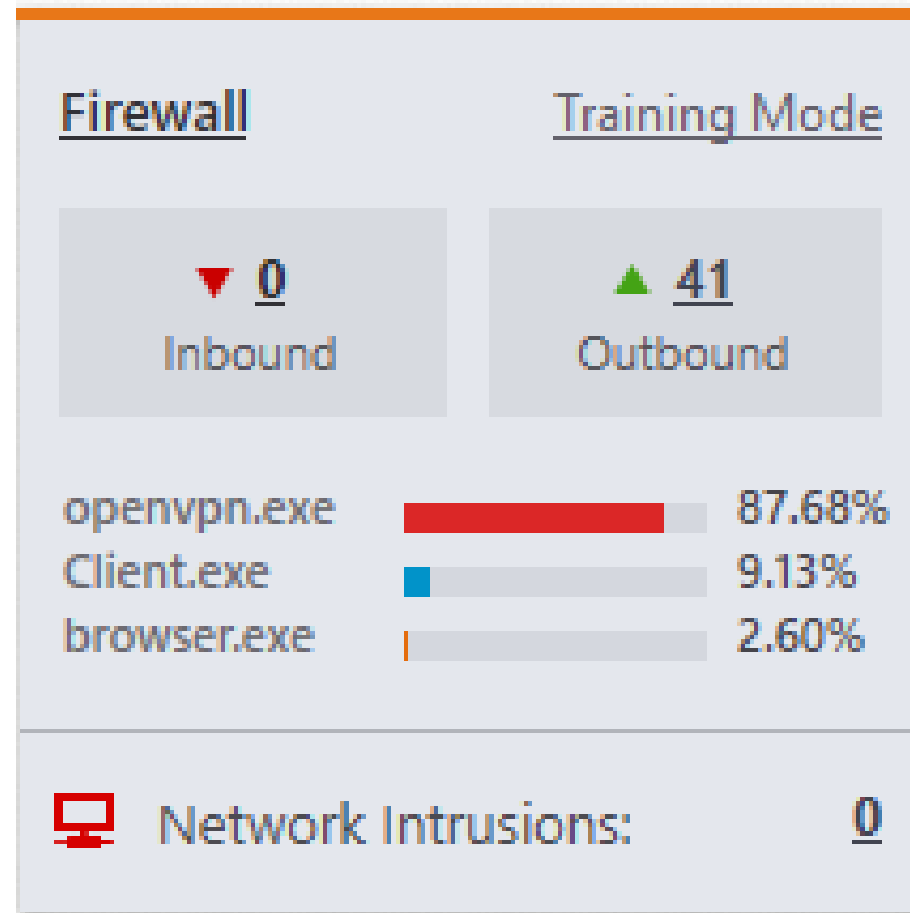
# Software-software Firewall

Untuk PC:



- Comodo Internet Security
- Windows Firewall
- Uncomplicated FireWall

Untuk Router:

- CISCO IOS
- IPCop Linux




# Windows Firewall



 **Private networks** Connected 

Networks at home or work where you know and trust the people and devices on the network

---


Windows Defender Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active private networks:	 Network
Notification state:	Notify me when Windows Defender Firewall blocks a new app

---

 **Guest or public networks** Connected 

Networks in public places such as airports or coffee shops

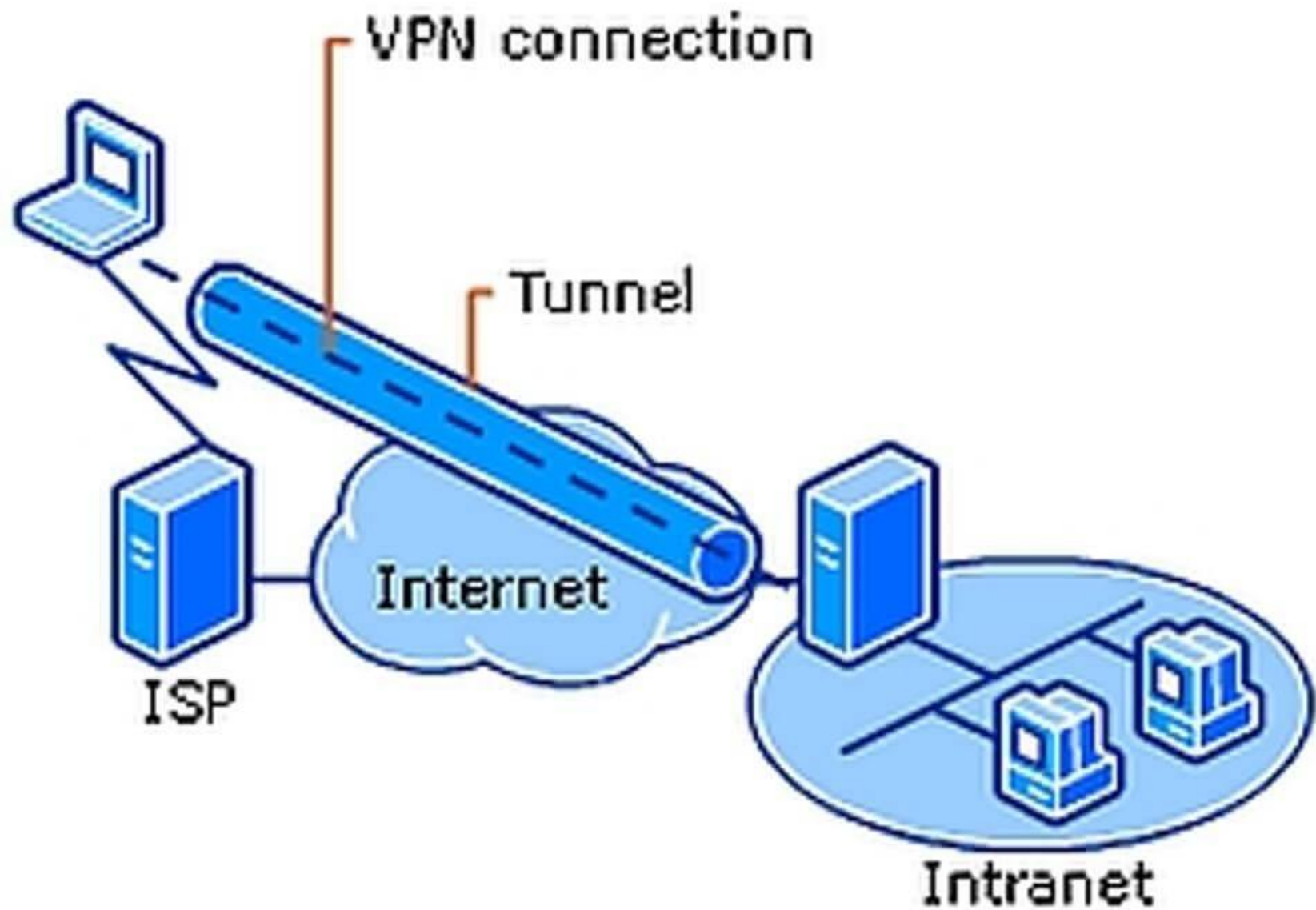
---

Windows Defender Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active public networks:	 Unidentified network
Notification state:	Notify me when Windows Defender Firewall blocks a new app

# Virtual Private Network

- Sebuah koneksi virtual yang menghubungkan Kita ke Jaringan Perusahaan untuk memudahkan penggunaan sumber daya perusahaan.
- VPN memerlukan UserName dan Password yang terdaftar di perusahaan tersebut.
- Dan koneksi VPN sudah dienkripsi untuk mengamankan transmisi data

# Ilustrasi VPN



# VPN itu Penting!

- Menghindar dari Sniffer!
- Untuk mengakses sumber daya Kampus/Perusahaan
- Privasi
- Mengamankan download, baik biasa maupun torrent



# Tujuan VPN

- Keamanan Transmisi Data
- Mengganti IP Kita
- Melewati Blokir
- Anonymosity

# Kelebihan Kekurangan VPN

- + Aman
- + Privasi Terjaga
- Kecepatan Akses Tergantung Jarak
- Jika Koneksi Tidak Bagus, Sering DC

# Jenis-Jenis Protocol VPN

- IPSec
- SSL/Transport Layer Security
- Datagram Transport Layer Security (UDP)
- Microsoft Point-to-Point Encryption (MPPE)
- Secure Shell (SSH)

Apapun protokolnya, semua memerlukan Server dan Pengamanan

# Software-Software VPN

- **Internal Microsoft**
- IPSec
- TLS
- **OpenVPN (dari perusahaan)**
- TLS
- **Softether (dari Universitas Tsukuba Jepang)**
- SSL-VPN

# <https://www.vpngate.net/en/>

Your IP: FL1-133-205-118-144.myg.mesh.ad.jp (133.205.118.144)



Your country: Japan

Let's change your IP address by using VPN Gate!



Japan

vpn256467566.opengw.net

123.1.93.39

(123-1-93-39.dz.commufa.jp)

**107 sessions**

26 days

Total 865,098 users

**155.42 Mbps**

Ping: 8 ms

**196,127.43 GB**

Logging policy:

2 Weeks

# VPN Gratis dan Berbayar

- Pada dasarnya VPN itu tidak gratis, tapi ada beberapa alternative yang bisa digunakan.
- Softether dari Univ. Tsukuba ini VPN gratis, servernya volunteer dari berbagai negara.
- Ada beberapa yang berbayar, yang di mana VPN ini dikhususkan untuk bisnis dan gaming
- Ada VPN gratis dari penyedia berbayar, namun user dibatasi per GB/hari nya

# Untuk Smartphone?

- TunnelBear (Cross Platform)
- HotSpot Shield (Cross Platform)
- OpenVPN (Cross Platform)
- AnyConnect SSL

# TOR – Bukan VPN Biasa

- TOR adalah sebuah Jaringan yang berlapis-lapis layaknya Bawang! (Icon dari TOR adalah Bawang Ungu)
- TOR akan menyambung ke beberapa relay yang ada di Internet, kita akan tersambung maksimal 3 IP, dan bisa di ganti!
- Web di dalam TOR disebut juga *deep web/dark web*, yang isinya ada yang berbahaya, bahkan illegal!
- Koneksi TOR tergantung dari banyaknya relay yang aktif di sekitar kita



# Aplikasi TOR

TOR Service – sebuah program background yang bekerja sebagai proxy ke jaringan TOR.

TOR Browser – firefox yang sudah dimodifikasi untuk terhubung ke jaringan TOR

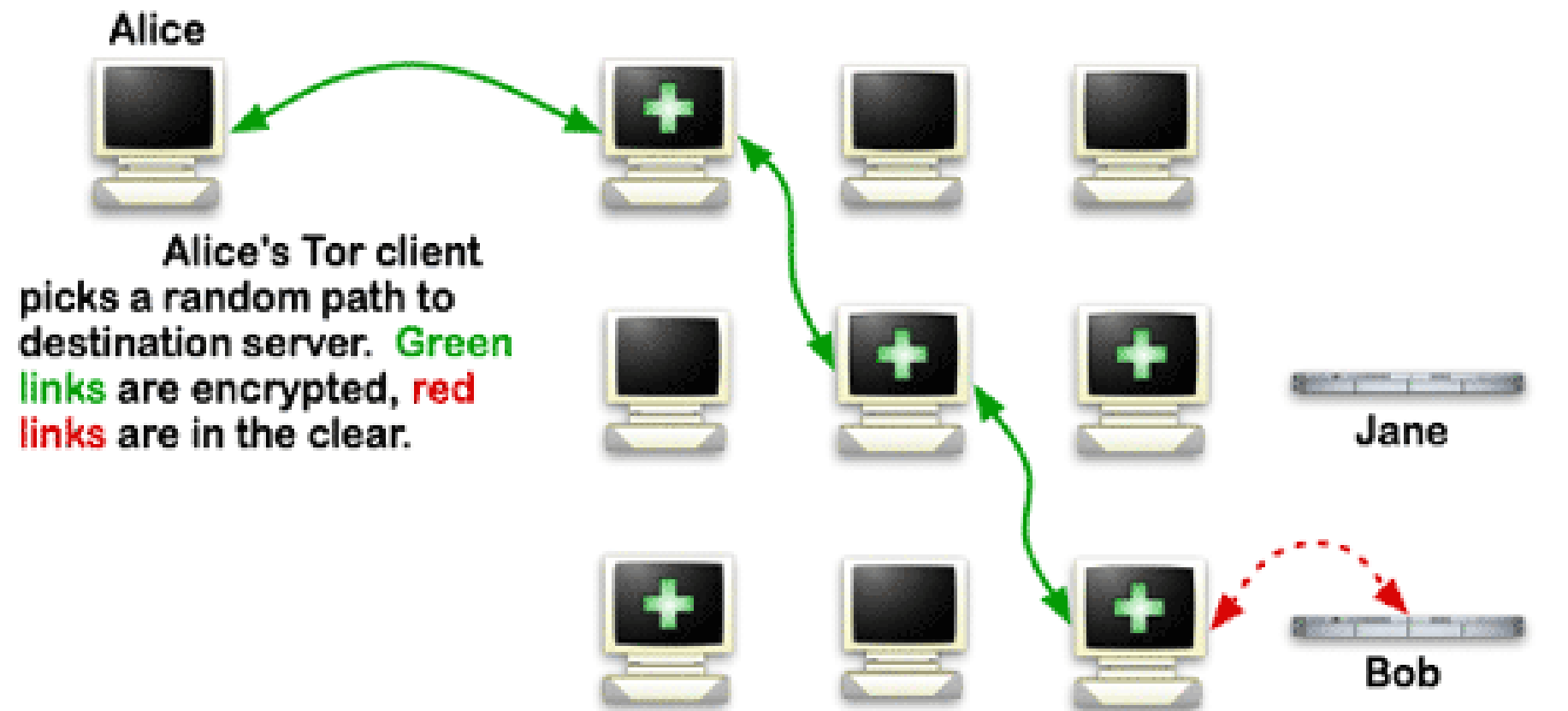
ORBOT – program khusus Android untuk menghubungkan Android ke jaringan TOR

Relay Search – program informasi relay

Tails - satu set system operasi khusus operasi TOR

# Ilustrasi TOR

## How Tor Works



# Anti Virus dan Anti Malware

- Keduanya memiliki kegunaan untuk melindungi file-file di dalam computer.
- Ancaman virus maupun malware datang dari segala arah
  - Internet
  - Colok flashdisk sembarangan (warnet)
  - Asal install program tanpa tahu apa yang dilakukan

# Anti Virus

- Sebuah program yang memiliki kemampuan untuk mengidentifikasi apakah file terinfeksi atau tidak.
- AV jaman dahulu hanya menggunakan Database saja.
- Di jaman sekarang AV menggunakan Database yang di-update per hari, dan kemampuan Heuristic
- Beberapa AV tidak bisa menyembuhkan kode yang terinjeksi di sebuah file, jadi beresiko tidak bisa kembali.

# Anti Malware

- Sebuah program yang dapat menangani masalah virus, serangan malware (adware, spyware, bahkan ransomware)
- Dapat memulihkan system jika ada yang berubah (registry editor di Windows)
- Membuang aplikasi-aplikasi tidak jelas yang terdeteksi sebagai Spyware, Adware, bahkan Ransomware)

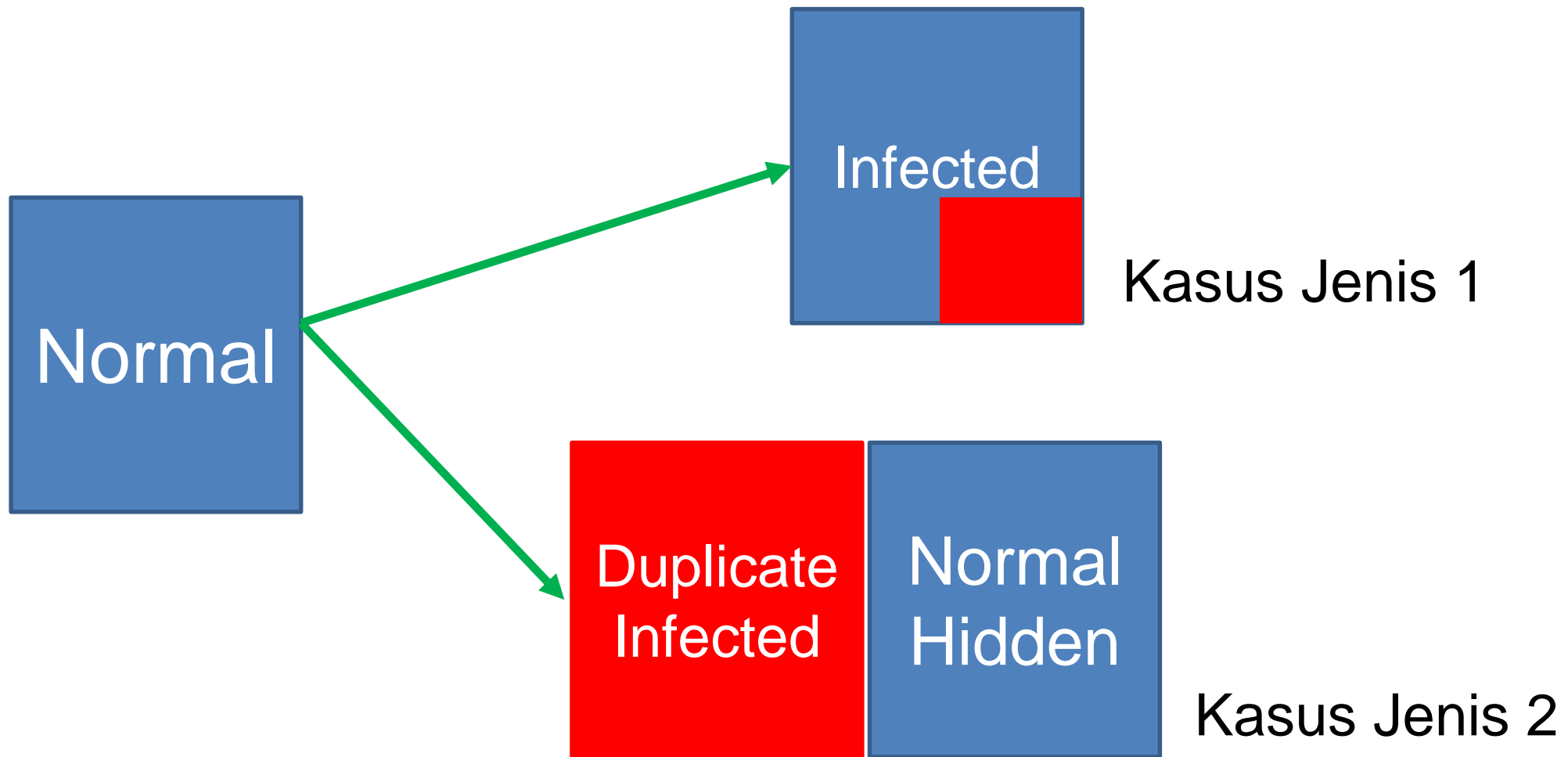
# Virus vs Malware

Virus adalah sebuah potongan kode yang dapat menduplikasikan diri, dan dapat mengganggu kinerja system operasi.

Malware adalah sebuah program yang tujuannya mengganggu kinerja system, dan biasanya menyertakan virus di dalamnya. Contoh Trojan, Worm, Adware, Spyware, bahkan Ransomware

**Virus adalah Malware, tapi Malware bukan Virus**

# Ilustrasi Virus

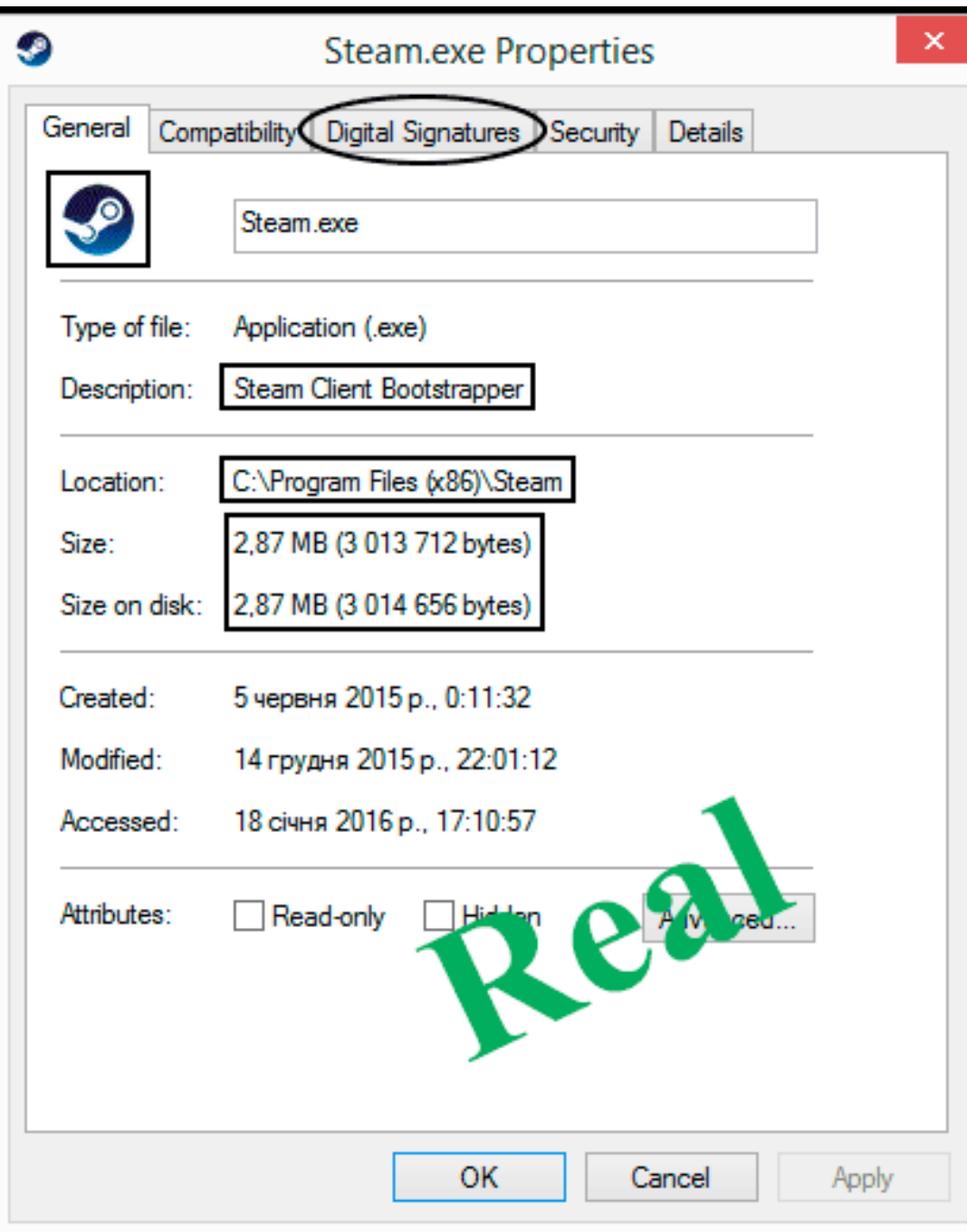
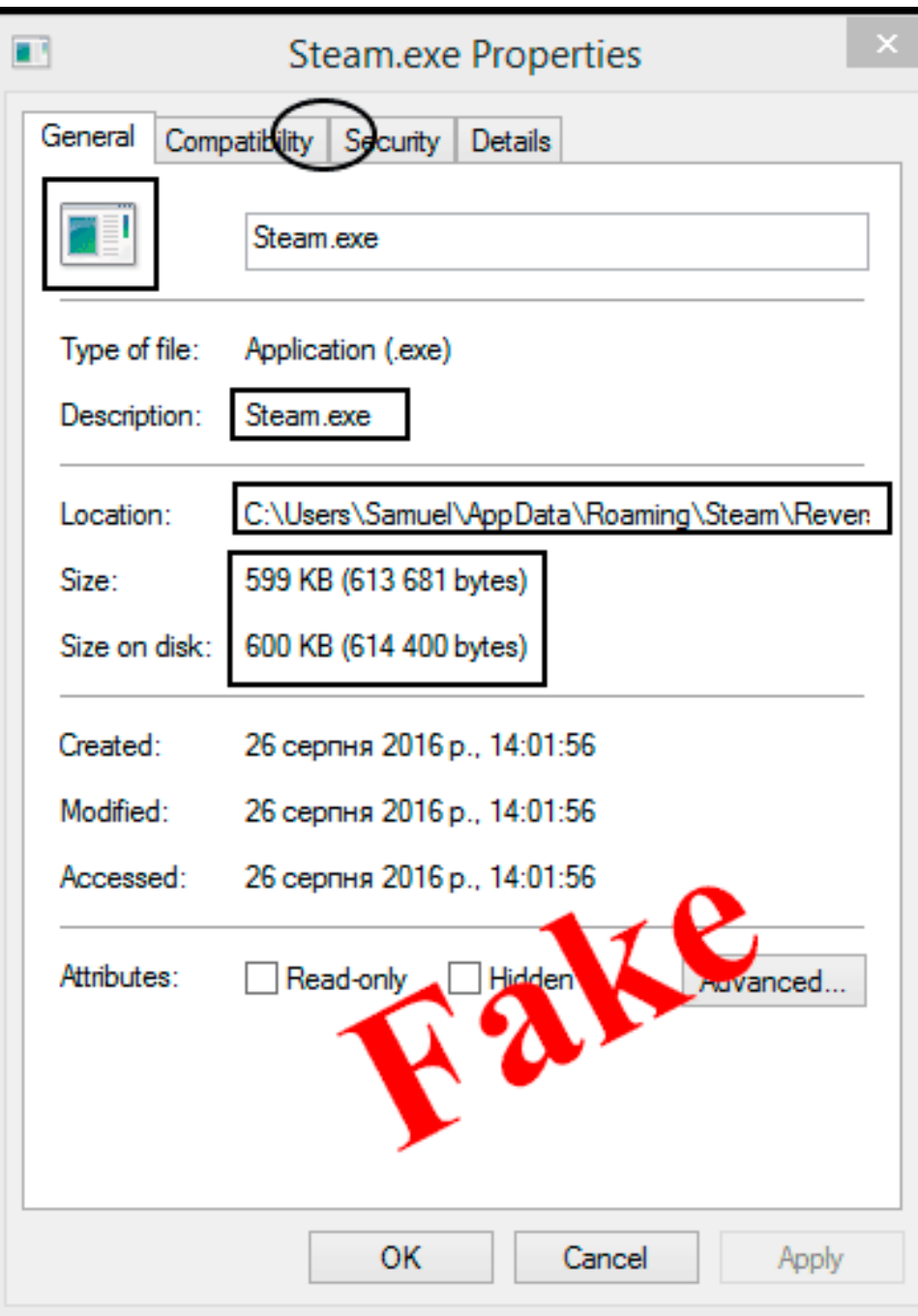


# Efek dari Virus

- Icon berubah jadi aneh
- File dokumen menjadi exe bahkan scr (file screensaver)
- Komputer terasa lambat
- Ukuran file berubah drastis



# Contoh Efek Virus



# Indonesia Juga Petani Virus

- Virus RontokBro/ Brontok
- Virus Rapi
- Virus Riyani\_Jangkaru
- Virus Pendekar “blank”
- Virus Aksika
- Virus Blue Fantassy
- Virus Ramnit dan Sality paling terkenal dan menginfeksi

# Jenis-Jenis Malware

- **Virus**
- **Adware**
- Program yang disisipi iklan demi uang tambahan developer
- **Spyware**
- Program yang tersembunyi digunakan untuk merekam aktivitas user
- **Worm**
- Program yang bisa menduplikasikan diri dan menghancurkan system
- **Trojan**
- Program yang menyamar seolah aman digunakan
- **Ransomware**

# Ransomware

- Sebuah program yang memblokir akses user, blokir akan dibuka setelah user membayar sejumlah uang ke pemilik ransomware itu.
- Ransomware ada yang lunak, dan ada yang agresif.
- Ransomware lunak berbentuk software antivirus/optimasi/cleaner disk, dia akan meminta user untuk membeli lisensinya secara penuh,
- Ransomware agresif secara paksa menutup akses ke file/program dan memberi peringatan untuk membayar.

# Ransomware Agresif

Wana Decrypt0r 2.0



## Ooops, your files have been encrypted!

not so enough time.  
You can decrypt some of your files for free. Try now by clicking <Decrypt>  
But if you want to decrypt all your files, you need to pay.  
You only have 3 days to submit the payment. After that the price will be d  
Also, if you don't pay in 7 days, you won't be able to recover your files for  
We will have free events for users who are so poor that they couldn't pay

**Payment will be raised on**  
1/4/1970 00:00:00  
**Time Left**  
00:00:00:00

**Your files will be lost on**  
1/8/1970 00:00:00  
**Time Left**  
00:00:00:00

### How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About I  
Please check the current price of Bitcoin and buy some bitcoins. For more  
click <How to buy bitcoins>.  
And send the correct amount to the address specified in this window.  
After your payment, click <Check Payment>. Best time to check: 9:00am -  
GMT from Monday to Friday.  
Once the payment is checked, you can start decrypting your files immedi

### Contact

If you need our assistance, send a message by clicking <Contact Us>.

We strongly recommend you to not remove this software, and disable you  
for a while, until you pay and the payment gets processed. If your anti-virus gets  
updated and removes this software automatically, it will not be able to recover your  
files even if you pay!

English  
English  
Bulgarian  
Chinese (simplified)  
Chinese (traditional)  
Croatian  
Czech  
Danish  
Dutch  
Filipino  
Finnish  
French  
German  
Greek  
Indonesian  
Italian  
Japanese  
Korean  
Latvian  
Norwegian  
Polish  
Portuguese  
Romanian  
Russian  
Slovak  
Spanish  
Swedish  
Turkish  
Vietnamese

# Software-software AV & AM

- Comodo Internet Security (AV&AM)
- Avast (AV)
- AVG (AV)
- MalwareBytes (AM)
- Anti AdAware (AM)
- Windows Defender (AV&AM)

# Demi Keamanan Data Selalu:

- Update Antivirus setiap hari
- Lakukan Full Scanning 1 bulan sekali
- Lakukan Quick Scanning 1 minggu sekali
- Berhati-hati jika mendownload file dari internet
- Firewall harus kondisi menyala jika menyambung internet
- Gunakan Linux untuk membantu pemulihan data yang hilang



# Kuis

1. Mengapa kita perlu mengamankan komunikasi dan data?
2. Bagaimana cara kriptografi menyembunyikan informasi yang kita buat?
3. Apa saja kelebihan dan kekurangan Remoting secara umum?
4. Sebutkan tujuan kita melakukan Monitoring!
5. Sebutkan dan jelaskan jenis-jenis serangan!