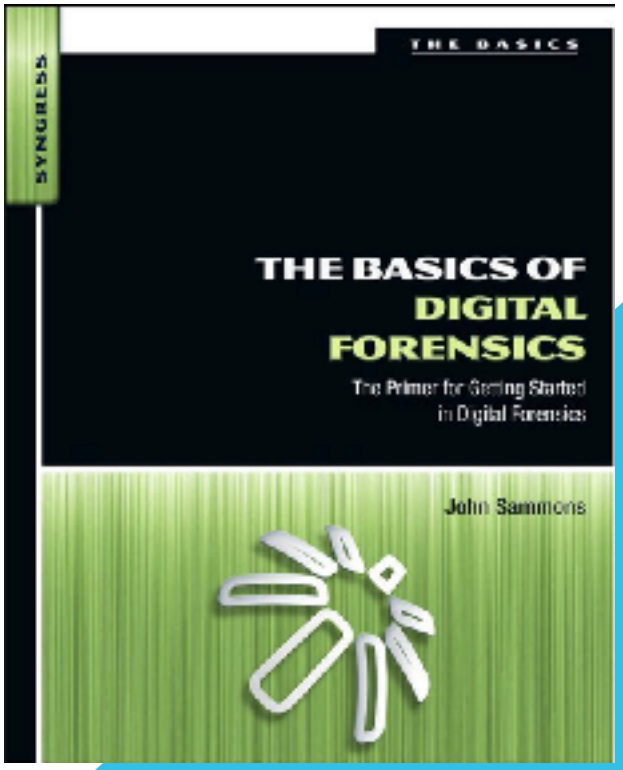


9. NETWORK FORENSICS

TOPIK

- Networking Fundamentals
- Types of Networks
- Network Security Tools
- Network Attacks
- Incident Response
- Network Evidence & Investigation

NETWORKING FUNDAMENTALS

NETWORK CONCEPTS

- TCP/IP (Transmission Control Protocol / Internet Protocol)
  - Bahasa yang umum digunakan untuk Internet
- Client/Server Network
  - Setiap komputer memiliki salah satu peran: klien atau server
  - Komputer modern mencampur peran
- Peer-to-peer Network
  - Setiap anggota memiliki peran yang sama, baik sebagai klien dan server
  - Umumnya digunakan dengan bittorrent untuk berbagi file ilegal

JENIS NETWORK

- LAN (Local Area Network)
  - Dalam sebuah gedung atau bangunan yang berdekatan
- WAN (Wide Area Network)
  - Area lebih besar
- Internet
  - Area paling besar WAN, mencakup seluruh dunia
- MAN (Metropolitan Area Network)
- PAN (Personal Area Network)
  - Bluetooth: max. range 10 meters
- CAN (Campus Area Network)

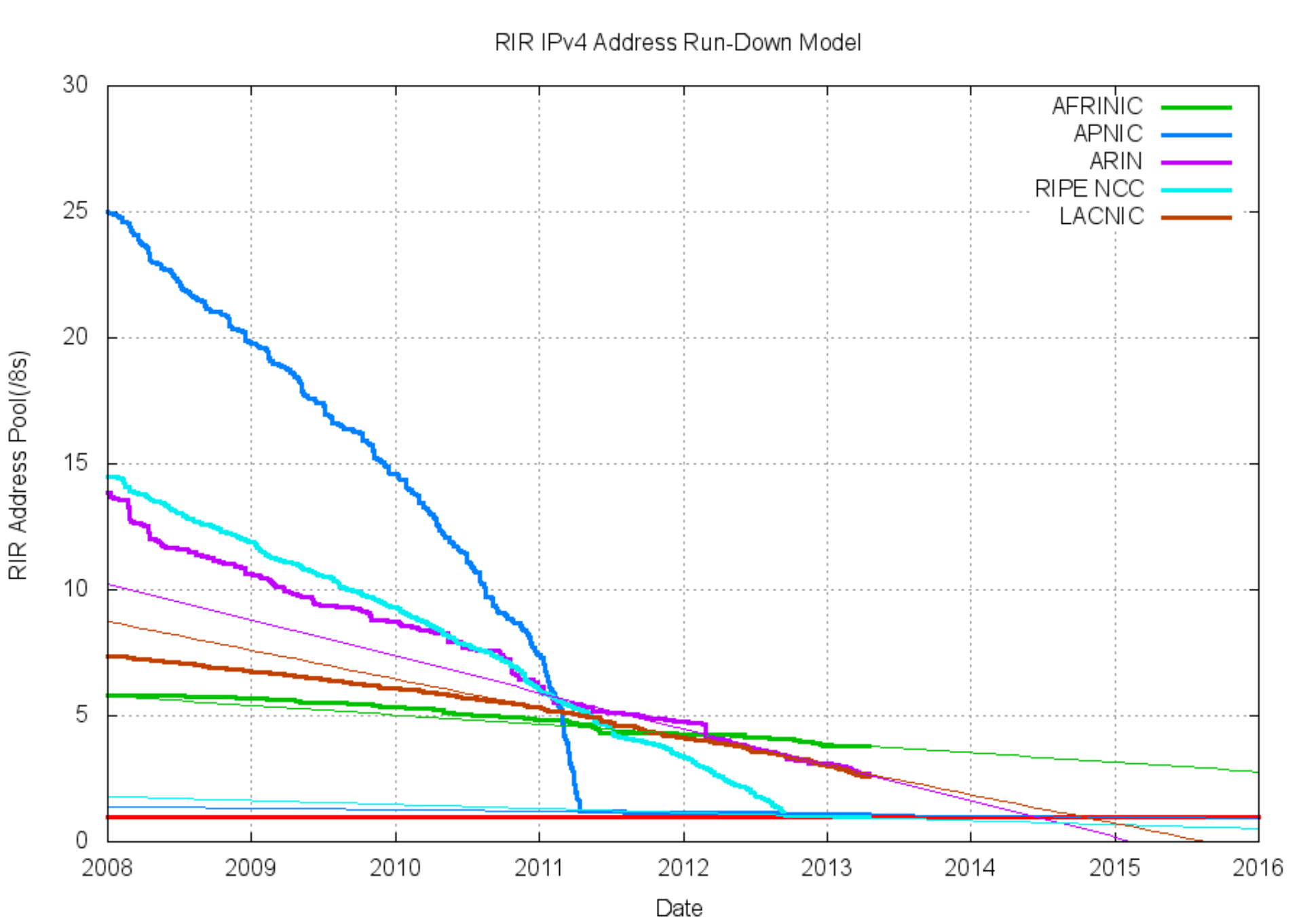
IP ADDRESSES

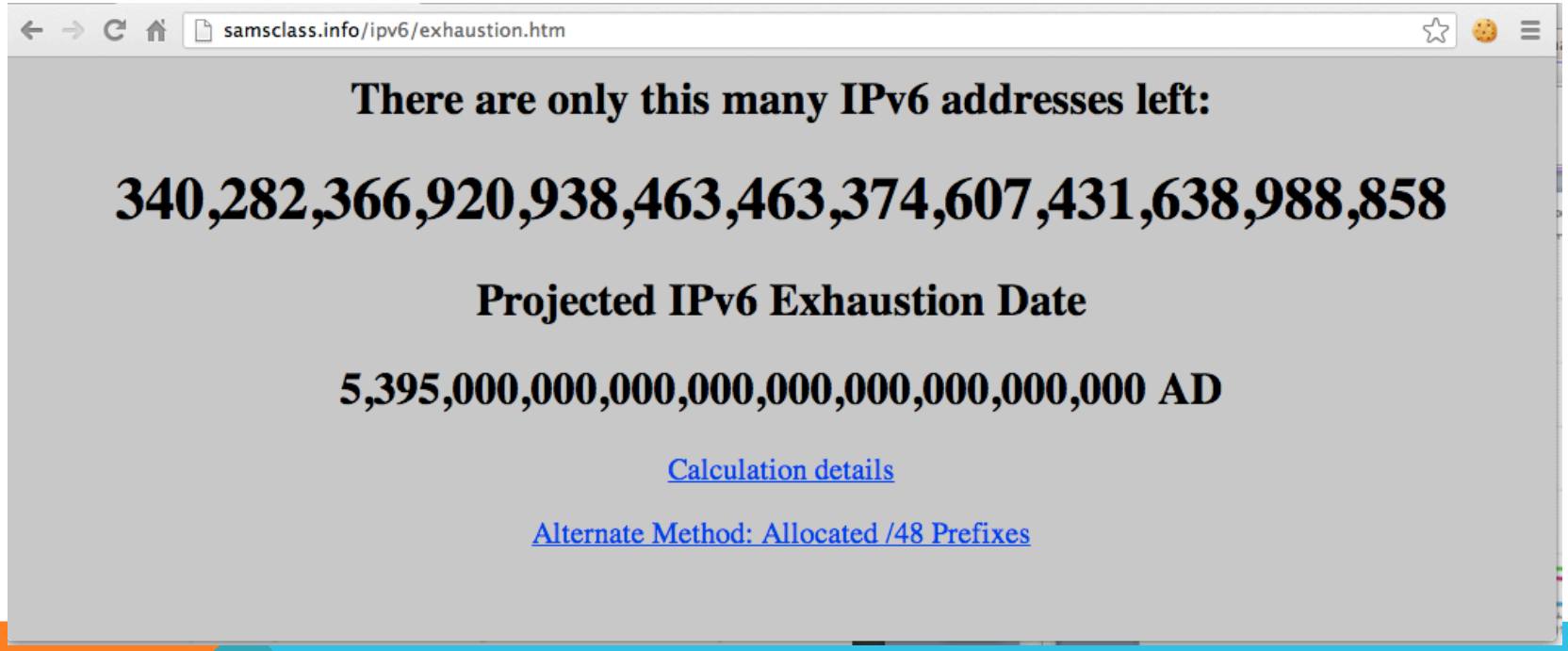
IPv4: 32 bits, dalam empat octets

- Tiap octet ditulis sebagai angka desimal 0-255
- Contoh: 192.168.1.101
- Hanya empat miliar jumlah alamat Total
- Mulai habis

IPv6: 128 bit in eight 16-bit fields

- Tiap field terdiri dari a 4- karakter hexadecimal
- Range 0000 – FFFF
- Contoh: 2001:0db8:0000:0000:1111:2222:3333:4444
- Banyak alamat: 300 miliar miliar miliar miliar


RIR IPv4 Address Run-Down Model
AFRINIC
APNIC
ARIN
RIPE NCC
LACNIC
RIR Address Pool(/8s)
Date
0
5
10
15
20
25
30
2008
2009
2010
2011
2012
2013
2014
2015
2016


samsclass.info/ipv6/exhaustion.htm
There are only this many IPv6 addresses left:
340,282,366,920,938,463,463,374,607,431,638,988,858
Projected IPv6 Exhaustion Date
5,395,000,000,000,000,000,000,000,000 AD
Calculation details
Alternate Method: Allocated /48 Prefixes

NETWORK SECURITY TOOLS

FIREWALLS, IDS, DAN SNIFFERS

- Filters inbound dan, optionally, outbound traffic
- Filter firewalls simple berdasarkan pada packet headers
  - IP address, port number
- Layer 7 firewall
  - Melihat ke dalam packet untuk bisa lebih membedakan paket
  - Bisa mendeteksi Facebook, TeamViewer, BitTorrent
- Intrusion Detection System
  - Memblocks malicious traffic berdasarkan serangkaian definisi/ aturan yang sudah ditentukan
  - Contoh: Snort
- Sniffer
  - Captures packets untuk analisis
  - Contoh: Wireshark

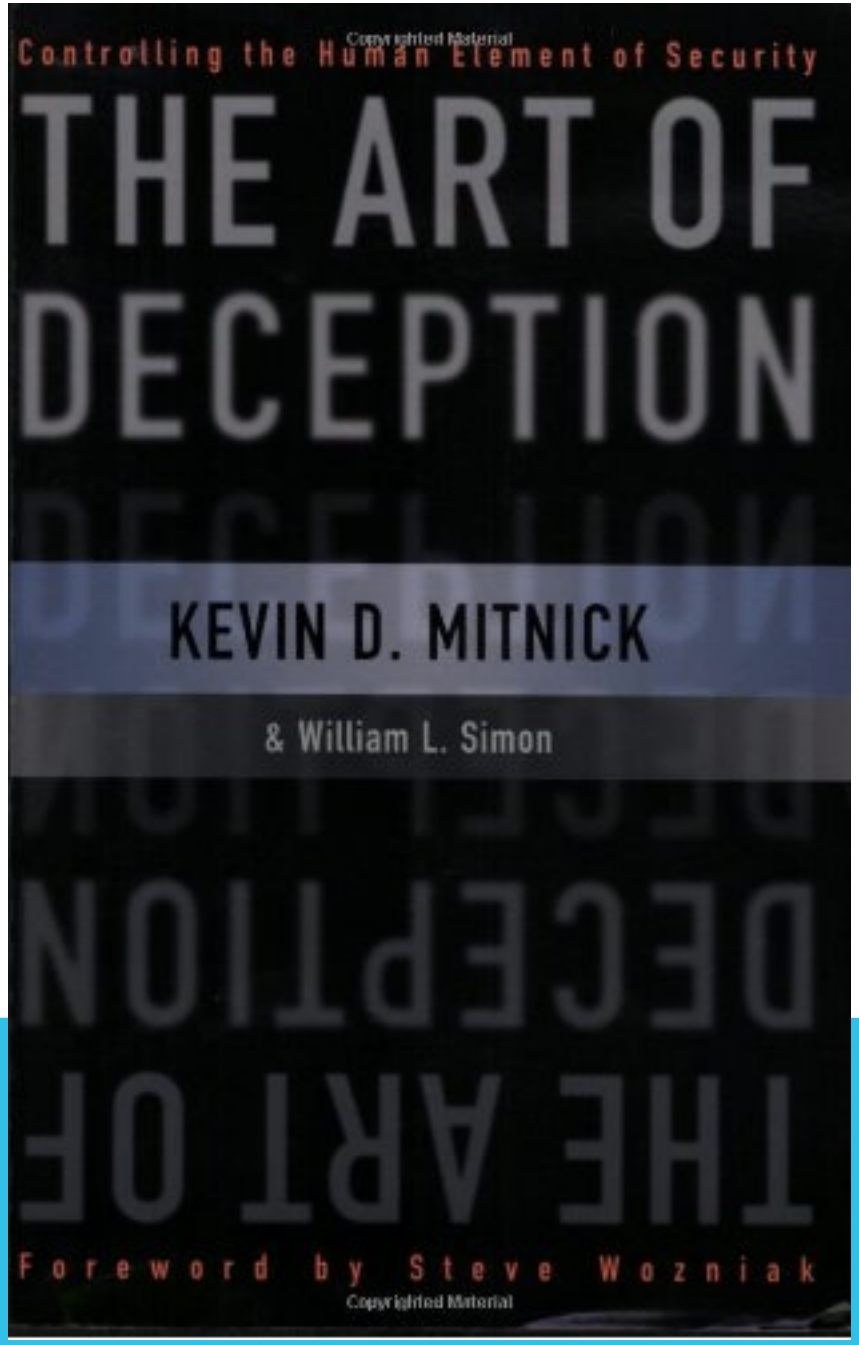
SERANGAN DI JARINGAN

NETWORK ATTACKS

- DDoS (Distributed Denial of Service)
  - Menggunakan banyak bots untuk menyerang server
- IP Spoofing
  - Memalsukan Source IP dalam packets
  - Dapat membuat serangan tampaknya datang dari sumber terpercaya
- Man-in-the-Middle
  - mencegat trafik
  - Penyerang dapat memeriksa atau mengubah data
  - Dapat meniru pengguna
  - Pertahanannya menggunakan SSL

SOCIAL ENGINEERING

Menipu orang untuk pelanggaran keamanan



METODE HACKING YANG BANYAK DIGUNAKAN

- Exploitation of backdoor or command/control channel.
- Exploitation of default or guessable credentials.
- Brute force and dictionary attacks.
- Footprinting and fingerprinting.
- Use of stolen login credentials.

- Backdoor
  - Dari infeksi malware yang memungkinkan remote control
- Footprinting
  - Mengumpulkan informasi publik mengenai target
- Fingerprinting
  - Melakuan Scanning target untuk mengetahui port yang terbuka dan informasi lainnya
- Berdasarkan studi 2012 Verizon
  - Link Ch9a: Verizon-Data-Breach-Report 2012

INSIDER THREAT

- Ancaman terbesar
- Terkadang lebih berbahaya daripada serangan eksternal
- Sulit untuk mendeteksi atau mencegah

Ch9b:City College Of San Francisco Computer Lab Security Breached

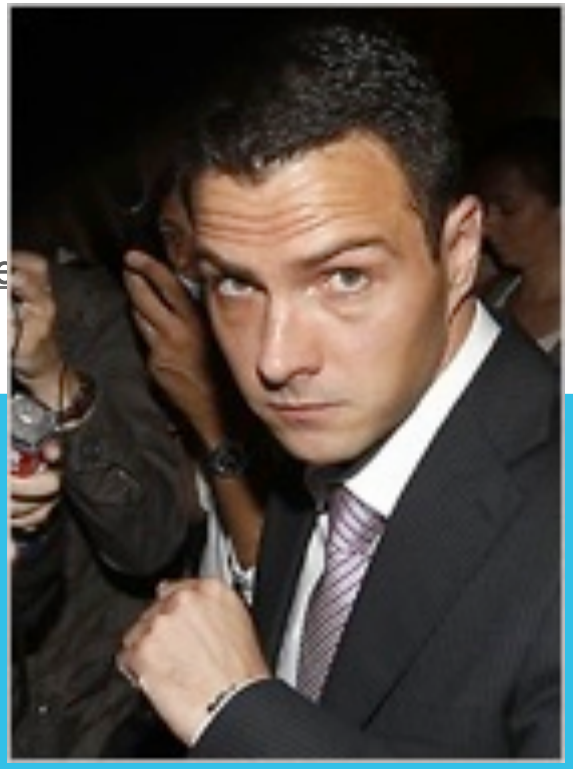
Jerome Kerviel, The Most Indebted Person In The World, Owes $6.3 Billion To Former Employer, Societe Generale

The Huffington Post | By Ryan Grenoble

Posted: 11/05/2012 1:05 pm EST Updated: 11/05/2012 1:16 pm EST

Link

ch 9c: Jerome Kerviel, The Most Indebted Person In The
Former Employer, Societe



INCIDENT RESPONSE

NIST PROCESS

- Persiapan
  - Perencanaan untuk insiden keamanan
  - Pertahanan proaktif, seperti
    - Hardening systems
    - Patching
    - Perimeter defense
    - Pelatihan kesadaran pengguna
    - Kebijakan, prosedur, dan pedoman
- Deteksi dan Analisis
  - IDS menghasilkan false positives
  - Network traffic yang tidak menentu

NIST PROCESS

- Containment (pengendalian)
- Eradication (pemberantasan)
- Recovery (pemulihan)
- Review Postincident (Pasca Kejadian)
  - Root-cause analysis
  - Analisis akar-penyebab
  - Rencanakan bagaimana mencegah incident di masa depan
  - Merevisi kebijakan dan prosedur

NETWORK EVIDENCE & INVESTIGATION

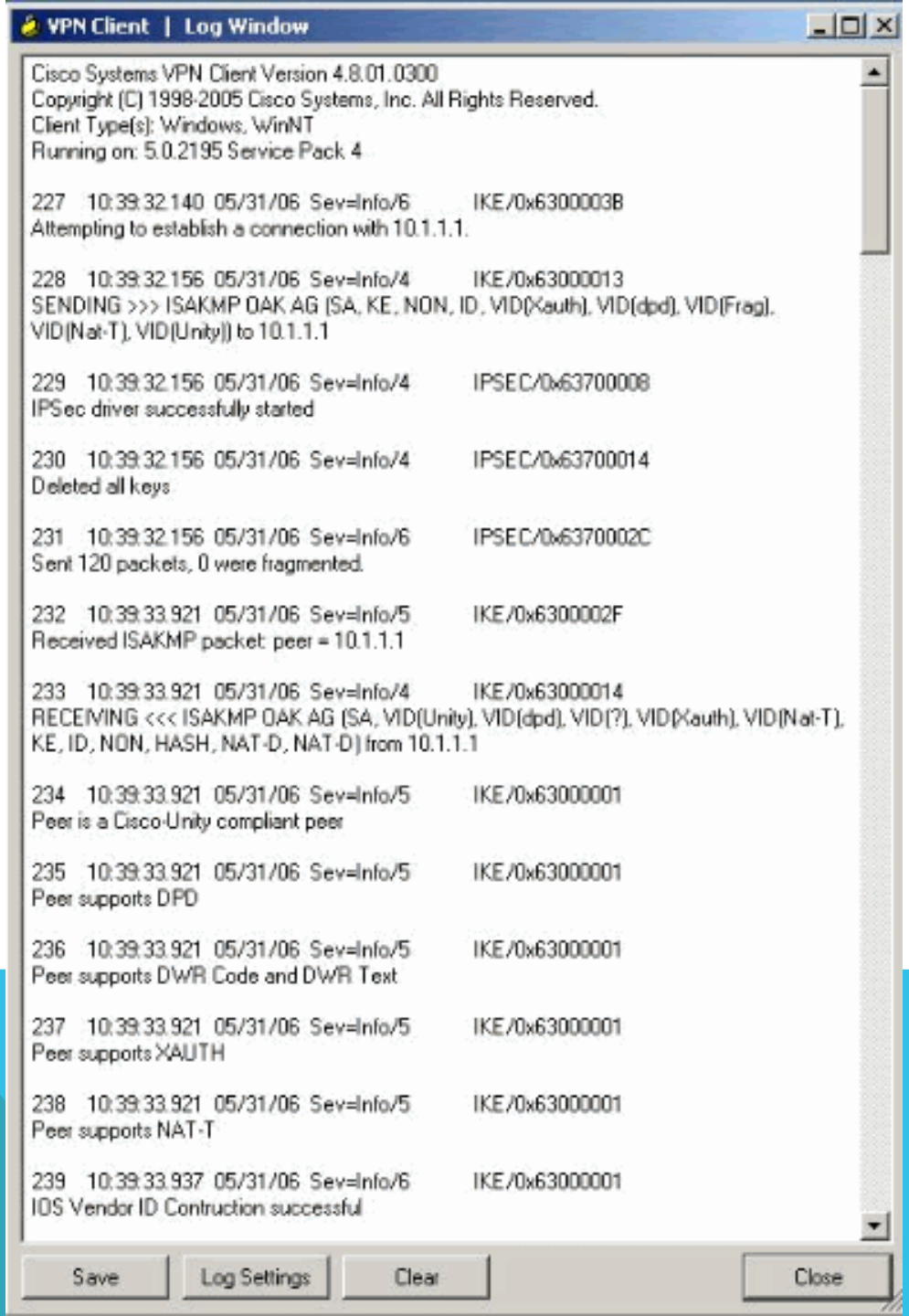
WHERE IS THE EVIDENCE?

Semua perangkat sepanjang rute dapat berisi file-file log

- Servers
- Routers
- Firewalls
- Evidence may be volatile

LOG FILES

- Authentication log
  - Account dan IP address user
- Application log
  - Timestamp yang menunjukkan saat aplikasi digunakan dan oleh siap
- Operating system log
  - Track reboots, file access, clients yang dilayani, dan banyak lagi
- Device logs
  - Di routers dan firewalls


VPN Client | Log Window
Cisco Systems VPN Client Version 4.8.01.0300
Copyright (C) 1998-2005 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.0.2195 Service Pack 4
227 10:39:32.140 05/31/06 Sev=Info/6 IKE/0x6300003B
Attempting to establish a connection with 10.1.1.1.
228 10:39:32.156 05/31/06 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK AG (SA, KE, NON, ID, VID(Xauth), VID(dpd), VID(Frag), VID(Nat-T), VID(Unity)) to 10.1.1.1
229 10:39:32.156 05/31/06 Sev=Info/4 IPSEC/0x63700008
IPSec driver successfully started
230 10:39:32.156 05/31/06 Sev=Info/4 IPSEC/0x63700014
Deleted all keys
231 10:39:32.156 05/31/06 Sev=Info/6 IPSEC/0x6370002C
Sent 120 packets, 0 were fragmented.
232 10:39:33.921 05/31/06 Sev=Info/5 IKE/0x6300002F
Received ISAKMP packet: peer = 10.1.1.1
233 10:39:33.921 05/31/06 Sev=Info/4 IKE/0x63000014
RECEIVING <<< ISAKMP OAK AG (SA, VID(Unity), VID(dpd), VID(?), VID(Xauth), VID(Nat-T), KE, ID, NON, HASH, NAT-D, NAT-D) from 10.1.1.1
234 10:39:33.921 05/31/06 Sev=Info/5 IKE/0x63000001
Peer is a Cisco-Unity compliant peer
235 10:39:33.921 05/31/06 Sev=Info/5 IKE/0x63000001
Peer supports DPD
236 10:39:33.921 05/31/06 Sev=Info/5 IKE/0x63000001
Peer supports DWR Code and DWR Text
237 10:39:33.921 05/31/06 Sev=Info/5 IKE/0x63000001
Peer supports XAUTH
238 10:39:33.921 05/31/06 Sev=Info/5 IKE/0x63000001
Peer supports NAT-T
239 10:39:33.937 05/31/06 Sev=Info/6 IKE/0x63000001
IOS Vendor ID Contruction successful
Save
Log Settings
Clear
Close

NETWORK INVESTIGATIVE TOOLS

- Wireshark
  - Sniffer
- NetIntercept
  - Hardware applicance untuk merekam lalu lintas jaringan
- NetWitness Investigator
  - Dapat mengumpulkan dan menganalisis lalu lintas jaringan
- Snort
  - IDS

NETINTERCEPT

- Study an external break-in attempt
- Monitor correspondence and watch for confidential data being sent outwards
- Display the contents of a remote login or a web session
- Become aware of unusual or potentially troublesome traffic on the network
- Use the GUI to interactively view traffic categorized or sorted by dozens of attributes, such as time of day, username, client and server machine identities, or session size
- Select connections of interest by criteria, such as keywords found in text objects, email header fields, Ethernet addresses, TCP or UDP port numbers, file names, and Web Uniform Resource Identifiers (URIs)

Links

ch 9d: NIKSUN Know the Unknown

ch9e: NIKSUN NetIntercept - securitywizardry

TANTANGAN NETWORK INVESTIGATION

- **IP addresses bisa dipalsukan**
  - Bounced melalui proxies
  - Atau melalui sistem yang terganggu
  - Atau melalui jaringan anonimitas Tor
    - Link : ch 9f: Tor Project _ Anonymity Online
- **Log sering tidak lengkap atau tidak ada**
  - Log akan terhapus setelah beberapa waktu
  - Penyerang dapat menghapus log
- **Juridikasi**
  - Serangan dapat menyeberangi batas-batas negara atau nasional