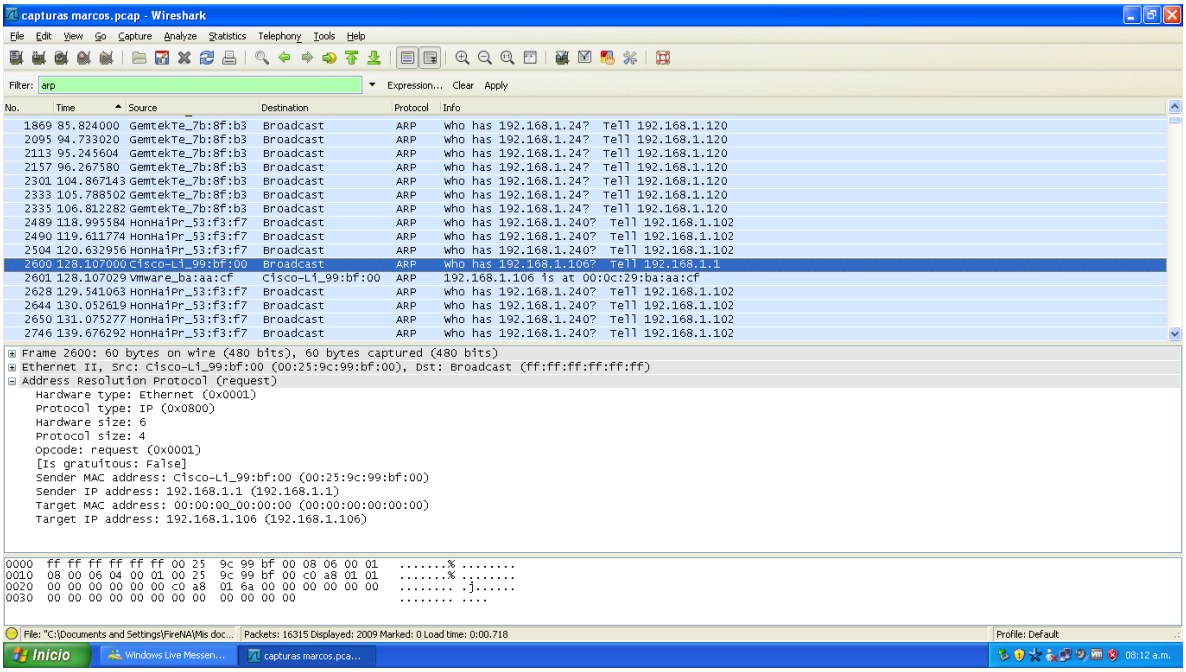
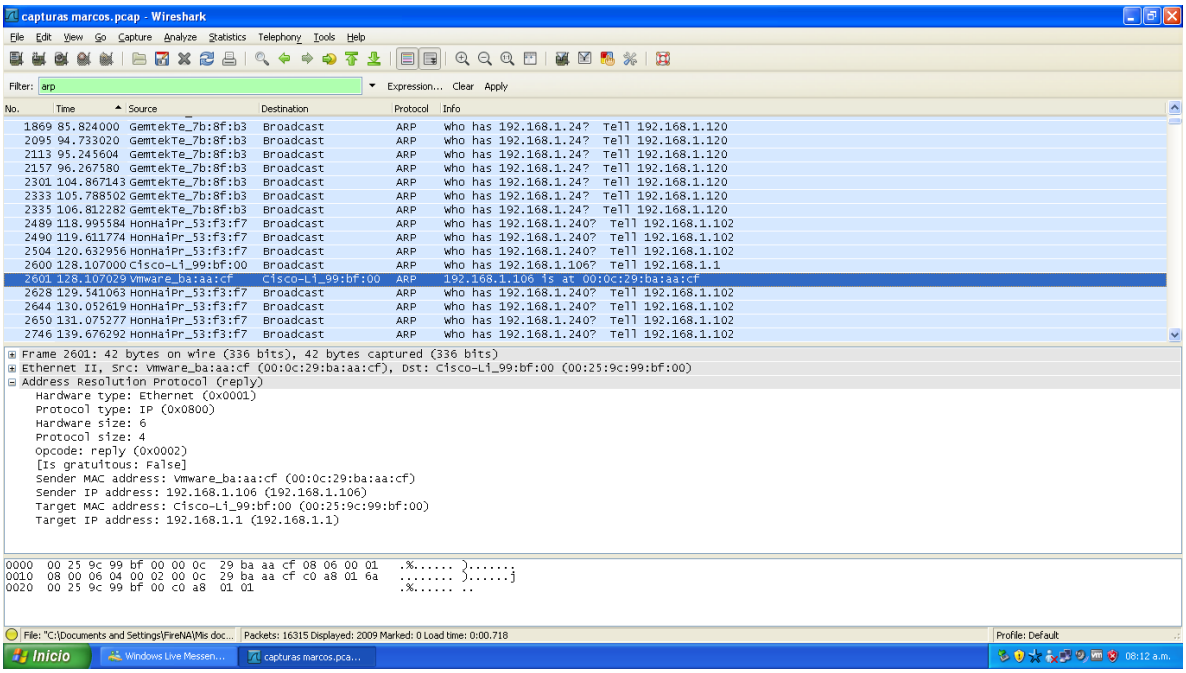
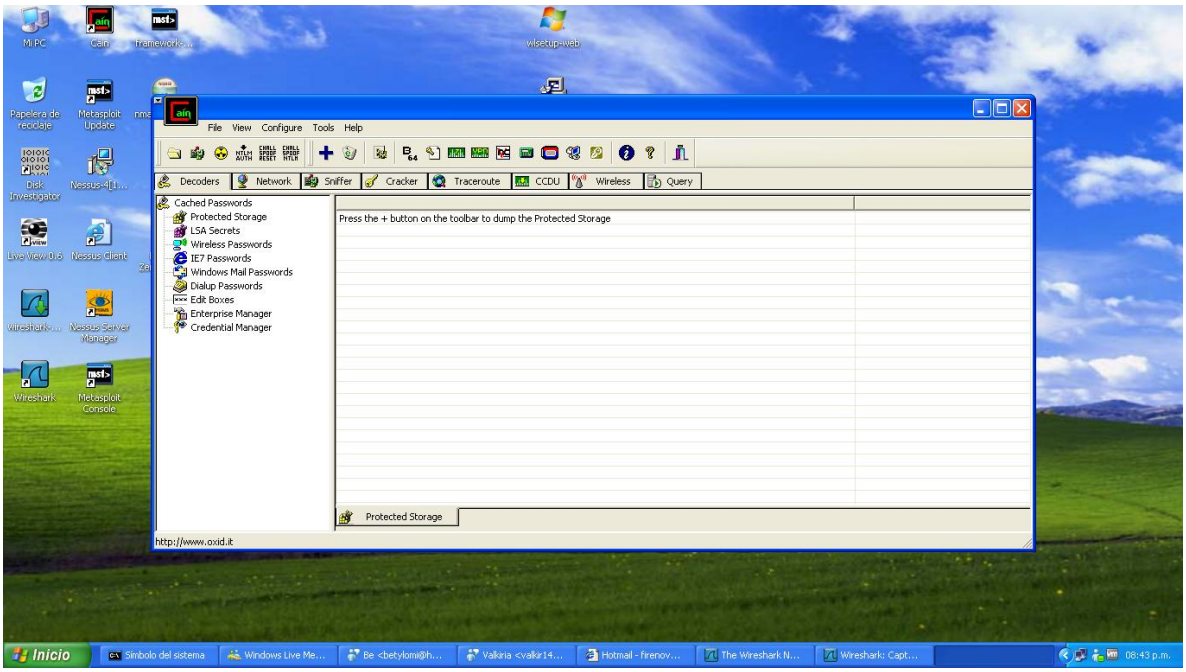
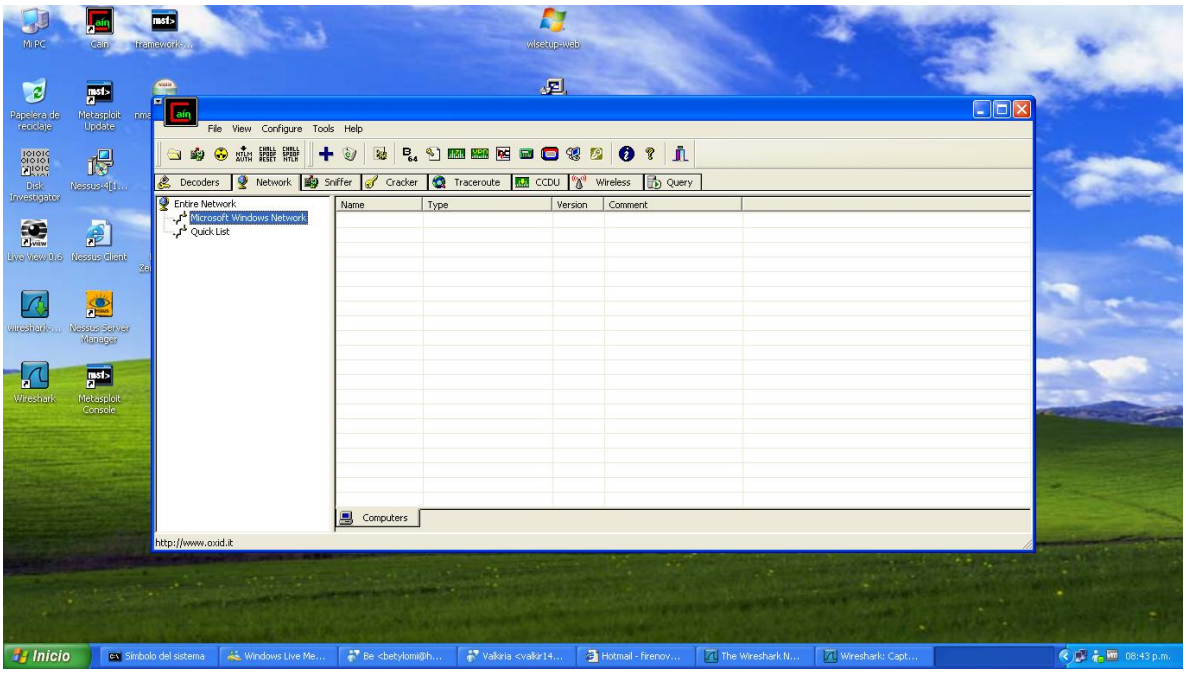
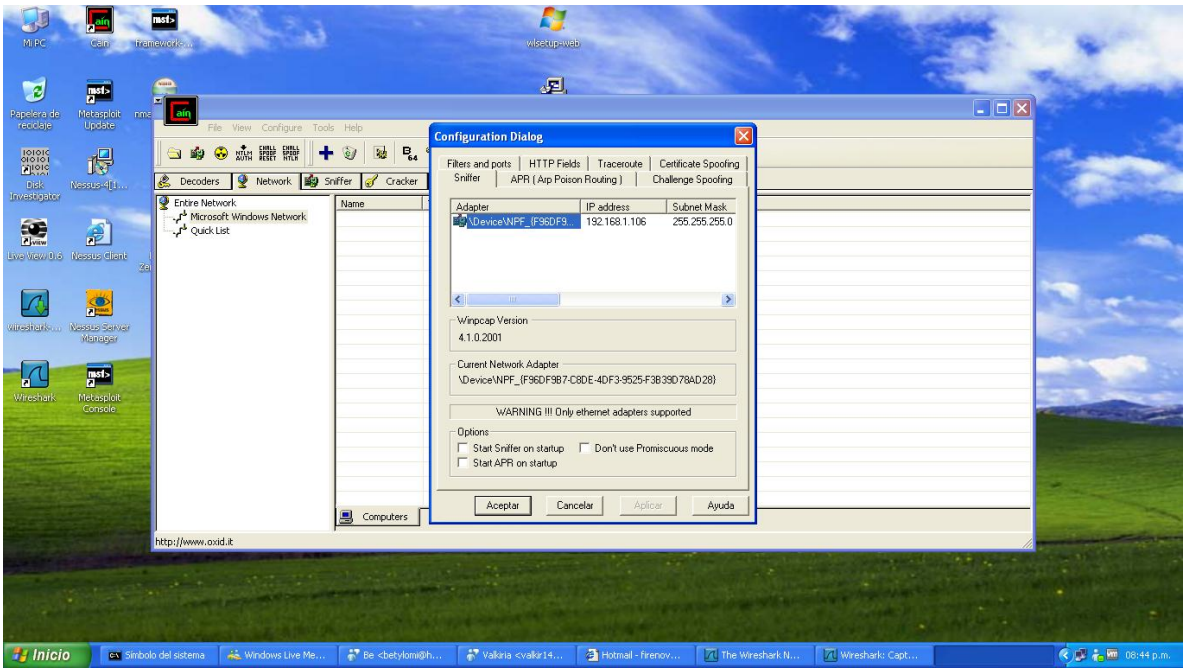
```
C:\Documents and Settings\FireNA>ping 192.168.1.1

Haciendo ping a 192.168.1.1 con 32 bytes de datos:

Respuesta desde 192.168.1.1: bytes=32 tiempo=2ms TTL=64
Respuesta desde 192.168.1.1: bytes=32 tiempo=1ms TTL=111
Respuesta desde 192.168.1.1: bytes=32 tiempo=1ms TTL=1

Estadísticas de ping para 192.168.1.1:
    Paquetes: enviados = 3, recibidos = 3, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 2ms, Media = 1ms
Control-C
^C
C:\Documents and Settings\FireNA>arp -a

Interfaz: 192.168.1.106 --- 0x2
  Dirección IP          Dirección física      Tipo
  192.168.1.1           00-25-9c-99-bf-00     dinámico
  192.168.1.102         5c-ac-4c-53-f3-f7     dinámico
```

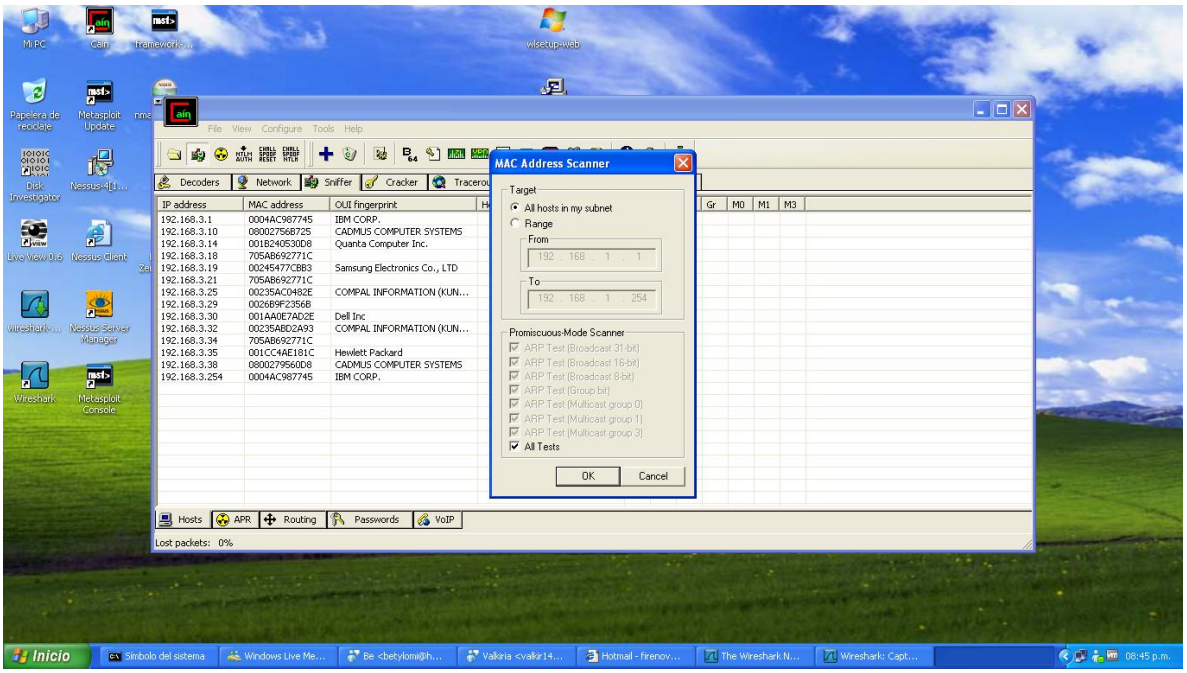


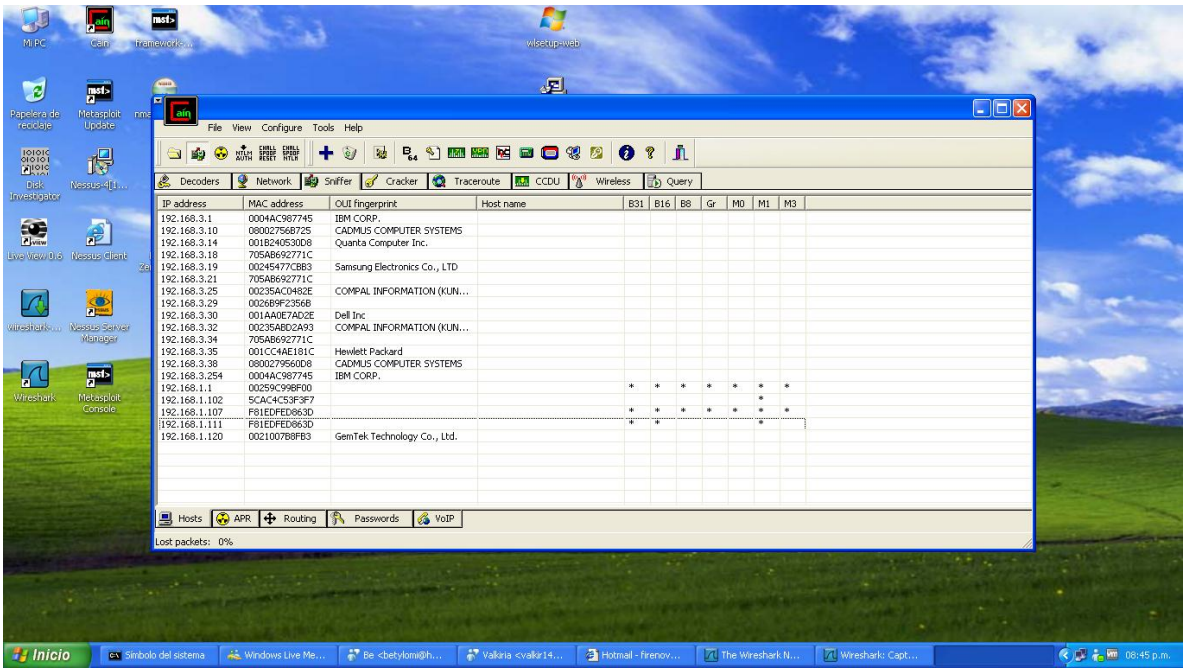

capturas marcos.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: arp
Expression... Clear Apply
No. Time Source Destination Protocol Info
1869 85.824000 GemtekTe_7b:8f:b3 Broadcast ARP who has 192.168.1.24? Tell 192.168.1.120
2095 94.733020 GemtekTe_7b:8f:b3 Broadcast ARP who has 192.168.1.24? Tell 192.168.1.120
2113 95.245604 GemtekTe_7b:8f:b3 Broadcast ARP who has 192.168.1.24? Tell 192.168.1.120
2157 96.267580 GemtekTe_7b:8f:b3 Broadcast ARP who has 192.168.1.24? Tell 192.168.1.120
2301 104.867143 GemtekTe_7b:8f:b3 Broadcast ARP who has 192.168.1.24? Tell 192.168.1.120
2333 105.788502 GemtekTe_7b:8f:b3 Broadcast ARP who has 192.168.1.24? Tell 192.168.1.120
2335 106.812282 GemtekTe_7b:8f:b3 Broadcast ARP who has 192.168.1.24? Tell 192.168.1.120
2489 118.995584 HonHaiPr_53:f3:f7 Broadcast ARP who has 192.168.1.240? Tell 192.168.1.102
2490 119.611774 HonHaiPr_53:f3:f7 Broadcast ARP who has 192.168.1.240? Tell 192.168.1.102
2504 120.632956 HonHaiPr_53:f3:f7 Broadcast ARP who has 192.168.1.240? Tell 192.168.1.102
2600 128.107000 Cisco-Li_99:bf:00 Broadcast ARP who has 192.168.1.106? Tell 192.168.1.1
2601 128.107029 Vmware_ba:aa:cf Cisco-Li_99:bf:00 ARP 192.168.1.106 is at 00:0c:29:ba:aa:cf
2628 129.541063 HonHaiPr_53:f3:f7 Broadcast ARP who has 192.168.1.240? Tell 192.168.1.102
2644 130.052619 HonHaiPr_53:f3:f7 Broadcast ARP who has 192.168.1.240? Tell 192.168.1.102
2650 131.075277 HonHaiPr_53:f3:f7 Broadcast ARP who has 192.168.1.240? Tell 192.168.1.102
2746 139.676292 HonHaiPr_53:f3:f7 Broadcast ARP who has 192.168.1.240? Tell 192.168.1.102
Frame 2601: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
Ethernet II, Src: Vmware_ba:aa:cf (00:0c:29:ba:aa:cf), Dst: Cisco-Li_99:bf:00 (00:25:9c:99:bf:00)
Address Resolution Protocol (reply)
Hardware type: Ethernet (0x0001)
Protocol type: IP (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: reply (0x0002)
[Is gratuitous: False]
Sender MAC address: Vmware_ba:aa:cf (00:0c:29:ba:aa:cf)
Sender IP address: 192.168.1.106 (192.168.1.106)
Target MAC address: Cisco-Li_99:bf:00 (00:25:9c:99:bf:00)
Target IP address: 192.168.1.1 (192.168.1.1)
0000 00 25 9c 99 bf 00 00 0c 29 ba aa cf 08 06 00 01 .%.....).....
0010 08 00 06 04 00 02 00 0c 29 ba aa cf c0 a8 01 6a .....)....j
0020 00 25 9c 99 bf 00 c0 a8 01 01 .%..... ..
File: "C:\Documents and Settings\FireNA\Mis doc...
Packets: 16315 Displayed: 2009 Marked: 0 Load time: 0:00.718
Profile: Default
Inicio
Windows Live Messen...
capturas marcos.pca...
08:12 a.m.

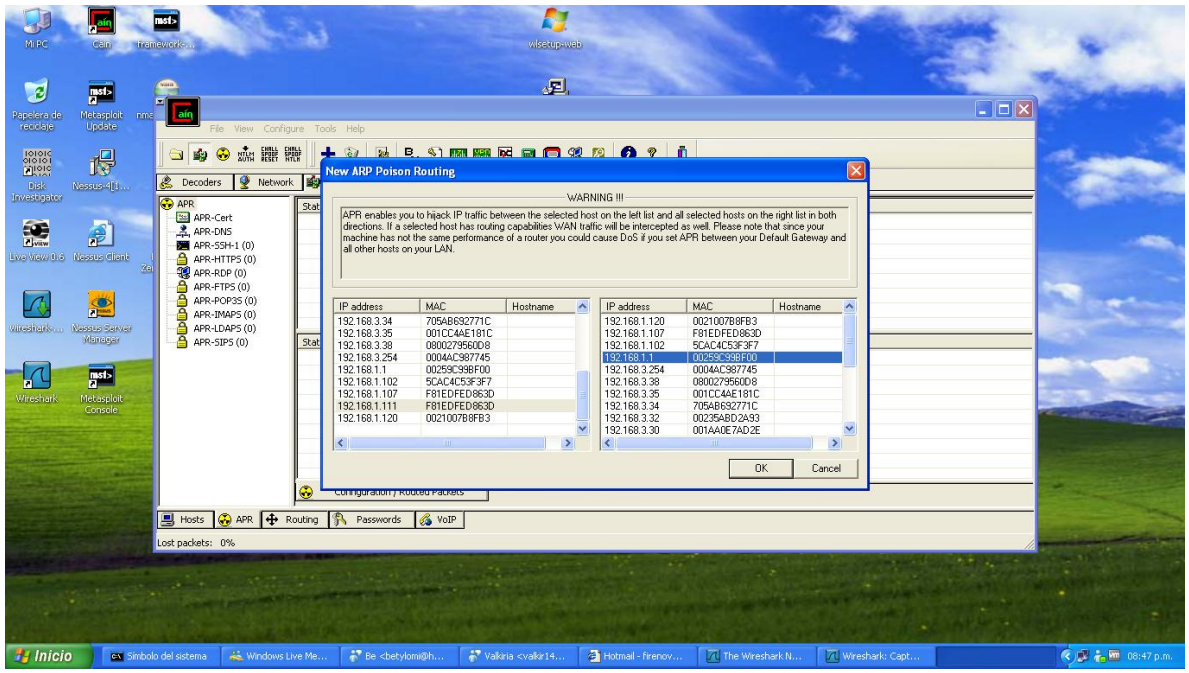

Mi PC
Cain
Framework...
wlsetup-web
Papelera de reciclaje
Metasploit Update
Disk Investigator
Nessus-4[1]...
Live View 0.6
Nessus Client
Wireshark-...
Nessus Server Manager
Wireshark
Metasploit Console
File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
Cached Passwords
Protected Storage
LSA Secrets
Wireless Passwords
IE7 Passwords
Windows Mail Passwords
Dialup Passwords
Edit Boxes
Enterprise Manager
Credential Manager
Press the + button on the toolbar to dump the Protected Storage
Protected Storage
http://www.oxid.it
Inicio
Símbolo del sistema
Windows Live Me...
Be <betylomi@h...
Valkiria <valkir14...
Hotmail - Firenov...
The Wireshark N...
Wireshark: Capt...
08:43 p.m.

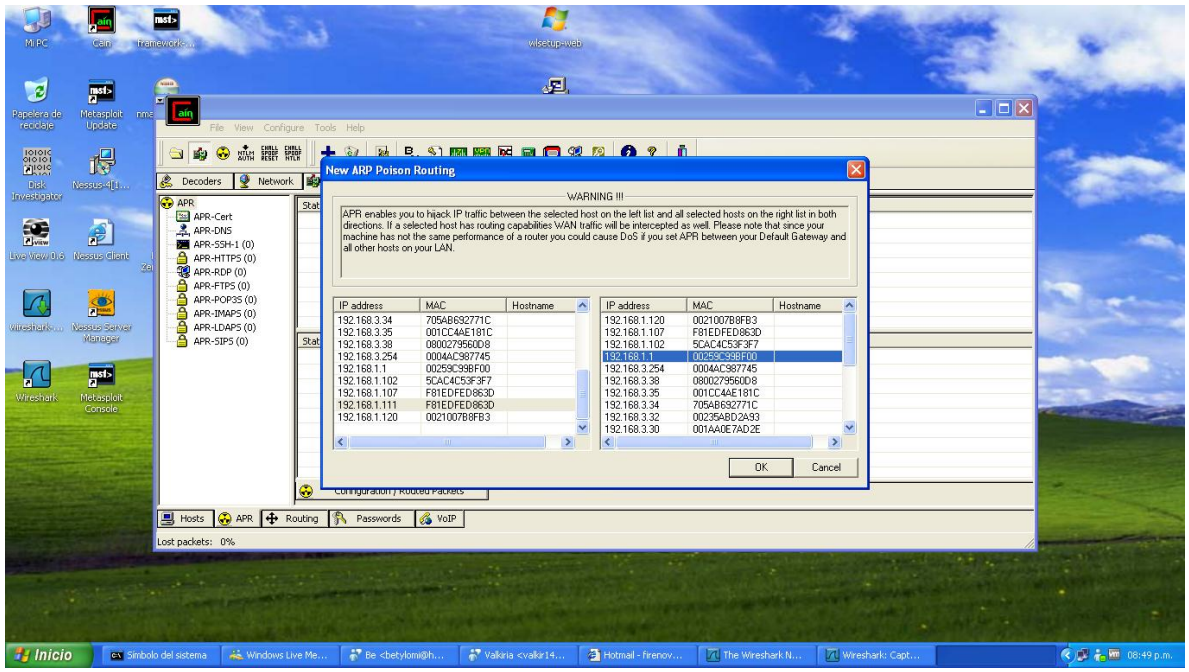

File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
Entire Network
Microsoft Windows Network
Quick List
Name Type Version Comment
Computers
http://www.oxid.it
Inicio

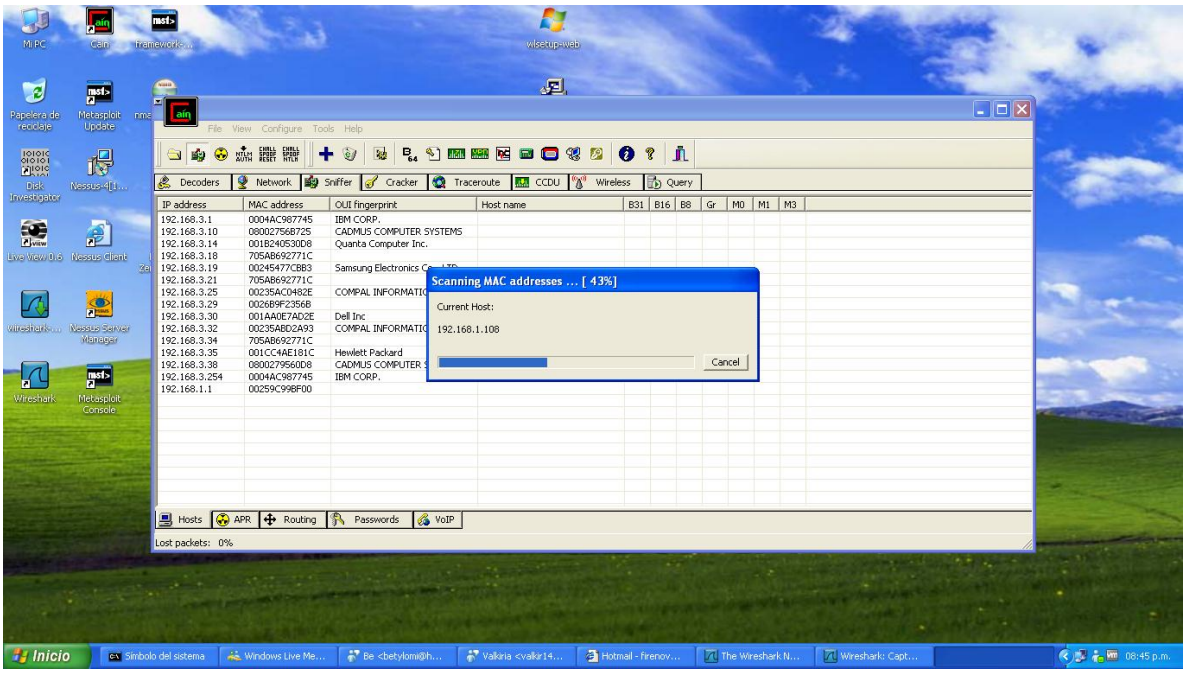

Configuration Dialog
Filters and ports HTTP Fields Traceroute Certificate Spoofing
Sniffer APR (Arp Poison Routing) Challenge Spoofing
Adapter IP address Subnet Mask
\Device\NPF_{F96DF9... 192.168.1.106 255.255.255.0
Winpcap Version
4.1.0.2001
Current Network Adapter
\Device\NPF_{F96DF9B7-C8DE-4DF3-9525-F3B39D78AD28}
WARNING !!! Only ethernet adapters supported
Options
Start Sniffer on startup
Don't use Promiscuous mode
Start APR on startup
Aceptar Cancelar Aplicar Ayuda
Inicio

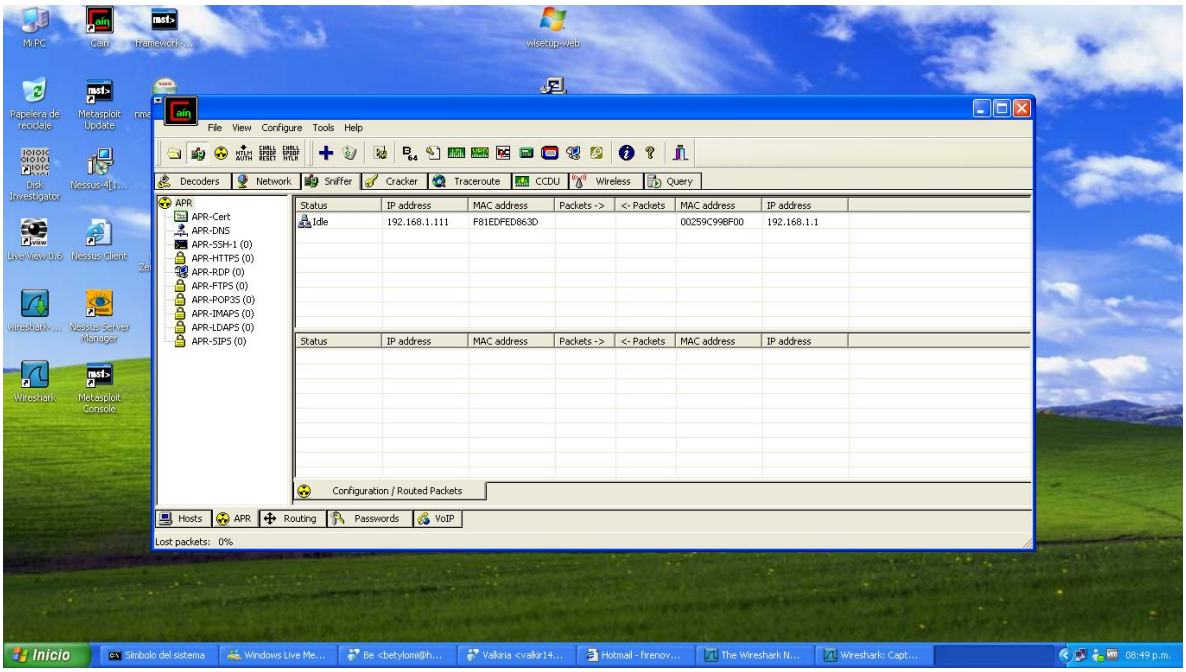

MAC Address Scanner
Target
All hosts in my subnet
Range
From
192 . 168 . 1 . 1
To
192 . 168 . 1 . 254
Promiscuous-Mode Scanner
ARP Test (Broadcast 31-bit)
ARP Test (Broadcast 16-bit)
ARP Test (Broadcast 8-bit)
ARP Test (Group bit)
ARP Test (Multicast group 0)
ARP Test (Multicast group 1)
ARP Test (Multicast group 3)
All Tests
OK
Cancel
File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute
IP address MAC address OUI fingerprint
192.168.3.1 0004AC987745 IBM CORP.
192.168.3.10 08002756B725 CADMUS COMPUTER SYSTEMS
192.168.3.14 001B240530D8 Quanta Computer Inc.
192.168.3.18 705AB692771C
192.168.3.19 00245477CBB3 Samsung Electronics Co., LTD
192.168.3.21 705AB692771C
192.168.3.25 00235AC0482E COMPAL INFORMATION (KUN...
192.168.3.29 0026B9F2356B
192.168.3.30 001AA0E7AD2E Dell Inc
192.168.3.32 00235ABD2A93 COMPAL INFORMATION (KUN...
192.168.3.34 705AB692771C
192.168.3.35 001CC4AE181C Hewlett Packard
192.168.3.38 080027960D8 CADMUS COMPUTER SYSTEMS
192.168.3.254 0004AC987745 IBM CORP.
Hosts APR Routing Passwords VoIP
Lost packets: 0%
Inicio
Simbolo del sistema
Windows Live Me...
Be <betylomi@h...
Valkiria <valkir14...
Hotmail - firenov...
The Wireshark N...
Wireshark: Capt...
08:45 p.m.

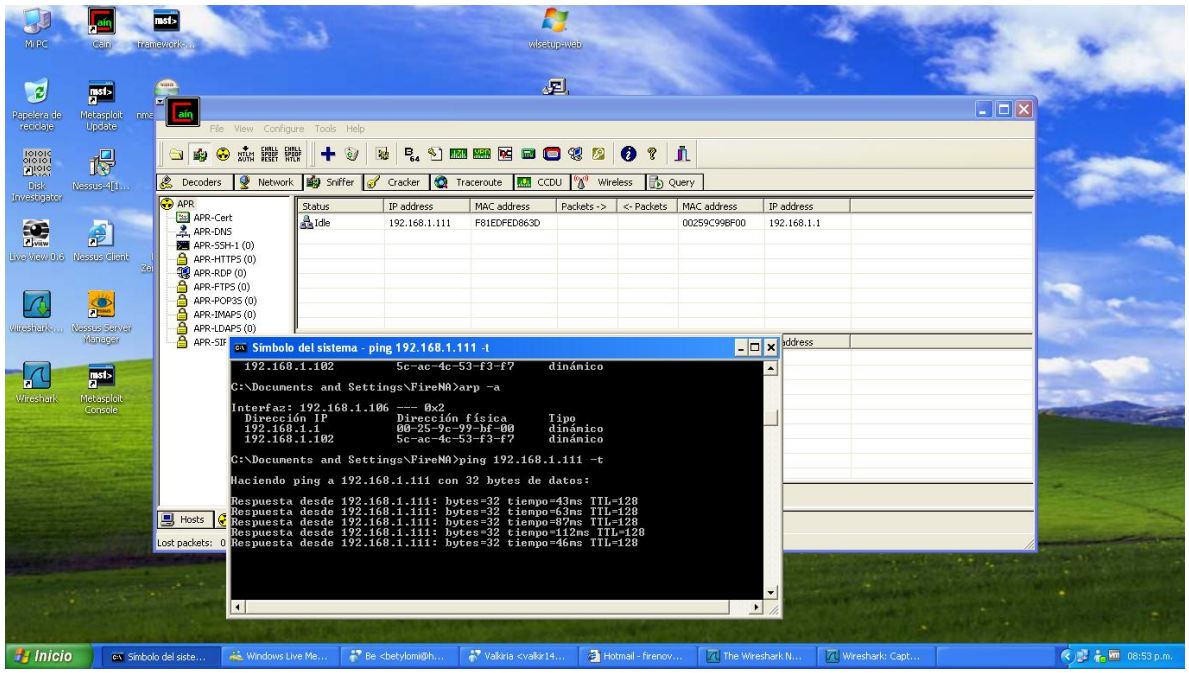

File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
IP address MAC address OUI fingerprint Host name B31 B16 B8 Gr M0 M1 M3
192.168.3.1 0004AC987745 IBM CORP.
192.168.3.10 08002756B725 CADMUS COMPUTER SYSTEMS
192.168.3.14 001B240530D8 Quanta Computer Inc.
192.168.3.18 705AB692771C
192.168.3.19 00245477CBB3 Samsung Electronics Co., LTD
192.168.3.21 705AB692771C
192.168.3.25 00235AC0482E COMPAL INFORMATION (KUN...
192.168.3.29 0026B9F2356B
192.168.3.30 001AA0E7AD2E Dell Inc
192.168.3.32 00235ABD2A93 COMPAL INFORMATION (KUN...
192.168.3.34 705AB692771C
192.168.3.35 001CC4AE181C Hewlett Packard
192.168.3.38 080027960D8 CADMUS COMPUTER SYSTEMS
192.168.3.254 0004AC987745 IBM CORP.
192.168.1.1 00259C99BF00 * * * * * * *
192.168.1.102 5CAC4C53F3F7 *
192.168.1.107 F81EDFED863D * * * * * * *
192.168.1.111 F81EDFED863D * * *
192.168.1.120 0021007B8FB3 GemTek Technology Co., Ltd.
Hosts APR Routing Passwords VoIP
Lost packets: 0%
Inicio
Simbolo del sistema
Windows Live Me...
Be <betylomi@h...
Valkiria <valkir14...
Hotmail - firenov...
The Wireshark N...
Wireshark: Capt...
08:45 p.m.

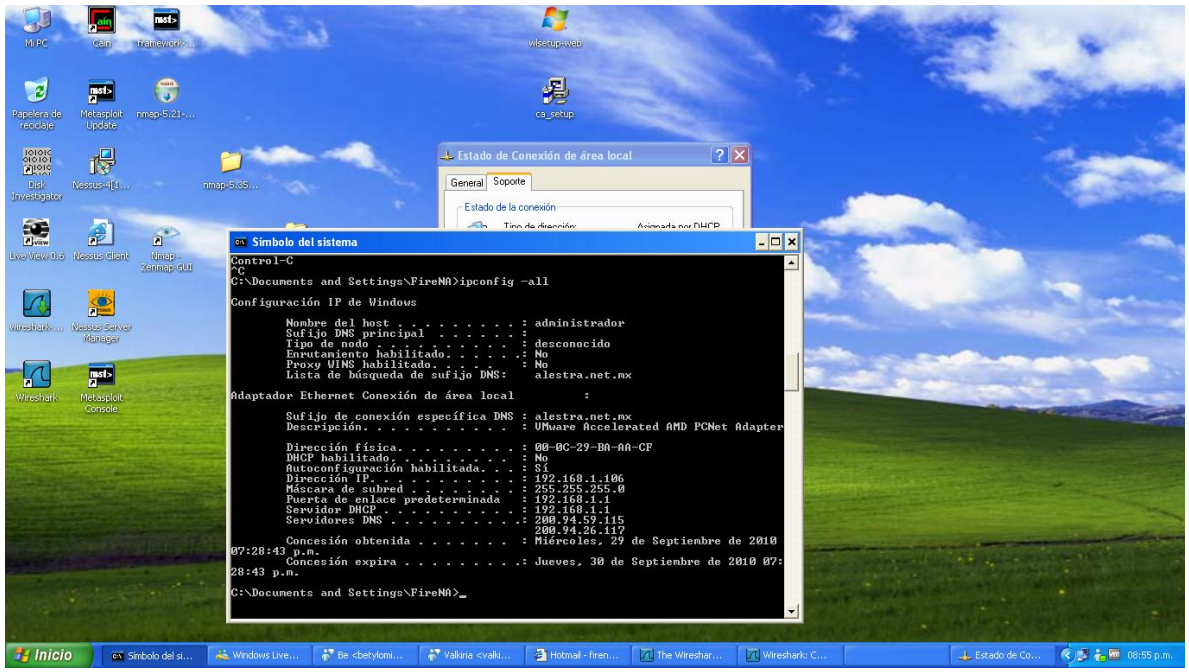

New ARP Poison Routing
WARNING !!!
APR enables you to hijack IP traffic between the selected host on the left list and all selected hosts on the right list in both directions. If a selected host has routing capabilities WAN traffic will be intercepted as well. Please note that since your machine has not the same performance of a router you could cause DoS if you set APR between your Default Gateway and all other hosts on your LAN.
IP address MAC Hostname
192.168.3.34 705AB692771C
192.168.3.35 001CC4AE181C
192.168.3.38 0800279560D8
192.168.3.254 0004AC987745
192.168.1.1 00259C99BF00
192.168.1.102 5CAC4C53F3F7
192.168.1.107 F81EDFED863D
192.168.1.111 F81EDFED863D
192.168.1.120 0021007B8FB3
192.168.1.120 0021007B8FB3
192.168.1.107 F81EDFED863D
192.168.1.102 5CAC4C53F3F7
192.168.1.1 00259C99BF00
192.168.3.254 0004AC987745
192.168.3.38 0800279560D8
192.168.3.35 001CC4AE181C
192.168.3.34 705AB692771C
192.168.3.32 00235ABD2A93
192.168.3.30 001AA0E7AD2E
OK
Cancel
Hosts
APR
Routing
Passwords
VoIP
Lost packets: 0%
Inicio
08:47 p.m.


New ARP Poison Routing
WARNING !!!
APR enables you to hijack IP traffic between the selected host on the left list and all selected hosts on the right list in both directions. If a selected host has routing capabilities WAN traffic will be intercepted as well. Please note that since your machine has not the same performance of a router you could cause DoS if you set APR between your Default Gateway and all other hosts on your LAN.
IP address MAC Hostname
192.168.3.34 705AB692771C
192.168.3.35 001CC4AE181C
192.168.3.38 0800279560D8
192.168.3.254 0004AC987745
192.168.1.1 00259C99BF00
192.168.1.102 5CAC4C53F3F7
192.168.1.107 F81EDFED863D
192.168.1.111 F81EDFED863D
192.168.1.120 0021007B8FB3
192.168.1.120 0021007B8FB3
192.168.1.107 F81EDFED863D
192.168.1.102 5CAC4C53F3F7
192.168.1.1 00259C99BF00
192.168.3.254 0004AC987745
192.168.3.38 0800279560D8
192.168.3.35 001CC4AE181C
192.168.3.34 705AB692771C
192.168.3.32 00235ABD2A93
192.168.3.30 001AA0E7AD2E
OK
Cancel
Hosts
APR
Routing
Passwords
VoIP
Lost packets: 0%
Inicio
08:49 p.m.

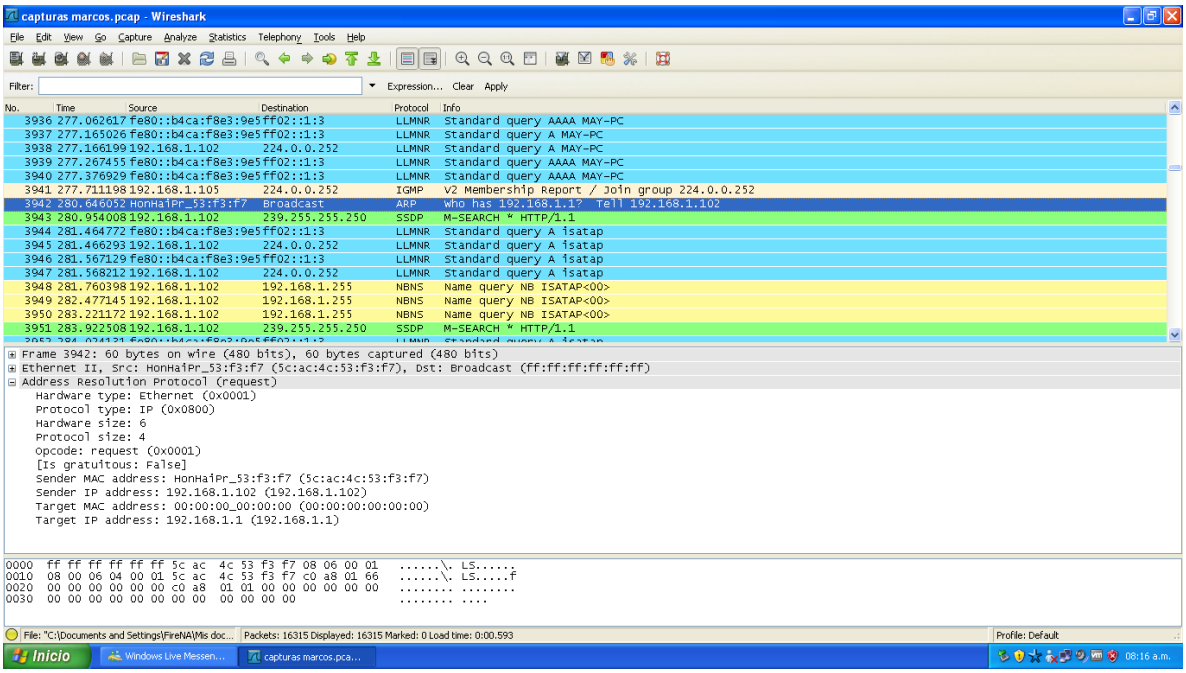

File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
IP address MAC address OUI fingerprint Host name B31 B16 B8 Gr M0 M1 M3
192.168.3.1 0004AC987745 IBM CORP.
192.168.3.10 08002756B725 CADMUS COMPUTER SYSTEMS
192.168.3.14 001B240530D8 Quanta Computer Inc.
192.168.3.18 705AB692771C
192.168.3.19 00245477CBB3 Samsung Electronics
192.168.3.21 705AB692771C
192.168.3.25 00235AC0482E COMPAL INFORMATI
192.168.3.29 0026B9F2356B
192.168.3.30 001AA0E7AD2E Dell Inc
192.168.3.32 00235ABD2A93 COMPAL INFORMATI
192.168.3.34 705AB692771C
192.168.3.35 001CC4AE181C Hewlett Packard
192.168.3.38 080027960D8 CADMUS COMPUTER
192.168.3.254 0004AC987745 IBM CORP.
192.168.1.1 00259C99BF00
Scanning MAC addresses ... [43%]
Current Host:
192.168.1.108
Cancel
Hosts APR Routing Passwords VoIP
Lost packets: 0%
Inicio
08:45 p.m.

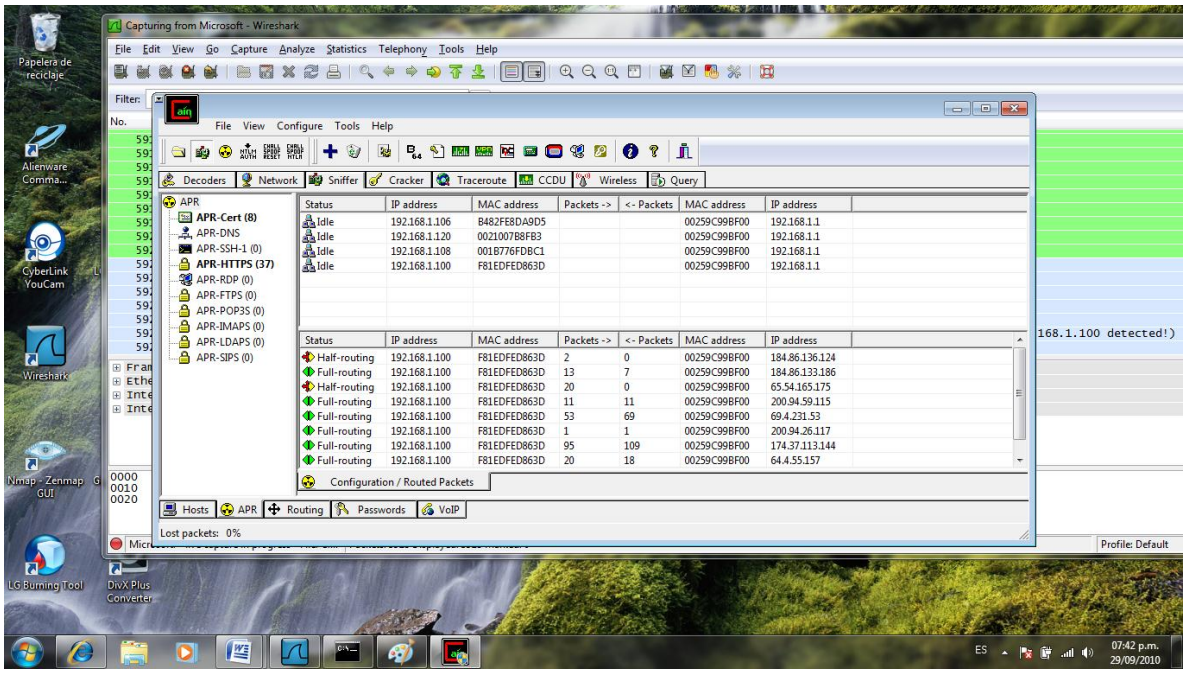

File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
APR
APR-Cert
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (0)
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
Status IP address MAC address Packets -> <- Packets MAC address IP address
Idle 192.168.1.111 F81EDFED863D 00259C99BF00 192.168.1.1
Configuration / Routed Packets
Hosts APR Routing Passwords VoIP
Lost packets: 0%
Inicio
08:49 p.m.

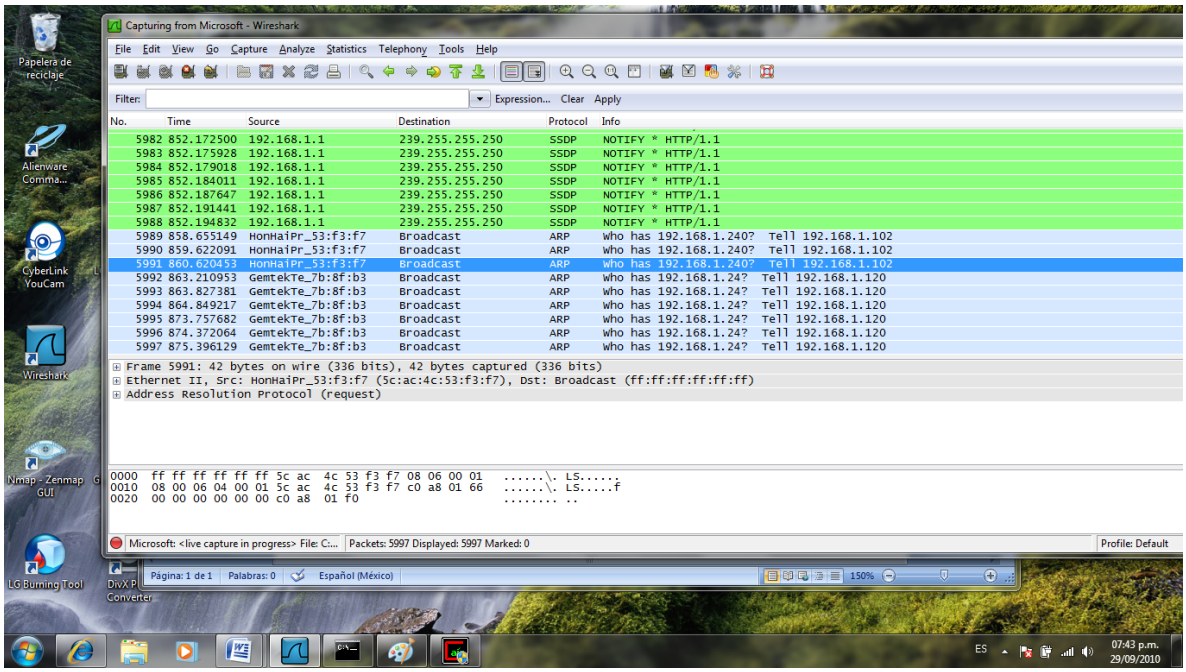

Símbolo del sistema - ping 192.168.1.111 -t
192.168.1.102 5c-ac-4c-53-f3-f7 dinámico
C:\Documents and Settings\FireNA>arp -a
Interfaz: 192.168.1.106 --- 0x2
Dirección IP Dirección física Tipo
192.168.1.1 00-25-9c-99-bf-00 dinámico
192.168.1.102 5c-ac-4c-53-f3-f7 dinámico
C:\Documents and Settings\FireNA>ping 192.168.1.111 -t
Haciendo ping a 192.168.1.111 con 32 bytes de datos:
Respuesta desde 192.168.1.111: bytes=32 tiempo=43ms TTL=128
Respuesta desde 192.168.1.111: bytes=32 tiempo=63ms TTL=128
Respuesta desde 192.168.1.111: bytes=32 tiempo=87ms TTL=128
Respuesta desde 192.168.1.111: bytes=32 tiempo=112ms TTL=128
Respuesta desde 192.168.1.111: bytes=32 tiempo=46ms TTL=128
Inicio

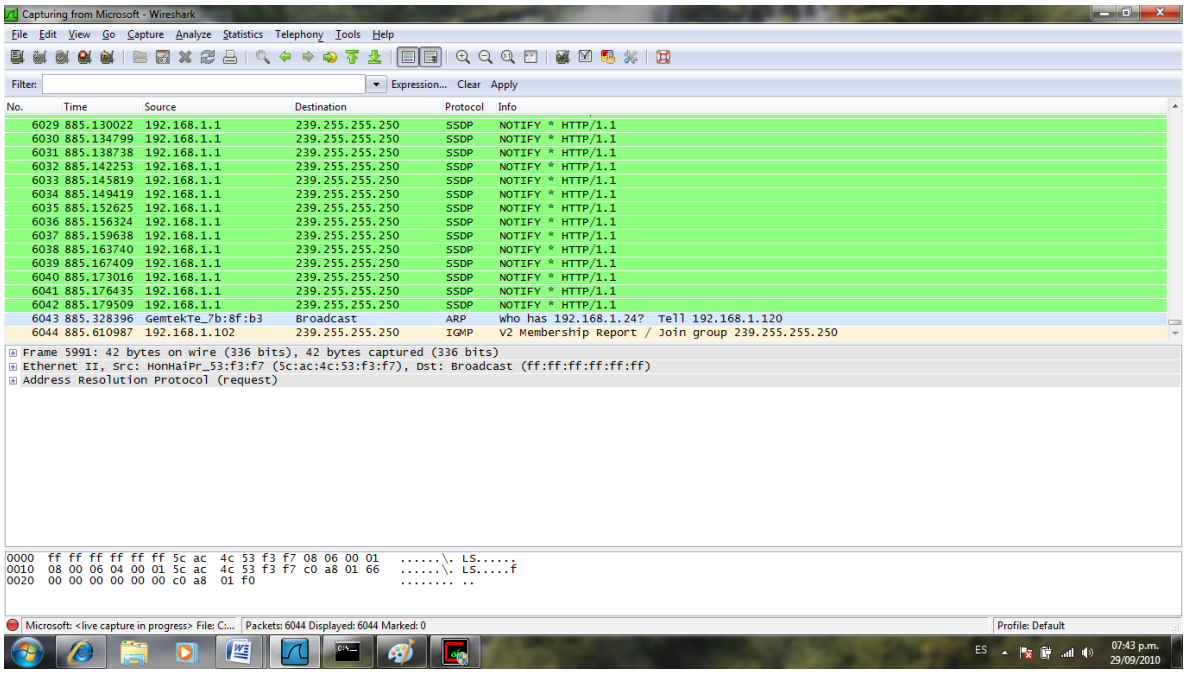

Símbolo del sistema
Control-C
^C
C:\Documents and Settings\FireNA>ipconfig -all
Configuración IP de Windows
Nombre del host . . . . . : administrador
Sufijo DNS principal . . . . . :
Tipo de nodo . . . . . : desconocido
Enrutamiento habilitado. . . . . : No
Proxy WINS habilitado. . . . . : No
Lista de búsqueda de sufijo DNS: alestra.net.mx
Adaptador Ethernet Conexión de área local :
Sufijo de conexión específica DNS : alestra.net.mx
Descripción. . . . . : VMware Accelerated AMD PCNet Adapter
Dirección física. . . . . : 00-0C-29-BA-AA-CF
DHCP habilitado. . . . . : No
Autoconfiguración habilitada. . . : Sí
Dirección IP. . . . . : 192.168.1.106
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada : 192.168.1.1
Servidor DHCP . . . . . : 192.168.1.1
Servidores DNS . . . . . : 200.94.59.115
200.94.26.117
Concesión obtenida . . . . . : Miércoles, 29 de Septiembre de 2010 07:28:43 p.m.
Concesión expira . . . . . : Jueves, 30 de Septiembre de 2010 07:28:43 p.m.
C:\Documents and Settings\FireNA>
Estado de Conexión de área local
General
Soporte
Inicio

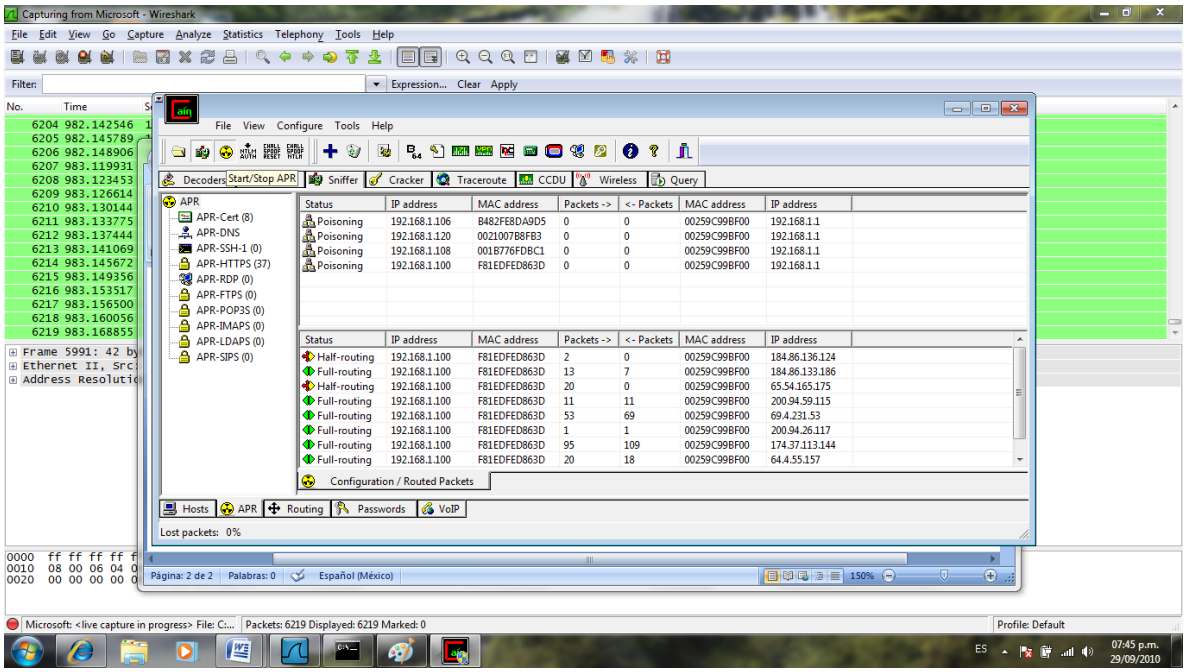
```
Estadísticas de ping para 192.168.1.1:
    Paquetes: enviados = 3, recibidos = 3, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 1ms, Máximo = 2ms, Media = 1ms
Control-C
^C
C:\Documents and Settings\FireNA>arp -a

Interfaz: 192.168.1.106 --- 0x2
  Dirección IP          Dirección física      Tipo
  192.168.1.1           00-25-9c-99-bf-00     dinámico
  192.168.1.102         5c-ac-4c-53-f3-f7     dinámico

C:\Documents and Settings\FireNA>arp -a

Interfaz: 192.168.1.106 --- 0x2
  Dirección IP          Dirección física      Tipo
  192.168.1.1           5c-ac-4c-53-f3-f7     dinámico
  192.168.1.102         5c-ac-4c-53-f3-f7     dinámico
```

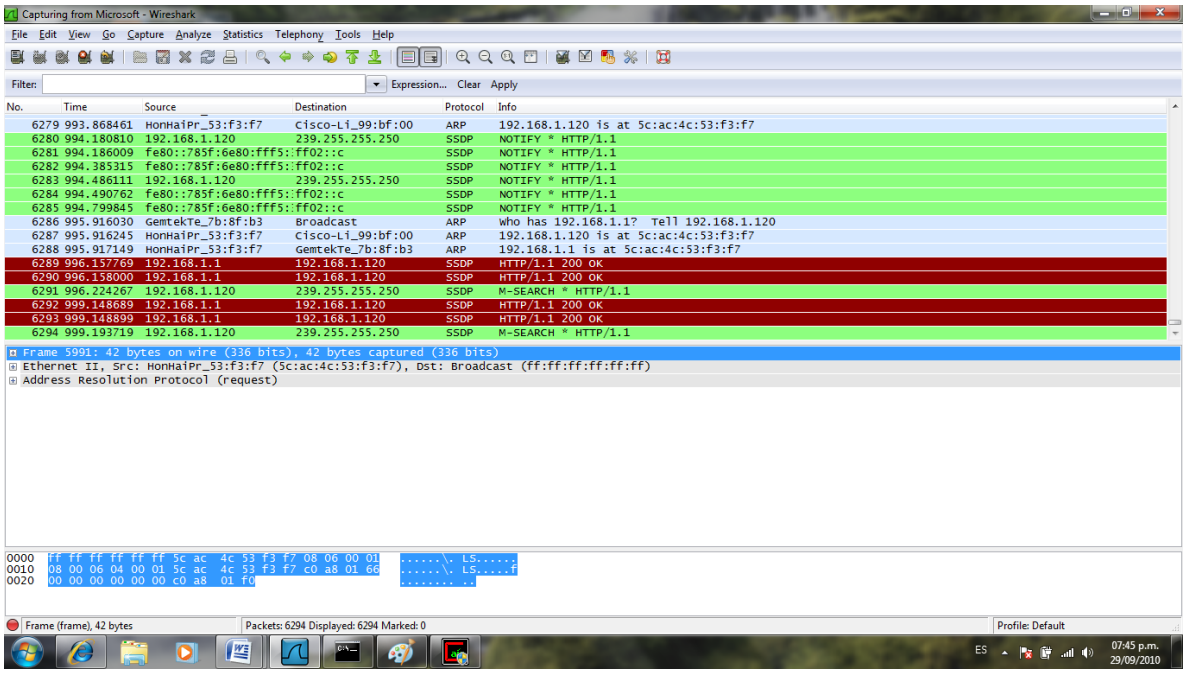


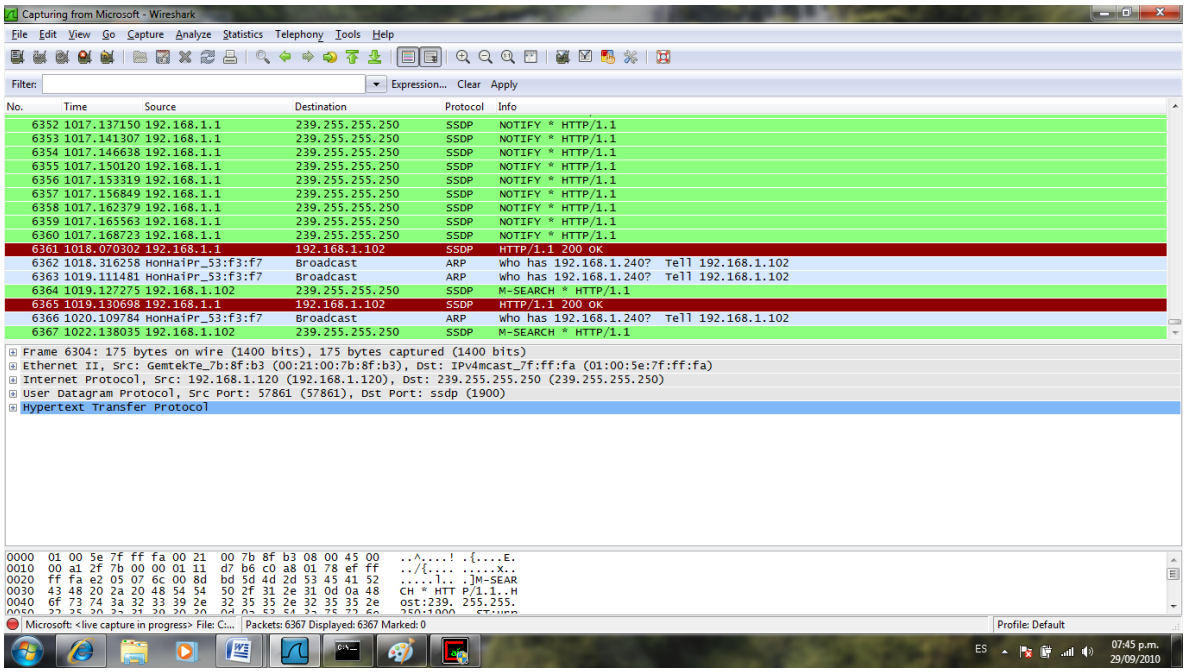

Capturing from Microsoft - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
APR
APR-Cert (8)
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (37)
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
Status IP address MAC address Packets -> <- Packets MAC address IP address
Idle 192.168.1.106 B482FE8DA9D5 00259C99BF00 192.168.1.1
Idle 192.168.1.120 0021007B8FB3 00259C99BF00 192.168.1.1
Idle 192.168.1.108 001B776FDBC1 00259C99BF00 192.168.1.1
Idle 192.168.1.100 F81EDFED863D 00259C99BF00 192.168.1.1
Half-routing 192.168.1.100 F81EDFED863D 2 0 00259C99BF00 184.86.136.124
Full-routing 192.168.1.100 F81EDFED863D 13 7 00259C99BF00 184.86.133.186
Half-routing 192.168.1.100 F81EDFED863D 20 0 00259C99BF00 65.54.165.175
Full-routing 192.168.1.100 F81EDFED863D 11 11 00259C99BF00 200.94.59.115
Full-routing 192.168.1.100 F81EDFED863D 53 69 00259C99BF00 69.4.231.53
Full-routing 192.168.1.100 F81EDFED863D 1 1 00259C99BF00 200.94.26.117
Full-routing 192.168.1.100 F81EDFED863D 95 109 00259C99BF00 174.37.113.144
Full-routing 192.168.1.100 F81EDFED863D 20 18 00259C99BF00 64.4.55.157
Configuration / Routed Packets
Hosts APR Routing Passwords VoIP
Lost packets: 0%
168.1.100 detected!)
Profile: Default
07:42 p.m.
29/09/2010

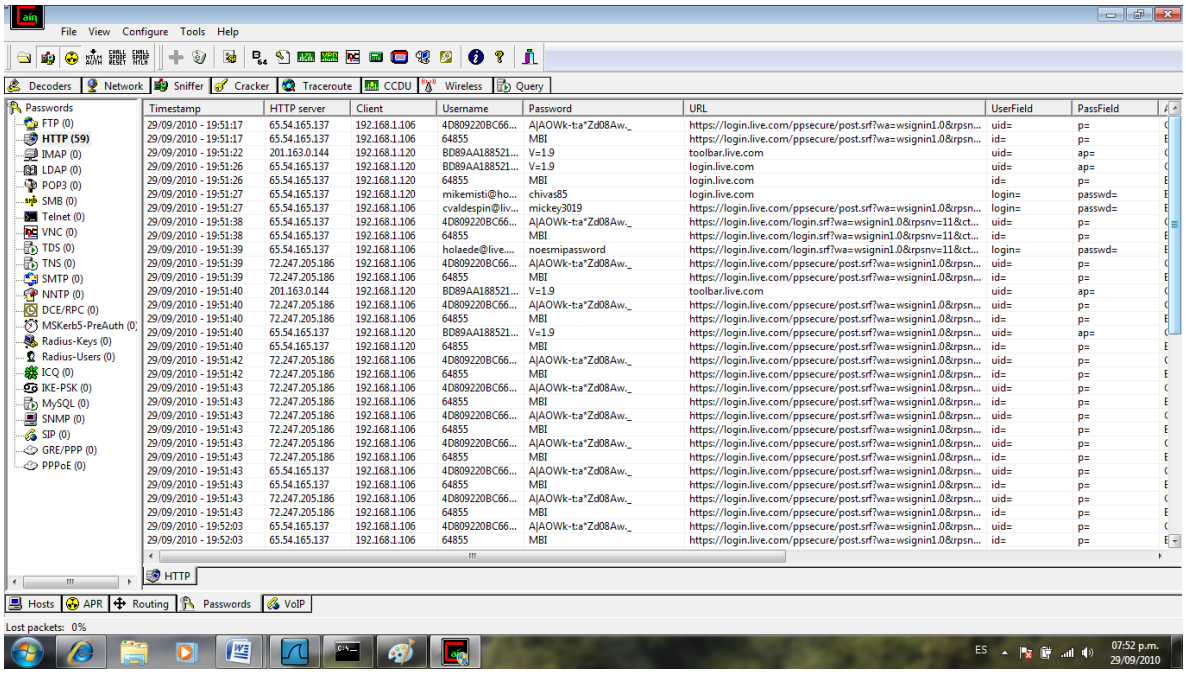

Capturing from Microsoft - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
5982 852.172500 192.168.1.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
5983 852.175928 192.168.1.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
5984 852.179018 192.168.1.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
5985 852.184011 192.168.1.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
5986 852.187647 192.168.1.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
5987 852.191441 192.168.1.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
5988 852.194832 192.168.1.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
5989 858.655149 HonHaiPr_53:f3:f7 Broadcast ARP Who has 192.168.1.240? Tell 192.168.1.102
5990 859.622091 HonHaiPr_53:f3:f7 Broadcast ARP Who has 192.168.1.240? Tell 192.168.1.102
5991 860.620453 HonHaiPr_53:f3:f7 Broadcast ARP Who has 192.168.1.240? Tell 192.168.1.102
5992 863.210953 GemtekTe_7b:8f:b3 Broadcast ARP Who has 192.168.1.24? Tell 192.168.1.120
5993 863.827381 GemtekTe_7b:8f:b3 Broadcast ARP Who has 192.168.1.24? Tell 192.168.1.120
5994 864.849217 GemtekTe_7b:8f:b3 Broadcast ARP Who has 192.168.1.24? Tell 192.168.1.120
5995 873.757682 GemtekTe_7b:8f:b3 Broadcast ARP Who has 192.168.1.24? Tell 192.168.1.120
5996 874.372064 GemtekTe_7b:8f:b3 Broadcast ARP Who has 192.168.1.24? Tell 192.168.1.120
5997 875.396129 GemtekTe_7b:8f:b3 Broadcast ARP Who has 192.168.1.24? Tell 192.168.1.120
Frame 5991: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
Ethernet II, Src: HonHaiPr_53:f3:f7 (5c:ac:4c:53:f3:f7), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff 5c ac 4c 53 f3 f7 08 06 00 01 ......\. LS......
0010 08 00 06 04 00 01 5c ac 4c 53 f3 f7 c0 a8 01 66 ......\. LS.....f
0020 00 00 00 00 00 00 c0 a8 01 f0 ....
Microsoft: <live capture in progress> File: C:... Packets: 5997 Displayed: 5997 Marked: 0
Profile: Default
Página: 1 de 1 Palabras: 0 Español (México) 150%
07:43 p.m.
29/09/2010

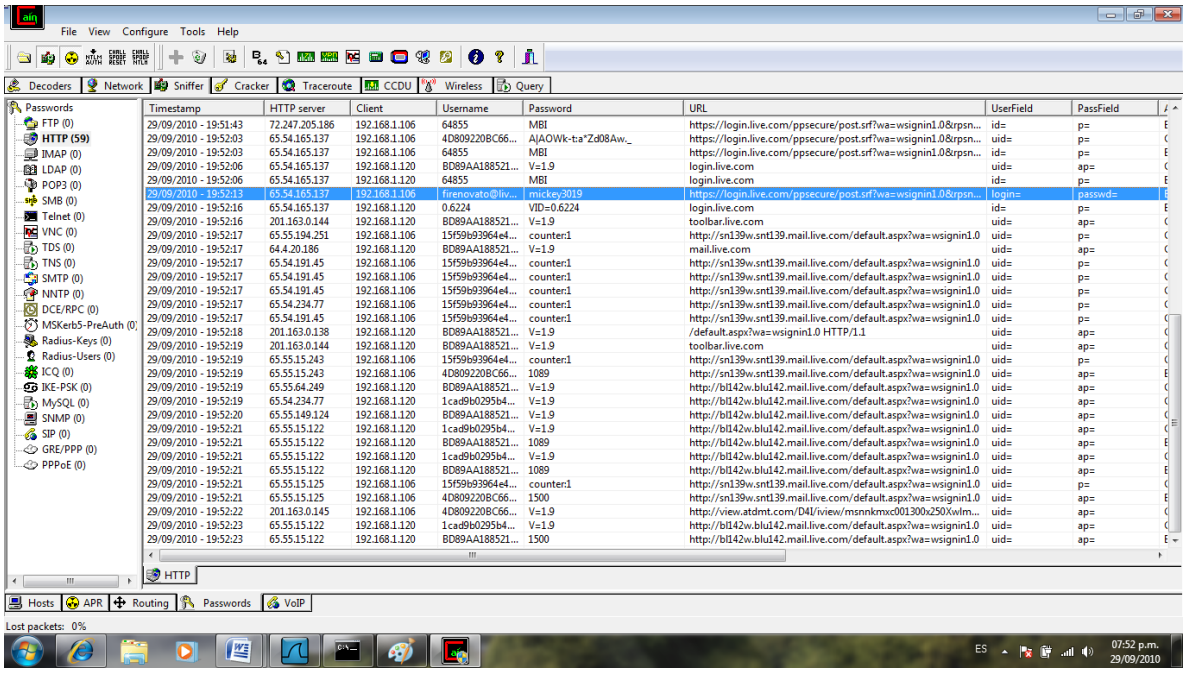

Capturing from Microsoft - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
6029 885.130022 192.168.1.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
6030 885.134799 192.168.1.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
6031 885.138738 192.168.1.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
6032 885.142253 192.168.1.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
6033 885.145819 192.168.1.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
6034 885.149419 192.168.1.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
6035 885.152625 192.168.1.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
6036 885.156324 192.168.1.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
6037 885.159638 192.168.1.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
6038 885.163740 192.168.1.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
6039 885.167409 192.168.1.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
6040 885.173016 192.168.1.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
6041 885.176435 192.168.1.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
6042 885.179509 192.168.1.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
6043 885.328396 GemtekTe_7b:8f:b3 Broadcast ARP who has 192.168.1.24? Tell 192.168.1.120
6044 885.610987 192.168.1.102 239.255.255.250 IGMP V2 Membership Report / Join group 239.255.255.250
Frame 5991: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
Ethernet II, Src: HonHaiPr_53:f3:f7 (5c:ac:4c:53:f3:f7), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff 5c ac 4c 53 f3 f7 08 06 00 01
0010 08 00 06 04 00 01 5c ac 4c 53 f3 f7 c0 a8 01 66
0020 00 00 00 00 00 00 c0 a8 01 f0
Microsoft: <live capture in progress> File: C:... Packets: 6044 Displayed: 6044 Marked: 0
Profile: Default
07:43 p.m.
29/09/2010

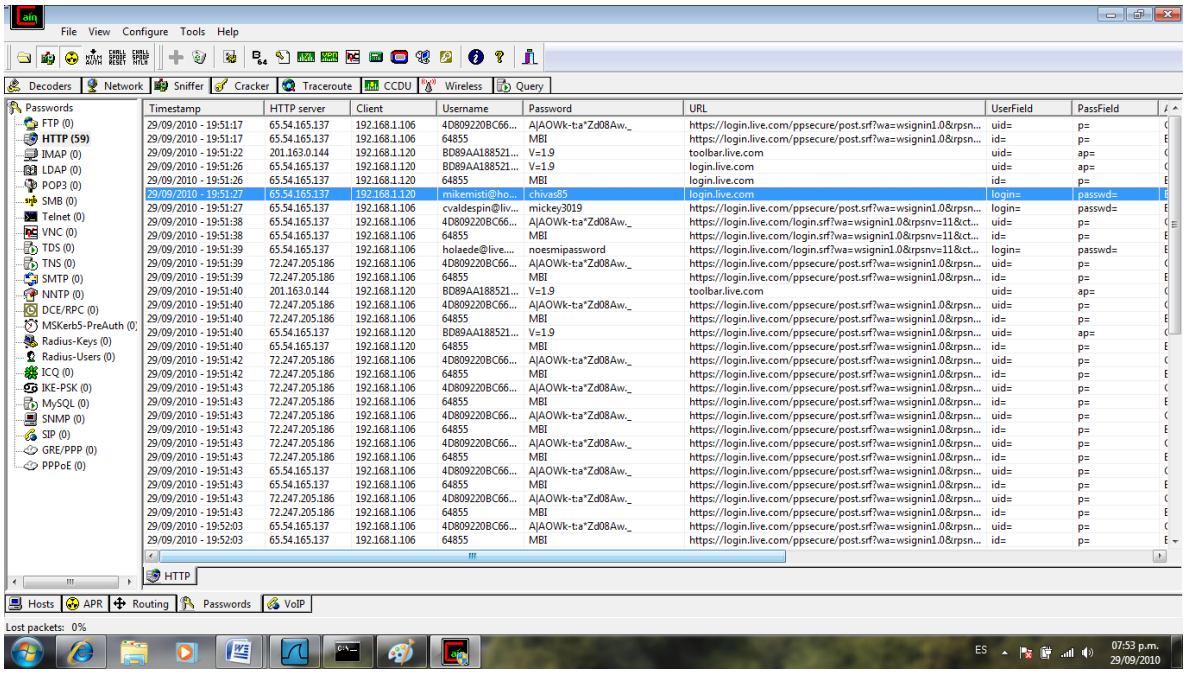

Capturing from Microsoft - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: Expression... Clear Apply
File View Configure Tools Help
Decoders Start/Stop APR Sniffer Cracker Traceroute CCDU Wireless Query
APR
APR-Cert (8)
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (37)
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
Status IP address MAC address Packets -> <- Packets MAC address IP address
Poisoning 192.168.1.106 B482FE8DA9D5 0 0 00259C99BF00 192.168.1.1
Poisoning 192.168.1.120 0021007B8FB3 0 0 00259C99BF00 192.168.1.1
Poisoning 192.168.1.108 001B776FDBC1 0 0 00259C99BF00 192.168.1.1
Poisoning 192.168.1.100 F81EDFED863D 0 0 00259C99BF00 192.168.1.1
Status IP address MAC address Packets -> <- Packets MAC address IP address
Half-routing 192.168.1.100 F81EDFED863D 2 0 00259C99BF00 184.86.136.124
Full-routing 192.168.1.100 F81EDFED863D 13 7 00259C99BF00 184.86.133.186
Half-routing 192.168.1.100 F81EDFED863D 20 0 00259C99BF00 65.54.165.175
Full-routing 192.168.1.100 F81EDFED863D 11 11 00259C99BF00 200.94.59.115
Full-routing 192.168.1.100 F81EDFED863D 53 69 00259C99BF00 69.4.231.53
Full-routing 192.168.1.100 F81EDFED863D 1 1 00259C99BF00 200.94.26.117
Full-routing 192.168.1.100 F81EDFED863D 95 109 00259C99BF00 174.37.113.144
Full-routing 192.168.1.100 F81EDFED863D 20 18 00259C99BF00 64.4.55.157
Configuration / Routed Packets
Hosts APR Routing Passwords VoIP
Lost packets: 0%
Página: 2 de 2 Palabras: 0 Español (México) 150%
Microsoft: <live capture in progress> File: C:... Packets: 6219 Displayed: 6219 Marked: 0
Profile: Default
07:45 p.m.
29/09/2010

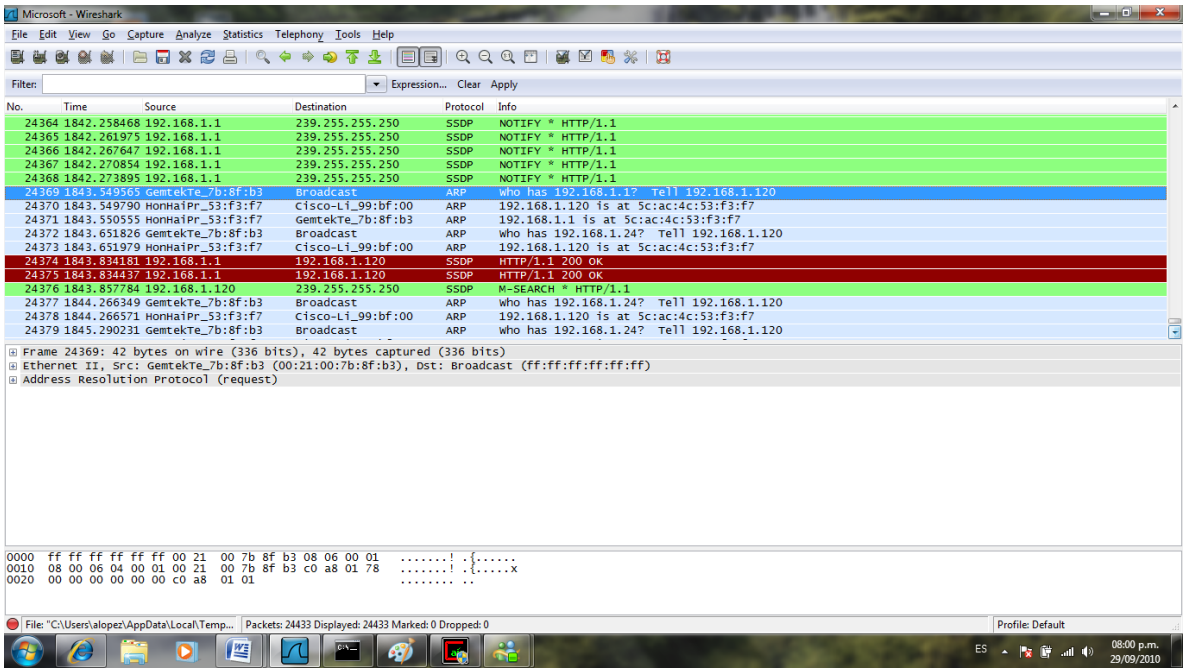

Capturing from Microsoft - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
6279 993.868461 HonHaiPr_53:f3:f7 Cisco-Li_99:bf:00 ARP 192.168.1.120 is at 5c:ac:4c:53:f3:f7
6280 994.180810 192.168.1.120 239.255.255.250 SSDP NOTIFY * HTTP/1.1
6281 994.186009 fe80::785f:6e80:fff5:ff02::c SSDP NOTIFY * HTTP/1.1
6282 994.385315 fe80::785f:6e80:fff5:ff02::c SSDP NOTIFY * HTTP/1.1
6283 994.486111 192.168.1.120 239.255.255.250 SSDP NOTIFY * HTTP/1.1
6284 994.490762 fe80::785f:6e80:fff5:ff02::c SSDP NOTIFY * HTTP/1.1
6285 994.799845 fe80::785f:6e80:fff5:ff02::c SSDP NOTIFY * HTTP/1.1
6286 995.916030 GemtekTe_7b:8f:b3 Broadcast ARP who has 192.168.1.1? Tell 192.168.1.120
6287 995.916245 HonHaiPr_53:f3:f7 Cisco-Li_99:bf:00 ARP 192.168.1.120 is at 5c:ac:4c:53:f3:f7
6288 995.917149 HonHaiPr_53:f3:f7 GemtekTe_7b:8f:b3 ARP 192.168.1.1 is at 5c:ac:4c:53:f3:f7
6289 996.157769 192.168.1.1 192.168.1.120 SSDP HTTP/1.1 200 OK
6290 996.158000 192.168.1.1 192.168.1.120 SSDP HTTP/1.1 200 OK
6291 996.224267 192.168.1.120 239.255.255.250 SSDP M-SEARCH * HTTP/1.1
6292 999.148689 192.168.1.1 192.168.1.120 SSDP HTTP/1.1 200 OK
6293 999.148899 192.168.1.1 192.168.1.120 SSDP HTTP/1.1 200 OK
6294 999.193719 192.168.1.120 239.255.255.250 SSDP M-SEARCH * HTTP/1.1
Frame 5991: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
Ethernet II, Src: HonHaiPr_53:f3:f7 (5c:ac:4c:53:f3:f7), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff 5c ac 4c 53 f3 f7 08 06 00 01 ......\. LS......
0010 08 00 06 04 00 01 5c ac 4c 53 f3 f7 c0 a8 01 66 ......\. LS.....f
0020 00 00 00 00 00 00 c0 a8 01 f0 ....
Frame (frame), 42 bytes
Packets: 6294 Displayed: 6294 Marked: 0
Profile: Default
ES
07:45 p.m.
29/09/2010

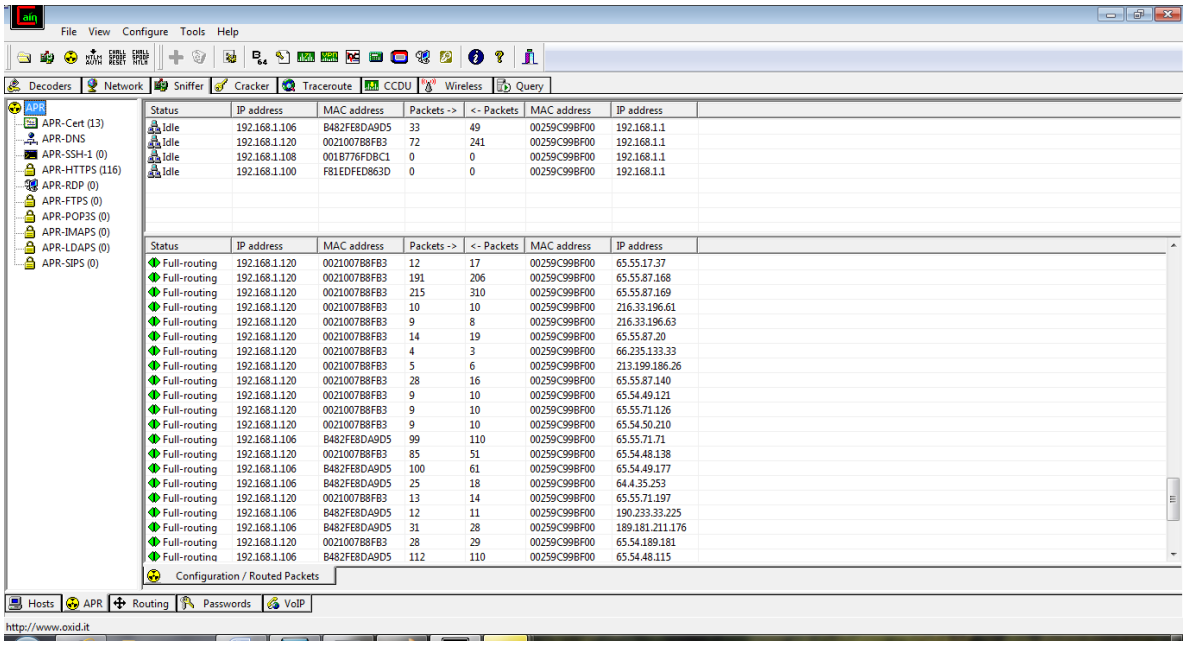

Capturing from Microsoft - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
6352 1017.137150 192.168.1.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
6353 1017.141307 192.168.1.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
6354 1017.146638 192.168.1.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
6355 1017.150120 192.168.1.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
6356 1017.153319 192.168.1.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
6357 1017.156849 192.168.1.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
6358 1017.162379 192.168.1.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
6359 1017.165563 192.168.1.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
6360 1017.168723 192.168.1.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
6361 1018.070302 192.168.1.1 192.168.1.102 SSDP HTTP/1.1 200 OK
6362 1018.316258 HonHaiPr_53:f3:f7 Broadcast ARP who has 192.168.1.240? Tell 192.168.1.102
6363 1019.111481 HonHaiPr_53:f3:f7 Broadcast ARP who has 192.168.1.240? Tell 192.168.1.102
6364 1019.127275 192.168.1.102 239.255.255.250 SSDP M-SEARCH * HTTP/1.1
6365 1019.130698 192.168.1.1 192.168.1.102 SSDP HTTP/1.1 200 OK
6366 1020.109784 HonHaiPr_53:f3:f7 Broadcast ARP who has 192.168.1.240? Tell 192.168.1.102
6367 1022.138035 192.168.1.102 239.255.255.250 SSDP M-SEARCH * HTTP/1.1
Frame 6304: 175 bytes on wire (1400 bits), 175 bytes captured (1400 bits)
Ethernet II, Src: GemtekTe_7b:8f:b3 (00:21:00:7b:8f:b3), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Internet Protocol, Src: 192.168.1.120 (192.168.1.120), Dst: 239.255.255.250 (239.255.255.250)
User Datagram Protocol, Src Port: 57861 (57861), Dst Port: ssdp (1900)
Hypertext Transfer Protocol
0000 01 00 5e 7f ff fa 00 21 00 7b 8f b3 08 00 45 00 ..^....! .{....E.
0010 00 a1 2f 7b 00 00 01 11 d7 b6 c0 a8 01 78 ef ff ../{.... .....x..
0020 ff fa e2 05 07 6c 00 8d bd 5d 4d 2d 53 45 41 52 .....l.. .]M-SEAR
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 CH * HTT P/1.1..H
0040 6f 73 74 3a 32 33 39 2e 32 35 35 2e 32 35 35 2e ost:239. 255.255.
Microsoft: <live capture in progress> File: C:...
Packets: 6367 Displayed: 6367 Marked: 0
Profile: Default
ES
07:45 p.m.
29/09/2010

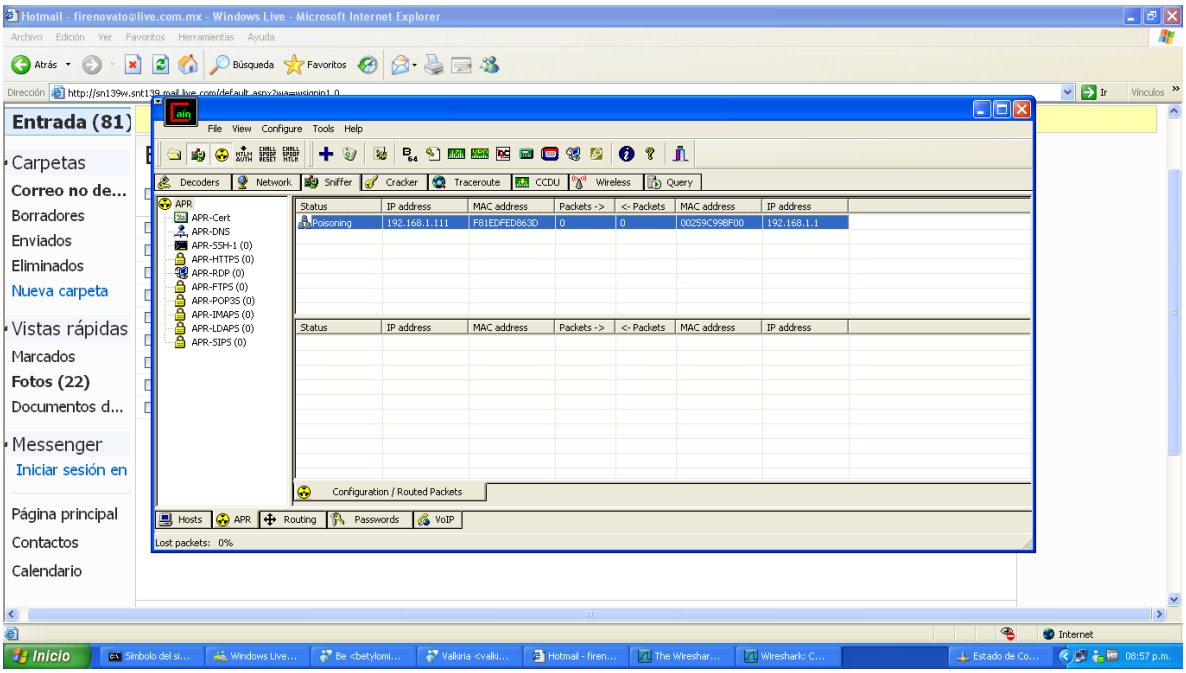

File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
Passwords
FTP (0)
HTTP (59)
IMAP (0)
LDAP (0)
POP3 (0)
SMB (0)
Telnet (0)
VNC (0)
TDS (0)
TNS (0)
SMTP (0)
NNTP (0)
DCE/RPC (0)
MSKerb5-PreAuth (0)
Radius-Keys (0)
Radius-Users (0)
ICQ (0)
IKE-PSK (0)
MySQL (0)
SNMP (0)
SIP (0)
GRE/PPP (0)
PPPoE (0)
Timestamp | HTTP server | Client | Username | Password | URL | UserField | PassField
29/09/2010 - 19:51:17 | 65.54.165.137 | 192.168.1.106 | 4D809220BC66... | A|AOWk-t:a*Zd08Aw._ | https://login.live.com/ppsecure/post.srf?wa=wsignin1.0&rpsn... | uid= | p=
29/09/2010 - 19:51:17 | 65.54.165.137 | 192.168.1.106 | 64855 | MBI | https://login.live.com/ppsecure/post.srf?wa=wsignin1.0&rpsn... | id= | p=
29/09/2010 - 19:51:22 | 201.163.0.144 | 192.168.1.120 | BD89AA188521... | V=1.9 | toolbar.live.com | uid= | ap=
29/09/2010 - 19:51:26 | 65.54.165.137 | 192.168.1.120 | BD89AA188521... | V=1.9 | login.live.com | uid= | ap=
29/09/2010 - 19:51:26 | 65.54.165.137 | 192.168.1.120 | 64855 | MBI | login.live.com | id= | p=
29/09/2010 - 19:51:27 | 65.54.165.137 | 192.168.1.120 | mikemisti@ho... | chivas85 | login.live.com | login= | passwd=
29/09/2010 - 19:51:27 | 65.54.165.137 | 192.168.1.106 | cvaldespin@liv... | mickey3019 | https://login.live.com/ppsecure/post.srf?wa=wsignin1.0&rpsn... | login= | passwd=
29/09/2010 - 19:51:38 | 65.54.165.137 | 192.168.1.106 | 4D809220BC66... | A|AOWk-t:a*Zd08Aw._ | https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=11&ct... | uid= | p=
29/09/2010 - 19:51:38 | 65.54.165.137 | 192.168.1.106 | 64855 | MBI | https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=11&ct... | id= | p=
29/09/2010 - 19:51:39 | 65.54.165.137 | 192.168.1.106 | holaede@live.... | noesmipassword | https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=11&ct... | login= | passwd=
29/09/2010 - 19:51:39 | 72.247.205.186 | 192.168.1.106 | 4D809220BC66... | A|AOWk-t:a*Zd08Aw._ | https://login.live.com/ppsecure/post.srf?wa=wsignin1.0&rpsn... | uid= | p=
29/09/2010 - 19:51:39 | 72.247.205.186 | 192.168.1.106 | 64855 | MBI | https://login.live.com/ppsecure/post.srf?wa=wsignin1.0&rpsn... | id= | p=
29/09/2010 - 19:51:40 | 201.163.0.144 | 192.168.1.120 | BD89AA188521... | V=1.9 | toolbar.live.com | uid= | ap=
29/09/2010 - 19:51:40 | 72.247.205.186 | 192.168.1.106 | 4D809220BC66... | A|AOWk-t:a*Zd08Aw._ | https://login.live.com/ppsecure/post.srf?wa=wsignin1.0&rpsn... | uid= | p=
29/09/2010 - 19:51:40 | 72.247.205.186 | 192.168.1.106 | 64855 | MBI | https://login.live.com/ppsecure/post.srf?wa=wsignin1.0&rpsn... | id= | p=
29/09/2010 - 19:51:40 | 65.54.165.137 | 192.168.1.120 | BD89AA188521... | V=1.9 | https://login.live.com/ppsecure/post.srf?wa=wsignin1.0&rpsn... | uid= | ap=
29/09/2010 - 19:51:40 | 65.54.165.137 | 192.168.1.120 | 64855 | MBI | https://login.live.com/ppsecure/post.srf?wa=wsignin1.0&rpsn... | id= | p=
29/09/2010 - 19:51:42 | 72.247.205.186 | 192.168.1.106 | 4D809220BC66... | A|AOWk-t:a*Zd08Aw._ | https://login.live.com/ppsecure/post.srf?wa=wsignin1.0&rpsn... | uid= | p=
29/09/2010 - 19:51:42 | 72.247.205.186 | 192.168.1.106 | 64855 | MBI | https://login.live.com/ppsecure/post.srf?wa=wsignin1.0&rpsn... | id= | p=
29/09/2010 - 19:51:43 | 72.247.205.186 | 192.168.1.106 | 4D809220BC66... | A|AOWk-t:a*Zd08Aw._ | https://login.live.com/ppsecure/post.srf?wa=wsignin1.0&rpsn... | uid= | p=
29/09/2010 - 19:51:43 | 72.247.205.186 | 192.168.1.106 | 64855 | MBI | https://login.live.com/ppsecure/post.srf?wa=wsignin1.0&rpsn... | id= | p=
29/09/2010 - 19:51:43 | 72.247.205.186 | 192.168.1.106 | 4D809220BC66... | A|AOWk-t:a*Zd08Aw._ | https://login.live.com/ppsecure/post.srf?wa=wsignin1.0&rpsn... | uid= | p=
29/09/2010 - 19:51:43 | 72.247.205.186 | 192.168.1.106 | 64855 | MBI | https://login.live.com/ppsecure/post.srf?wa=wsignin1.0&rpsn... | id= | p=
29/09/2010 - 19:51:43 | 65.54.165.137 | 192.168.1.106 | 4D809220BC66... | A|AOWk-t:a*Zd08Aw._ | https://login.live.com/ppsecure/post.srf?wa=wsignin1.0&rpsn... | uid= | p=
29/09/2010 - 19:51:43 | 65.54.165.137 | 192.168.1.106 | 64855 | MBI | https://login.live.com/ppsecure/post.srf?wa=wsignin1.0&rpsn... | id= | p=
29/09/2010 - 19:51:43 | 72.247.205.186 | 192.168.1.106 | 4D809220BC66... | A|AOWk-t:a*Zd08Aw._ | https://login.live.com/ppsecure/post.srf?wa=wsignin1.0&rpsn... | uid= | p=
29/09/2010 - 19:51:43 | 72.247.205.186 | 192.168.1.106 | 64855 | MBI | https://login.live.com/ppsecure/post.srf?wa=wsignin1.0&rpsn... | id= | p=
29/09/2010 - 19:52:03 | 65.54.165.137 | 192.168.1.106 | 4D809220BC66... | A|AOWk-t:a*Zd08Aw._ | https://login.live.com/ppsecure/post.srf?wa=wsignin1.0&rpsn... | uid= | p=
29/09/2010 - 19:52:03 | 65.54.165.137 | 192.168.1.106 | 64855 | MBI | https://login.live.com/ppsecure/post.srf?wa=wsignin1.0&rpsn... | id= | p=
HTTP
Hosts APR Routing Passwords VoIP
Lost packets: 0%
ES 07:52 p.m. 29/09/2010

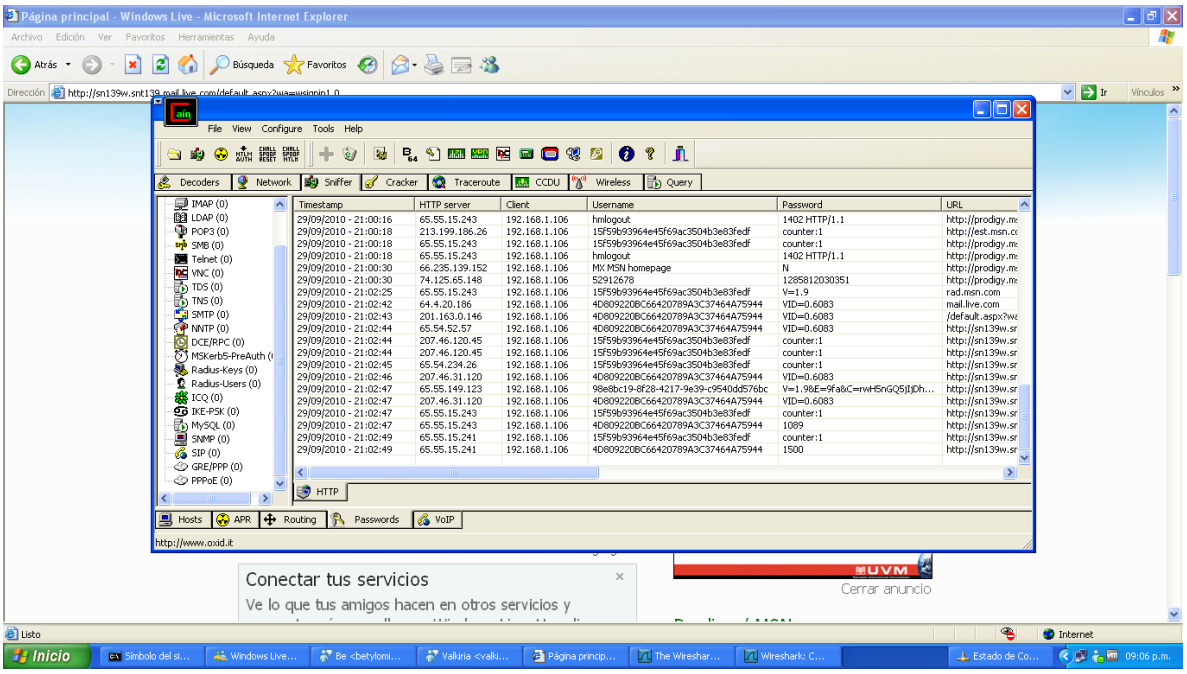

File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
Passwords
FTP (0)
HTTP (59)
IMAP (0)
LDAP (0)
POP3 (0)
SMB (0)
Telnet (0)
VNC (0)
TDS (0)
TNS (0)
SMTP (0)
NNTP (0)
DCE/RPC (0)
MSKerb5-PreAuth (0)
Radius-Keys (0)
Radius-Users (0)
ICQ (0)
IKE-PSK (0)
MySQL (0)
SNMP (0)
SIP (0)
GRE/PPP (0)
PPPoE (0)
Timestamp | HTTP server | Client | Username | Password | URL | UserField | PassField
29/09/2010 - 19:51:43 | 72.247.205.186 | 192.168.1.106 | 64855 | MBI | https://login.live.com/ppsecure/post.srf?wa=wsignin1.0&rpsn... | id= | p=
29/09/2010 - 19:52:03 | 65.54.165.137 | 192.168.1.106 | 4D809220BC66... | A|AOWk-t:a*Zd08Aw._ | https://login.live.com/ppsecure/post.srf?wa=wsignin1.0&rpsn... | uid= | p=
29/09/2010 - 19:52:03 | 65.54.165.137 | 192.168.1.106 | 64855 | MBI | https://login.live.com/ppsecure/post.srf?wa=wsignin1.0&rpsn... | id= | p=
29/09/2010 - 19:52:06 | 65.54.165.137 | 192.168.1.120 | BD89AA188521... | V=1.9 | login.live.com | uid= | ap=
29/09/2010 - 19:52:06 | 65.54.165.137 | 192.168.1.120 | 64855 | MBI | login.live.com | id= | p=
29/09/2010 - 19:52:13 | 65.54.165.137 | 192.168.1.106 | firenovato@liv... | mickey3019 | https://login.live.com/ppsecure/post.srf?wa=wsignin1.0&rpsn... | login= | passwd=
29/09/2010 - 19:52:16 | 65.54.165.137 | 192.168.1.120 | 0.6224 | VID=0.6224 | login.live.com | id= | p=
29/09/2010 - 19:52:16 | 201.163.0.144 | 192.168.1.120 | BD89AA188521... | V=1.9 | toolbar.live.com | uid= | ap=
29/09/2010 - 19:52:17 | 65.55.194.251 | 192.168.1.106 | 15f59b93964e4... | counter:1 | http://sn139w.snt139.mail.live.com/default.aspx?wa=wsignin1.0 | uid= | p=
29/09/2010 - 19:52:17 | 64.4.20.186 | 192.168.1.120 | BD89AA188521... | V=1.9 | mail.live.com | uid= | ap=
29/09/2010 - 19:52:17 | 65.54.191.45 | 192.168.1.106 | 15f59b93964e4... | counter:1 | http://sn139w.snt139.mail.live.com/default.aspx?wa=wsignin1.0 | uid= | p=
29/09/2010 - 19:52:17 | 65.54.191.45 | 192.168.1.106 | 15f59b93964e4... | counter:1 | http://sn139w.snt139.mail.live.com/default.aspx?wa=wsignin1.0 | uid= | p=
29/09/2010 - 19:52:17 | 65.54.191.45 | 192.168.1.106 | 15f59b93964e4... | counter:1 | http://sn139w.snt139.mail.live.com/default.aspx?wa=wsignin1.0 | uid= | p=
29/09/2010 - 19:52:17 | 65.54.234.77 | 192.168.1.106 | 15f59b93964e4... | counter:1 | http://sn139w.snt139.mail.live.com/default.aspx?wa=wsignin1.0 | uid= | p=
29/09/2010 - 19:52:17 | 65.54.191.45 | 192.168.1.106 | 15f59b93964e4... | counter:1 | http://sn139w.snt139.mail.live.com/default.aspx?wa=wsignin1.0 | uid= | p=
29/09/2010 - 19:52:18 | 201.163.0.138 | 192.168.1.120 | BD89AA188521... | V=1.9 | /default.aspx?wa=wsignin1.0 HTTP/1.1 | uid= | ap=
29/09/2010 - 19:52:19 | 201.163.0.144 | 192.168.1.120 | BD89AA188521... | V=1.9 | toolbar.live.com | uid= | ap=
29/09/2010 - 19:52:19 | 65.55.15.243 | 192.168.1.106 | 15f59b93964e4... | counter:1 | http://sn139w.snt139.mail.live.com/default.aspx?wa=wsignin1.0 | uid= | p=
29/09/2010 - 19:52:19 | 65.55.15.243 | 192.168.1.106 | 4D809220BC66... | 1089 | http://sn139w.snt139.mail.live.com/default.aspx?wa=wsignin1.0 | uid= | ap=
29/09/2010 - 19:52:19 | 65.55.64.249 | 192.168.1.120 | BD89AA188521... | V=1.9 | http://bl142w.blu142.mail.live.com/default.aspx?wa=wsignin1.0 | uid= | ap=
29/09/2010 - 19:52:19 | 65.54.234.77 | 192.168.1.120 | 1cad9b0295b4... | V=1.9 | http://bl142w.blu142.mail.live.com/default.aspx?wa=wsignin1.0 | uid= | ap=
29/09/2010 - 19:52:20 | 65.55.149.124 | 192.168.1.120 | BD89AA188521... | V=1.9 | http://bl142w.blu142.mail.live.com/default.aspx?wa=wsignin1.0 | uid= | ap=
29/09/2010 - 19:52:21 | 65.55.15.122 | 192.168.1.120 | 1cad9b0295b4... | V=1.9 | http://bl142w.blu142.mail.live.com/default.aspx?wa=wsignin1.0 | uid= | ap=
29/09/2010 - 19:52:21 | 65.55.15.122 | 192.168.1.120 | BD89AA188521... | 1089 | http://bl142w.blu142.mail.live.com/default.aspx?wa=wsignin1.0 | uid= | ap=
29/09/2010 - 19:52:21 | 65.55.15.122 | 192.168.1.120 | 1cad9b0295b4... | V=1.9 | http://bl142w.blu142.mail.live.com/default.aspx?wa=wsignin1.0 | uid= | ap=
29/09/2010 - 19:52:21 | 65.55.15.122 | 192.168.1.120 | BD89AA188521... | 1089 | http://bl142w.blu142.mail.live.com/default.aspx?wa=wsignin1.0 | uid= | ap=
29/09/2010 - 19:52:21 | 65.55.15.125 | 192.168.1.106 | 15f59b93964e4... | counter:1 | http://sn139w.snt139.mail.live.com/default.aspx?wa=wsignin1.0 | uid= | p=
29/09/2010 - 19:52:21 | 65.55.15.125 | 192.168.1.106 | 4D809220BC66... | 1500 | http://sn139w.snt139.mail.live.com/default.aspx?wa=wsignin1.0 | uid= | ap=
29/09/2010 - 19:52:22 | 201.163.0.145 | 192.168.1.106 | 4D809220BC66... | V=1.9 | http://view.atdmt.com/D4I/iview/msnnkmxc001300x250Xwlm... | uid= | ap=
29/09/2010 - 19:52:23 | 65.55.15.122 | 192.168.1.120 | 1cad9b0295b4... | V=1.9 | http://bl142w.blu142.mail.live.com/default.aspx?wa=wsignin1.0 | uid= | ap=
29/09/2010 - 19:52:23 | 65.55.15.122 | 192.168.1.120 | BD89AA188521... | 1500 | http://bl142w.blu142.mail.live.com/default.aspx?wa=wsignin1.0 | uid= | ap=
HTTP
Hosts APR Routing Passwords VoIP
Lost packets: 0%
ES 07:52 p.m. 29/09/2010

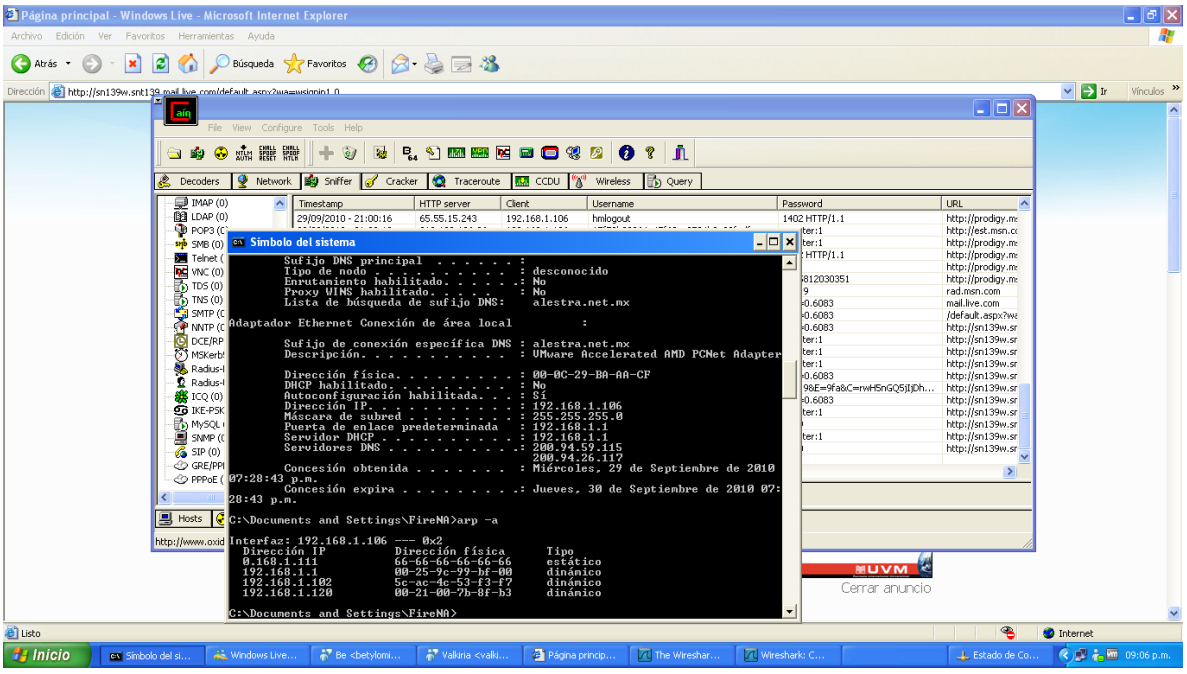

File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
Passwords
FTP (0)
HTTP (59)
IMAP (0)
LDAP (0)
POP3 (0)
SMB (0)
Telnet (0)
VNC (0)
TDS (0)
TNS (0)
SMTP (0)
NNTP (0)
DCE/RPC (0)
MSKerb5-PreAuth (0)
Radius-Keys (0)
Radius-Users (0)
ICQ (0)
IKE-PSK (0)
MySQL (0)
SNMP (0)
SIP (0)
GRE/PPP (0)
PPPoE (0)
Timestamp HTTP server Client Username Password URL UserField PassField
HTTP
Hosts APR Routing Passwords VoIP
Lost packets: 0%
ES 07:53 p.m. 29/09/2010


Microsoft - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
24364 1842.258468 192.168.1.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
24365 1842.261975 192.168.1.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
24366 1842.267647 192.168.1.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
24367 1842.270854 192.168.1.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
24368 1842.273895 192.168.1.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
24369 1843.549565 GemtekTe_7b:8f:b3 Broadcast ARP Who has 192.168.1.1? Tell 192.168.1.120
24370 1843.549790 HonHaiPr_53:f3:f7 Cisco-Li_99:bf:00 ARP 192.168.1.120 is at 5c:ac:4c:53:f3:f7
24371 1843.550555 HonHaiPr_53:f3:f7 GemtekTe_7b:8f:b3 ARP 192.168.1.1 is at 5c:ac:4c:53:f3:f7
24372 1843.651826 GemtekTe_7b:8f:b3 Broadcast ARP who has 192.168.1.24? Tell 192.168.1.120
24373 1843.651979 HonHaiPr_53:f3:f7 Cisco-Li_99:bf:00 ARP 192.168.1.120 is at 5c:ac:4c:53:f3:f7
24374 1843.834181 192.168.1.1 192.168.1.120 SSDP HTTP/1.1 200 OK
24375 1843.834437 192.168.1.1 192.168.1.120 SSDP HTTP/1.1 200 OK
24376 1843.857784 192.168.1.120 239.255.255.250 SSDP M-SEARCH * HTTP/1.1
24377 1844.266349 GemtekTe_7b:8f:b3 Broadcast ARP Who has 192.168.1.24? Tell 192.168.1.120
24378 1844.266571 HonHaiPr_53:f3:f7 Cisco-Li_99:bf:00 ARP 192.168.1.120 is at 5c:ac:4c:53:f3:f7
24379 1845.290231 GemtekTe_7b:8f:b3 Broadcast ARP Who has 192.168.1.24? Tell 192.168.1.120
Frame 24369: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
Ethernet II, Src: GemtekTe_7b:8f:b3 (00:21:00:7b:8f:b3), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff 00 21 00 7b 8f b3 08 06 00 01 ....! .{......
0010 08 00 06 04 00 01 00 21 00 7b 8f b3 c0 a8 01 78 ....! .{.....x
0020 00 00 00 00 00 00 c0 a8 01 01 ....
File: "C:\Users\alopez\AppData\Local\Temp... Packets: 24433 Displayed: 24433 Marked: 0 Dropped: 0
Profile: Default
ES 08:00 p.m. 29/09/2010

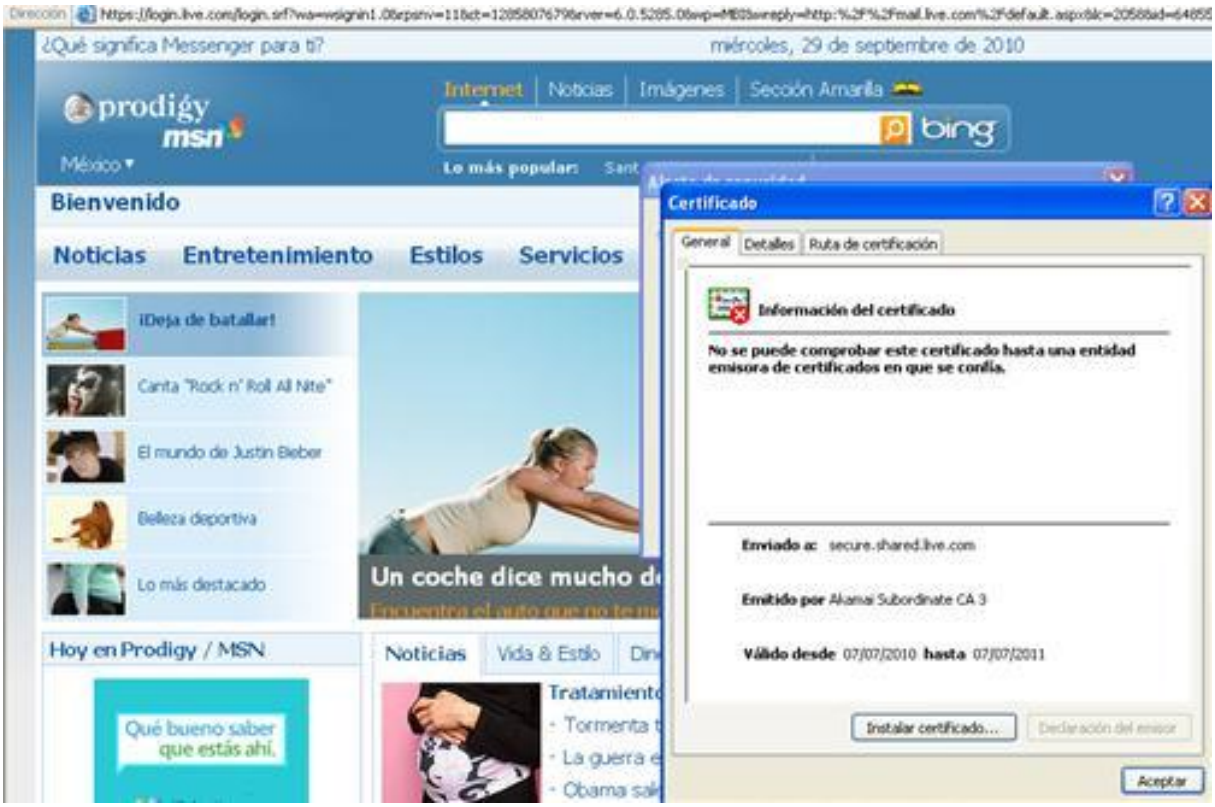

File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
APR
APR-Cert (13)
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (116)
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
Status IP address MAC address Packets -> <- Packets MAC address IP address
Idle 192.168.1.106 B482FE8DA9D5 33 49 00259C99BF00 192.168.1.1
Idle 192.168.1.120 0021007B8FB3 72 241 00259C99BF00 192.168.1.1
Idle 192.168.1.108 001B776FDBC1 0 0 00259C99BF00 192.168.1.1
Idle 192.168.1.100 F81EDFED863D 0 0 00259C99BF00 192.168.1.1
Status IP address MAC address Packets -> <- Packets MAC address IP address
Full-routing 192.168.1.120 0021007B8FB3 12 17 00259C99BF00 65.55.17.37
Full-routing 192.168.1.120 0021007B8FB3 191 206 00259C99BF00 65.55.87.168
Full-routing 192.168.1.120 0021007B8FB3 215 310 00259C99BF00 65.55.87.169
Full-routing 192.168.1.120 0021007B8FB3 10 10 00259C99BF00 216.33.196.61
Full-routing 192.168.1.120 0021007B8FB3 9 8 00259C99BF00 216.33.196.63
Full-routing 192.168.1.120 0021007B8FB3 14 19 00259C99BF00 65.55.87.20
Full-routing 192.168.1.120 0021007B8FB3 4 3 00259C99BF00 66.235.133.33
Full-routing 192.168.1.120 0021007B8FB3 5 6 00259C99BF00 213.199.186.26
Full-routing 192.168.1.120 0021007B8FB3 28 16 00259C99BF00 65.55.87.140
Full-routing 192.168.1.120 0021007B8FB3 9 10 00259C99BF00 65.54.49.121
Full-routing 192.168.1.120 0021007B8FB3 9 10 00259C99BF00 65.55.71.126
Full-routing 192.168.1.120 0021007B8FB3 9 10 00259C99BF00 65.54.50.210
Full-routing 192.168.1.106 B482FE8DA9D5 99 110 00259C99BF00 65.55.71.71
Full-routing 192.168.1.120 0021007B8FB3 85 51 00259C99BF00 65.54.48.138
Full-routing 192.168.1.106 B482FE8DA9D5 100 61 00259C99BF00 65.54.49.177
Full-routing 192.168.1.106 B482FE8DA9D5 25 18 00259C99BF00 64.4.35.253
Full-routing 192.168.1.120 0021007B8FB3 13 14 00259C99BF00 65.55.71.197
Full-routing 192.168.1.106 B482FE8DA9D5 12 11 00259C99BF00 190.233.33.225
Full-routing 192.168.1.106 B482FE8DA9D5 31 28 00259C99BF00 189.181.211.176
Full-routing 192.168.1.120 0021007B8FB3 28 29 00259C99BF00 65.54.189.181
Full-routing 192.168.1.106 B482FE8DA9D5 112 110 00259C99BF00 65.54.48.115
Configuration / Routed Packets
Hosts APR Routing Passwords VoIP
http://www.oxid.it

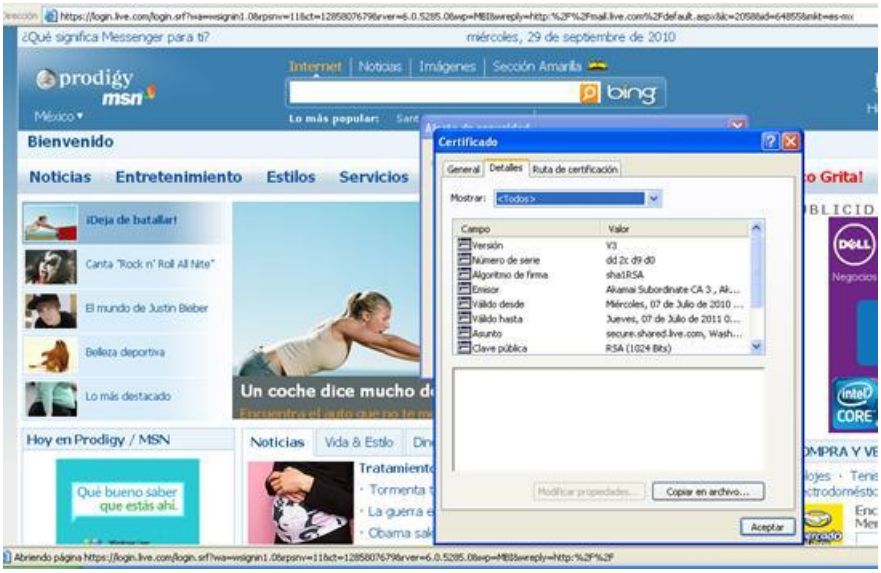

Hotmail - firenovato@live.com.mx - Windows Live - Microsoft Internet Explorer
Entrada (81)
Carpetas
Correo no de...
Borradores
Enviados
Eliminados
Nueva carpeta
Vistas rápidas
Marcados
Fotos (22)
Documentos d...
Messenger
Iniciar sesión en
Página principal
Contactos
Calendario
File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
Poisoning 192.168.1.111 F81EDFED863D 0 0 00259C99BF00 192.168.1.1
Configuration / Routed Packets
Hosts APR Routing Passwords VoIP
Lost packets: 0%
Inicio
08:57 p.m.

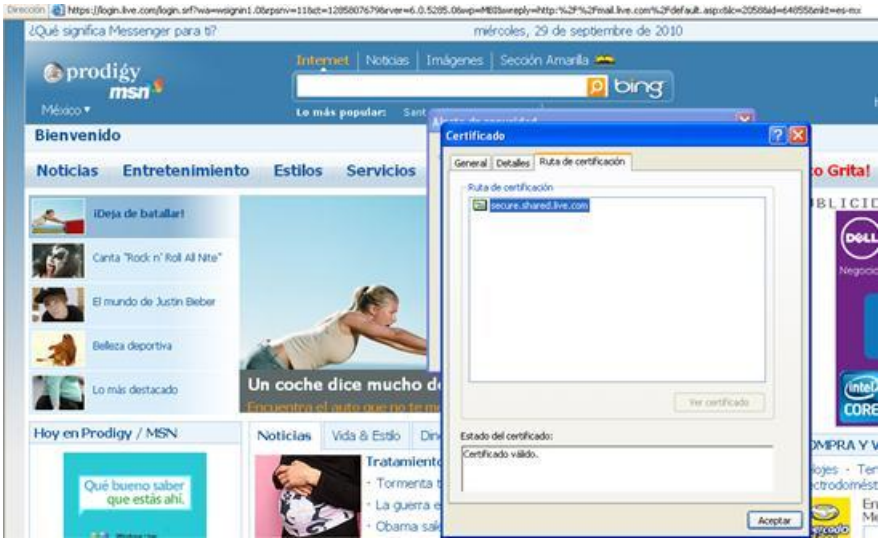

Página principal - Windows Live - Microsoft Internet Explorer
File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
Timestamp HTTP server Client Username Password URL
Hosts APR Routing Passwords VoIP
http://www.oxid.it
Conectar tus servicios
Ve lo que tus amigos hacen en otros servicios y
Cerrar anuncio
Listo
Internet
Inicio
09:06 p.m.

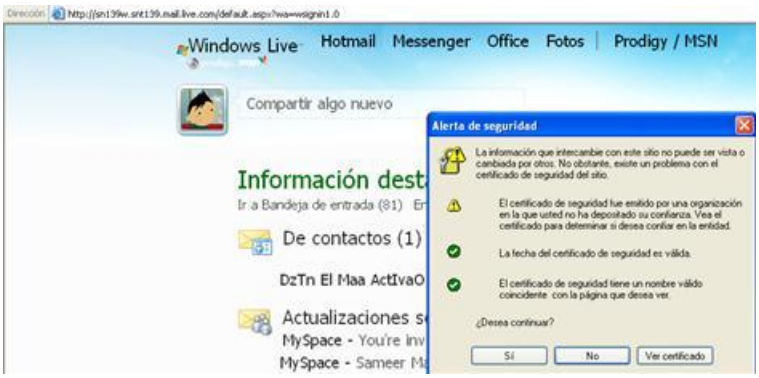

Página principal - Windows Live - Microsoft Internet Explorer
Símbolo del sistema
Sufijo DNS principal . . . . . :
Tipo de nodo . . . . . : desconocido
Enrutamiento habilitado. . . . . : No
Proxy WINS habilitado. . . . . : No
Lista de búsqueda de sufijo DNS: alestra.net.mx
Adaptador Ethernet Conexión de área local :
Sufijo de conexión específica DNS : alestra.net.mx
Descripción. . . . . : VMware Accelerated AMD PCNet Adapter
Dirección física. . . . . : 00-0C-29-BA-AA-CF
DHCP habilitado. . . . . : No
Autoconfiguración habilitada. . . : Sí
Dirección IP. . . . . : 192.168.1.106
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada : 192.168.1.1
Servidor DHCP . . . . . : 192.168.1.1
Servidores DNS . . . . . : 200.94.59.115
200.94.26.117
Concesión obtenida . . . . . : Miércoles, 29 de Septiembre de 2010 07:28:43 p.m.
Concesión expira . . . . . : Jueves, 30 de Septiembre de 2010 07:28:43 p.m.
C:\Documents and Settings\FireNA>arp -a
Interfaz: 192.168.1.106 --- 0x2
Dirección IP Dirección física Tipo
0.168.1.111 66-66-66-66-66-66 estático
192.168.1.1 00-25-9c-99-bf-00 dinámico
192.168.1.102 5c-ac-4c-53-f3-f7 dinámico
192.168.1.120 00-21-00-7b-8f-b3 dinámico
C:\Documents and Settings\FireNA>
Cerrar anuncio
Listo
Internet
Inicio
09:06 p.m.

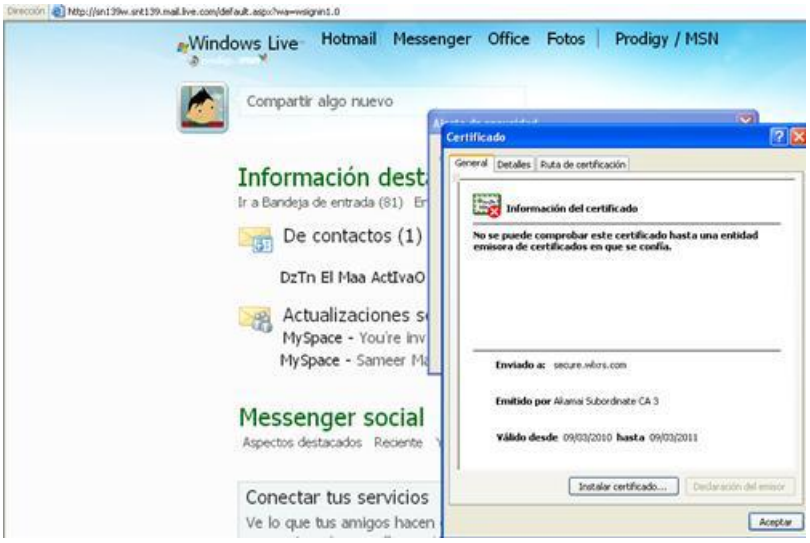

Dirección http://prodigy.msn.com/?rd=1
¿Qué significa Messenger para ti?
miércoles, 29 de septiembre de 2010
prodigy msn
México
Internet | Noticias | Imágenes | Sección Amarilla
bing
Lo más popular:
Bienvenido
Noticias Entretenimiento Estilos Servicios
¡Deja de batallar!
Canta "Rock n' Roll All Nite"
El mundo de Justin Bieber
Belleza deportiva
Alerta de seguridad
La información que intercambie con este sitio no puede ser vista o cambiada por otros. No obstante, existe un problema con el certificado de seguridad del sitio.
El certificado de seguridad fue emitido por una organización en la que usted no ha depositado su confianza. Vea el certificado para determinar si desea confiar en la entidad.
La fecha del certificado de seguridad es válida.
El certificado de seguridad tiene un nombre válido coincidente con la página que desea ver.
¿Desea continuar?
Sí
No
Ver certificado

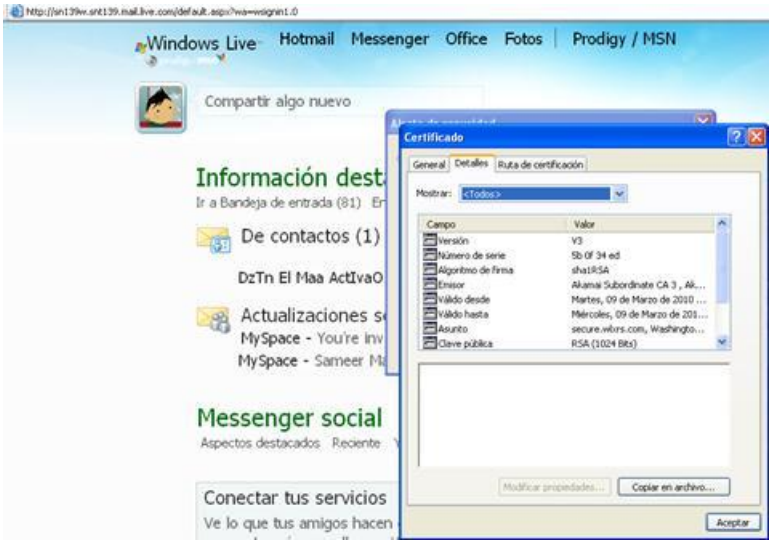

Dirección https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=11&ct=1285807679&rver=6.0.5285.0&wp=MBI&wreply=http:%2F%2Fmail.live.com%2Fdefault.aspx&lc=2058&id=64855
¿Qué significa Messenger para ti?
miércoles, 29 de septiembre de 2010
prodigy msn
México
Internet | Noticias | Imágenes | Sección Amarilla
bing
Lo más popular:
Bienvenido
Noticias Entretenimiento Estilos Servicios
¡Deja de batallar!
Canta "Rock n' Roll All Nite"
El mundo de Justin Bieber
Belleza deportiva
Lo más destacado
Un coche dice mucho d
Hoy en Prodigy / MSN
Noticias Vida & Estilo
Qué bueno saber que estás ahí.
Certificado
General Detalles Ruta de certificación
Información del certificado
No se puede comprobar este certificado hasta una entidad emisora de certificados en que se confía.
Enviado a: secure.shared.live.com
Emitido por: Akamai Subordinate CA 3
Válido desde 07/07/2010 hasta 07/07/2011
Instalar certificado...
Aceptar

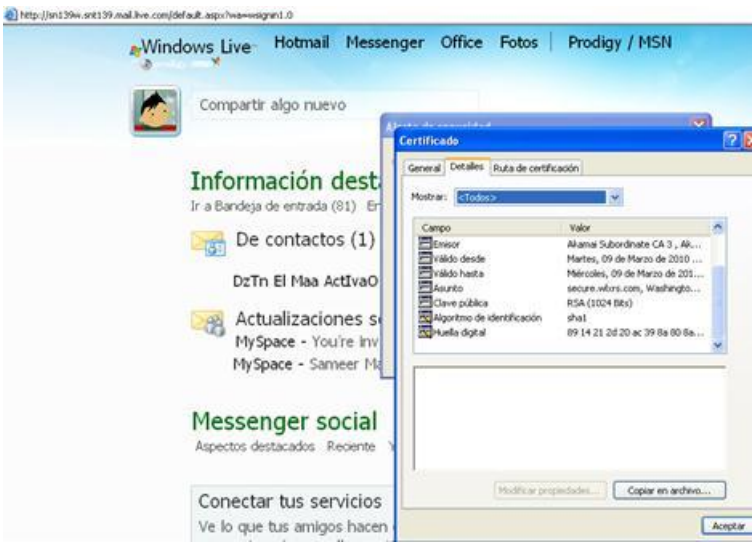

¿Qué significa Messenger para ti?
miércoles, 29 de septiembre de 2010
prodigy msn
México
Internet | Noticias | Imágenes | Sección Amarilla
bing
Lo más popular:
Bienvenido
Noticias Entretenimiento Estilos Servicios
¡Deja de batallar!
Canta "Rock n' Roll All Nite"
El mundo de Justin Bieber
Belleza deportiva
Lo más destacado
Un coche dice mucho d
Hoy en Prodigy / MSN
Noticias Vida & Estilo
Qué bueno saber que estás ahí.
Certificado
General Detalles Ruta de certificación
Mostrar: <Todos>
Campo Valor
Versión V3
Número de serie dd 2c d9 d0
Algoritmo de firma sha1RSA
Emisor Akamai Subordinate CA 3 , Ak...
Válido desde Miércoles, 07 de Julio de 2010 ...
Válido hasta Jueves, 07 de Julio de 2011 0...
Asunto secure.shared.live.com, Wash...
Clave pública RSA (1024 Bits)
Modificar propiedades...
Copiar en archivo...
Aceptar
Abriendo página https://login.live.com/login.srf?wa=wsignin1.0&rpsnv=11&ct=1285807679&rver=6.0.5285.0&wp=MBI&wreply=http:%2F%2F

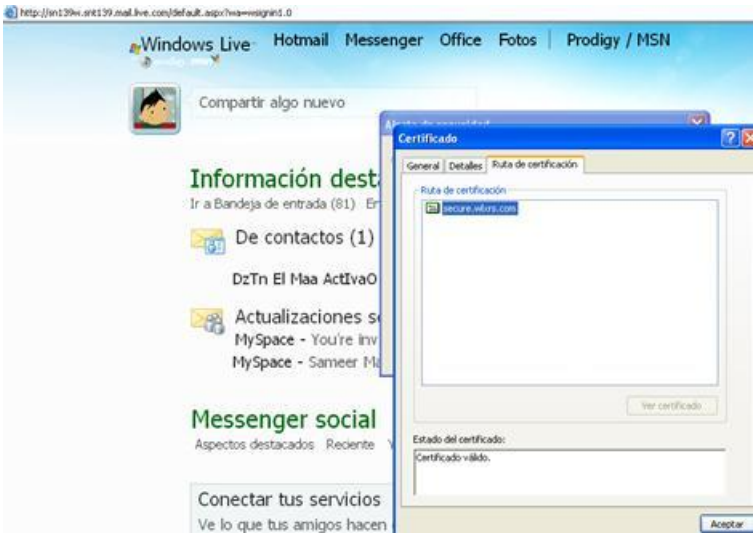

¿Qué significa Messenger para ti?
miércoles, 29 de septiembre de 2010
prodigy msn
México
Internet | Noticias | Imágenes | Sección Amarilla
bing
Lo más popular:
Bienvenido
Noticias Entretenimiento Estilos Servicios
¡Deja de batallar!
Canta "Rock n' Roll All Nite"
El mundo de Justin Bieber
Belleza deportiva
Lo más destacado
Un coche dice mucho d
Hoy en Prodigy / MSN
Noticias Vida & Estilo
Qué bueno saber que estás ahí.
Certificado
General Detalles Ruta de certificación
Ruta de certificación
secure.shared.live.com
Ver certificado
Estado del certificado:
Certificado válido.
Aceptar

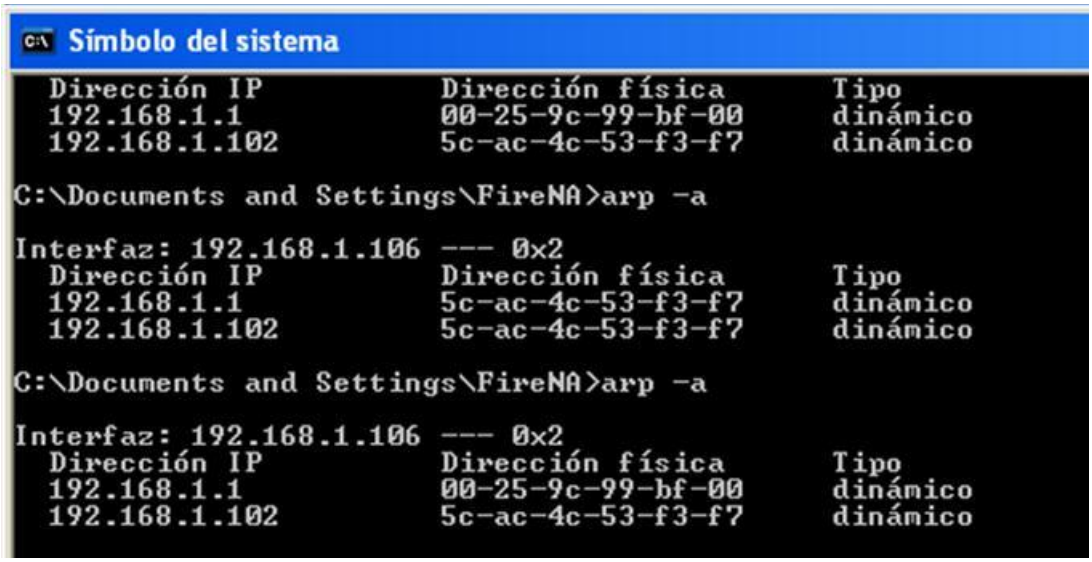

Windows Live
Hotmail Messenger Office Fotos | Prodigy / MSN
Compartir algo nuevo
Información dest
Ir a Bandeja de entrada (81)
De contactos (1)
DzTn El Maa ActIvaO
Actualizaciones s
MySpace - You're inv
MySpace - Sameer M
Alerta de seguridad
La información que intercambie con este sitio no puede ser vista o cambiada por otros. No obstante, existe un problema con el certificado de seguridad del sitio.
El certificado de seguridad fue emitido por una organización en la que usted no ha depositado su confianza. Vea el certificado para determinar si desea confiar en la entidad.
La fecha del certificado de seguridad es válida.
El certificado de seguridad tiene un nombre válido coincidente con la página que desea ver.
¿Desea continuar?
Sí
No
Ver certificado

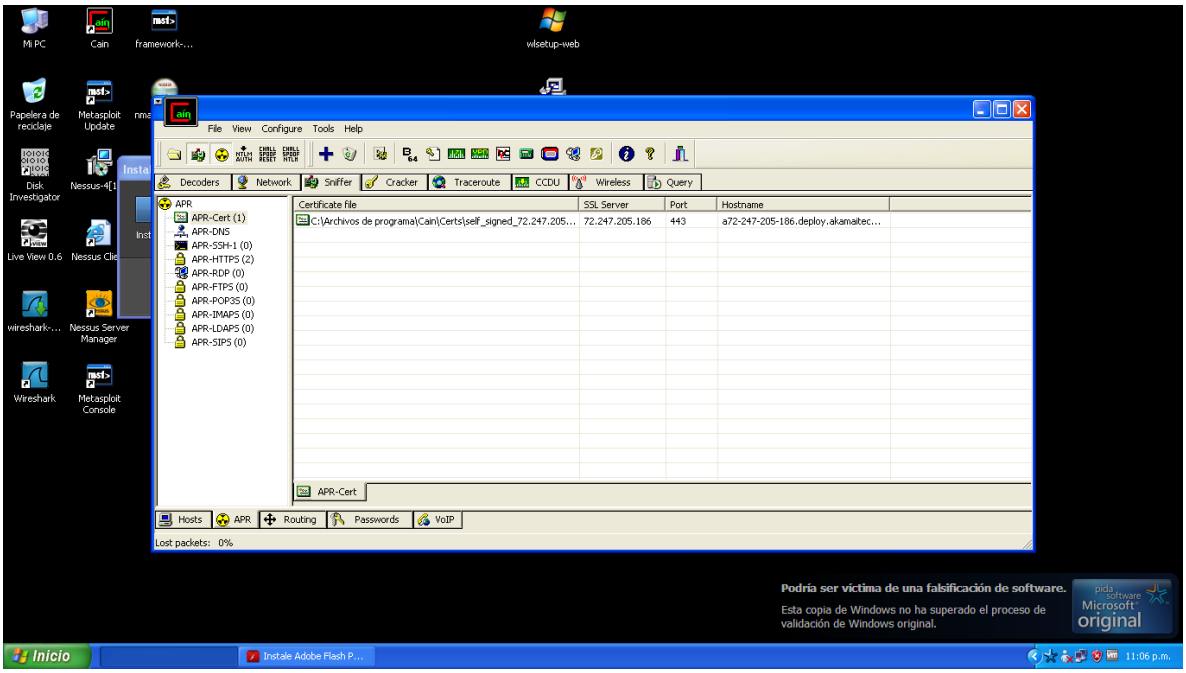

Windows Live
Hotmail
Messenger
Office
Fotos
Prodigy / MSN
Compartir algo nuevo
Información dest
Ir a Bandeja de entrada (81)
De contactos (1)
DzTn El Maa ActIvaO
Actualizaciones s
MySpace - You're inv
MySpace - Sameer M
Messenger social
Aspectos destacados
Conectar tus servicios
Ve lo que tus amigos hacen
Certificado
General
Detalles
Ruta de certificación
Información del certificado
No se puede comprobar este certificado hasta una entidad emisora de certificados en que se confía.
Enviado a: secure.wlxrs.com
Emitido por Akamai Subordinate CA 3
Válido desde 09/03/2010 hasta 09/03/2011
Instalar certificado...
Aceptar

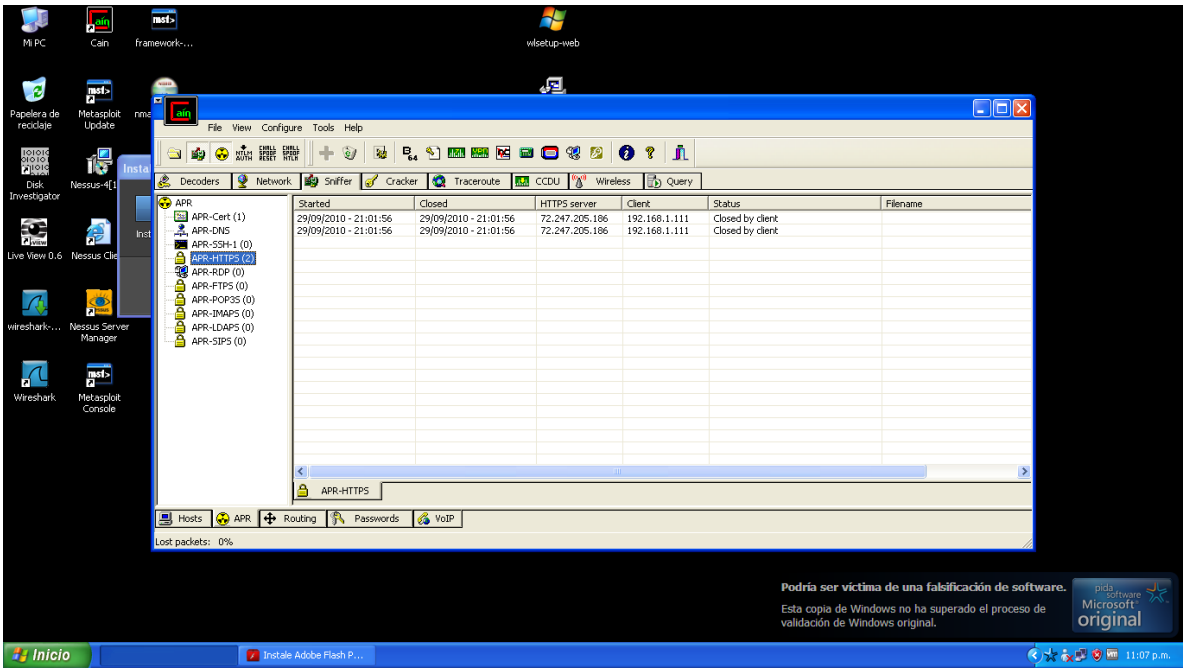

Windows Live
Hotmail
Messenger
Office
Fotos
Prodigy / MSN
Compartir algo nuevo
Información dest
Ir a Bandeja de entrada (81)
De contactos (1)
DzTn El Maa ActIvaO
Actualizaciones s
MySpace - You're inv
MySpace - Sameer M
Messenger social
Aspectos destacados
Conectar tus servicios
Ve lo que tus amigos hacen
Certificado
General
Detalles
Ruta de certificación
Mostrar: <Todos>
Campo
Valor
Versión
V3
Número de serie
Algoritmo de firma
sha1RSA
Emisor
Válido desde
Válido hasta
Asunto
Clave pública
RSA (1024 Bits)
Modificar propiedades...
Copiar en archivo...
Aceptar

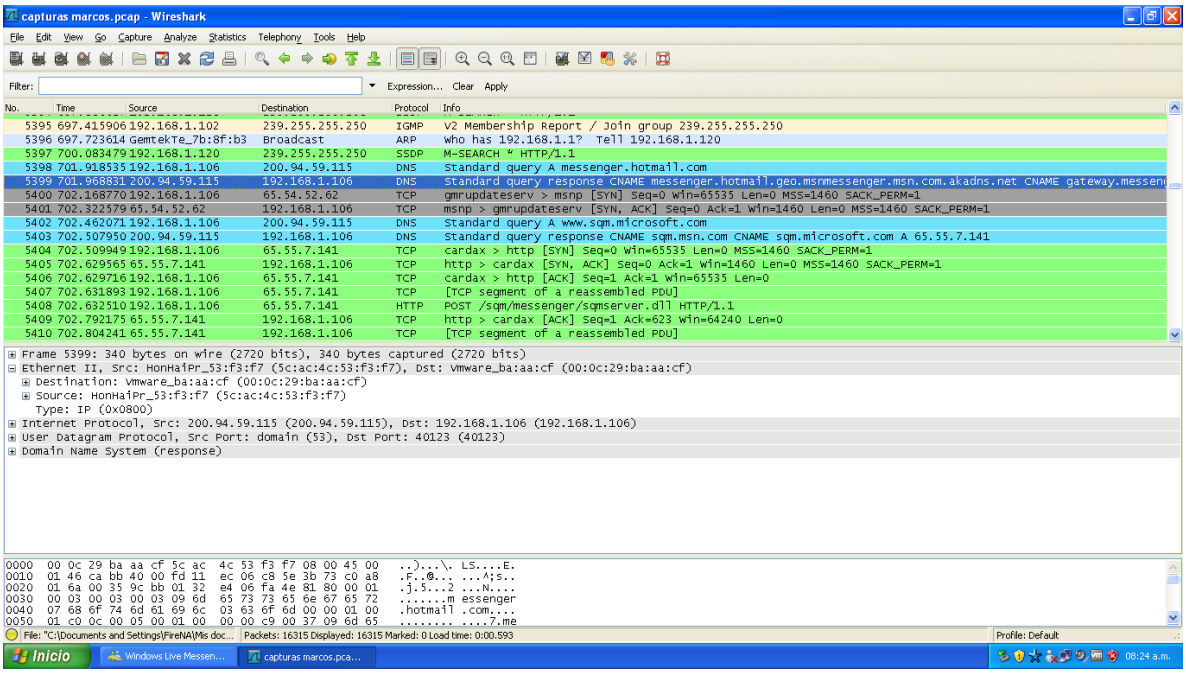

Windows Live
Hotmail
Messenger
Office
Fotos
Prodigy / MSN
Compartir algo nuevo
Información dest
Ir a Bandeja de entrada (81)
De contactos (1)
DzTn El Maa ActIvaO
Actualizaciones s
MySpace - You're inv
MySpace - Sameer M
Messenger social
Aspectos destacados
Conectar tus servicios
Ve lo que tus amigos hacen
Certificado
General
Detalles
Ruta de certificación
Mostrar: <Todos>
Campo
Valor
Emisor
Válido desde
Válido hasta
Asunto
Clave pública
RSA (1024 Bits)
Algoritmo de identificación
sha1
Huella digital
Modificar propiedades...
Copiar en archivo...
Aceptar

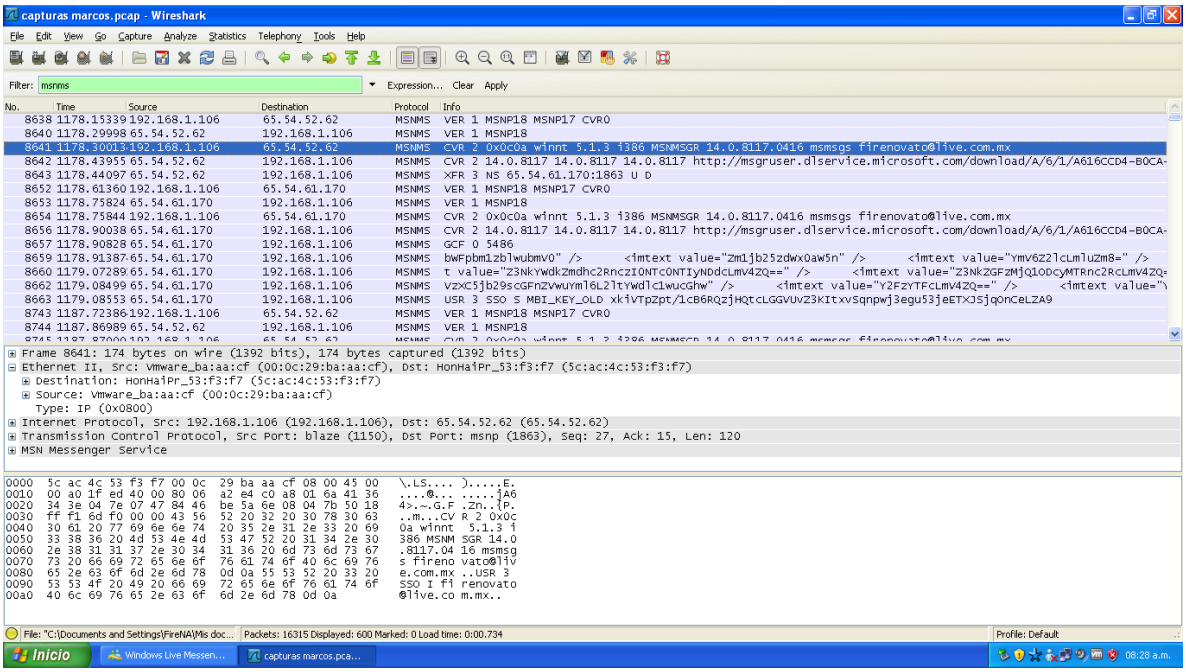

Windows Live
Hotmail
Messenger
Office
Fotos
Prodigy / MSN
Compartir algo nuevo
Información dest
Ir a Bandeja de entrada (81)
De contactos (1)
DzTn El Maa ActIvaO
Actualizaciones s
MySpace - You're inv
MySpace - Sameer M
Messenger social
Aspectos destacados
Reciente
Conectar tus servicios
Ve lo que tus amigos hacen
Certificado
General
Detalles
Ruta de certificación
Ruta de certificación
secure.wlxrs.com
Ver certificado
Estado del certificado:
Certificado válido.
Aceptar

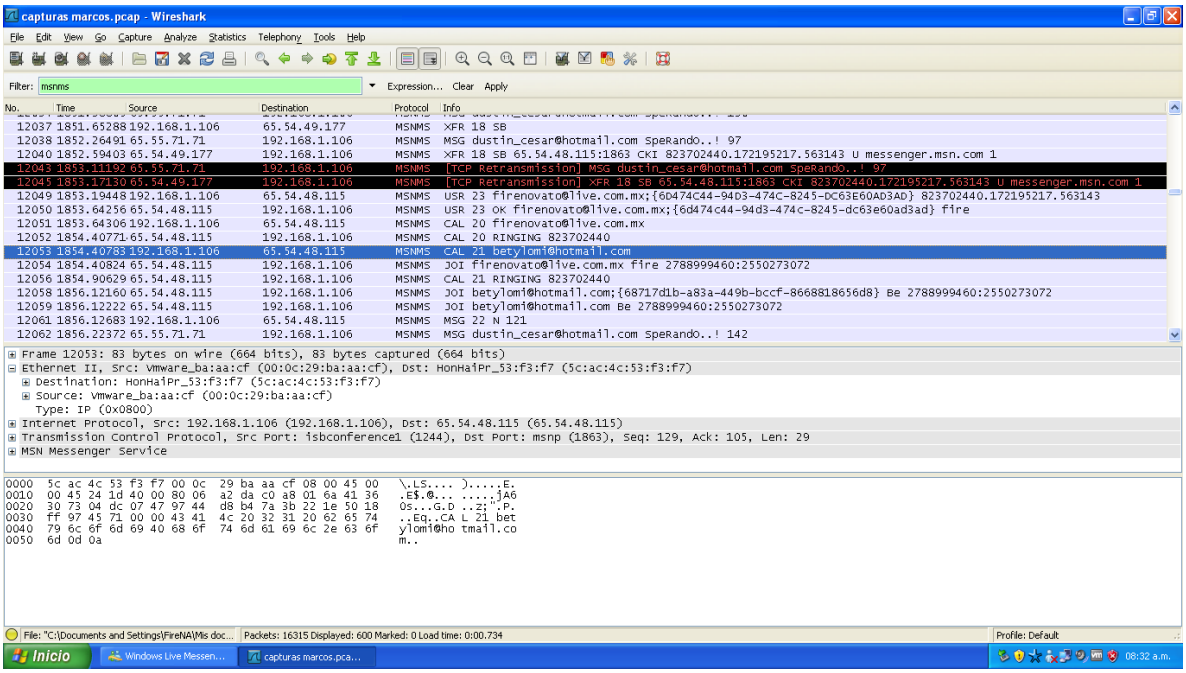

Símbolo del sistema
Dirección IP Dirección física Tipo
192.168.1.1 00-25-9c-99-bf-00 dinámico
192.168.1.102 5c-ac-4c-53-f3-f7 dinámico
C:\Documents and Settings\FireNA>arp -a
Interfaz: 192.168.1.106 --- 0x2
Dirección IP Dirección física Tipo
192.168.1.1 5c-ac-4c-53-f3-f7 dinámico
192.168.1.102 5c-ac-4c-53-f3-f7 dinámico
C:\Documents and Settings\FireNA>arp -a
Interfaz: 192.168.1.106 --- 0x2
Dirección IP Dirección física Tipo
192.168.1.1 00-25-9c-99-bf-00 dinámico
192.168.1.102 5c-ac-4c-53-f3-f7 dinámico

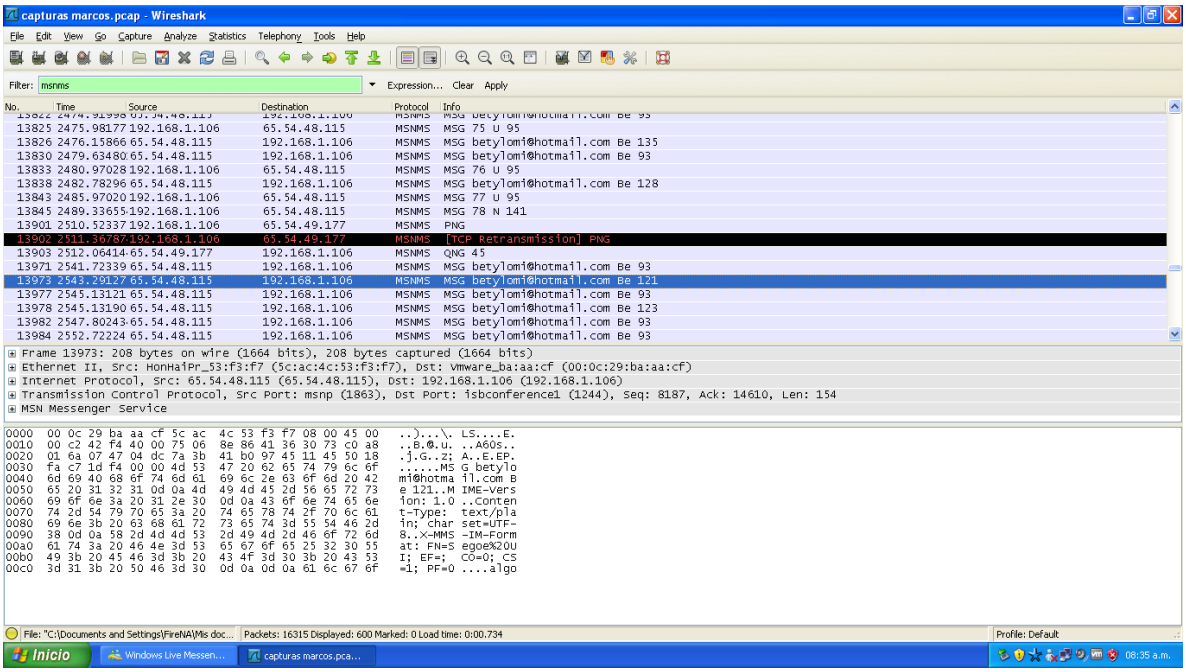

Mi PC
Cain
framework-...
wlsetup-web
Papelera de reciclaje
Metasploit Update
Disk Investigator
Live View 0.6
wireshark-...
Nessus Server Manager
Wireshark
Metasploit Console
File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
APR
APR-Cert (1)
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (2)
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
Certificate file
SSL Server
Port
Hostname
C:\Archivos de programa\Cain\Certs\self_signed_72.247.205...
72.247.205.186
443
a72-247-205-186.deploy.akamaitec...
APR-Cert
Hosts APR Routing Passwords VoIP
Lost packets: 0%
Podría ser víctima de una falsificación de software.
Esta copia de Windows no ha superado el proceso de validación de Windows original.
Inicio
Instale Adobe Flash P...
11:06 p.m.

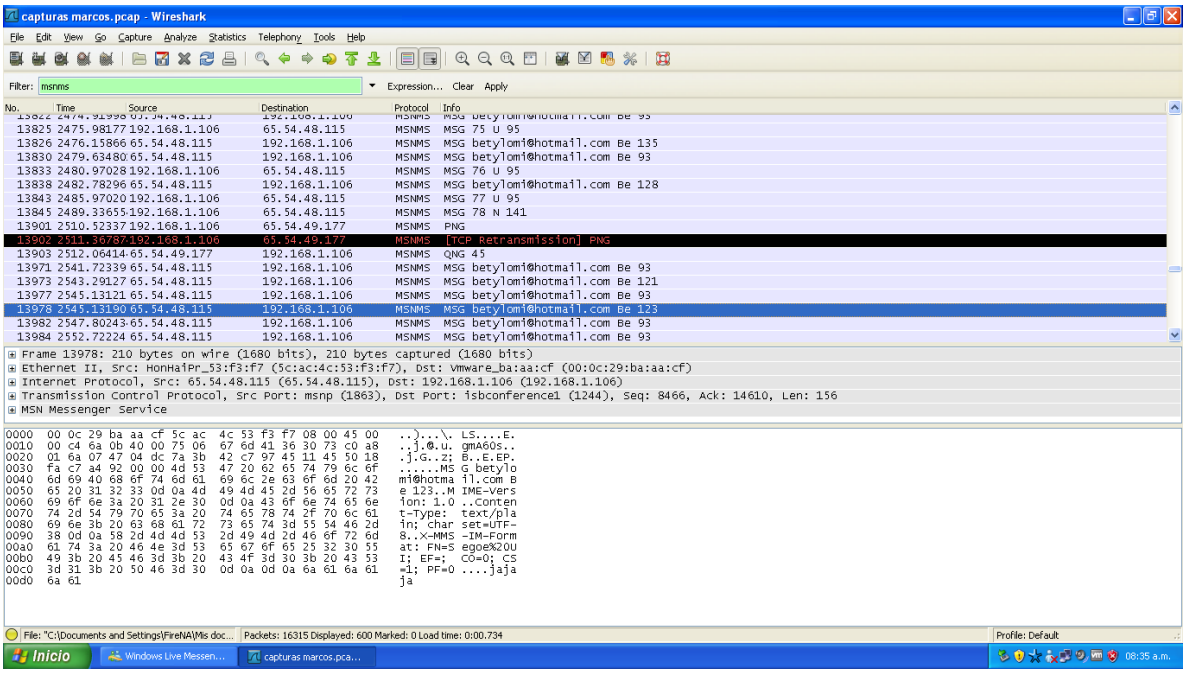

Mi PC
Cain
framework-...
wlsetup-web
Papelera de reciclaje
Metasploit Update
Disk Investigator
Live View 0.6
wireshark-...
Nessus Server Manager
Wireshark
Metasploit Console
File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
APR
APR-Cert (1)
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (2)
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
Started
Closed
HTTPS server
Client
Status
Filename
29/09/2010 - 21:01:56
29/09/2010 - 21:01:56
72.247.205.186
192.168.1.111
Closed by client
APR-HTTPS
Hosts APR Routing Passwords VoIP
Lost packets: 0%
Podría ser víctima de una falsificación de software.
Esta copia de Windows no ha superado el proceso de validación de Windows original.
Inicio
Instale Adobe Flash P...
11:07 p.m.

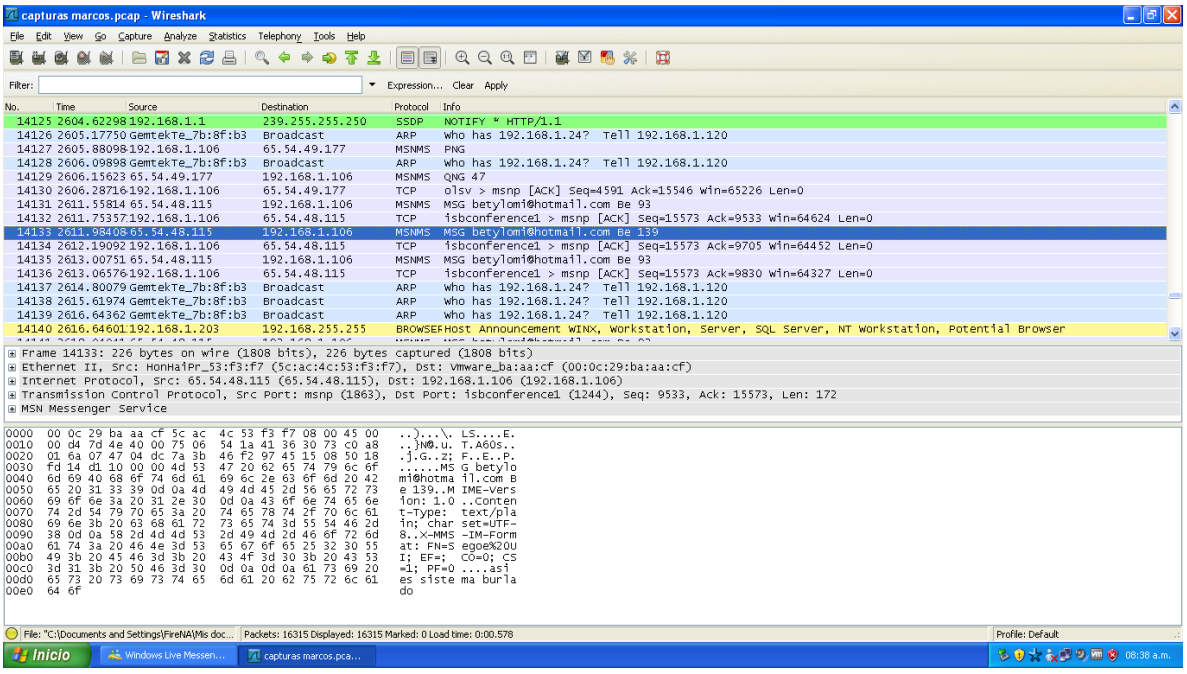

capturas marcos.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply
No. Time Source Destination Protocol Info
5395 697.415906 192.168.1.102 239.255.255.250 IGMP V2 Membership Report / Join group 239.255.255.250
5396 697.723614 GemtekTe_7b:8f:b3 Broadcast ARP Who has 192.168.1.1? Tell 192.168.1.120
5397 700.083479 192.168.1.120 239.255.255.250 SSDP M-SEARCH * HTTP/1.1
5398 701.918535 192.168.1.106 200.94.59.115 DNS Standard query A messenger.hotmail.com
5399 701.968831 200.94.59.115 192.168.1.106 DNS Standard query response CNAME messenger.hotmail.geo.msnmessenger.msn.com.akadns.net CNAME gateway.messenger
5400 702.168770 192.168.1.106 65.54.52.62 TCP gmrupdateserv > msnp [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
5401 702.322579 65.54.52.62 192.168.1.106 TCP msnp > gmrupdateserv [SYN, ACK] Seq=0 Ack=1 Win=1460 Len=0 MSS=1460 SACK_PERM=1
5402 702.462071 192.168.1.106 200.94.59.115 DNS Standard query A www.sqm.microsoft.com
5403 702.507950 200.94.59.115 192.168.1.106 DNS Standard query response CNAME sqm.msn.com CNAME sqm.microsoft.com A 65.55.7.141
5404 702.509949 192.168.1.106 65.55.7.141 TCP cardax > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
5405 702.629565 65.55.7.141 192.168.1.106 TCP http > cardax [SYN, ACK] Seq=0 Ack=1 Win=1460 Len=0 MSS=1460 SACK_PERM=1
5406 702.629716 192.168.1.106 65.55.7.141 TCP cardax > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
5407 702.631893 192.168.1.106 65.55.7.141 TCP [TCP segment of a reassembled PDU]
5408 702.632510 192.168.1.106 65.55.7.141 HTTP POST /sqm/messenger/sqmserver.dll HTTP/1.1
5409 702.792175 65.55.7.141 192.168.1.106 TCP http > cardax [ACK] Seq=1 Ack=623 Win=64240 Len=0
5410 702.804241 65.55.7.141 192.168.1.106 TCP [TCP segment of a reassembled PDU]
Frame 5399: 340 bytes on wire (2720 bits), 340 bytes captured (2720 bits)
Ethernet II, Src: HonHaiPr_53:f3:f7 (5c:ac:4c:53:f3:f7), Dst: Vmware_ba:aa:cf (00:0c:29:ba:aa:cf)
Destination: Vmware_ba:aa:cf (00:0c:29:ba:aa:cf)
Source: HonHaiPr_53:f3:f7 (5c:ac:4c:53:f3:f7)
Type: IP (0x0800)
Internet Protocol, Src: 200.94.59.115 (200.94.59.115), Dst: 192.168.1.106 (192.168.1.106)
User Datagram Protocol, Src Port: domain (53), Dst Port: 40123 (40123)
Domain Name System (response)
0000 00 0c 29 ba aa cf 5c ac 4c 53 f3 f7 08 00 45 00 ..)...\. LS....E.
0010 01 46 ca bb 40 00 fd 11 ec 06 c8 5e 3b 73 c0 a8 .F..@... ...^;s..
0020 01 6a 00 35 9c bb 01 32 e4 06 fa 4e 81 80 00 01 .j.5...2 ...N....
0030 00 03 00 03 00 09 6d 65 73 73 65 6e 67 65 72 ....m essenger
0040 07 68 6f 74 6d 61 69 6c 03 63 6f 6d 00 00 01 00 .hotmail .com....
0050 01 c0 0c 00 05 00 01 00 00 00 c9 00 37 09 6d 65 ....7.me
File: "C:\Documents and Settings\FireNA\Mis doc... Packets: 16315 Displayed: 16315 Marked: 0 Load time: 0:00.593 Profile: Default
Inicio Windows Live Messen... capturas marcos.pca... 08:24 a.m.

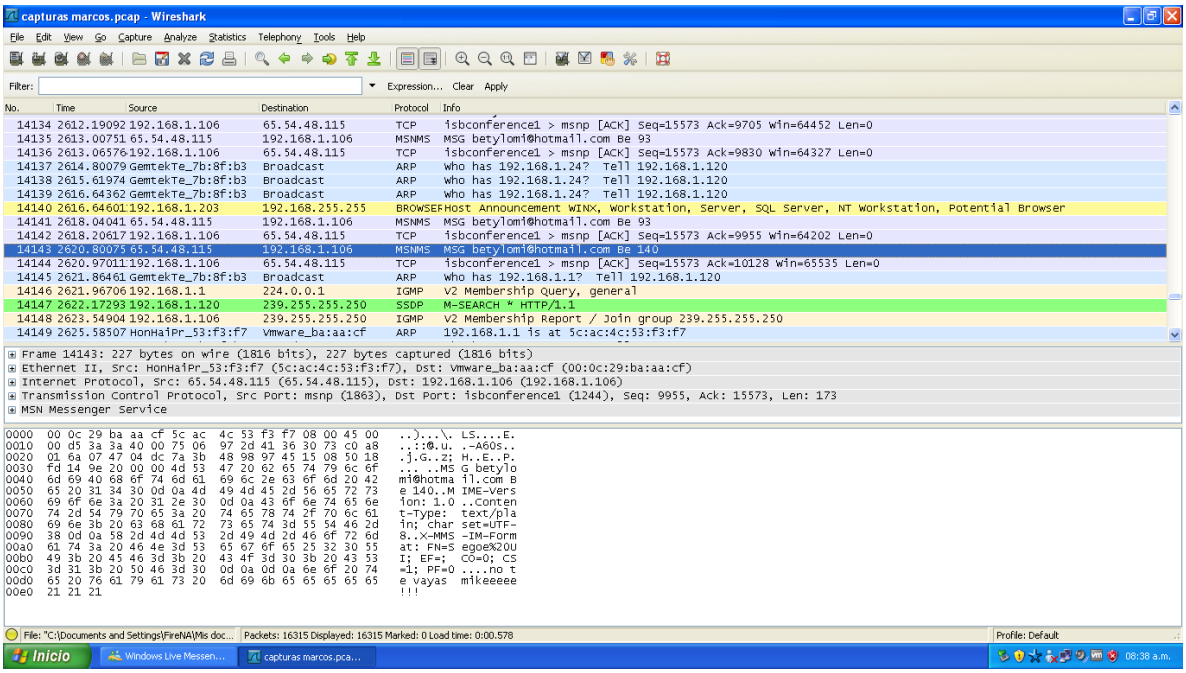

capturas marcos.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: msnms
Expression... Clear Apply
No. Time Source Destination Protocol Info
8638 1178.15339 192.168.1.106 65.54.52.62 MSNMS VER 1 MSNP18 MSNP17 CVR0
8640 1178.29998 65.54.52.62 192.168.1.106 MSNMS VER 1 MSNP18
8641 1178.30013 192.168.1.106 65.54.52.62 MSNMS CVR 2 0x0c0a winnt 5.1.3 i386 MSNMSGR 14.0.8117.0416 msmsgs firenovato@live.com.mx
8642 1178.43955 65.54.52.62 192.168.1.106 MSNMS CVR 2 14.0.8117 14.0.8117 14.0.8117 http://msgruser.dlservice.microsoft.com/download/A/6/1/A616CCD4-B0CA-
8643 1178.44097 65.54.52.62 192.168.1.106 MSNMS XFR 3 NS 65.54.61.170:1863 U D
8652 1178.61360 192.168.1.106 65.54.61.170 MSNMS VER 1 MSNP18 MSNP17 CVR0
8653 1178.75824 65.54.61.170 192.168.1.106 MSNMS VER 1 MSNP18
8654 1178.75844 192.168.1.106 65.54.61.170 MSNMS CVR 2 0x0c0a winnt 5.1.3 i386 MSNMSGR 14.0.8117.0416 msmsgs firenovato@live.com.mx
8656 1178.90038 65.54.61.170 192.168.1.106 MSNMS CVR 2 14.0.8117 14.0.8117 14.0.8117 http://msgruser.dlservice.microsoft.com/download/A/6/1/A616CCD4-B0CA-
8657 1178.90828 65.54.61.170 192.168.1.106 MSNMS GCF 0 5486
8659 1178.91387 65.54.61.170 192.168.1.106 MSNMS bWFpbm1zblwubmV0" /> <imtext value="Zm1jb25zdWx0aW5n" /> <imtext value="YmV6Z2lcLmluZm8=" />
8660 1179.07289 65.54.61.170 192.168.1.106 MSNMS t value="Z3NkYWdkZmdhc2RnczI0NTc0NTIyNDdcLmV4ZQ==" /> <imtext value="Z3NkZGFzMjQ1ODcyMTRnc2RcLmV4ZQ=
8662 1179.08499 65.54.61.170 192.168.1.106 MSNMS VzXC5jb29scGFnZVwuYml6L2ltYWdlc1wucGhw" /> <imtext value="Y2FzYTFcLmV4ZQ==" /> <imtext value="\
8663 1179.08553 65.54.61.170 192.168.1.106 MSNMS USR 3 SSO S MBI_KEY_OLD xkiVTpZpt/1cB6RQzjHQtcLGGVUvZ3KItxvSqnpwj3egu53jeETXJSjqOnCeLZA9
8743 1187.72386 192.168.1.106 65.54.52.62 MSNMS VER 1 MSNP18 MSNP17 CVR0
8744 1187.86989 65.54.52.62 192.168.1.106 MSNMS VER 1 MSNP18
Frame 8641: 174 bytes on wire (1392 bits), 174 bytes captured (1392 bits)
Ethernet II, Src: Vmware_ba:aa:cf (00:0c:29:ba:aa:cf), Dst: HonHaiPr_53:f3:f7 (5c:ac:4c:53:f3:f7)
Destination: HonHaiPr_53:f3:f7 (5c:ac:4c:53:f3:f7)
Source: Vmware_ba:aa:cf (00:0c:29:ba:aa:cf)
Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 65.54.52.62 (65.54.52.62)
Transmission Control Protocol, Src Port: blaze (1150), Dst Port: msnp (1863), Seq: 27, Ack: 15, Len: 120
MSN Messenger Service
0000 5c ac 4c 53 f3 f7 00 0c 29 ba aa cf 08 00 45 00 \.LS....).....E.
0010 00 a0 1f ed 40 00 80 06 a2 e4 c0 a8 01 6a 41 36 ....@... .....jA6
0020 34 3e 04 7e 07 47 84 46 be 5a 6e 08 04 7b 50 18 4>.~.G.F .Zn..{P.
0030 ff f1 6d f0 00 00 43 56 52 20 32 20 30 78 30 63 ..m...CV R 2 0x0c
0040 30 61 20 77 69 6e 6e 74 20 35 2e 31 2e 33 20 69 0a winnt 5.1.3 i
0050 33 38 36 20 4d 53 4e 4d 53 47 52 20 31 34 2e 30 386 MSNM SGR 14.0
0060 2e 38 31 31 37 2e 30 34 31 36 20 6d 73 6d 73 67 .8117.04 16 msmsg
0070 73 20 66 69 72 65 6e 6f 76 61 74 6f 40 6c 69 76 s fireno vato@liv
0080 65 2e 63 6f 6d 2e 6d 78 0d 0a 55 53 52 20 33 20 e.com.mx ..USR 3
0090 53 53 4f 20 49 20 66 69 72 65 6e 6f 76 61 74 6f SSO I fi renovato
00a0 40 6c 69 76 65 2e 63 6f 6d 2e 6d 78 0d 0a @live.co m.mx..
File: "C:\Documents and Settings\FireNA\Mis doc... Packets: 16315 Displayed: 600 Marked: 0 Load time: 0:00.734 Profile: Default
Inicio Windows Live Messen... capturas marcos.pca... 08:28 a.m.


capturas marcos.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: msnms
Expression... Clear Apply
No. Time Source Destination Protocol Info
12037 1851.65288 192.168.1.106 65.54.49.177 MSNMS XFR 18 SB
12038 1852.26491 65.55.71.71 192.168.1.106 MSNMS MSG dustin_cesar@hotmail.com SpeRando..! 97
12040 1852.59403 65.54.49.177 192.168.1.106 MSNMS XFR 18 SB 65.54.48.115:1863 CKI 823702440.172195217.563143 U messenger.msn.com 1
12043 1853.11192 65.55.71.71 192.168.1.106 MSNMS [TCP Retransmission] MSG dustin_cesar@hotmail.com SpeRando..! 97
12045 1853.17130 65.54.49.177 192.168.1.106 MSNMS [TCP Retransmission] XFR 18 SB 65.54.48.115:1863 CKI 823702440.172195217.563143 U messenger.msn.com 1
12049 1853.19448 192.168.1.106 65.54.48.115 MSNMS USR 23 firenovato@live.com.mx;{6D474C44-94D3-474C-8245-DC63E60AD3AD} 823702440.172195217.563143
12050 1853.64256 65.54.48.115 192.168.1.106 MSNMS USR 23 OK firenovato@live.com.mx;{6d474c44-94d3-474c-8245-dc63e60ad3ad} fire
12051 1853.64306 192.168.1.106 65.54.48.115 MSNMS CAL 20 firenovato@live.com.mx
12052 1854.40771 65.54.48.115 192.168.1.106 MSNMS CAL 20 RINGING 823702440
12053 1854.40783 192.168.1.106 65.54.48.115 MSNMS CAL 21 betylomi@hotmail.com
12054 1854.40824 65.54.48.115 192.168.1.106 MSNMS JOI firenovato@live.com.mx fire 2788999460:2550273072
12056 1854.90629 65.54.48.115 192.168.1.106 MSNMS CAL 21 RINGING 823702440
12058 1856.12160 65.54.48.115 192.168.1.106 MSNMS JOI betylomi@hotmail.com;{68717d1b-a83a-449b-bccf-8668818656d8} Be 2788999460:2550273072
12059 1856.12222 65.54.48.115 192.168.1.106 MSNMS JOI betylomi@hotmail.com Be 2788999460:2550273072
12061 1856.12683 192.168.1.106 65.54.48.115 MSNMS MSG 22 N 121
12062 1856.22372 65.55.71.71 192.168.1.106 MSNMS MSG dustin_cesar@hotmail.com SpeRando..! 142
Frame 12053: 83 bytes on wire (664 bits), 83 bytes captured (664 bits)
Ethernet II, Src: Vmware_ba:aa:cf (00:0c:29:ba:aa:cf), Dst: HonHaiPr_53:f3:f7 (5c:ac:4c:53:f3:f7)
Destination: HonHaiPr_53:f3:f7 (5c:ac:4c:53:f3:f7)
Source: Vmware_ba:aa:cf (00:0c:29:ba:aa:cf)
Type: IP (0x0800)
Internet Protocol, Src: 192.168.1.106 (192.168.1.106), Dst: 65.54.48.115 (65.54.48.115)
Transmission Control Protocol, Src Port: isbconference1 (1244), Dst Port: msnp (1863), Seq: 129, Ack: 105, Len: 29
MSN Messenger Service
0000 5c ac 4c 53 f3 f7 00 0c 29 ba aa cf 08 00 45 00 \.LS....).....E.
0010 00 45 24 1d 40 00 80 06 a2 da c0 a8 01 6a 41 36 .E$.@... .....jA6
0020 30 73 04 dc 07 47 97 44 d8 b4 7a 3b 22 1e 50 18 0s...G.D ..z;".P.
0030 ff 97 45 71 00 00 43 41 4c 20 32 31 20 62 65 74 ..Eq..CA L 21 bet
0040 79 6c 6f 6d 69 40 68 6f 74 6d 61 69 6c 2e 63 6f ylomi@ho tmail.co
0050 6d 0d 0a m..
File: "C:\Documents and Settings\FireNA\Mis doc... Packets: 16315 Displayed: 600 Marked: 0 Load time: 0:00.734 Profile: Default
Inicio Windows Live Messen... capturas marcos.pca... 08:32 a.m.


capturas marcos.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: msnms
Expression... Clear Apply
No. Time Source Destination Protocol Info
13825 2475.98177 192.168.1.106 65.54.48.115 MSNMS MSG 75 U 95
13826 2476.15866 65.54.48.115 192.168.1.106 MSNMS MSG betylomi@hotmail.com Be 135
13830 2479.63480 65.54.48.115 192.168.1.106 MSNMS MSG betylomi@hotmail.com Be 93
13833 2480.97028 192.168.1.106 65.54.48.115 MSNMS MSG 76 U 95
13838 2482.78296 65.54.48.115 192.168.1.106 MSNMS MSG betylomi@hotmail.com Be 128
13843 2485.97020 192.168.1.106 65.54.48.115 MSNMS MSG 77 U 95
13845 2489.33655 192.168.1.106 65.54.48.115 MSNMS MSG 78 N 141
13901 2510.52337 192.168.1.106 65.54.49.177 MSNMS PNG
13902 2511.36787 192.168.1.106 65.54.49.177 MSNMS [TCP Retransmission] PNG
13903 2512.06414 65.54.49.177 192.168.1.106 MSNMS QNG 45
13971 2541.72339 65.54.48.115 192.168.1.106 MSNMS MSG betylomi@hotmail.com Be 93
13973 2543.29127 65.54.48.115 192.168.1.106 MSNMS MSG betylomi@hotmail.com Be 121
13977 2545.13121 65.54.48.115 192.168.1.106 MSNMS MSG betylomi@hotmail.com Be 93
13978 2545.13190 65.54.48.115 192.168.1.106 MSNMS MSG betylomi@hotmail.com Be 123
13982 2547.80243 65.54.48.115 192.168.1.106 MSNMS MSG betylomi@hotmail.com Be 93
13984 2552.72224 65.54.48.115 192.168.1.106 MSNMS MSG betylomi@hotmail.com Be 93
Frame 13973: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits)
Ethernet II, Src: HonHaiPr_53:f3:f7 (5c:ac:4c:53:f3:f7), Dst: Vmware_ba:aa:cf (00:0c:29:ba:aa:cf)
Internet Protocol, Src: 65.54.48.115 (65.54.48.115), Dst: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: msnp (1863), Dst Port: isbconference1 (1244), Seq: 8187, Ack: 14610, Len: 154
MSN Messenger Service
0000 00 0c 29 ba aa cf 5c ac 4c 53 f3 f7 08 00 45 00 ..)...\. LS....E.
0010 00 c2 42 f4 40 00 75 06 8e 86 41 36 30 73 c0 a8 ..B.@.u. ..A60s..
0020 01 6a 07 47 04 dc 7a 3b 41 b0 97 45 11 45 50 18 .j.G..z; A..E.EP.
0030 fa c7 1d f4 00 00 4d 53 47 20 62 65 74 79 6c 6f ......MS G betylo
0040 6d 69 40 68 6f 74 6d 61 69 6c 2e 63 6f 6d 20 42 mi@hotma il.com B
0050 65 20 31 32 31 0d 0a 4d 49 4d 45 2d 56 65 72 73 e 121..M IME-Vers
0060 69 6f 6e 3a 20 31 2e 30 0d 0a 43 6f 6e 74 65 6e ion: 1.0 ..Conten
0070 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 t-Type: text/pla
0080 69 6e 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d in; char set=UTF-
0090 38 0d 0a 58 2d 4d 4d 53 2d 49 4d 2d 46 6f 72 6d 8..X-MMS -IM-Form
00a0 61 74 3a 20 46 4e 3d 53 65 67 6f 65 25 32 30 55 at: FN=S egoe%20U
00b0 49 3b 20 45 46 3d 3b 20 43 4f 3d 30 3b 20 43 53 I; EF=; CO=0; CS
00c0 3d 31 3b 20 50 46 3d 30 0d 0a 0d 0a 61 6c 67 6f =1; PF=0 ....algo
File: "C:\Documents and Settings\FireNA\Mis doc... Packets: 16315 Displayed: 600 Marked: 0 Load time: 0:00.734 Profile: Default
Inicio Windows Live Messen... capturas marcos.pca... 08:35 a.m.


capturas marcos.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: msnms
Expression... Clear Apply
No. Time Source Destination Protocol Info
13825 2475.98177 192.168.1.106 65.54.48.115 MSNMS MSG 75 U 95
13826 2476.15866 65.54.48.115 192.168.1.106 MSNMS MSG betylomi@hotmail.com Be 135
13830 2479.63480 65.54.48.115 192.168.1.106 MSNMS MSG betylomi@hotmail.com Be 93
13833 2480.97028 192.168.1.106 65.54.48.115 MSNMS MSG 76 U 95
13838 2482.78296 65.54.48.115 192.168.1.106 MSNMS MSG betylomi@hotmail.com Be 128
13843 2485.97020 192.168.1.106 65.54.48.115 MSNMS MSG 77 U 95
13845 2489.33655 192.168.1.106 65.54.48.115 MSNMS MSG 78 N 141
13901 2510.52337 192.168.1.106 65.54.49.177 MSNMS PNG
13902 2511.36787 192.168.1.106 65.54.49.177 MSNMS [TCP Retransmission] PNG
13903 2512.06414 65.54.49.177 192.168.1.106 MSNMS QNG 45
13971 2541.72339 65.54.48.115 192.168.1.106 MSNMS MSG betylomi@hotmail.com Be 93
13973 2543.29127 65.54.48.115 192.168.1.106 MSNMS MSG betylomi@hotmail.com Be 121
13977 2545.13121 65.54.48.115 192.168.1.106 MSNMS MSG betylomi@hotmail.com Be 93
13978 2545.13190 65.54.48.115 192.168.1.106 MSNMS MSG betylomi@hotmail.com Be 123
13982 2547.80243 65.54.48.115 192.168.1.106 MSNMS MSG betylomi@hotmail.com Be 93
13984 2552.72224 65.54.48.115 192.168.1.106 MSNMS MSG betylomi@hotmail.com Be 93
Frame 13978: 210 bytes on wire (1680 bits), 210 bytes captured (1680 bits)
Ethernet II, Src: HonHaiPr_53:f3:f7 (5c:ac:4c:53:f3:f7), Dst: Vmware_ba:aa:cf (00:0c:29:ba:aa:cf)
Internet Protocol, Src: 65.54.48.115 (65.54.48.115), Dst: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: msnp (1863), Dst Port: isbconference1 (1244), Seq: 8466, Ack: 14610, Len: 156
MSN Messenger Service
0000 00 0c 29 ba aa cf 5c ac 4c 53 f3 f7 08 00 45 00 ..)...\. LS....E.
0010 00 c4 6a 0b 40 00 75 06 67 6d 41 36 30 73 c0 a8 ..j.@.u. gmA60s..
0020 01 6a 07 47 04 dc 7a 3b 42 c7 97 45 11 45 50 18 .j.G..z; B..E.EP.
0030 fa c7 a4 92 00 00 4d 53 47 20 62 65 74 79 6c 6f ......MS G betylo
0040 6d 69 40 68 6f 74 6d 61 69 6c 2e 63 6f 6d 20 42 mi@hotma il.com B
0050 65 20 31 32 33 0d 0a 4d 49 4d 45 2d 56 65 72 73 e 123..M IME-Vers
0060 69 6f 6e 3a 20 31 2e 30 0d 0a 43 6f 6e 74 65 6e ion: 1.0 ..Conten
0070 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 t-Type: text/pla
0080 69 6e 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d in; char set=UTF-
0090 38 0d 0a 58 2d 4d 4d 53 2d 49 4d 2d 46 6f 72 6d 8..X-MMS -IM-Form
00a0 61 74 3a 20 46 4e 3d 53 65 67 6f 65 25 32 30 55 at: FN=S egoe%20U
00b0 49 3b 20 45 46 3d 3b 20 43 4f 3d 30 3b 20 43 53 I; EF=; CO=0; CS
00c0 3d 31 3b 20 50 46 3d 30 0d 0a 0d 0a 6a 61 6a 61 =1; PF=0 ....jaja
00d0 6a 61 ja
File: "C:\Documents and Settings\FireNA\Mis doc... Packets: 16315 Displayed: 600 Marked: 0 Load time: 0:00.734 Profile: Default
Inicio Windows Live Messen... capturas marcos.pca... 08:35 a.m.


capturas marcos.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply
No. Time Source Destination Protocol Info
14125 2604.62298 192.168.1.1 239.255.255.250 SSDP NOTIFY * HTTP/1.1
14126 2605.17750 GemtekTe_7b:8f:b3 Broadcast ARP Who has 192.168.1.24? Tell 192.168.1.120
14127 2605.88098 192.168.1.106 65.54.49.177 MSNMS PNG
14128 2606.09898 GemtekTe_7b:8f:b3 Broadcast ARP Who has 192.168.1.24? Tell 192.168.1.120
14129 2606.15623 65.54.49.177 192.168.1.106 MSNMS QNG 47
14130 2606.28716 192.168.1.106 65.54.49.177 TCP olsv > msnp [ACK] Seq=4591 Ack=15546 Win=65226 Len=0
14131 2611.55814 65.54.48.115 192.168.1.106 MSNMS MSG betylomi@hotmail.com Be 93
14132 2611.75357 192.168.1.106 65.54.48.115 TCP isbconference1 > msnp [ACK] Seq=15573 Ack=9533 Win=64624 Len=0
14133 2611.98408 65.54.48.115 192.168.1.106 MSNMS MSG betylomi@hotmail.com Be 139
14134 2612.19092 192.168.1.106 65.54.48.115 TCP isbconference1 > msnp [ACK] Seq=15573 Ack=9705 Win=64452 Len=0
14135 2613.00751 65.54.48.115 192.168.1.106 MSNMS MSG betylomi@hotmail.com Be 93
14136 2613.06576 192.168.1.106 65.54.48.115 TCP isbconference1 > msnp [ACK] Seq=15573 Ack=9830 Win=64327 Len=0
14137 2614.80079 GemtekTe_7b:8f:b3 Broadcast ARP Who has 192.168.1.24? Tell 192.168.1.120
14138 2615.61974 GemtekTe_7b:8f:b3 Broadcast ARP Who has 192.168.1.24? Tell 192.168.1.120
14139 2616.64362 GemtekTe_7b:8f:b3 Broadcast ARP Who has 192.168.1.24? Tell 192.168.1.120
14140 2616.64601 192.168.1.203 192.168.255.255 BROWSER Host Announcement WINX, Workstation, Server, SQL Server, NT Workstation, Potential Browser
Frame 14133: 226 bytes on wire (1808 bits), 226 bytes captured (1808 bits)
Ethernet II, Src: HonHaiPr_53:f3:f7 (5c:ac:4c:53:f3:f7), Dst: Vmware_ba:aa:cf (00:0c:29:ba:aa:cf)
Internet Protocol, Src: 65.54.48.115 (65.54.48.115), Dst: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: msnp (1863), Dst Port: isbconference1 (1244), Seq: 9533, Ack: 15573, Len: 172
MSN Messenger Service
0000 00 0c 29 ba aa cf 5c ac 4c 53 f3 f7 08 00 45 00 ..)...\. LS....E.
0010 00 d4 7d 4e 40 00 75 06 54 1a 41 36 30 73 c0 a8 ..}N@.u. T.A60s..
0020 01 6a 07 47 04 dc 7a 3b 46 f2 97 45 15 08 50 18 .j.G..z; F..E..P.
0030 fd 14 d1 10 00 00 4d 53 47 20 62 65 74 79 6c 6f ......MS G betylo
0040 6d 69 40 68 6f 74 6d 61 69 6c 2e 63 6f 6d 20 42 mi@hotma il.com B
0050 65 20 31 33 39 0d 0a 4d 49 4d 45 2d 56 65 72 73 e 139..M IME-Vers
0060 69 6f 6e 3a 20 31 2e 30 0d 0a 43 6f 6e 74 65 6e ion: 1.0 ..Conten
0070 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 t-Type: text/pla
0080 69 6e 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d in; char set=UTF-
0090 38 0d 0a 58 2d 4d 4d 53 2d 49 4d 2d 46 6f 72 6d 8..X-MMS -IM-Form
00a0 61 74 3a 20 46 4e 3d 53 65 67 6f 65 25 32 30 55 at: FN=S egoe%20U
00b0 49 3b 20 45 46 3d 3b 20 43 4f 3d 30 3b 20 43 53 I; EF=; CO=0; CS
00c0 3d 31 3b 20 50 46 3d 30 0d 0a 0d 0a 61 73 69 20 =1; PF=0 ....asi
00d0 65 73 20 73 69 73 74 65 6d 61 20 62 75 72 6c 61 es siste ma burla
00e0 64 6f do
File: "C:\Documents and Settings\FireNA\Mis doc... Packets: 16315 Displayed: 16315 Marked: 0 Load time: 0:00.578 Profile: Default
Inicio Windows Live Messen... capturas marcos.pca... 08:38 a.m.


capturas marcos.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
14134 2612.19092 192.168.1.106 65.54.48.115 TCP isbconference1 > msnp [ACK] Seq=15573 Ack=9705 Win=64452 Len=0
14135 2613.00751 65.54.48.115 192.168.1.106 MSNMS MSG betylomi@hotmail.com Be 93
14136 2613.06576 192.168.1.106 65.54.48.115 TCP isbconference1 > msnp [ACK] Seq=15573 Ack=9830 Win=64327 Len=0
14137 2614.80079 GemtekTe_7b:8f:b3 Broadcast ARP who has 192.168.1.24? Tell 192.168.1.120
14138 2615.61974 GemtekTe_7b:8f:b3 Broadcast ARP who has 192.168.1.24? Tell 192.168.1.120
14139 2616.64362 GemtekTe_7b:8f:b3 Broadcast ARP who has 192.168.1.24? Tell 192.168.1.120
14140 2616.64601 192.168.1.203 192.168.255.255 BROWSER Host Announcement WINX, Workstation, Server, SQL Server, NT Workstation, Potential Browser
14141 2618.04041 65.54.48.115 192.168.1.106 MSNMS MSG betylomi@hotmail.com Be 93
14142 2618.20617 192.168.1.106 65.54.48.115 TCP isbconference1 > msnp [ACK] Seq=15573 Ack=9955 Win=64202 Len=0
14143 2620.80075 65.54.48.115 192.168.1.106 MSNMS MSG betylomi@hotmail.com Be 140
14144 2620.97011 192.168.1.106 65.54.48.115 TCP isbconference1 > msnp [ACK] Seq=15573 Ack=10128 Win=65535 Len=0
14145 2621.86461 GemtekTe_7b:8f:b3 Broadcast ARP who has 192.168.1.1? Tell 192.168.1.120
14146 2621.96706 192.168.1.1 224.0.0.1 IGMP V2 Membership Query, general
14147 2622.17293 192.168.1.120 239.255.255.250 SSDP M-SEARCH * HTTP/1.1
14148 2623.54904 192.168.1.106 239.255.255.250 IGMP V2 Membership Report / Join group 239.255.255.250
14149 2625.58507 HonHaiPr_53:f3:f7 Vmware_ba:aa:cf ARP 192.168.1.1 is at 5c:ac:4c:53:f3:f7
Frame 14143: 227 bytes on wire (1816 bits), 227 bytes captured (1816 bits)
Ethernet II, Src: HonHaiPr_53:f3:f7 (5c:ac:4c:53:f3:f7), Dst: Vmware_ba:aa:cf (00:0c:29:ba:aa:cf)
Internet Protocol, Src: 65.54.48.115 (65.54.48.115), Dst: 192.168.1.106 (192.168.1.106)
Transmission Control Protocol, Src Port: msnp (1863), Dst Port: isbconference1 (1244), Seq: 9955, Ack: 15573, Len: 173
MSN Messenger Service
0000 00 0c 29 ba aa cf 5c ac 4c 53 f3 f7 08 00 45 00 ..)...\. LS....E.
0010 00 d5 3a 3a 40 00 75 06 97 2d 41 36 30 73 c0 a8 ..::@.u. .-A60s..
0020 01 6a 07 47 04 dc 7a 3b 48 98 97 45 15 08 50 18 .j.G..z; H..E..P.
0030 fd 14 9e 20 00 00 4d 53 47 20 62 65 74 79 6c 6f ... ..MS G betylo
0040 6d 69 40 68 6f 74 6d 61 69 6c 2e 63 6f 6d 20 42 mi@hotma il.com B
0050 65 20 31 34 30 0d 0a 4d 49 4d 45 2d 56 65 72 73 e 140..M IME-Vers
0060 69 6f 6e 3a 20 31 2e 30 0d 0a 43 6f 6e 74 65 6e ion: 1.0 ..Conten
0070 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 70 6c 61 t-Type: text/pla
0080 69 6e 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d in; char set=UTF-
0090 38 0d 0a 58 2d 4d 4d 53 2d 49 4d 2d 46 6f 72 6d 8..X-MMS -IM-Form
00a0 61 74 3a 20 46 4e 3d 53 65 67 6f 65 25 32 30 55 at: FN=S egoe%20U
00b0 49 3b 20 45 46 3d 3b 20 43 4f 3d 30 3b 20 43 53 I; EF=; CO=0; CS
00c0 3d 31 3b 20 50 46 3d 30 0d 0a 0d 0a 6e 6f 20 74 =1; PF=0 ....no t
00d0 65 20 76 61 79 61 73 20 6d 69 6b 65 65 65 65 65 e vayas mikeeeee
00e0 21 21 21 !!!
File: "C:\Documents and Settings\FireNA\Mis doc... Packets: 16315 Displayed: 16315 Marked: 0 Load time: 0:00.578 Profile: Default
Inicio Windows Live Messen... capturas marcos.pca... 08:38 a.m.