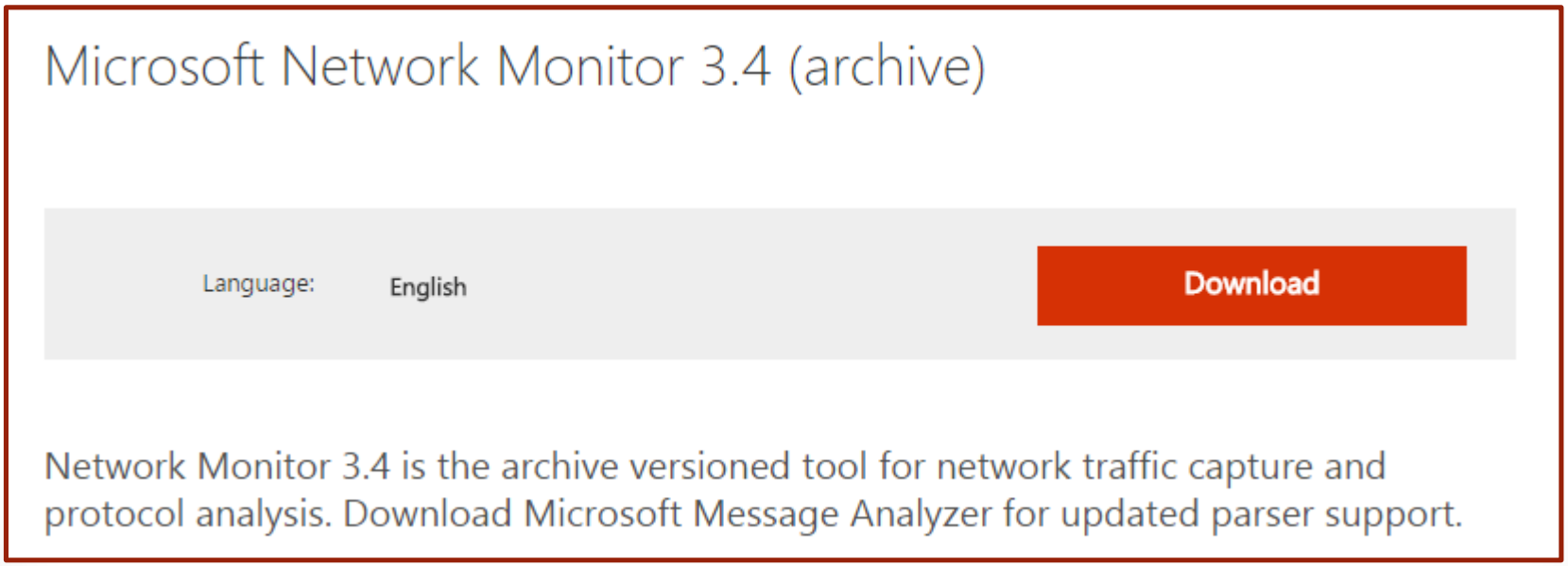
Windows Serwer 2008 R2

Moduł 7. Monitoring ruchu sieciowego

Windows Server System

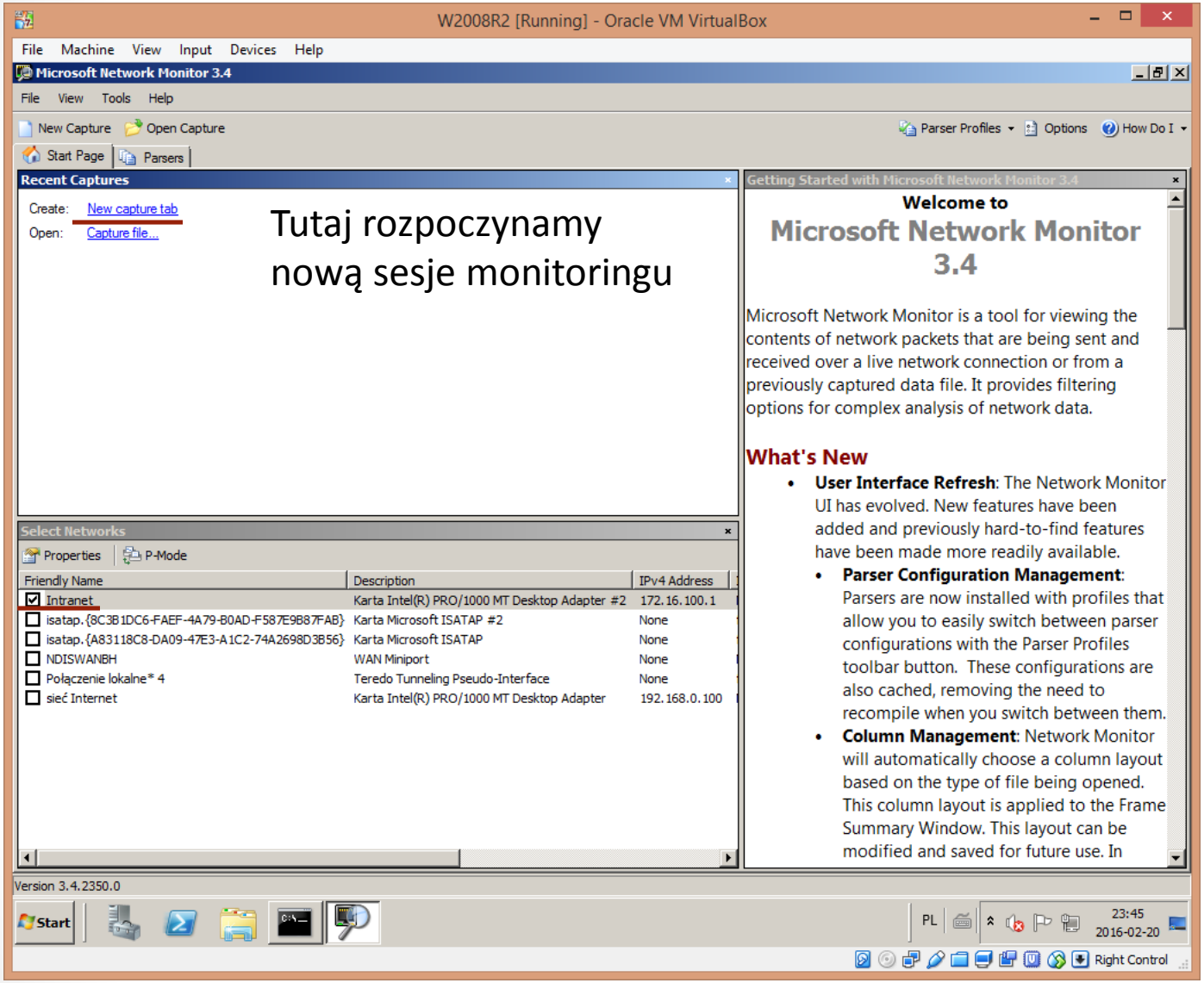
Microsoft Network Monitor

- Microsoft Network Monitor to bezpłatne, zaawansowane narzędzie dla administratorów sieci służące do przechwytywania i analizy ruchu sieciowego.
- Aby praca z dużą ilością danych była łatwiejsza program zawiera kilkadziesiąt wbudowanych filtrów (a także możliwość definiowania własnych) dzięki którym można zawęzić dane do analizy.



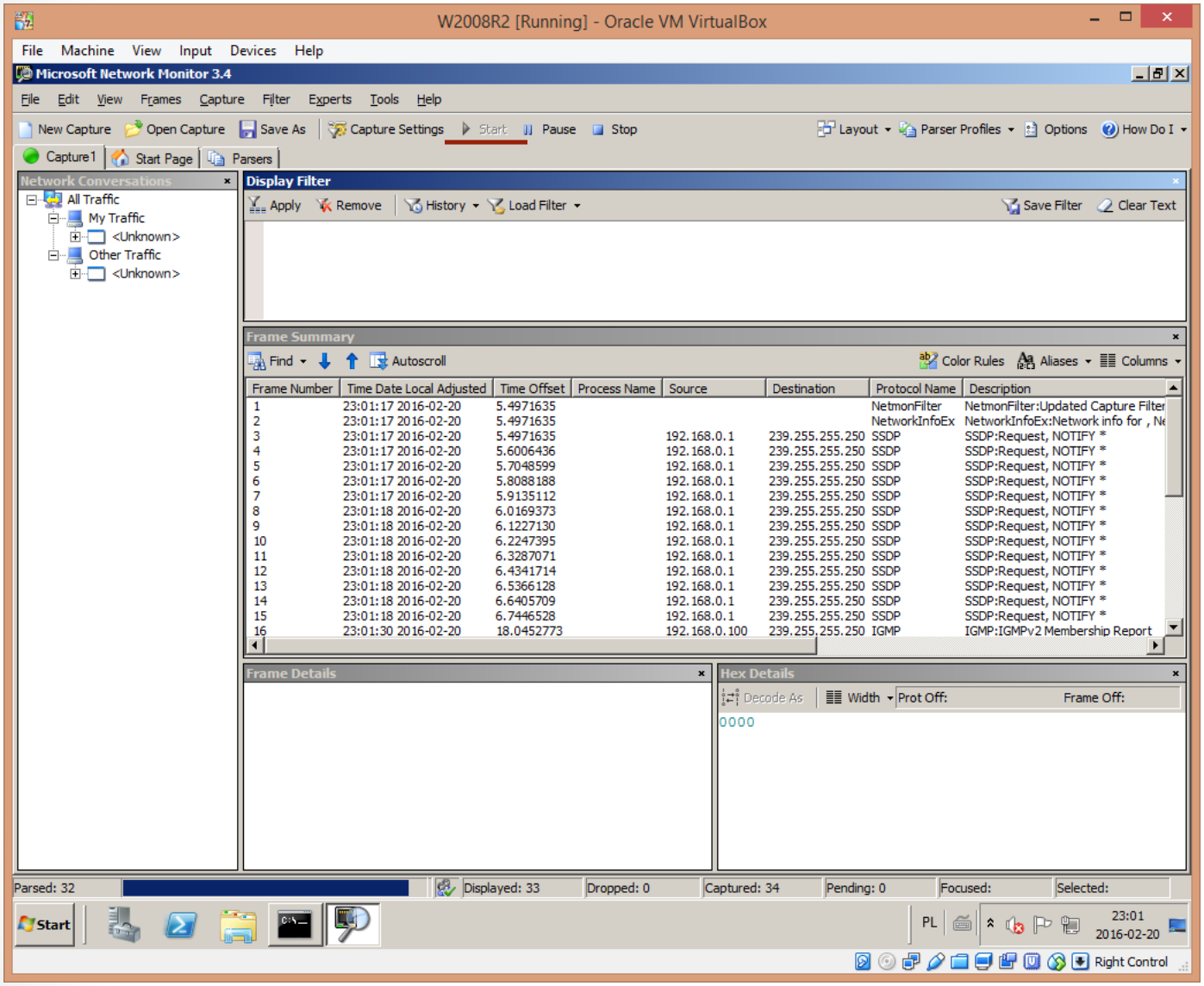
- https://www.microsoft.com/en-us/download/details.aspx?id=4865

Microsoft Network Monitor



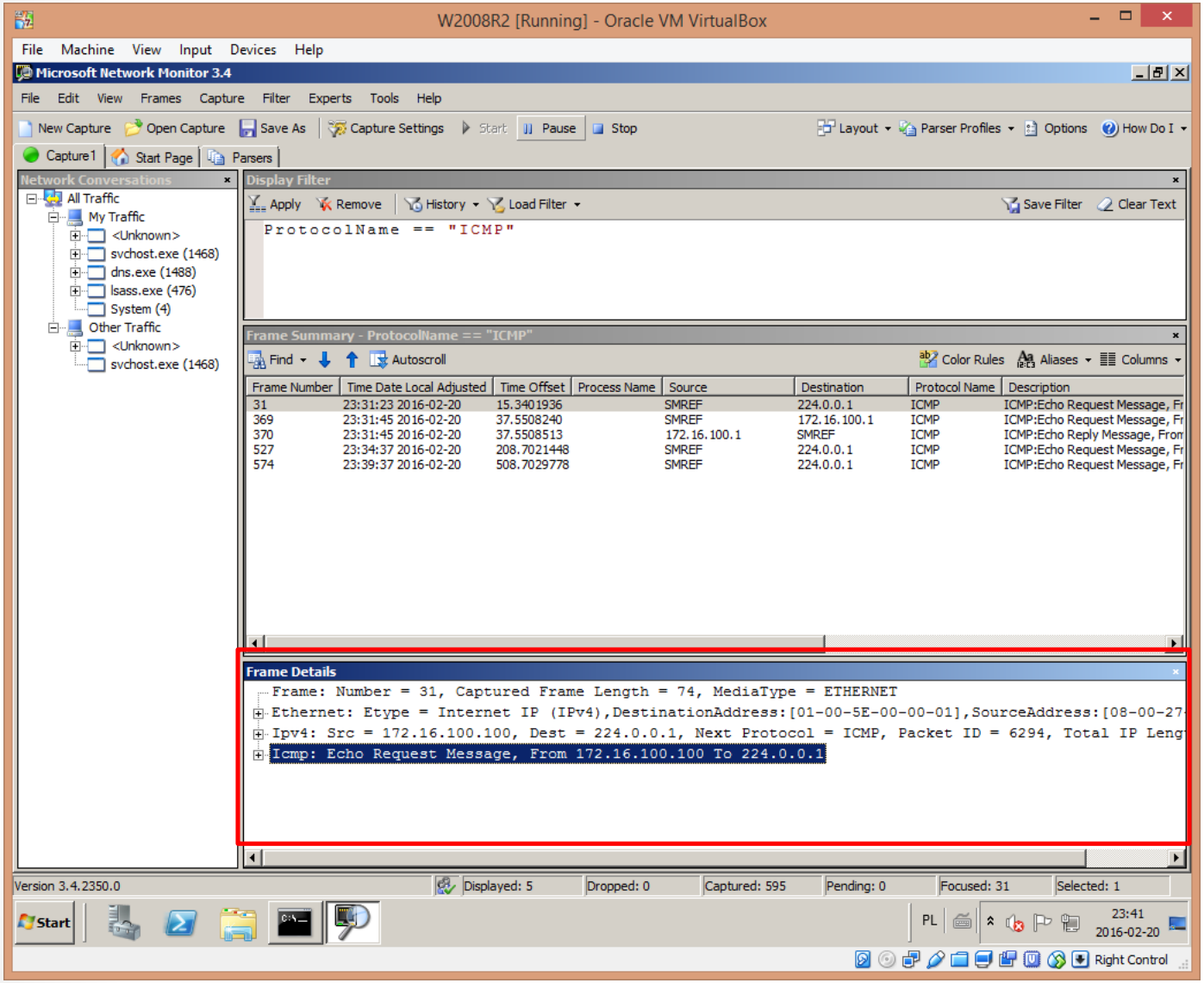
- Wybieramy interfejs, który będziemy monitorować: „Intranet”

Microsoft Network Monitor



- Rozpoczynamy przechwytywanie - **Start**

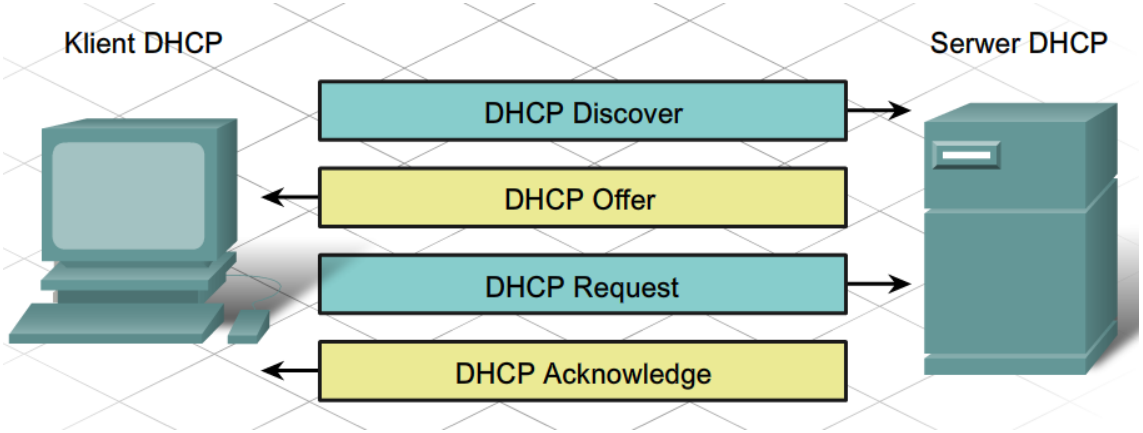
Microsoft Network Monitor



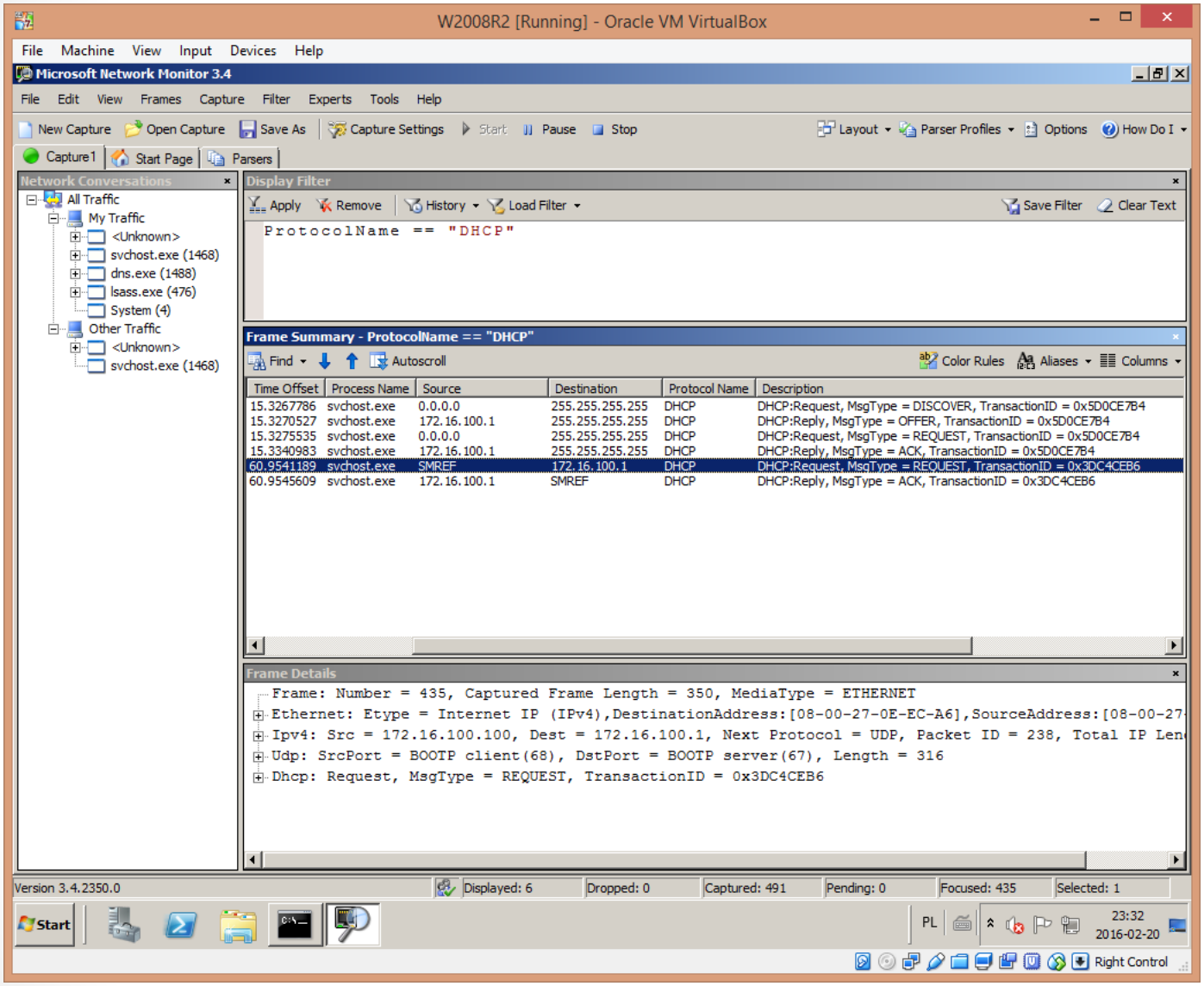
- Po zaznaczeniu wybranego pakietu mamy dostęp do okna szczegółów ramki

Proces pozyskiwania dzierżawy

1. Klient, który potrzebuje adresu IP, wysyła wiadomość **DHCP Discover**, która jest wiadomością typu broadcast, na adres 255.255.255.255 z docelowym adresem MAC FF-FF-FF-FF-FF-FF. Tę wiadomość DHCP otrzymają wszystkie hosty w sieci, ale tylko serwer DHCP na nią odpowie.
2. Serwer DHCP wysyła w odpowiedzi wiadomość **DHCP Offer** proponując klientowi adres IP.
3. Host odpowiada serwerowi wiadomością **DHCP Request** pytając o możliwość wykorzystania proponowanego adresu IP.
4. Serwer wysyła potwierdzenie wiadomością **DHCP Acknowledgment**.



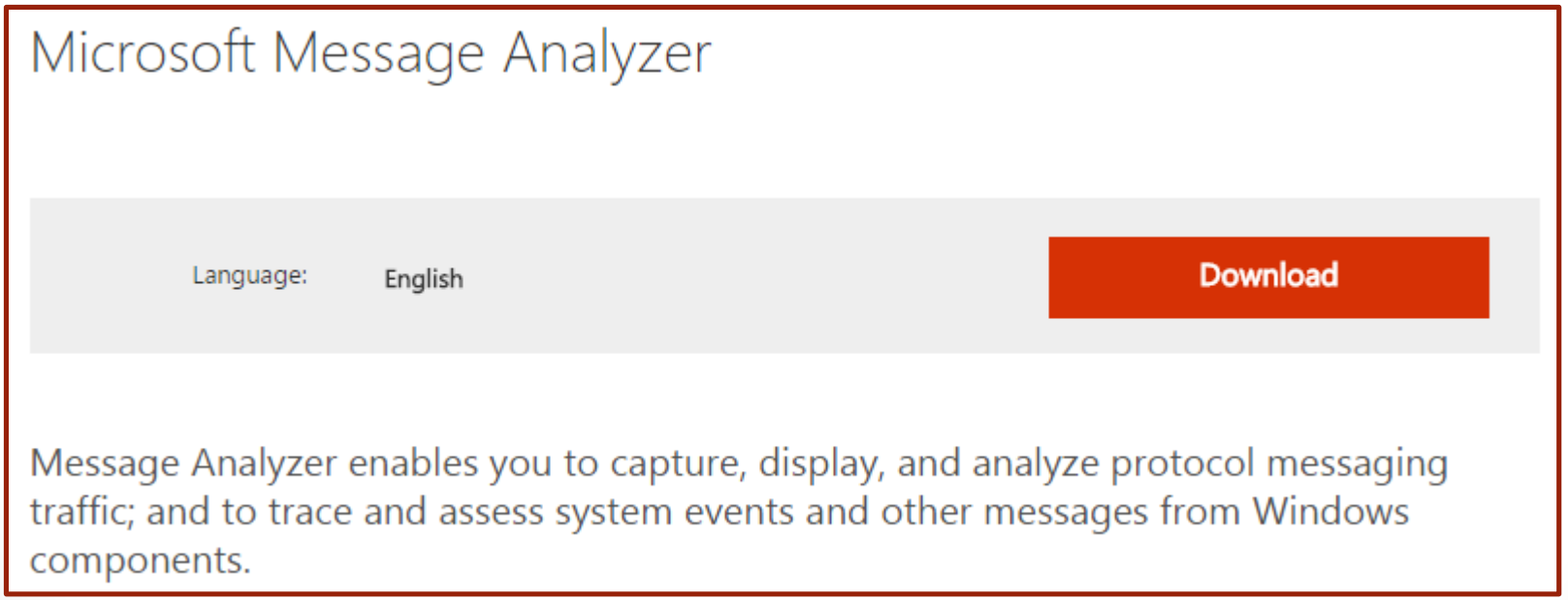
Microsoft Network Monitor



- Obserwujemy ruch DHCP

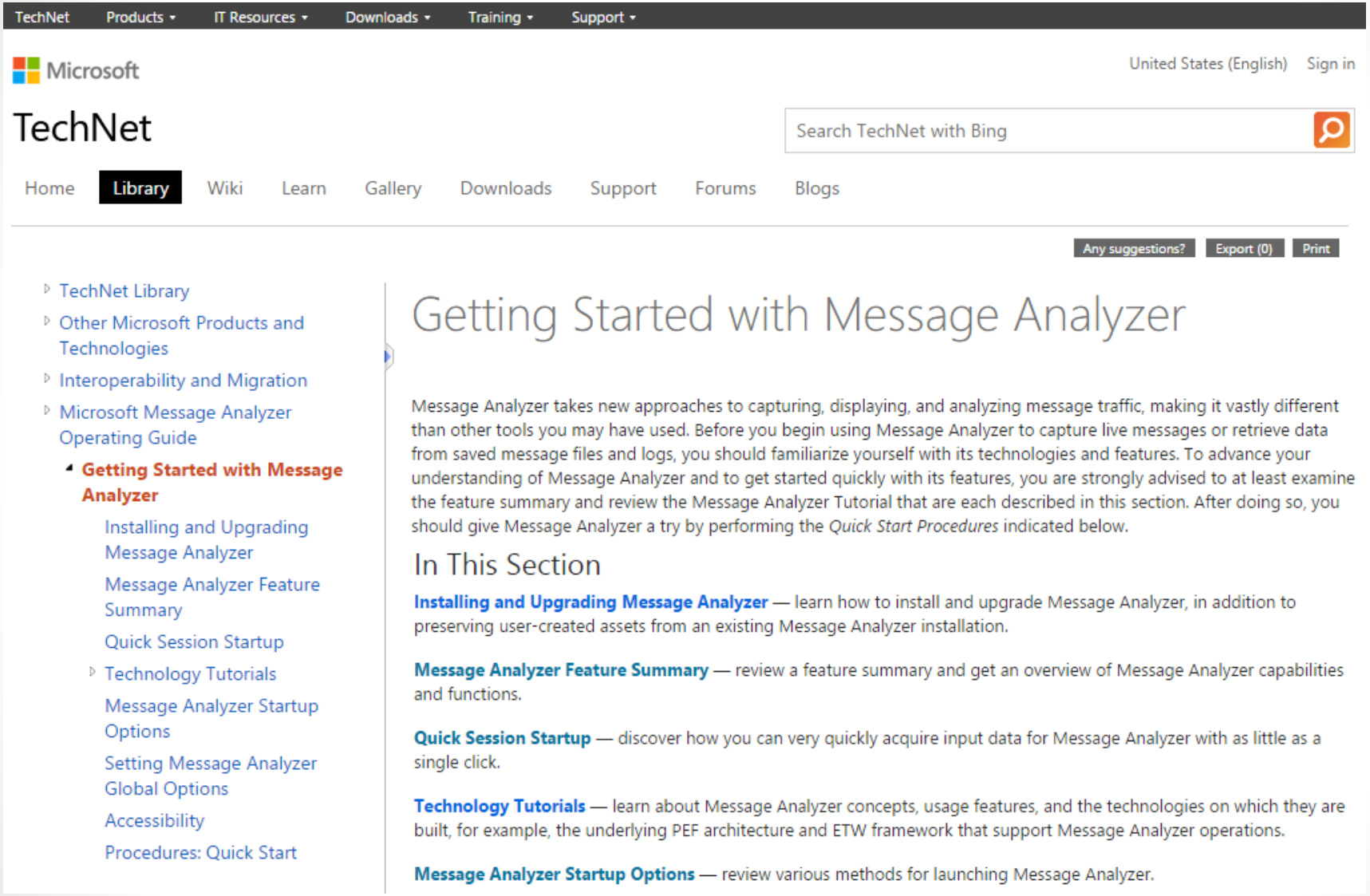
Microsoft Message Analyzer

- Message Analyzer to następca Network Monitor 3.X - ale to nie tylko snifer warstwy sieciowej, pozwala on również analizować informacje systemowe, wydarzenia i logi systemowe.
- Aplikacja umożliwia także importowanie, łączenie i analizę danych pochodzących z logów Windows oraz plików śledzenia, a także bieżące monitorowanie nowych wiadomości.



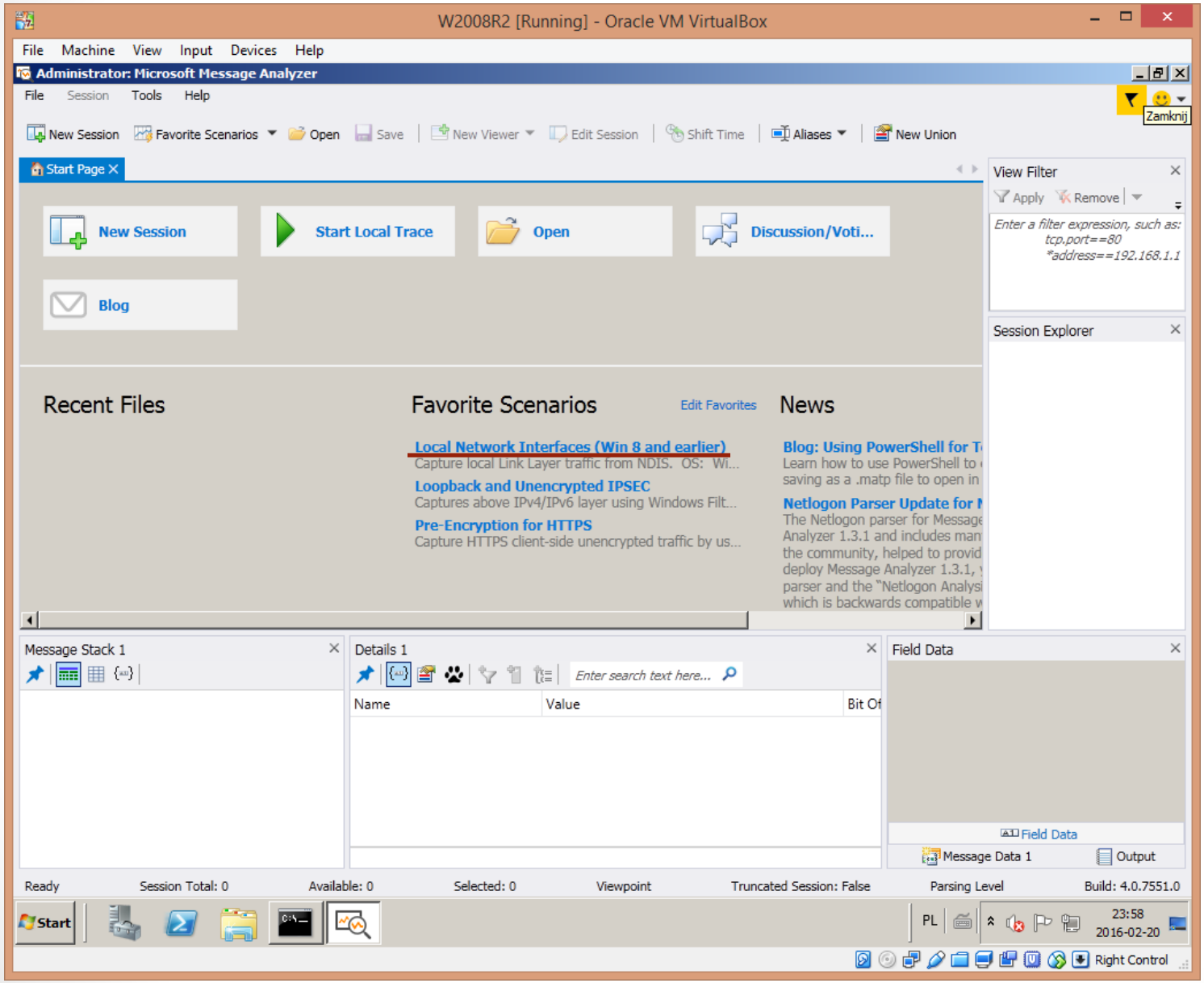
- https://www.microsoft.com/en-us/download/details.aspx?id=44226

Microsoft Message Analyzer

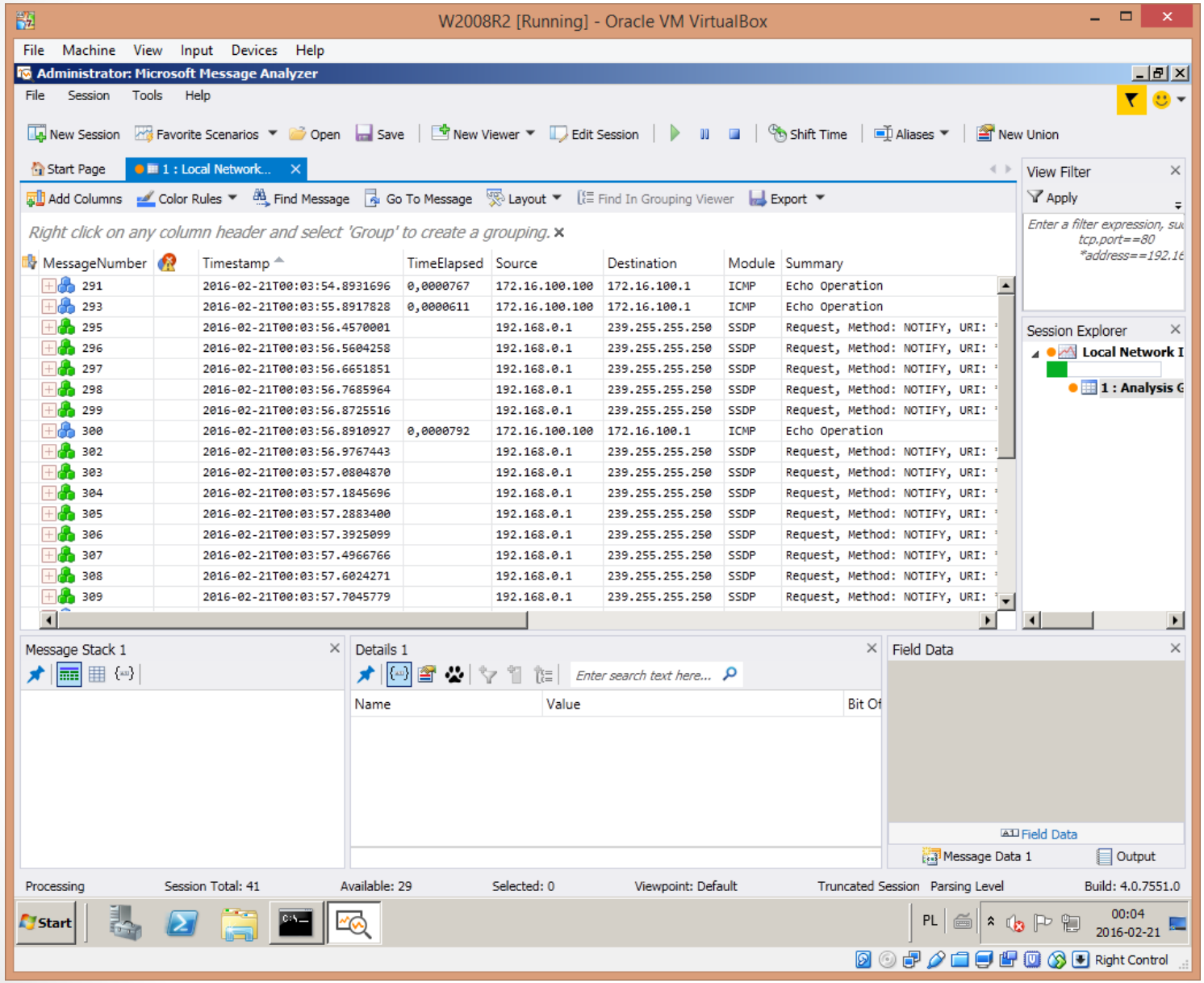


- https://technet.microsoft.com/en-us/library/jj819359.aspx

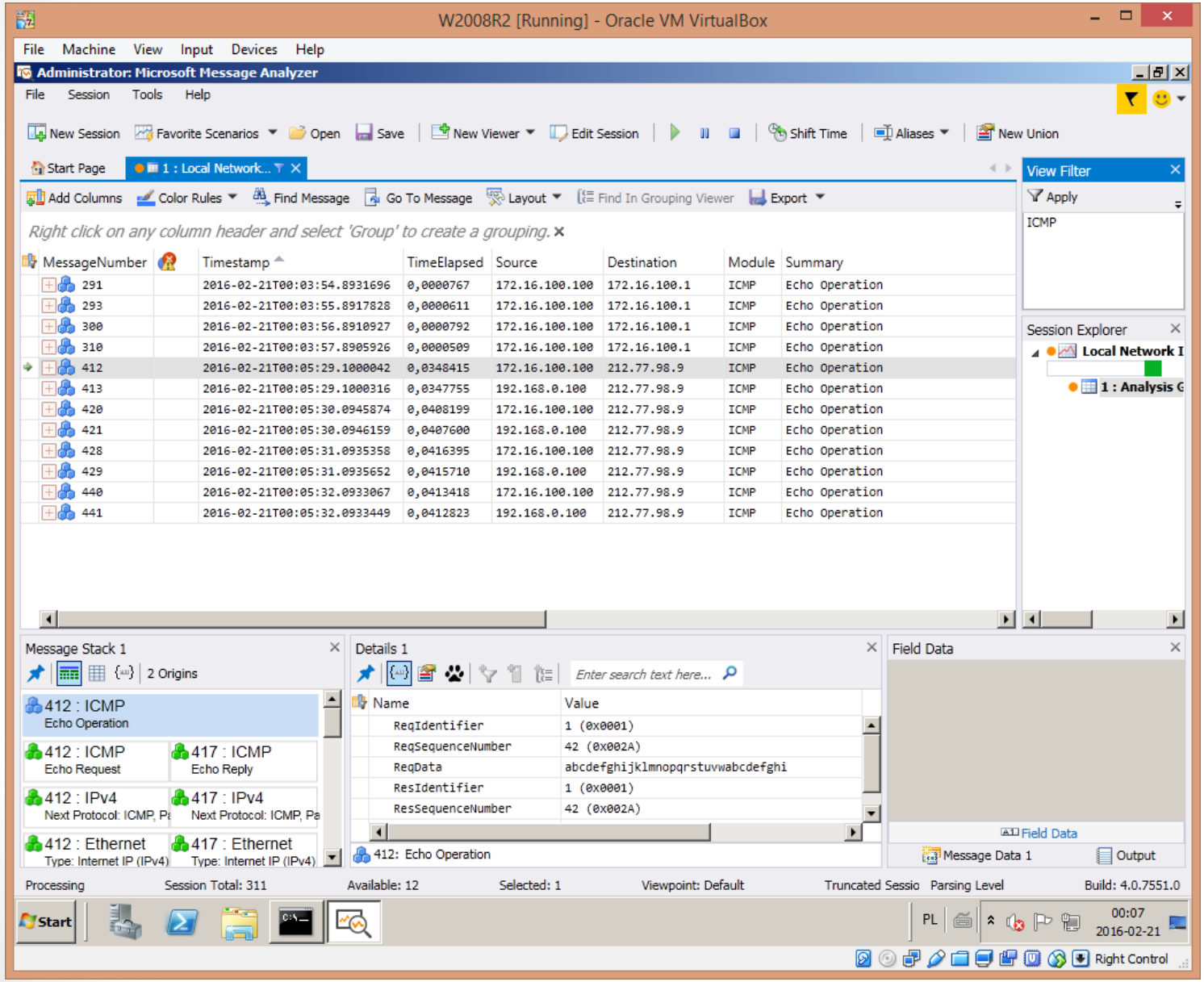
Microsoft Message Analyzer



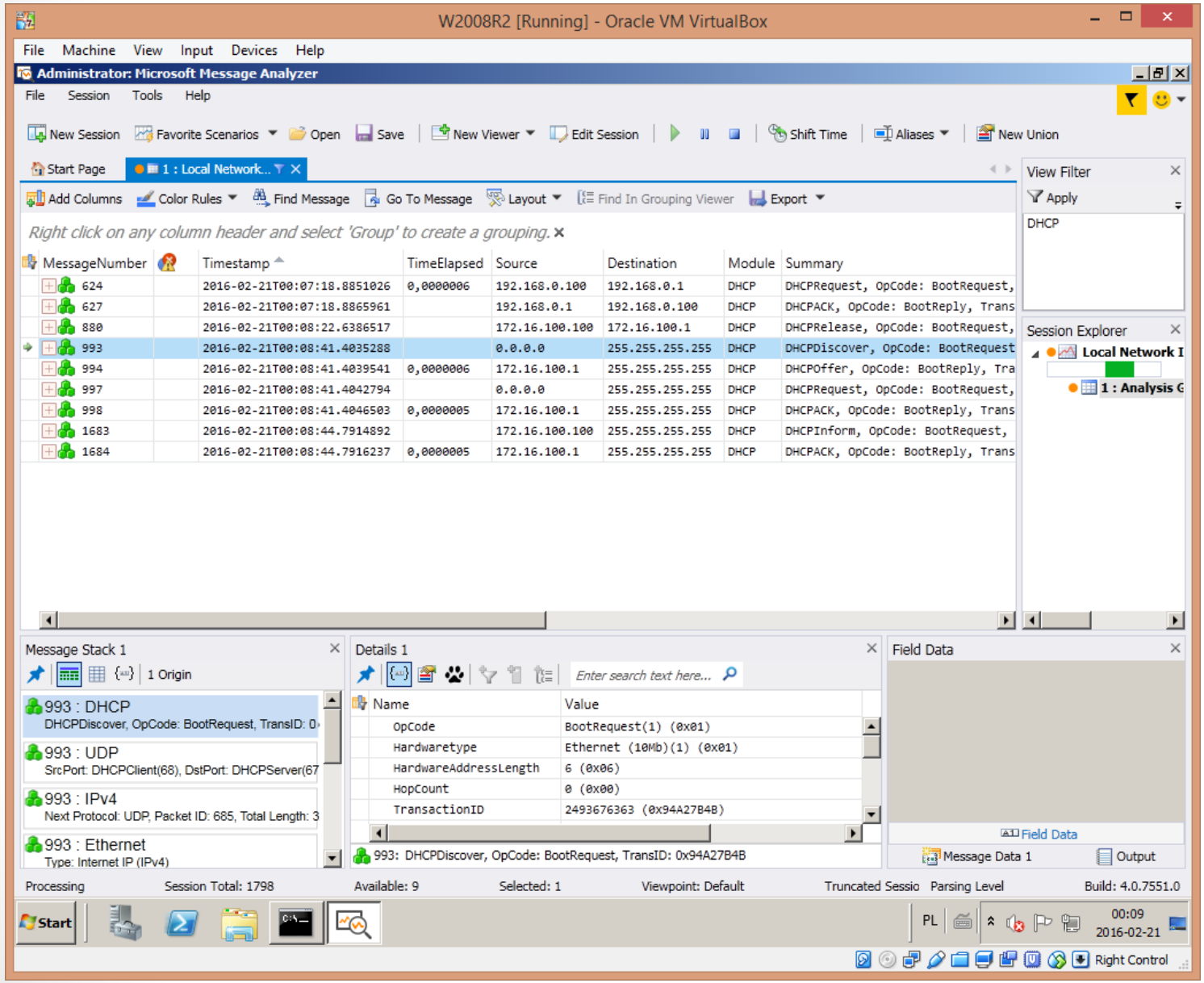
Microsoft Message Analyzer



Microsoft Message Analyzer

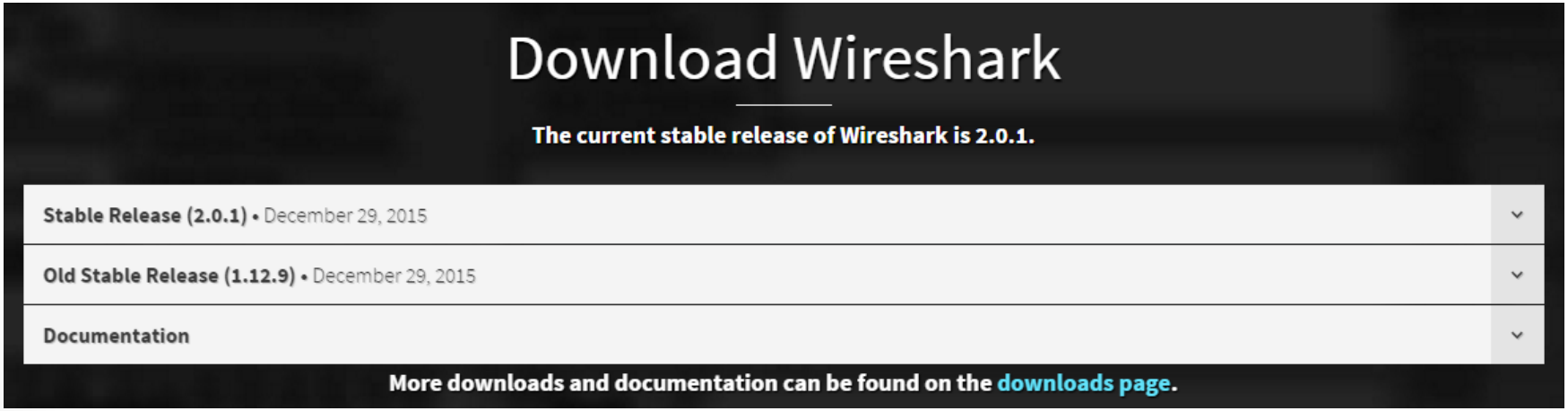


Microsoft Message Analyzer



Wireshark

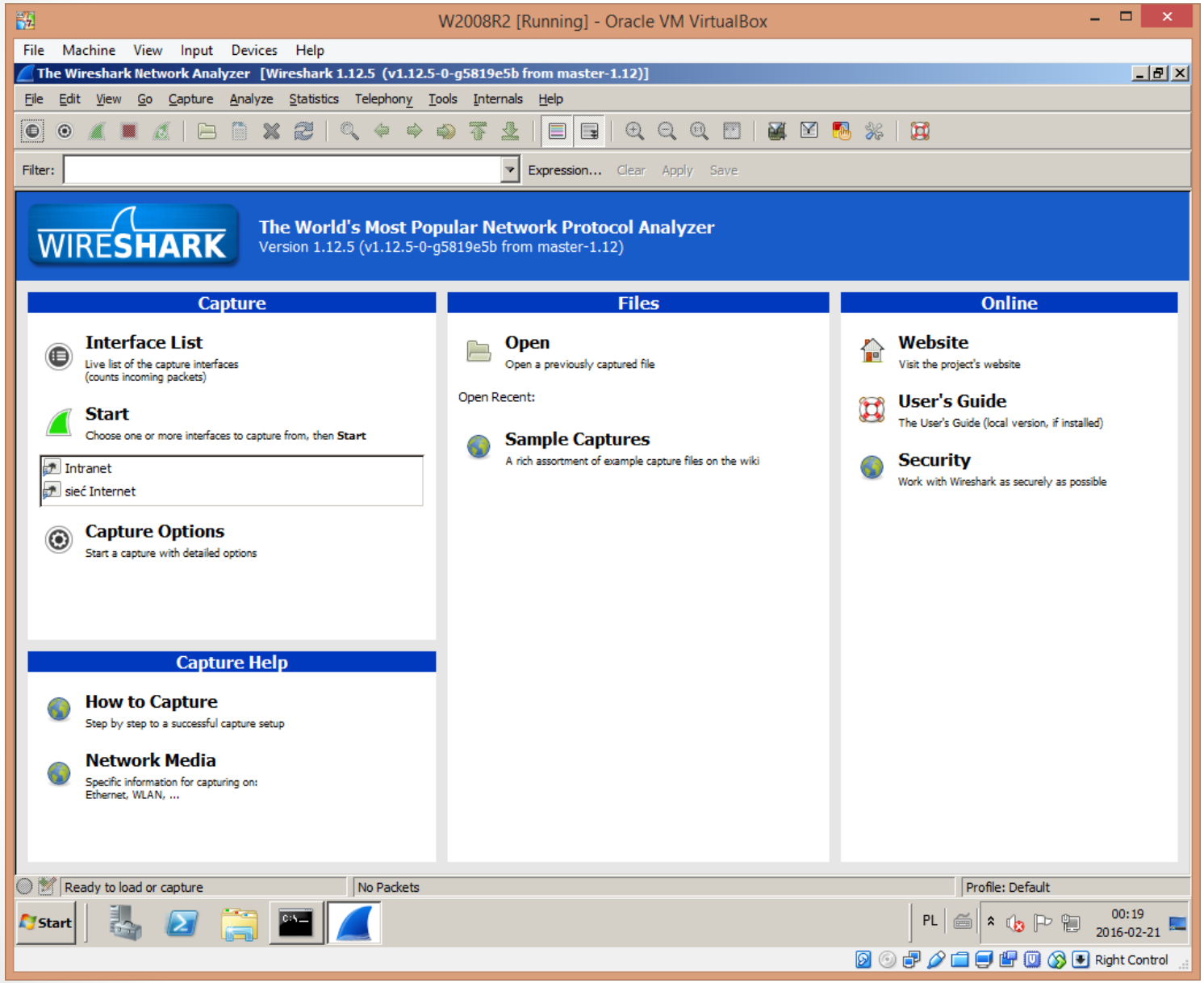
- Wireshark – sniffer będący wolnym oprogramowaniem. Umożliwia przechwytywanie i nagrywanie pakietów danych, a także ich dekodowanie.
- Dzięki dużej ilości pluginów potrafi rozpoznać i zdekodować wiele protokołów komunikacyjnych. W głównej mierze jest wykorzystywany przez administratorów sieci, służby specjalne oraz hackerów do śledzenia pakietów.



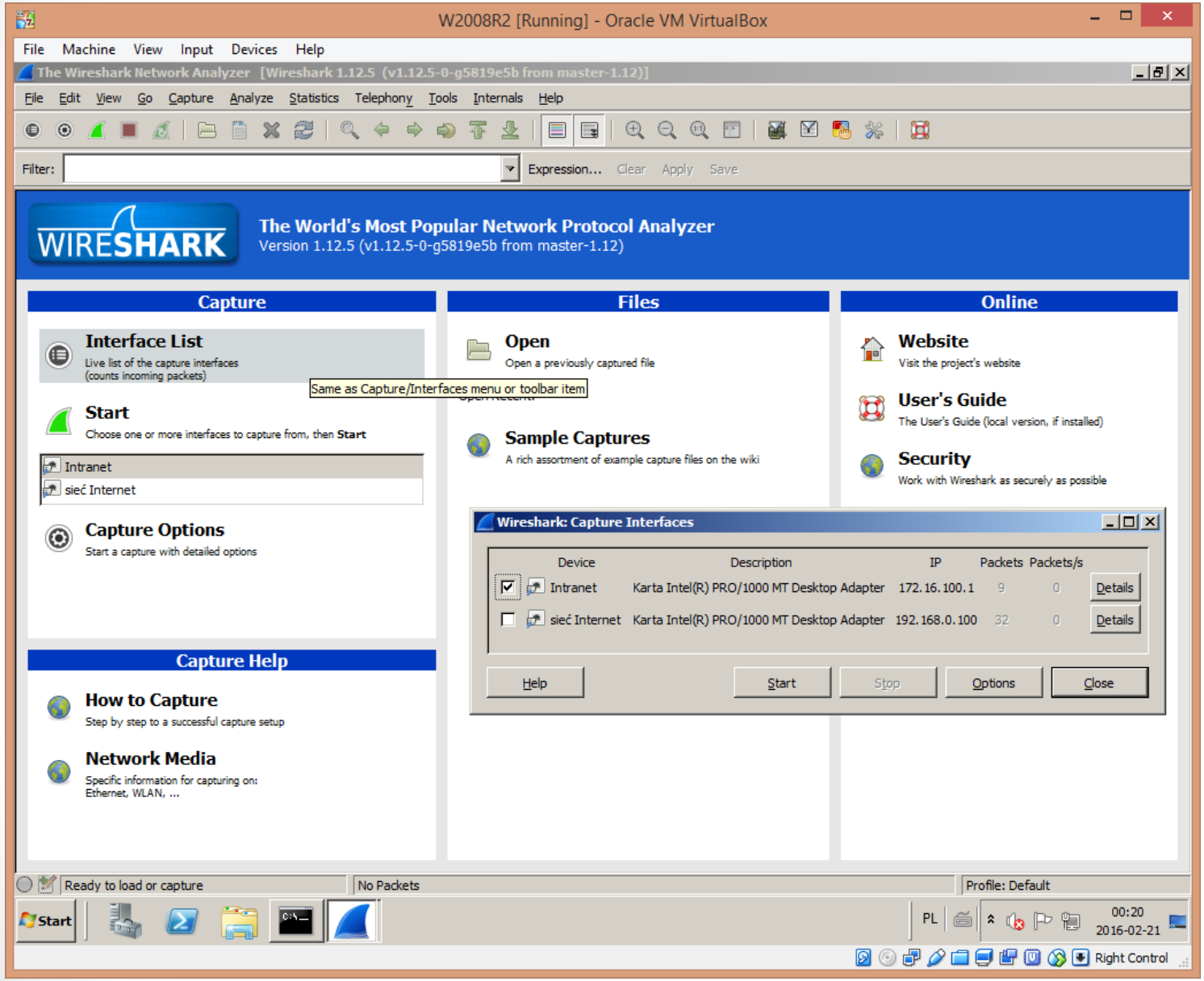
WIRESHARK

- https://www.wireshark.org/#download

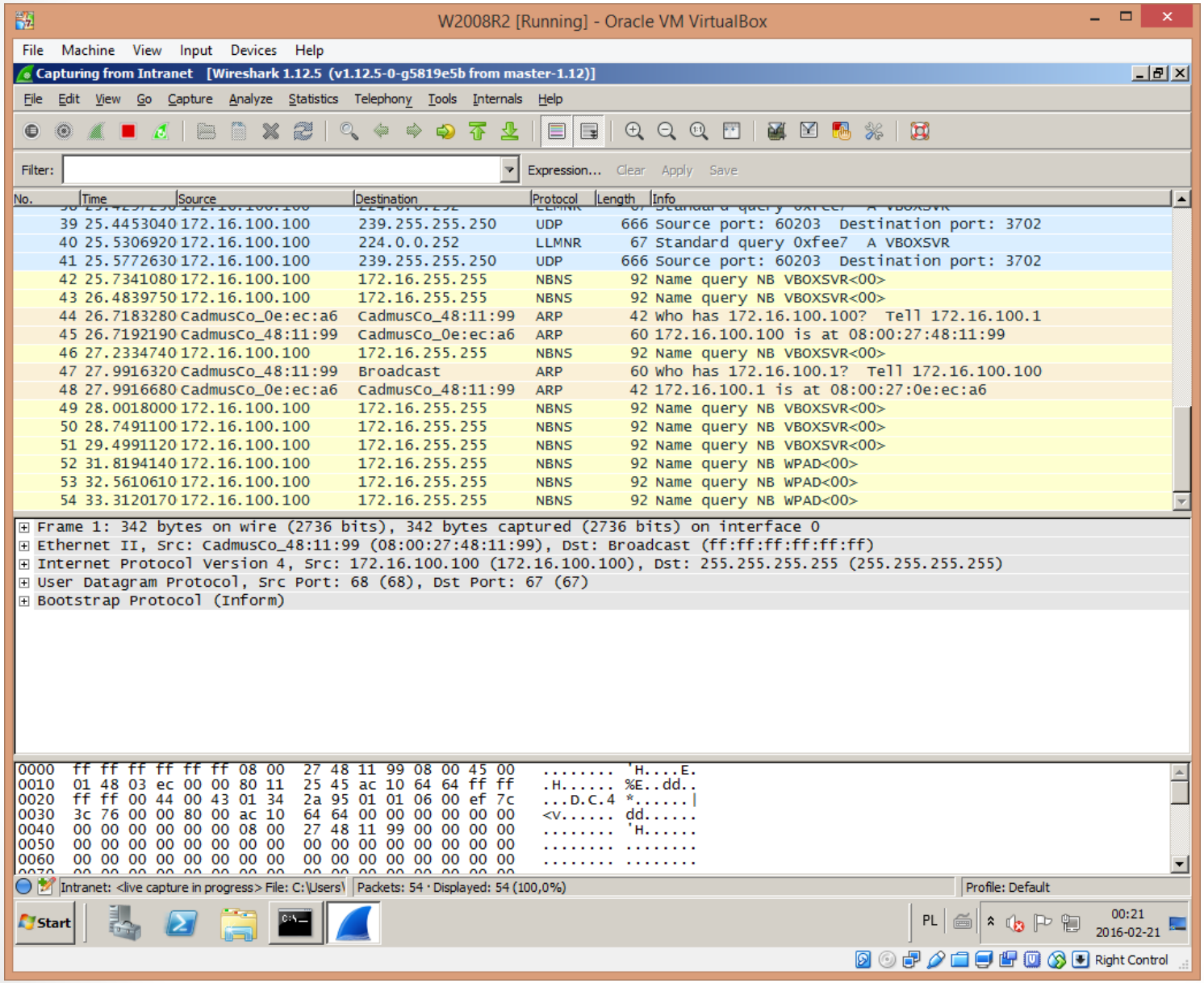
Wireshark


W2008R2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
The Wireshark Network Analyzer [Wireshark 1.12.5 (v1.12.5-0-g5819e5b from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
WIRESHARK
The World's Most Popular Network Protocol Analyzer
Version 1.12.5 (v1.12.5-0-g5819e5b from master-1.12)
Capture
Interface List
Live list of the capture interfaces
(counts incoming packets)
Start
Choose one or more interfaces to capture from, then Start
Intranet
sieć Internet
Capture Options
Start a capture with detailed options
Files
Open
Open a previously captured file
Open Recent:
Sample Captures
A rich assortment of example capture files on the wiki
Online
Website
Visit the project's website
User's Guide
The User's Guide (local version, if installed)
Security
Work with Wireshark as securely as possible
Capture Help
How to Capture
Step by step to a successful capture setup
Network Media
Specific information for capturing on:
Ethernet, WLAN, ...
Ready to load or capture
No Packets
Profile: Default
Start
PL
00:19
2016-02-21
Right Control

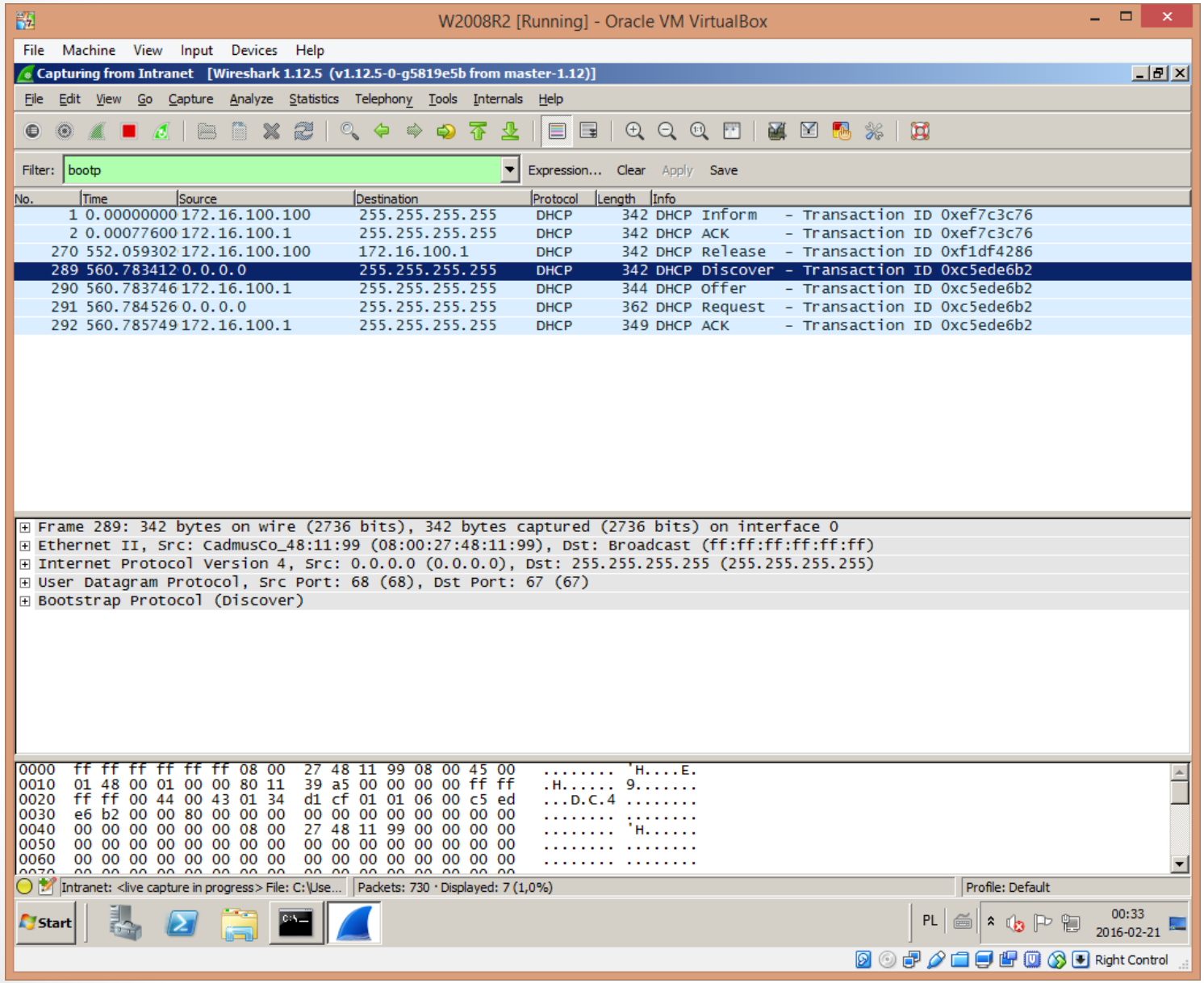
Wireshark


W2008R2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
The Wireshark Network Analyzer [Wireshark 1.12.5 (v1.12.5-0-g5819e5b from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
WIRESHARK
The World's Most Popular Network Protocol Analyzer
Version 1.12.5 (v1.12.5-0-g5819e5b from master-1.12)
Capture
Interface List
Live list of the capture interfaces
(counts incoming packets)
Same as Capture/Interfaces menu or toolbar item
Start
Choose one or more interfaces to capture from, then Start
Intranet
sieć Internet
Capture Options
Start a capture with detailed options
Files
Open
Open a previously captured file
Sample Captures
A rich assortment of example capture files on the wiki
Online
Website
Visit the project's website
User's Guide
The User's Guide (local version, if installed)
Security
Work with Wireshark as securely as possible
Capture Help
How to Capture
Step by step to a successful capture setup
Network Media
Specific information for capturing on:
Ethernet, WLAN, ...
Wireshark: Capture Interfaces
Device Description IP Packets Packets/s
Intranet Karta Intel(R) PRO/1000 MT Desktop Adapter 172.16.100.1 9 0 Details
sieć Internet Karta Intel(R) PRO/1000 MT Desktop Adapter 192.168.0.100 32 0 Details
Help Start Stop Options Close
Ready to load or capture
No Packets
Profile: Default
Start
PL
00:20
2016-02-21
Right Control

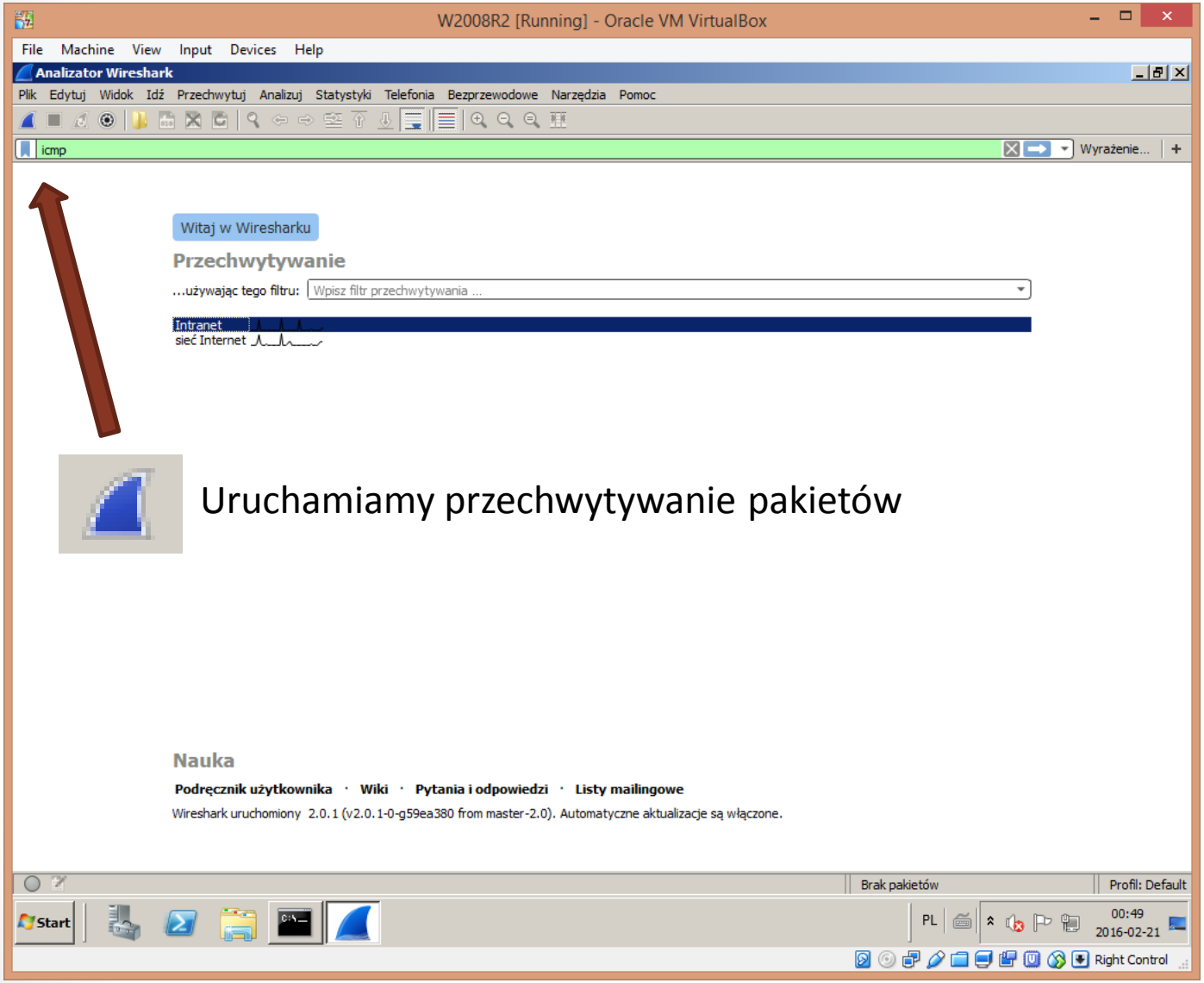
Wireshark


W2008R2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Capturing from Intranet [Wireshark 1.12.5 (v1.12.5-0-g5819e5b from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
39 25.4453040 172.16.100.100 239.255.255.250 UDP 666 Source port: 60203 Destination port: 3702
40 25.5306920 172.16.100.100 224.0.0.252 LLMNR 67 Standard query 0xfee7 A VBOXSVR
41 25.5772630 172.16.100.100 239.255.255.250 UDP 666 Source port: 60203 Destination port: 3702
42 25.7341080 172.16.100.100 172.16.255.255 NBNS 92 Name query NB VBOXSVR<00>
43 26.4839750 172.16.100.100 172.16.255.255 NBNS 92 Name query NB VBOXSVR<00>
44 26.7183280 CadmusCo_0e:ec:a6 CadmusCo_48:11:99 ARP 42 Who has 172.16.100.100? Tell 172.16.100.1
45 26.7192190 CadmusCo_48:11:99 CadmusCo_0e:ec:a6 ARP 60 172.16.100.100 is at 08:00:27:48:11:99
46 27.2334740 172.16.100.100 172.16.255.255 NBNS 92 Name query NB VBOXSVR<00>
47 27.9916320 CadmusCo_48:11:99 Broadcast ARP 60 Who has 172.16.100.1? Tell 172.16.100.100
48 27.9916680 CadmusCo_0e:ec:a6 CadmusCo_48:11:99 ARP 42 172.16.100.1 is at 08:00:27:0e:ec:a6
49 28.0018000 172.16.100.100 172.16.255.255 NBNS 92 Name query NB VBOXSVR<00>
50 28.7491100 172.16.100.100 172.16.255.255 NBNS 92 Name query NB VBOXSVR<00>
51 29.4991120 172.16.100.100 172.16.255.255 NBNS 92 Name query NB VBOXSVR<00>
52 31.8194140 172.16.100.100 172.16.255.255 NBNS 92 Name query NB WPAD<00>
53 32.5610610 172.16.100.100 172.16.255.255 NBNS 92 Name query NB WPAD<00>
54 33.3120170 172.16.100.100 172.16.255.255 NBNS 92 Name query NB WPAD<00>
Frame 1: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
Ethernet II, Src: CadmusCo_48:11:99 (08:00:27:48:11:99), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 172.16.100.100 (172.16.100.100), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: 68 (68), Dst Port: 67 (67)
Bootstrap Protocol (Inform)
0000 ff ff ff ff ff ff 08 00 27 48 11 99 08 00 45 00 .... 'H....E.
0010 01 48 03 ec 00 00 80 11 25 45 ac 10 64 64 ff ff .H...... %E..dd..
0020 ff ff 00 44 00 43 01 34 2a 95 01 01 06 00 ef 7c ...D.C.4 *......|
0030 3c 76 00 00 80 00 ac 10 64 64 00 00 00 00 00 00 <v...... dd......
0040 00 00 00 00 00 00 08 00 27 48 11 99 00 00 00 00 .... 'H......
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
Intranet: <live capture in progress> File: C:\Users\ Packets: 54 · Displayed: 54 (100,0%)
Profile: Default
Start
PL
00:21
2016-02-21
Right Control

Wireshark

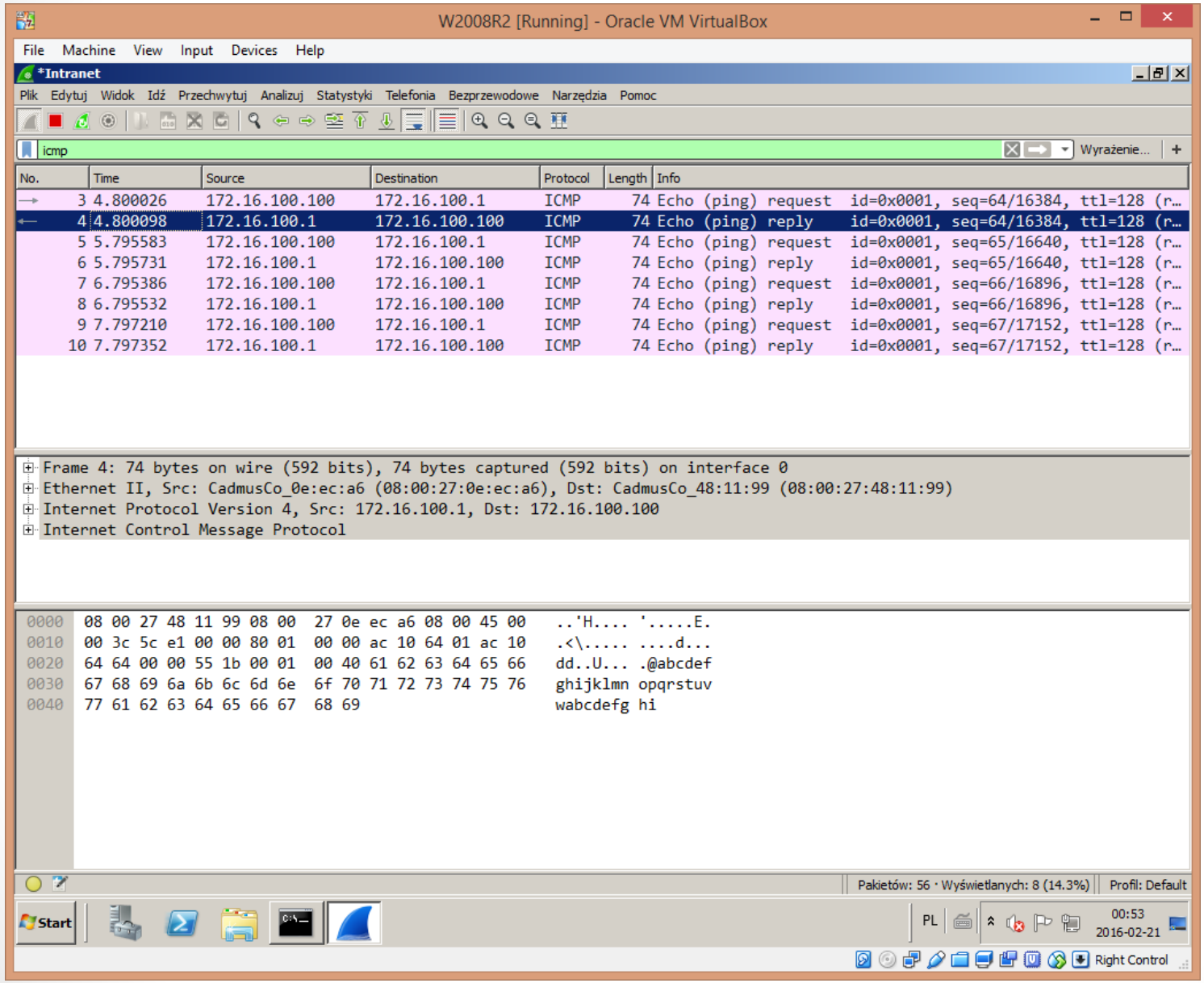

W2008R2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Capturing from Intranet [Wireshark 1.12.5 (v1.12.5-0-g5819e5b from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: bootp
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
1 0.00000000 172.16.100.100 255.255.255.255 DHCP 342 DHCP Inform - Transaction ID 0xef7c3c76
2 0.00077600 172.16.100.1 255.255.255.255 DHCP 342 DHCP ACK - Transaction ID 0xef7c3c76
270 552.059302 172.16.100.100 172.16.100.1 DHCP 342 DHCP Release - Transaction ID 0xf1df4286
289 560.783412 0.0.0.0 255.255.255.255 DHCP 342 DHCP Discover - Transaction ID 0xc5ede6b2
290 560.783746 172.16.100.1 255.255.255.255 DHCP 344 DHCP Offer - Transaction ID 0xc5ede6b2
291 560.784526 0.0.0.0 255.255.255.255 DHCP 362 DHCP Request - Transaction ID 0xc5ede6b2
292 560.785749 172.16.100.1 255.255.255.255 DHCP 349 DHCP ACK - Transaction ID 0xc5ede6b2
Frame 289: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
Ethernet II, Src: CadmusCo_48:11:99 (08:00:27:48:11:99), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: 68 (68), Dst Port: 67 (67)
Bootstrap Protocol (Discover)
0000 ff ff ff ff ff ff 08 00 27 48 11 99 08 00 45 00 .... 'H....E.
0010 01 48 00 01 00 00 80 11 39 a5 00 00 00 00 ff ff .H...... 9.......
0020 ff ff 00 44 00 43 01 34 d1 cf 01 01 06 00 c5 ed ...D.C.4 ....
0030 e6 b2 00 00 80 00 00 00 00 00 00 00 00 00 00 00 ....
0040 00 00 00 00 00 00 08 00 27 48 11 99 00 00 00 00 .... 'H......
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
Intranet: <live capture in progress> File: C:\Use...
Packets: 730 · Displayed: 7 (1,0%)
Profile: Default
Start
PL
00:33
2016-02-21
Right Control

Wireshark

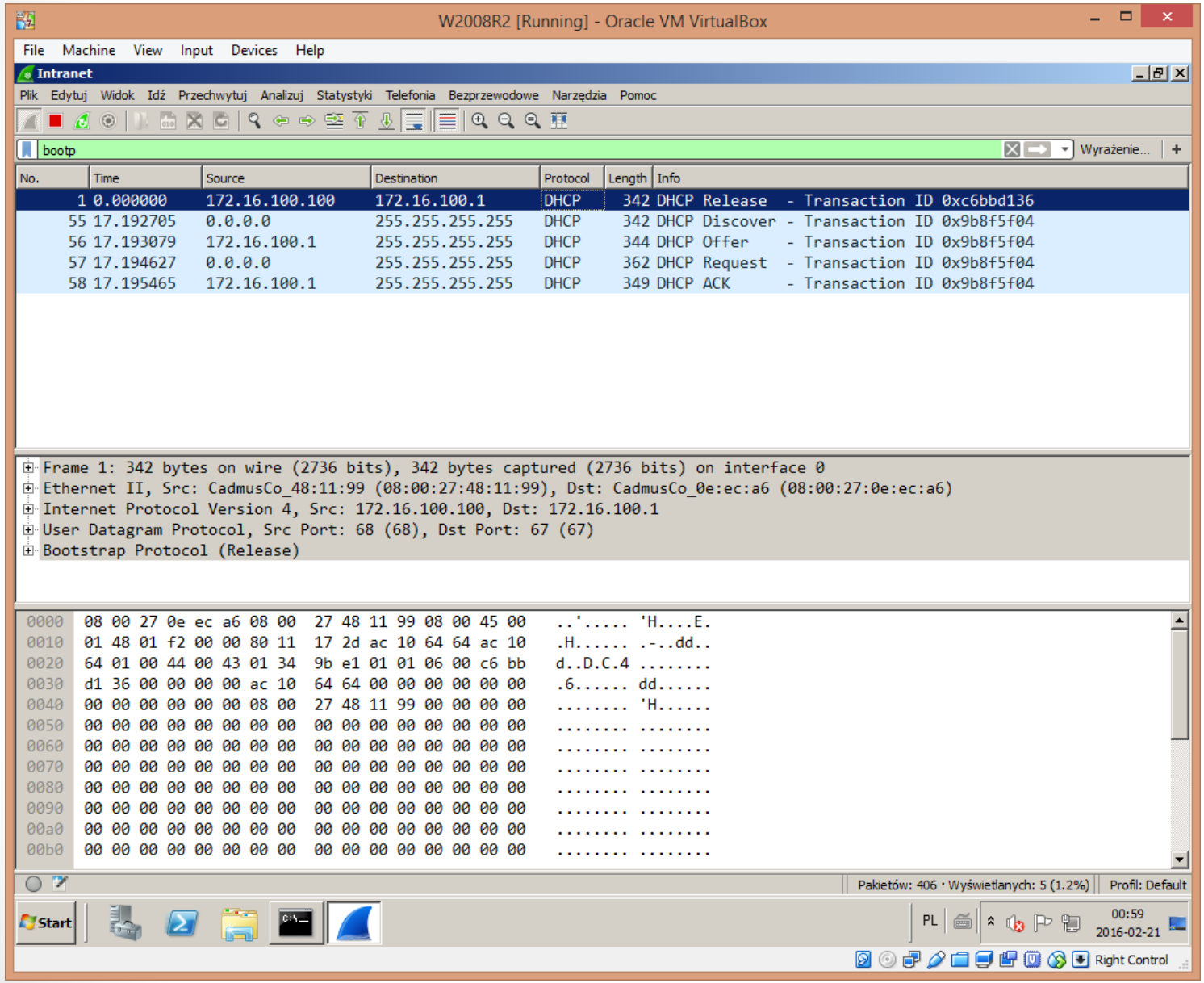


- **Wireshark** – w nowej odsłonie

Wireshark


W2008R2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
*Intranet
Plik Edytuj Widok Idź Przechwytuj Analizuj Statystyki Telefonia Bezprzewodowe Narzędzia Pomoc
icmp
Wyrażenie...
No. Time Source Destination Protocol Length Info
3 4.800026 172.16.100.100 172.16.100.1 ICMP 74 Echo (ping) request id=0x0001, seq=64/16384, ttl=128 (r...
4 4.800098 172.16.100.1 172.16.100.100 ICMP 74 Echo (ping) reply id=0x0001, seq=64/16384, ttl=128 (r...
5 5.795583 172.16.100.100 172.16.100.1 ICMP 74 Echo (ping) request id=0x0001, seq=65/16640, ttl=128 (r...
6 5.795731 172.16.100.1 172.16.100.100 ICMP 74 Echo (ping) reply id=0x0001, seq=65/16640, ttl=128 (r...
7 6.795386 172.16.100.100 172.16.100.1 ICMP 74 Echo (ping) request id=0x0001, seq=66/16896, ttl=128 (r...
8 6.795532 172.16.100.1 172.16.100.100 ICMP 74 Echo (ping) reply id=0x0001, seq=66/16896, ttl=128 (r...
9 7.797210 172.16.100.100 172.16.100.1 ICMP 74 Echo (ping) request id=0x0001, seq=67/17152, ttl=128 (r...
10 7.797352 172.16.100.1 172.16.100.100 ICMP 74 Echo (ping) reply id=0x0001, seq=67/17152, ttl=128 (r...
Frame 4: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: CadmusCo_0e:ec:a6 (08:00:27:0e:ec:a6), Dst: CadmusCo_48:11:99 (08:00:27:48:11:99)
Internet Protocol Version 4, Src: 172.16.100.1, Dst: 172.16.100.100
Internet Control Message Protocol
0000 08 00 27 48 11 99 08 00 27 0e ec a6 08 00 45 00 ..'H.... '.....E.
0010 00 3c 5c e1 00 00 80 01 00 00 ac 10 64 01 ac 10 .<\..... ....d...
0020 64 64 00 00 55 1b 00 01 00 40 61 62 63 64 65 66 dd..U... .@abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv
0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi
Pakietów: 56 · Wyświetlanych: 8 (14.3%)
Profil: Default
Start
PL
00:53
2016-02-21
Right Control

Wireshark

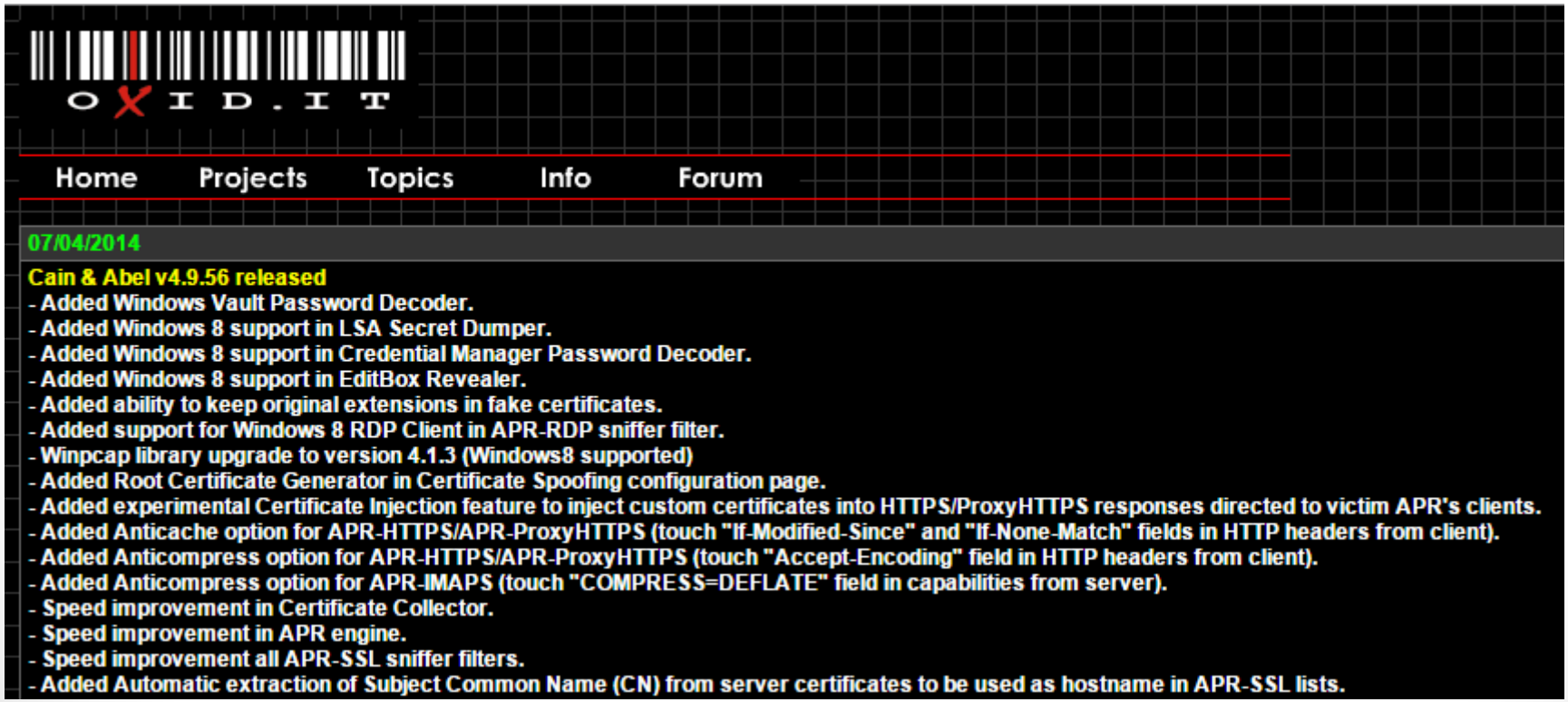

W2008R2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Intranet
Plik Edytuj Widok Idź Przechwytuj Analizuj Statystyki Telefonia Bezprzewodowe Narzędzia Pomoc
bootp
Wyrażenie...
No. Time Source Destination Protocol Length Info
1 0.000000 172.16.100.100 172.16.100.1 DHCP 342 DHCP Release - Transaction ID 0xc6bbd136
55 17.192705 0.0.0.0 255.255.255.255 DHCP 342 DHCP Discover - Transaction ID 0x9b8f5f04
56 17.193079 172.16.100.1 255.255.255.255 DHCP 344 DHCP Offer - Transaction ID 0x9b8f5f04
57 17.194627 0.0.0.0 255.255.255.255 DHCP 362 DHCP Request - Transaction ID 0x9b8f5f04
58 17.195465 172.16.100.1 255.255.255.255 DHCP 349 DHCP ACK - Transaction ID 0x9b8f5f04
Frame 1: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
Ethernet II, Src: CadmusCo_48:11:99 (08:00:27:48:11:99), Dst: CadmusCo_0e:ec:a6 (08:00:27:0e:ec:a6)
Internet Protocol Version 4, Src: 172.16.100.100, Dst: 172.16.100.1
User Datagram Protocol, Src Port: 68 (68), Dst Port: 67 (67)
Bootstrap Protocol (Release)
0000 08 00 27 0e ec a6 08 00 27 48 11 99 08 00 45 00 ..'..... 'H....E.
0010 01 48 01 f2 00 00 80 11 17 2d ac 10 64 64 ac 10 .H..... .-..dd..
0020 64 01 00 44 00 43 01 34 9b e1 01 01 06 00 c6 bb d..D.C.4 ....
0030 d1 36 00 00 00 00 ac 10 64 64 00 00 00 00 00 00 .6...... dd......
0040 00 00 00 00 00 00 08 00 27 48 11 99 00 00 00 00 .... 'H......
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
Pakietów: 406 · Wyświetlanych: 5 (1.2%)
Profil: Default
Start
PL
00:59
2016-02-21
Right Control

Wireshark – ćwiczenia (mat. CISCO)

- Używanie programu Wireshark do badania ruchu sieciowego
  3.3.3.4 Lab - Using Wireshark to View Network Traffic
- Wykorzystanie programu Wireshark do badania ramek Ethernet
  5.1.4.3 Lab - Using Wireshark to Examine Ethernet Frames – ILM
- Badanie protokołu ARP w wierszu poleceń systemu Windows, wierszu poleceń IOS oraz w programie Wireshark
  5.2.1.8 Lab - Observing ARP with the Windows CLI, IOS CLI, and Wireshark - ILM
- Użytkowanie programu Wireshark do obserwacji mechanizmu uzgadniania trójetapowego TCP
  7.2.1.8 Lab - Using Wireshark to Observe the TCP 3-Way Handshake – ILM
- Przechwytywanie i badanie datagramów DNS w programie Wireshark *7.2.3.5 Lab - Using Wireshark to Examine a UDP DNS Capture – ILM*
- Użytkowanie programu Wireshark do przechwytywania danych pochodzących z protokołu FTP i TFTP
  7.2.4.3 Lab - Using Wireshark to Examine FTP and TFTP Captures - ILM

Cain & Abel

- Aplikacja pozwala w stosunkowo łatwy sposób odzyskać różnego rodzaju hasła dzięki takim metodom jak podsłuchiwanie sieci, crackowanie zaszyfrowanych haseł stosując słowniki, rejestrowanie połączeń VoIP, dekodowanie pomieszanych haseł, odzyskiwanie kluczy sieci bezprzewodowych, wykrywanie ukrytych haseł czy analizowanie protokołów.



- http://www.oxid.it/index.html

linki

- https://www.microsoft.com/en-us/download/details.aspx?id=4865
- https://www.microsoft.com/en-us/download/details.aspx?id=44226
- https://technet.microsoft.com/en-us/library/jj819359.aspx
- https://www.wireshark.org/#download
- http://www.oxid.it/index.html

KONIEC