

Windows Serwer 2008 R2

Moduł 7. Monitoring ruchu sieciowego

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.

Microsoft Network Monitor 3.4 (archive)

Language: English

Download

Network Monitor 3.4 is the archive versioned tool for network traffic capture and protocol analysis. Download Microsoft Message Analyzer for updated parser support.

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

Microsoft Network Monitor

The screenshot shows the Microsoft Network Monitor 3.4 application window. The main area is divided into two panes. The left pane, titled 'Recent Captures', contains the text 'Tutaj rozpoczynamy nową sesję monitoringu' (Here we start a new monitoring session). The right pane, titled 'Getting Started with Microsoft Network Monitor 3.4', displays a 'Welcome to Microsoft Network Monitor 3.4' message and a 'What's New' section with three bullet points: 'User Interface Refresh', 'Parser Configuration Management', and 'Column Management'. Below the panes is a 'Select Networks' dialog box with a table of network interfaces. The 'Intranet' interface is selected.

Friendly Name	Description	IPv4 Address
<input checked="" type="checkbox"/> Intranet	Karta Intel(R) PRO/1000 MT Desktop Adapter #2	172.16.100.1
<input type="checkbox"/> isatap.{8C3B1DC6-FAEF-4A79-B0AD-F587E9B87FAB}	Karta Microsoft ISATAP #2	None
<input type="checkbox"/> isatap.{A83118C8-DA09-47E3-A1C2-74A2698D3B56}	Karta Microsoft ISATAP	None
<input type="checkbox"/> NDISWANBH	WAN Miniport	None
<input type="checkbox"/> Połączenie lokalne* 4	Teredo Tunneling Pseudo-Interface	None
<input type="checkbox"/> sieć Internet	Karta Intel(R) PRO/1000 MT Desktop Adapter	192.168.0.100

- Wybieramy interfejs, który będziemy monitorować: „Intranet”

Microsoft Network Monitor

The screenshot displays the Microsoft Network Monitor 3.4 interface within an Oracle VM VirtualBox window. The application is running on a machine named 'W2008R2 [Running]'. The interface includes a menu bar (File, Machine, View, Input, Devices, Help), a toolbar with options like 'New Capture', 'Open Capture', 'Save As', 'Capture Settings', 'Start', 'Pause', and 'Stop', and a 'Parsers' section.

The main area is divided into several panes:

- Network Conversations:** A tree view on the left showing 'All Traffic', 'My Traffic', and 'Other Traffic'.
- Display Filter:** A pane for applying filters to the captured traffic.
- Frame Summary:** A table listing captured frames with columns for Frame Number, Time Date Local Adjusted, Time Offset, Process Name, Source, Destination, Protocol Name, and Description.
- Frame Details:** A pane for viewing the details of a selected frame.
- Hex Details:** A pane for viewing the hexadecimal representation of the selected frame.

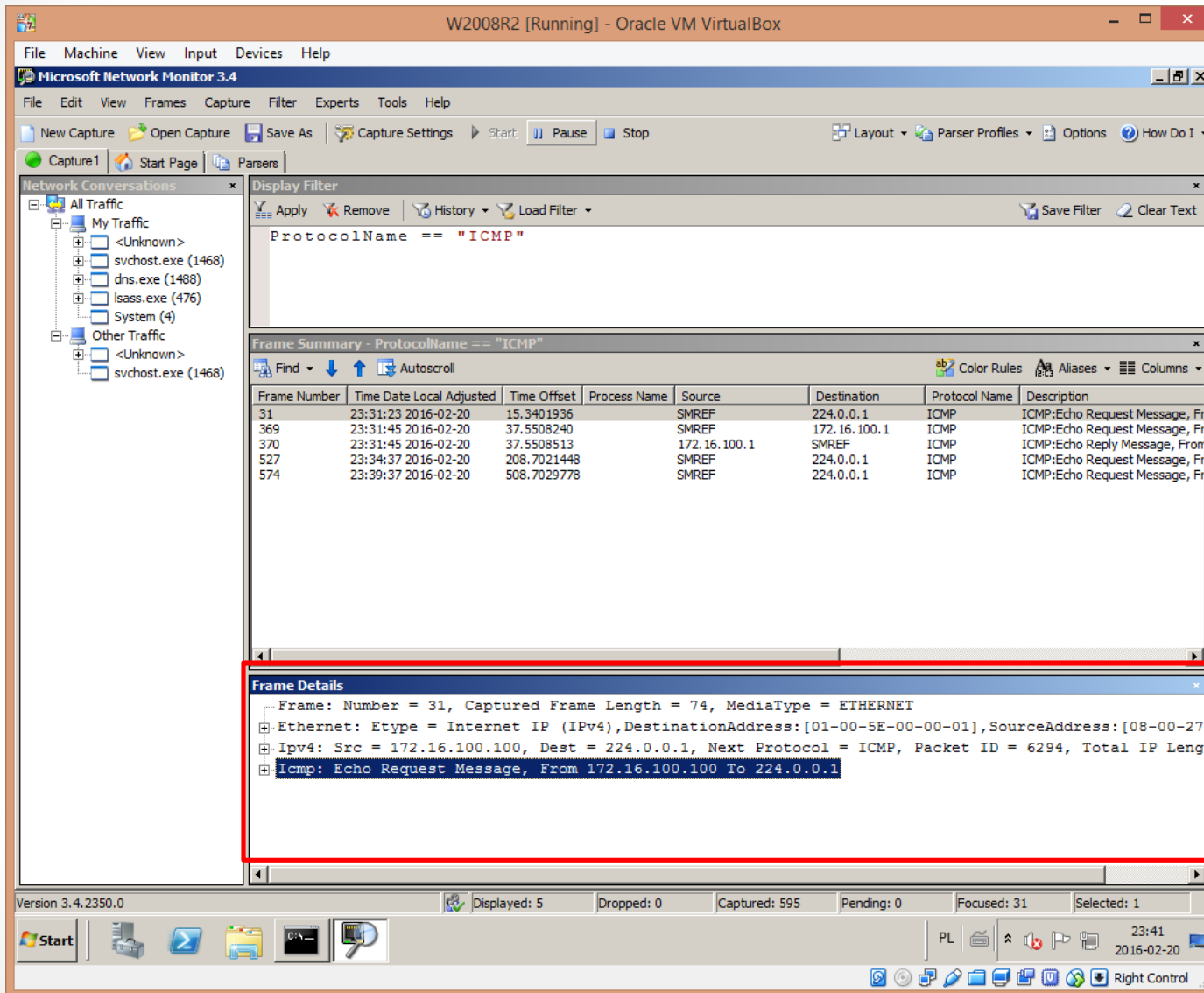
The Frame Summary table contains the following data:

Frame Number	Time Date Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description
1	23:01:17 2016-02-20	5.4971635				NetmonFilter	NetmonFilter:Updated Capture Filter
2	23:01:17 2016-02-20	5.4971635				NetworkInfoEx	NetworkInfoEx:Network info for , Ne
3	23:01:17 2016-02-20	5.4971635		192.168.0.1	239.255.255.250	SSDP	SSDP:Request, NOTIFY *
4	23:01:17 2016-02-20	5.6006436		192.168.0.1	239.255.255.250	SSDP	SSDP:Request, NOTIFY *
5	23:01:17 2016-02-20	5.7048599		192.168.0.1	239.255.255.250	SSDP	SSDP:Request, NOTIFY *
6	23:01:17 2016-02-20	5.8088188		192.168.0.1	239.255.255.250	SSDP	SSDP:Request, NOTIFY *
7	23:01:17 2016-02-20	5.9135112		192.168.0.1	239.255.255.250	SSDP	SSDP:Request, NOTIFY *
8	23:01:18 2016-02-20	6.0169373		192.168.0.1	239.255.255.250	SSDP	SSDP:Request, NOTIFY *
9	23:01:18 2016-02-20	6.1227130		192.168.0.1	239.255.255.250	SSDP	SSDP:Request, NOTIFY *
10	23:01:18 2016-02-20	6.2247395		192.168.0.1	239.255.255.250	SSDP	SSDP:Request, NOTIFY *
11	23:01:18 2016-02-20	6.3287071		192.168.0.1	239.255.255.250	SSDP	SSDP:Request, NOTIFY *
12	23:01:18 2016-02-20	6.4341714		192.168.0.1	239.255.255.250	SSDP	SSDP:Request, NOTIFY *
13	23:01:18 2016-02-20	6.5366128		192.168.0.1	239.255.255.250	SSDP	SSDP:Request, NOTIFY *
14	23:01:18 2016-02-20	6.6405709		192.168.0.1	239.255.255.250	SSDP	SSDP:Request, NOTIFY *
15	23:01:18 2016-02-20	6.7446528		192.168.0.1	239.255.255.250	SSDP	SSDP:Request, NOTIFY *
16	23:01:30 2016-02-20	18.0452773		192.168.0.100	239.255.255.250	IGMP	IGMP:IGMPv2 Membership Report

The status bar at the bottom shows: Parsed: 32, Displayed: 33, Dropped: 0, Captured: 34, Pending: 0, Focused: , Selected: . The system tray shows the time as 23:01 on 2016-02-20.

- Rozpoczynamy przechwytywanie - **Start**

Microsoft Network Monitor



W2008R2 [Running] - Oracle VM VirtualBox

Microsoft Network Monitor 3.4

File Edit View Frames Capture Filter Experts Tools Help

New Capture Open Capture Save As Capture Settings Start Pause Stop

Layout Parser Profiles Options How Do I

Capture1 Start Page Parsers

Network Conversations

- All Traffic
 - My Traffic
 - <Unknown>
 - svchost.exe (1468)
 - dns.exe (1488)
 - lsass.exe (476)
 - System (4)
 - Other Traffic
 - <Unknown>
 - svchost.exe (1468)

Display Filter

Apply Remove History Load Filter Save Filter Clear Text

ProtocolName == "ICMP"

Frame Summary - ProtocolName == "ICMP"

Find Autoscroll Color Rules Aliases Columns

Frame Number	Time Date Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description
31	23:31:23 2016-02-20	15.3401936	SMREF	224.0.0.1	ICMP	ICMP:Echo Request Message, Fr	
369	23:31:45 2016-02-20	37.5508240	SMREF	172.16.100.1	ICMP	ICMP:Echo Request Message, Fr	
370	23:31:45 2016-02-20	37.5508513	SMREF	172.16.100.1	ICMP	ICMP:Echo Reply Message, Fron	
527	23:34:37 2016-02-20	208.7021448	SMREF	224.0.0.1	ICMP	ICMP:Echo Request Message, Fr	
574	23:39:37 2016-02-20	508.7029778	SMREF	224.0.0.1	ICMP	ICMP:Echo Request Message, Fr	

Frame Details

Frame: Number = 31, Captured Frame Length = 74, MediaType = ETHERNET

- Ethernet: Etype = Internet IP (IPv4), DestinationAddress: [01-00-5E-00-00-01], SourceAddress: [08-00-27-...
- Ipv4: Src = 172.16.100.100, Dest = 224.0.0.1, Next Protocol = ICMP, Packet ID = 6294, Total IP Leng
- Icmp: Echo Request Message, From 172.16.100.100 To 224.0.0.1

Version 3.4.2350.0

Displayed: 5 Dropped: 0 Captured: 595 Pending: 0 Focused: 31 Selected: 1

Start

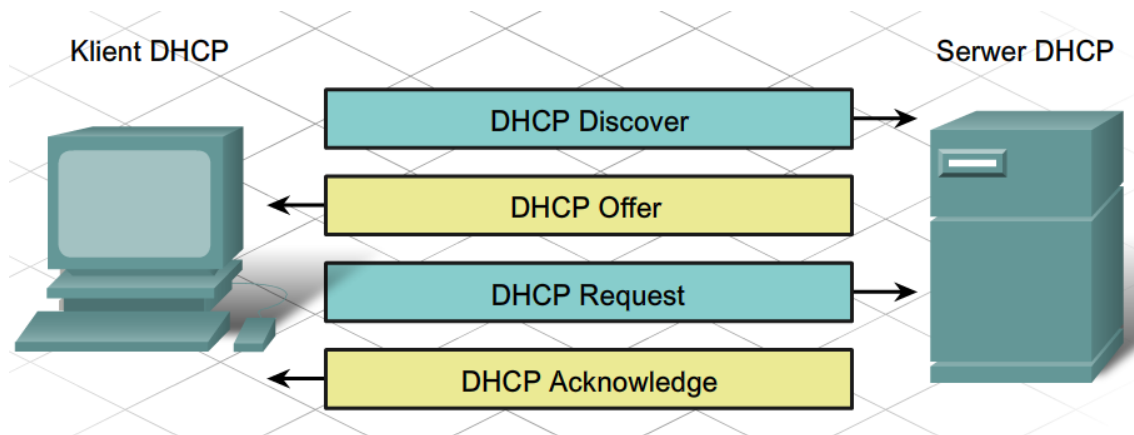
PL 23:41 2016-02-20

Right Control

- 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

W2008R2 [Running] - Oracle VM VirtualBox

Microsoft Network Monitor 3.4

File Edit View Frames Capture Filter Experts Tools Help

New Capture Open Capture Save As Capture Settings Start Pause Stop Layout Parser Profiles Options How Do I

Capture1 Start Page Parsers

Network Conversations

- All Traffic
 - My Traffic
 - <Unknown>
 - svchost.exe (1468)
 - dns.exe (1488)
 - lsass.exe (476)
 - System (4)
 - Other Traffic
 - <Unknown>
 - svchost.exe (1468)

Display Filter

Apply Remove History Load Filter Save Filter Clear Text

ProtocolName == "DHCP"

Frame Summary - ProtocolName == "DHCP"

Time Offset	Process Name	Source	Destination	Protocol Name	Description
15.3267786	svchost.exe	0.0.0.0	255.255.255.255	DHCP	DHCP:Request, MsgType = DISCOVER, TransactionID = 0x5D0CE7B4
15.3270527	svchost.exe	172.16.100.1	255.255.255.255	DHCP	DHCP:Reply, MsgType = OFFER, TransactionID = 0x5D0CE7B4
15.3275535	svchost.exe	0.0.0.0	255.255.255.255	DHCP	DHCP:Request, MsgType = REQUEST, TransactionID = 0x5D0CE7B4
15.3340983	svchost.exe	172.16.100.1	255.255.255.255	DHCP	DHCP:Reply, MsgType = ACK, TransactionID = 0x5D0CE7B4
60.9541189	svchost.exe	SMREF	172.16.100.1	DHCP	DHCP:Request, MsgType = REQUEST, TransactionID = 0x3DC4CEB6
60.9545609	svchost.exe	172.16.100.1	SMREF	DHCP	DHCP:Reply, MsgType = ACK, TransactionID = 0x3DC4CEB6

Frame Details

Frame: Number = 435, Captured Frame Length = 350, MediaType = ETHERNET

- Ethernet: Etype = Internet IP (IPv4), DestinationAddress: [08-00-27-0E-EC-A6], SourceAddress: [08-00-27-0E-EC-A6]
- Ipv4: Src = 172.16.100.100, Dest = 172.16.100.1, Next Protocol = UDP, Packet ID = 238, Total IP Len = 350
- Udp: SrcPort = BOOTP client (68), DstPort = BOOTP server (67), Length = 316
- Dhcp: Request, MsgType = REQUEST, TransactionID = 0x3DC4CEB6

Version 3.4.2350.0

Displayed: 6 Dropped: 0 Captured: 491 Pending: 0 Focused: 435 Selected: 1

Start

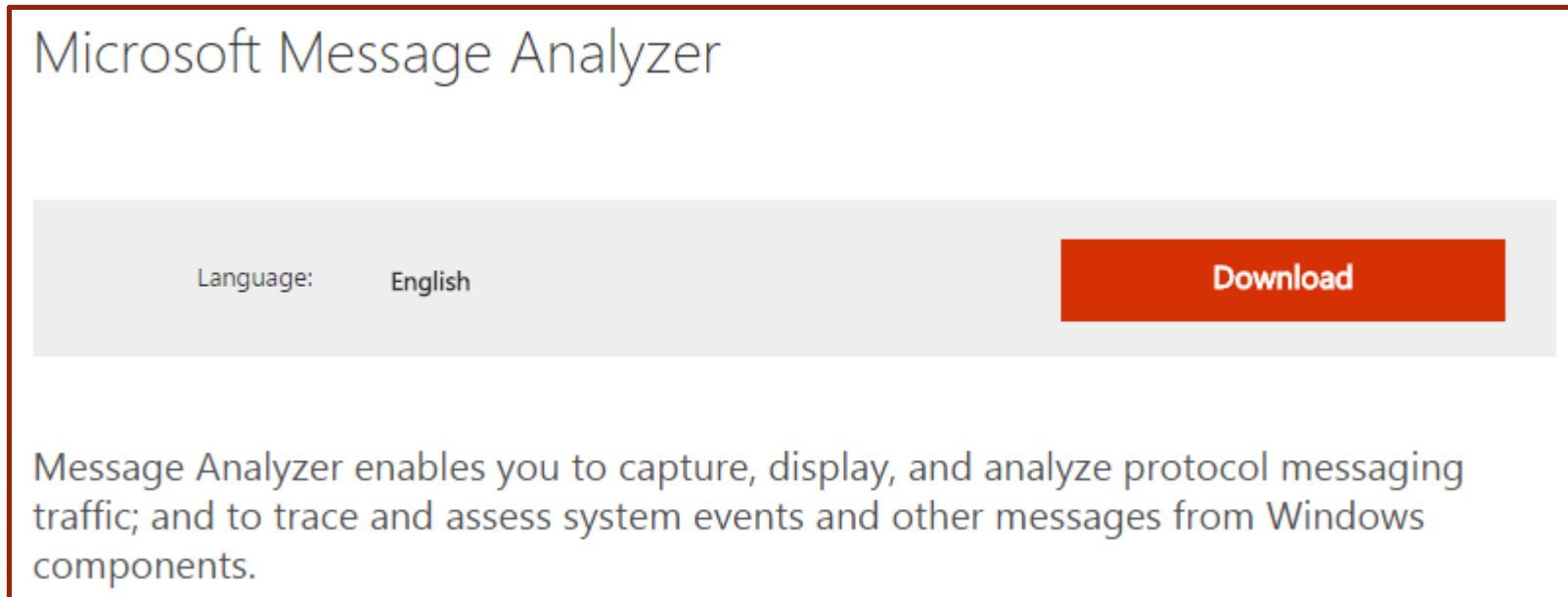
PL 23:32 2016-02-20

Right Control

- Obserwujemy ruch DHCP

Microsoft Message Analyzer

- Message Analyzer to następcą 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.



Microsoft Message Analyzer

Language: English [Download](#)

Message Analyzer enables you to capture, display, and analyze protocol messaging traffic; and to trace and assess system events and other messages from Windows components.

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

Microsoft Message Analyzer

The screenshot shows the Microsoft TechNet website interface. At the top, there is a navigation bar with links for TechNet, Products, IT Resources, Downloads, Training, and Support. Below this is the Microsoft logo and the TechNet logo. A search bar is present with the text 'Search TechNet with Bing'. The main navigation menu includes Home, Library (highlighted), Wiki, Learn, Gallery, Downloads, Support, Forums, and Blogs. On the right side of the page, there are buttons for 'Any suggestions?', 'Export (0)', and 'Print'.

Getting Started with Message Analyzer

Message Analyzer takes new approaches to capturing, displaying, and analyzing message traffic, making it vastly different than other tools you may have used. Before you begin using Message Analyzer to capture live messages or retrieve data from saved message files and logs, you should familiarize yourself with its technologies and features. To advance your understanding of Message Analyzer and to get started quickly with its features, you are strongly advised to at least examine the feature summary and review the Message Analyzer Tutorial that are each described in this section. After doing so, you should give Message Analyzer a try by performing the *Quick Start Procedures* indicated below.

In This Section

- Installing and Upgrading Message Analyzer** — learn how to install and upgrade Message Analyzer, in addition to preserving user-created assets from an existing Message Analyzer installation.
- Message Analyzer Feature Summary** — review a feature summary and get an overview of Message Analyzer capabilities and functions.
- Quick Session Startup** — discover how you can very quickly acquire input data for Message Analyzer with as little as a single click.
- Technology Tutorials** — learn about Message Analyzer concepts, usage features, and the technologies on which they are built, for example, the underlying PEF architecture and ETW framework that support Message Analyzer operations.
- Message Analyzer Startup Options** — review various methods for launching Message Analyzer.

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

Microsoft Message Analyzer

The screenshot shows the Microsoft Message Analyzer application running in a virtual machine. The window title is "W2008R2 [Running] - Oracle VM VirtualBox". The application interface includes a menu bar (File, Machine, View, Input, Devices, Help) and a toolbar with options like "New Session", "Favorite Scenarios", "Open", "Save", "New Viewer", "Edit Session", "Shift Time", "Aliases", and "New Union". The main area features a "Start Page" with buttons for "New Session", "Start Local Trace", "Open", "Discussion/Voti...", and "Blog". Below this are sections for "Recent Files", "Favorite Scenarios" (with links like "Local Network Interfaces (Win 8 and earlier)", "Loopback and Unencrypted IPSEC", and "Pre-Encryption for HTTPS"), and "News" (with links like "Blog: Using PowerShell for T...", "Netlogon Parser Update for..."). On the right, there are panels for "View Filter" (with a filter expression: "tcp.port==80 *address==192.168.1.1") and "Session Explorer". At the bottom, there are panels for "Message Stack 1", "Details 1" (with a search bar and a table with columns "Name", "Value", and "Bit Of"), and "Field Data". The status bar at the very bottom shows "Ready", "Session Total: 0", "Available: 0", "Selected: 0", "Viewpoint", "Truncated Session: False", "Parsing Level", "Build: 4.0.7551.0", and the system tray with the time "23:58 2016-02-20".

Microsoft Message Analyzer

The screenshot displays the Microsoft Message Analyzer (MMA) interface within a Windows environment. The main window title is "W2008R2 [Running] - Oracle VM VirtualBox". The application title bar reads "Administrator: Microsoft Message Analyzer".

The main workspace shows a list of network messages with the following columns: MessageNumber, Timestamp, TimeElapsed, Source, Destination, Module, and Summary. The messages listed are:

MessageNumber	Timestamp	TimeElapsed	Source	Destination	Module	Summary
291	2016-02-21T00:03:54.8931696	0,0000767	172.16.100.100	172.16.100.1	ICMP	Echo Operation
293	2016-02-21T00:03:55.8917828	0,0000611	172.16.100.100	172.16.100.1	ICMP	Echo Operation
295	2016-02-21T00:03:56.4570001		192.168.0.1	239.255.255.250	SSDP	Request, Method: NOTIFY, URI: ...
296	2016-02-21T00:03:56.5604258		192.168.0.1	239.255.255.250	SSDP	Request, Method: NOTIFY, URI: ...
297	2016-02-21T00:03:56.6651851		192.168.0.1	239.255.255.250	SSDP	Request, Method: NOTIFY, URI: ...
298	2016-02-21T00:03:56.7685964		192.168.0.1	239.255.255.250	SSDP	Request, Method: NOTIFY, URI: ...
299	2016-02-21T00:03:56.8725516		192.168.0.1	239.255.255.250	SSDP	Request, Method: NOTIFY, URI: ...
300	2016-02-21T00:03:56.8910927	0,0000792	172.16.100.100	172.16.100.1	ICMP	Echo Operation
302	2016-02-21T00:03:56.9767443		192.168.0.1	239.255.255.250	SSDP	Request, Method: NOTIFY, URI: ...
303	2016-02-21T00:03:57.0804870		192.168.0.1	239.255.255.250	SSDP	Request, Method: NOTIFY, URI: ...
304	2016-02-21T00:03:57.1845696		192.168.0.1	239.255.255.250	SSDP	Request, Method: NOTIFY, URI: ...
305	2016-02-21T00:03:57.2883400		192.168.0.1	239.255.255.250	SSDP	Request, Method: NOTIFY, URI: ...
306	2016-02-21T00:03:57.3925099		192.168.0.1	239.255.255.250	SSDP	Request, Method: NOTIFY, URI: ...
307	2016-02-21T00:03:57.4966766		192.168.0.1	239.255.255.250	SSDP	Request, Method: NOTIFY, URI: ...
308	2016-02-21T00:03:57.6024271		192.168.0.1	239.255.255.250	SSDP	Request, Method: NOTIFY, URI: ...
309	2016-02-21T00:03:57.7045779		192.168.0.1	239.255.255.250	SSDP	Request, Method: NOTIFY, URI: ...

The interface includes several toolbars and panels:

- Top Toolbar:** New Session, Favorite Scenarios, Open, Save, New Viewer, Edit Session, Shift Time, Aliases, New Union.
- Message Stack:** Add Columns, Color Rules, Find Message, Go To Message, Layout, Find In Grouping Viewer, Export.
- View Filter:** Apply, Enter a filter expression, su tcp.port==80 *address==192.16.
- Session Explorer:** Local Network I, 1: Analysis G.
- Message Stack 1:** Message Stack 1.
- Details 1:** Details 1, Enter search text here...
- Field Data:** Field Data, Message Data 1, Output.

The bottom status bar shows: Processing, Session Total: 41, Available: 29, Selected: 0, Viewpoint: Default, Truncated Session, Parsing Level, Build: 4.0.7551.0. The system tray shows the Start button, taskbar icons, and system clock (00:04, 2016-02-21).

Microsoft Message Analyzer

The screenshot displays the Microsoft Message Analyzer interface within a Windows VM. The main window shows a list of captured messages, with message 412 selected. Below the list, the 'Message Stack 1' pane shows the protocol stack for the selected message, and the 'Details 1' pane shows the raw data fields. The 'Field Data' pane is also visible.

MessageNumber	Timestamp	TimeElapsed	Source	Destination	Module	Summary
291	2016-02-21T00:03:54.8931696	0,0000767	172.16.100.100	172.16.100.1	ICMP	Echo operation
293	2016-02-21T00:03:55.8917828	0,0000611	172.16.100.100	172.16.100.1	ICMP	Echo operation
300	2016-02-21T00:03:56.8910927	0,0000792	172.16.100.100	172.16.100.1	ICMP	Echo operation
310	2016-02-21T00:03:57.8905926	0,0000509	172.16.100.100	172.16.100.1	ICMP	Echo operation
412	2016-02-21T00:05:29.1000042	0,0348415	172.16.100.100	212.77.98.9	ICMP	Echo operation
413	2016-02-21T00:05:29.1000316	0,0347755	192.168.0.100	212.77.98.9	ICMP	Echo operation
420	2016-02-21T00:05:30.0945874	0,0408199	172.16.100.100	212.77.98.9	ICMP	Echo operation
421	2016-02-21T00:05:30.0946159	0,0407600	192.168.0.100	212.77.98.9	ICMP	Echo operation
428	2016-02-21T00:05:31.0935358	0,0416395	172.16.100.100	212.77.98.9	ICMP	Echo operation
429	2016-02-21T00:05:31.0935652	0,0415710	192.168.0.100	212.77.98.9	ICMP	Echo operation
440	2016-02-21T00:05:32.0933067	0,0413418	172.16.100.100	212.77.98.9	ICMP	Echo operation
441	2016-02-21T00:05:32.0933449	0,0412823	192.168.0.100	212.77.98.9	ICMP	Echo operation

Message Stack 1
412 : ICMP Echo Operation
412 : ICMP Echo Request
417 : ICMP Echo Reply
412 : IPv4 Next Protocol: ICMP, Pa
417 : IPv4 Next Protocol: ICMP, Pa
412 : Ethernet Type: Internet IP (IPv4)
417 : Ethernet Type: Internet IP (IPv4)

Details 1
Name Value
ReqIdentifier 1 (0x0001)
ReqSequenceNumber 42 (0x002A)
ReqData abcdefghijklmnopqrstuvwxyzabcdefghi
ResIdentifier 1 (0x0001)
ResSequenceNumber 42 (0x002A)

Field Data
Message Data 1
Output

Processing Session Total: 311 Available: 12 Selected: 1 Viewpoint: Default Truncated Sessio Parsing Level Build: 4.0.7551.0
00:07 2016-02-21
Right Control

Microsoft Message Analyzer

The screenshot displays the Microsoft Message Analyzer (MMA) interface within an Oracle VM VirtualBox window titled 'W2008R2 [Running]'. The application window is titled 'Administrator: Microsoft Message Analyzer' and shows a session named '1 : Local Network...'. The main pane displays a list of network messages with columns for MessageNumber, Timestamp, TimeElapsed, Source, Destination, Module, and Summary. The selected message (ID 993) is a DHCP Discover packet from 0.0.0.0 to 255.255.255.255.

MessageNumber	Timestamp	TimeElapsed	Source	Destination	Module	Summary
624	2016-02-21T00:07:18.8851026	0,0000006	192.168.0.100	192.168.0.1	DHCP	DHCPRequest, OpCode: BootRequest,
627	2016-02-21T00:07:18.8865961		192.168.0.1	192.168.0.100	DHCP	DHCPACK, OpCode: BootReply, Trans
880	2016-02-21T00:08:22.6386517		172.16.100.100	172.16.100.1	DHCP	DHCPRelease, OpCode: BootRequest,
993	2016-02-21T00:08:41.4035288		0.0.0.0	255.255.255.255	DHCP	DHCPDiscover, OpCode: BootRequest
994	2016-02-21T00:08:41.4039541	0,0000006	172.16.100.1	255.255.255.255	DHCP	DHCPoffer, OpCode: BootReply, Tra
997	2016-02-21T00:08:41.4042794		0.0.0.0	255.255.255.255	DHCP	DHCPRequest, OpCode: BootRequest,
998	2016-02-21T00:08:41.4046503	0,0000005	172.16.100.1	255.255.255.255	DHCP	DHCPACK, OpCode: BootReply, Trans
1683	2016-02-21T00:08:44.7914892		172.16.100.100	255.255.255.255	DHCP	DHCPInform, OpCode: BootRequest,
1684	2016-02-21T00:08:44.7916237	0,0000005	172.16.100.1	255.255.255.255	DHCP	DHCPACK, OpCode: BootReply, Trans

The 'Details 1' pane shows the following fields for the selected DHCP Discover packet:

Name	Value
OpCode	BootRequest(1) (0x01)
Hardwaretype	Ethernet (10Mb) (1) (0x01)
HardwareAddressLength	6 (0x06)
HopCount	0 (0x00)
TransactionID	2493676363 (0x94A27B4B)

The 'Message Stack 1' pane shows the protocol stack for the selected message:

- 993 : DHCP
DHCPDiscover, OpCode: BootRequest, TransID: 0
- 993 : UDP
SrcPort: DHCPClient(68), DstPort: DHCPServer(67)
- 993 : IPv4
Next Protocol: UDP, Packet ID: 685, Total Length: 3
- 993 : Ethernet
Type: Internet IP (IPv4)

The 'Field Data' pane is currently empty. The bottom status bar shows 'Processing', 'Session Total: 1798', 'Available: 9', 'Selected: 1', 'Viewpoint: Default', 'Truncated Sessio', 'Parsing Level', and 'Build: 4.0.7551.0'. The system tray shows the time as 00:09 on 2016-02-21.

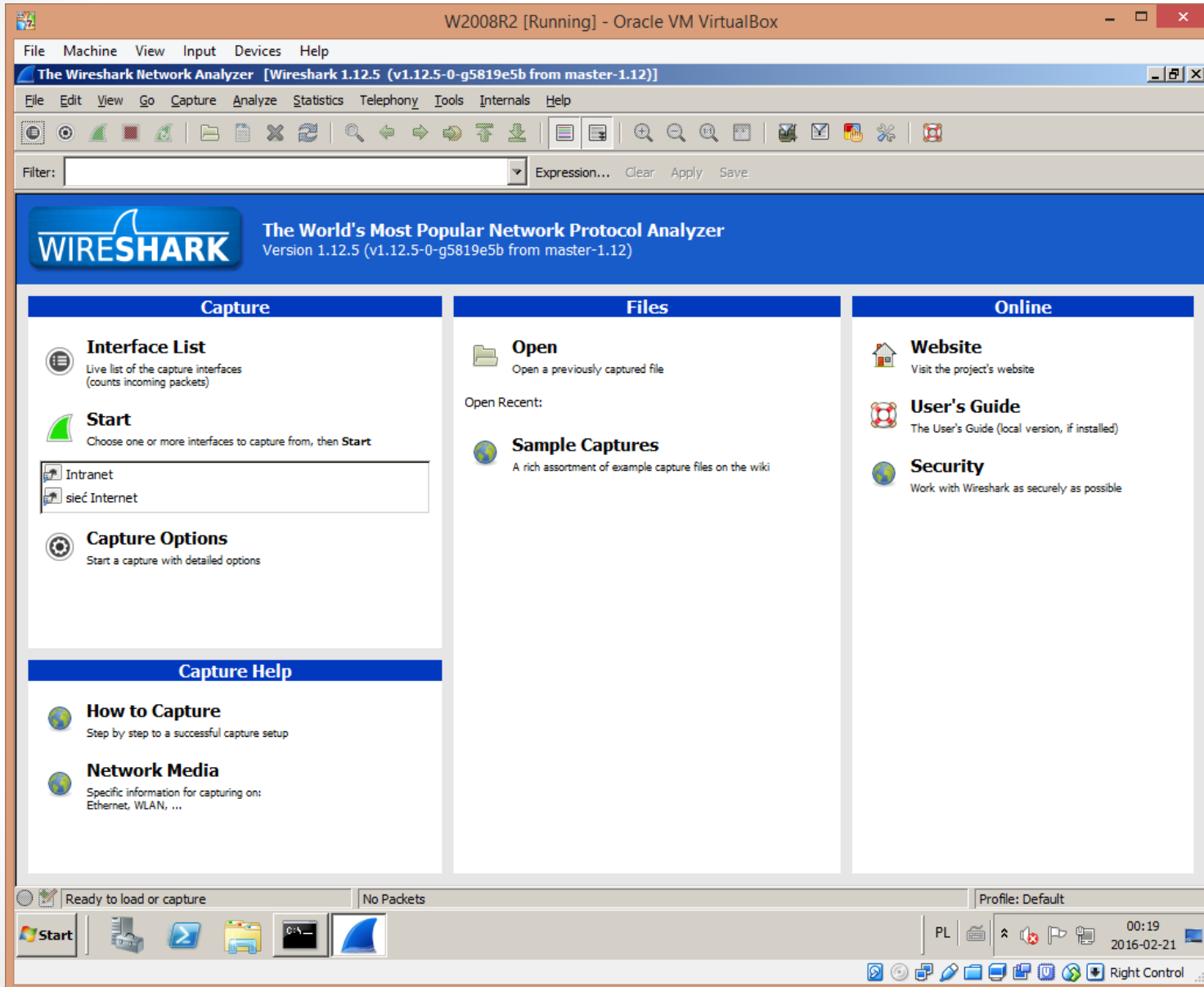
Wireshark

- 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.



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

Wireshark



Wireshark

The screenshot displays the Wireshark 1.12.5 interface within an Oracle VM VirtualBox window titled 'W2008R2 [Running]'. The main window has a menu bar (File, Machine, View, Input, Devices, Help) and a toolbar. The main content area is divided into three panes: 'Capture', 'Files', and 'Online'. The 'Capture' pane shows the 'Interface List' with two interfaces: 'Intranet' and 'sieć Internet'. A tooltip points to the 'Start' button, stating 'Same as Capture/Interfaces menu or toolbar item'. The 'Files' pane contains 'Open', 'Sample Captures', and 'Wireshark: Capture Interfaces' dialog boxes. The 'Online' pane contains 'Website', 'User's Guide', and 'Security' links. The 'Wireshark: Capture Interfaces' dialog box contains a table with the following data:

Device	Description	IP	Packets	Packets/s	
<input checked="" type="checkbox"/> Intranet	Karta Intel(R) PRO/1000 MT Desktop Adapter	172.16.100.1	9	0	Details
<input type="checkbox"/> sieć Internet	Karta Intel(R) PRO/1000 MT Desktop Adapter	192.168.0.100	32	0	Details

The status bar at the bottom shows 'Ready to load or capture', 'No Packets', and 'Profile: Default'. The system tray at the bottom right shows the time '00:20' and date '2016-02-21'.

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 0xfe7 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 .....
0070 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 [Taskbar icons] 00:21 2016-02-21 Right Control

Wireshark

The screenshot shows the Wireshark interface within an Oracle VM VirtualBox window titled 'W2008R2 [Running]'. The main window title is 'Capturing from Intranet [Wireshark 1.12.5 (v1.12.5-0-g5819e5b from master-1.12)]'. The menu bar includes File, Machine, View, Input, Devices, and Help. The toolbar contains various icons for file operations, capture control, and analysis. The filter bar is set to 'bootp'. The packet list pane shows several DHCP-related packets, with packet 289 (DHCP Discover) selected. The packet details pane shows the structure of the selected packet: Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Bootstrap Protocol (Discover). The packet bytes pane shows the raw data in hexadecimal and ASCII.

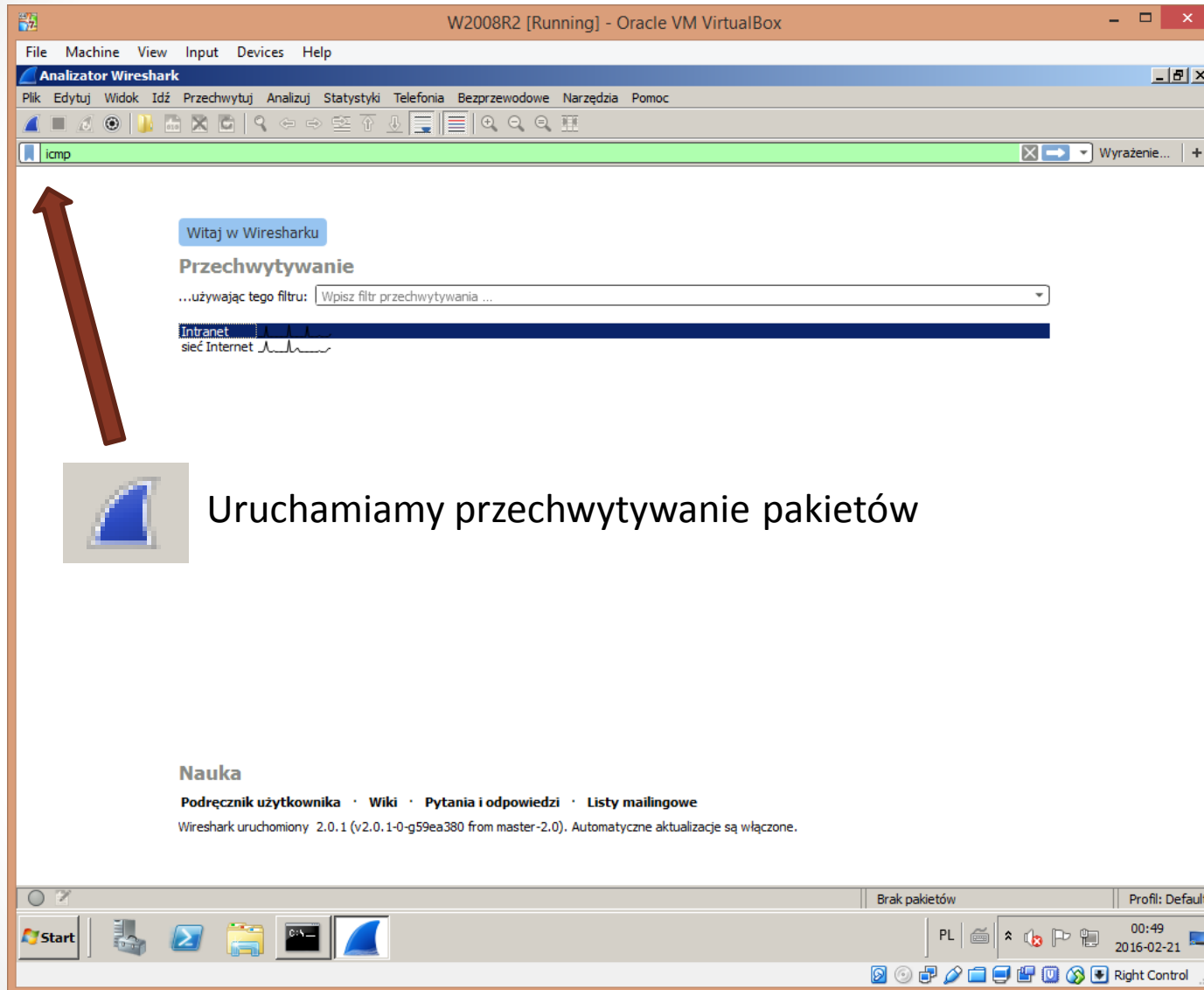
No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	172.16.100.100	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0xef7c3c76
2	0.00077600	172.16.100.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xef7c3c76
270	552.059302	172.16.100.100	172.16.100.1	DHCP	342	DHCP Release - Transaction 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  .....
0070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
```

Wireshark



- **Wireshark** – w nowej odsłonie

Wireshark

The screenshot displays the Wireshark network protocol analyzer interface. The main window shows a list of captured packets, with the selected packet (No. 4) expanded to show its details and raw data.

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
```

Wireshark

The screenshot shows the Wireshark interface within a Windows VM. The main window title is "W2008R2 [Running] - Oracle VM VirtualBox". The interface includes a menu bar (File, Machine, View, Input, Devices, Help), a toolbar, and a packet list pane. The packet list pane shows a list of captured packets, with packet 1 selected. The packet details pane shows the structure of the selected packet: Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Bootstrap Protocol (Release). The packet bytes pane shows the raw data in hexadecimal and ASCII.

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)

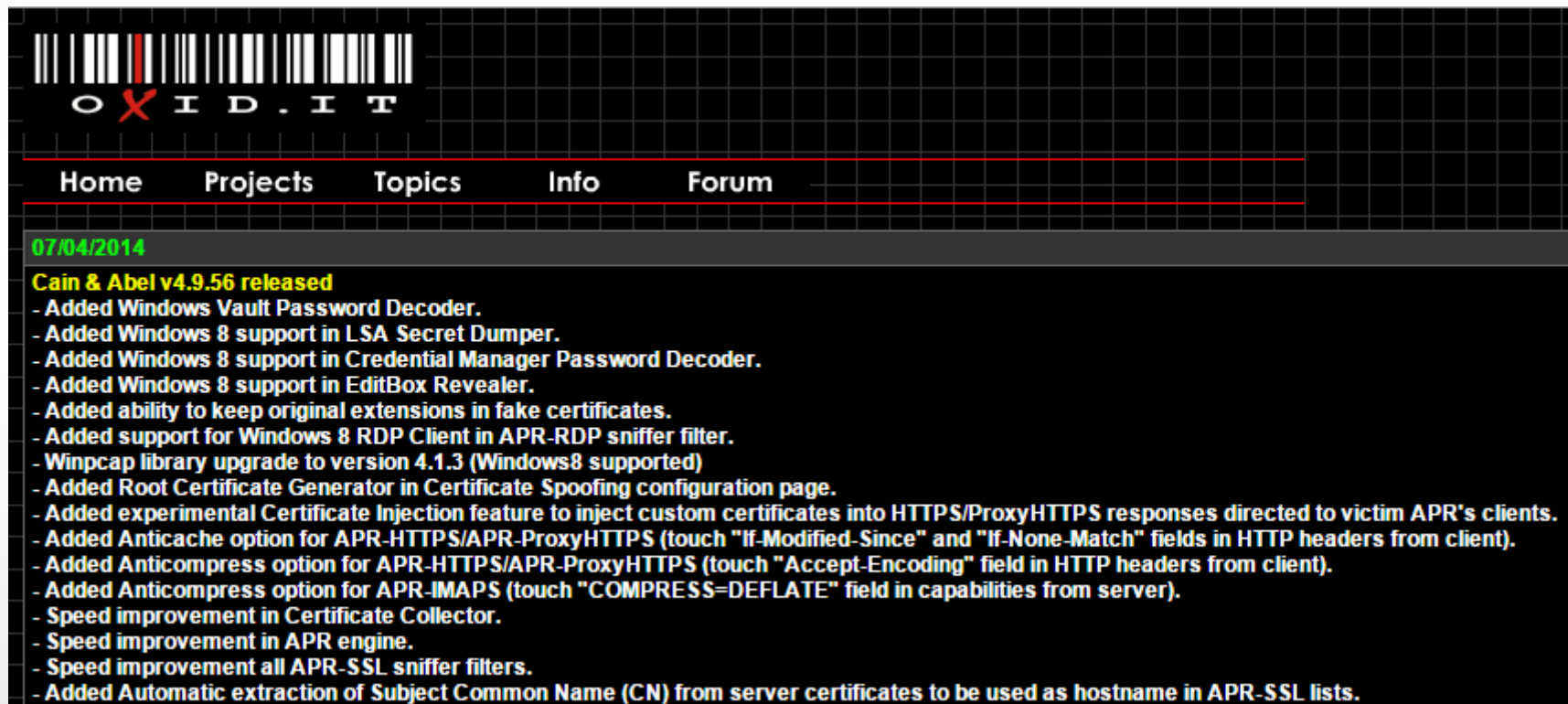
```
0000  08 00 27 0e ec a6 08 00 27 48 11 99 08 00 45 00  ..'.... 'H...E.
0010  01 48 01 f2 00 00 80 11 17 2d ac 10 64 64 ac 10  .H..... -...dd..
0020  64 01 00 44 00 43 01 34 9b e1 01 01 06 00 c6 bb  d..D.C.4 .....
0030  d1 36 00 00 00 00 ac 10 64 64 00 00 00 00 00 00  .6..... dd.....
0040  00 00 00 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  .....
```

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 trój etapowego 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.



The screenshot shows the Oxid.it website interface. At the top, there is a logo consisting of a barcode and the text "OXID.IT". Below the logo is a navigation menu with links for "Home", "Projects", "Topics", "Info", and "Forum". The main content area displays a date "07/04/2014" and a heading "Cain & Abel v4.9.56 released". A list of updates follows, detailing new features and improvements for the software.

07/04/2014

Cain & Abel v4.9.56 released

- Added Windows Vault Password Decoder.
- Added Windows 8 support in LSA Secret Dumper.
- Added Windows 8 support in Credential Manager Password Decoder.
- Added Windows 8 support in EditBox Revealer.
- Added ability to keep original extensions in fake certificates.
- Added support for Windows 8 RDP Client in APR-RDP sniffer filter.
- Winpcap library upgrade to version 4.1.3 (Windows8 supported)
- Added Root Certificate Generator in Certificate Spoofing configuration page.
- Added experimental Certificate Injection feature to inject custom certificates into HTTPS/ProxyHTTPS responses directed to victim APR's clients.
- Added Anticache option for APR-HTTPS/APR-ProxyHTTPS (touch "If-Modified-Since" and "If-None-Match" fields in HTTP headers from client).
- Added Anticompress option for APR-HTTPS/APR-ProxyHTTPS (touch "Accept-Encoding" field in HTTP headers from client).
- Added Anticompress option for APR-IMAPS (touch "COMPRESS=DEFLATE" field in capabilities from server).
- Speed improvement in Certificate Collector.
- Speed improvement in APR engine.
- Speed improvement all APR-SSL sniffer filters.
- Added Automatic extraction of Subject Common Name (CN) from server certificates to be used as hostname in APR-SSL lists.

- <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