

Ewa CZARNIK<sup>1</sup>  
Paweł DYMORA<sup>2</sup>  
Mirosław MAZUREK<sup>3</sup>

## MECHANIZMY WYSZUKIWANIA OBRAZEM W ORACLE 11g

W bazach danych zawierających dane graficzne (np. zdjęcia), niejednokrotnie zachodzi potrzeba szybkiego odnalezienia podobnego obrazu. W bazach danych np. firm magazynowych, ważną kwestią może być eliminacja duplikującego się asortymentu posiadającego różne opisy, dokumentację, a faktycznie posiadającego te same właściwości fizyczne, np. poprzez porównanie wyglądu poszczególnych produktów na podstawie posiadanego zdjęcia. Naprzeciw takim potrzebom wychodzi Oracle ze standardem SQL/MM, który udostępnia metody umożliwiające przeszukiwanie baz danych za pomocą właściwości wizualnych tzw. wyszukiwanie obrazem. Artykuł prezentuje możliwości technologii Oracle 11g obsługującej typy składowania danych multimedialnych (w tym danych graficznych) oraz przykład stworzonej aplikacji internetowej umożliwiającej implementację tych mechanizmów i wyszukiwanie obrazem. Aplikacja została wykorzystana do przeprowadzenia badań wydajnościowych różnych metod wyszukiwania obrazem.

**Słowa kluczowe:** Oracle 11g, SCORE, wyszukiwanie obrazem.

### REVERSE IMAGE-SEARCHING MECHANISMS IN ORACLE 11g

#### Summary

The main aim of this paper is to present mechanisms and types of multimedia data storage in Oracle 11g Database System along with a web application that allows reverse image search mechanism implementation in order to test its efficiency. First part shows Oracle Multimedia and SQL/MM standard, with supported data types, metadata and methods. The second part is focused on presentation the original database application with appropriate tables and procedures implementing reverse image search. The application with appropriate database is used to determinate on the base of series tests the most efficient image search methods.

**Keywords:** Oracle Multimedia, SQL/MM, images, reverse image searching, SCORE

DOI: 10.7862/re.2017.13

*Tekst złożono w redakcji: wrzesień 2017  
Przyjęto do druku: październik 2017*

---

<sup>1</sup> Autor do korespondencji: Ewa Czarnik, Politechnika Rzeszowska, adres e-mail: ewa1927@gmail.com

<sup>2</sup> Paweł Dymora, Politechnika Rzeszowska, Zakład Systemów Złożonych, pawel.dymora@prz.edu.pl

<sup>3</sup> Mirosław Mazurek, Politechnika Rzeszowska, Zakład Systemów Złożonych, miroslaw.mazurek@prz.edu.pl

**Bartosz KOWAL**<sup>4</sup>  
**Paweł DYMORA**<sup>5</sup>  
**Mirosław MAZUREK**<sup>6</sup>

## **NS2 – JAKO ŚRODOWISKO SYMULACYJNE DO BADAŃ NAD BEZPRZEWODOWYMI SIECIAMI SENSOROWYMI**

Wraz z rozwojem bezprzewodowych systemów sensorowych rośnie zainteresowanie Internetem Rzeczy (ang. *Internet of Things*). Celem artykułu jest przybliżenie możliwości jakie dostarcza środowisko symulacyjne NS2 do badań nad bezprzewodowymi sieciami sensorowymi. W artykule opisano symulator sieci NS2, scharakteryzowano główne funkcje symulatora, przedstawiono i opisano przykładowy proces budowy skryptu sieci WSN oraz analizę wyników symulacji testowanej sieci.

**Słowa kluczowe:** sensory, WSN, NS2, bezprzewodowa sieć sensorowa.

### **NS2 - A SIMULATION ENVIRONMENT FOR RESEARCH ON WIRELESS SENSOR NETWORKS**

#### **S u m m a r y**

Nowadays, with the growing interest in the Internet of Things, in most cases sensor network technology is used. The purpose of this article is to introduce the readers to the possibilities that provides the NS2 simulation environment for the study of wireless sensor networks. The article describes the network simulator NS2, characterized the most essential functions that it meets. In this article will be described a diagram of the WSN networks script, and how to correctly read the results obtained from the simulation.

**Keywords:** sensors, WSN, NS2, wireless sensor network

DOI: 10.7862/re.2017.14

*Tekst złożono w redakcji: wrzesień 2017*  
*Przyjęto do druku: październik 2017*

---

<sup>4</sup> Autor do korespondencji: Bartosz Kowal, Politechnika Rzeszowska, Zakład Systemów Złożonych, bartosz.kowal@prz.edu.pl

<sup>5</sup> Paweł Dymora, Politechnika Rzeszowska, Zakład Systemów Złożonych, pawel.dymora@prz.edu.pl

<sup>6</sup> Mirosław Mazurek, Politechnika Rzeszowska, Zakład Systemów Złożonych, miroslaw.mazurek@prz.edu.pl

**Patrycja MARGOL**<sup>7</sup>  
**Paweł DYMORA**<sup>8</sup>  
**Mirosław MAZUREK**<sup>9</sup>

## **STRATEGIE ARCHIWIZACJI I ODTWARZANIA BAZ DANYCH**

Systemy bazodanowe są narażone na różnego rodzaju awarie, które mogą być spowodowane zarówno uszkodzeniem sprzętu, jak i błędem użytkownika czy systemu. Jednym ze skutecznych sposobów ochrony danych przed utratą jest tworzenie kopii zapasowych. Artykuł omawia kluczowe elementy dotyczące tworzenia strategii archiwizacji i odtwarzania danych. Ma na celu uświadomienie jak ważnym elementem pracy administratorów baz danych jest tworzenie odpowiednich strategii tworzenia kopii zapasowych i ich testowanie.

**Słowa kluczowe:** systemy bazodanowe, bazy danych, archiwizacja, odtwarzanie.

### **DATABASE BACKUP AND RECOVERY STRATEGIES**

#### **S u m m a r y**

Database systems are prone to different types of failure. Cause of them could be both the hard disk failure or user error. One way to protect data against loss is by making backups. This article discusses key elements in development of database backup and recovery strategies. It aims to make people aware of how important is to do and test backups.

**Keywords:** backup, recovery, database, database systems

DOI: 10.7862/re.2017.15

*Tekst złożono w redakcji: wrzesień 2017*  
*Przyjęto do druku: październik 2017*

---

<sup>7</sup> Autor do korespondencji: Patrycja Margol, Politechnika Rzeszowska, adres e-mail: margol.pat@gmail.com

<sup>8</sup> Paweł Dymora, Politechnika Rzeszowska, Zakład Systemów Złożonych, pawel.dymora@prz.edu.pl

<sup>9</sup> Mirosław Mazurek, Politechnika Rzeszowska, Zakład Systemów Złożonych, miroslaw.mazurek@prz.edu.pl

**Maksymilian BURDACKI**<sup>10</sup>  
**Paweł DYMORA**<sup>11</sup>  
**Mirosław MAZUREK**<sup>12</sup>

## **ANALIZA RUCHU W SIECI KOMPUTEROWEJ W OPARCIU O MODELE MULTIFRAKTALNE**

Celem badań była analiza ruchu w sieci komputerowej z wykorzystaniem wybranych modeli multifraktalnych. W części teoretycznej omówiono podstawowe zagadnienia związane z oprogramowaniem zbierającym dane w sieci komputerowej, klasyfikacją przebiegów czasowych przy użyciu wykładnika Hurst'a. Opisano metody wykorzystane do wyznaczenia widm multifraktalnych. W części badawczej dokonano analizy przepływu ruchu w sieci komputerowej na podstawie liczby pakietów oraz prędkości przesyłania danych. Wykonano analizę wykładnika Hurst'a wyznaczanego dla poszczególnych przebiegów czasowych. Dokonano analizy widm multifraktalnych utworzonych dla badanych rodzajów ruchu sieciowego.

**Słowa kluczowe:** analiza ruchu sieciowego, sniffing, analiza samopodobieństwa, analiza multifraktalna, wykładnik Hursta.

### **COMPUTER NETWORK TRAFFIC ANALYSIS BASED ON MULTIFRACTAL MODELS**

#### **S u m m a r y**

The aim of this work was computer network traffic analysis. Theoretical part de-scribes issues referring to network traffic capture software, time-series classification using Hurst exponent and multifractal spectrum creating methods. In research part was made an analysis of network traffic based on a number of packets and data transfer speed. It was also made a Hurst exponent analysis and a multifractal spectrum analysis for each type of analyzed network traffic. After the research it was possible to draw conclusions about characteristic of analyzed network traffic.

**Keywords:** network traffic analysis, sniffing, self-similarity analysis, multifractal analysis

DOI: 10.7862/re.2017.16

*Tekst złożono w redakcji: wrzesień 2017*

*Przyjęto do druku: październik 2017*

---

<sup>10</sup> Autor do korespondencji: Maksymilian Burdacki, Politechnika Rzeszowska, adres e-mail: maxb931@gmail.com

<sup>11</sup> Paweł Dymora, Politechnika Rzeszowska, Zakład Systemów Złożonych, pawel.dymora@prz.edu.pl

<sup>12</sup> Mirosław Mazurek, Politechnika Rzeszowska, Zakład Systemów Złożonych, miroslaw.mazurek@prz.edu.pl

## ANALIZA MOŻLIWOŚCI ATAKU CZASOWEGO ORAZ SŁOWNIKOWEGO NA KOMUNIKACJĘ Z UŻYCIEM KRYPTOGRAFII ELIPTYCZNEJ

Przez tysiąclecia tworzono, udoskonalano i łamano dziesiątki rozwiązań, których jedynym celem było uniemożliwienie odczytania informacji przez postronnych. Doprowadziło to do powstania dwóch przeciwstawnych w swoich działaniach dziedzin – kryptografii i kryptoanalizy. W dobie komputerów zrezygnowano ze wszystkich dotychczasowych rozwiązań i wprowadzono zupełnie nowe, z których za najbezpieczniejsza można uznać RSA i szyfry oparte o krzywe eliptyczne. Oba są uznawane za niemożliwe do złamania. Wynika to bezpośrednio z zależności matematycznych użytych w ich definicji. W dotychczasowych badaniach wykazano już kilka ich słabości, lecz nadal nie ma rozwiązania, które działałoby w każdym jednym przypadku. Z uwagi na to postanowiono przyjrzeć się głębiej słabym punktom szyfrów eliptycznych z uwzględnieniem wszystkich dotychczas do-stępnych informacji.

**Słowa kluczowe:** kryptografia, krzywe eliptyczne, ataki słownikowe, ataki czasowe.

### ANALYSIS OF THE POSSIBILITY OF THE TIME AND DICTIONARY BASED ATTACKS ON ELLIPTIC CURVE CRYPTOGRAPHY BASED COMMUNICATION

#### Summary

For millennia, dozens of solutions, which sole purpose was to prevent outsiders from reading information, have been developed, refined and broken. This led to the emergence of two opposing fields - cryptography and cryptanalysis. In the age of computers, all existing solutions have been abandoned and new ones have been introduced, with the most secure ones RSA and ciphers based on elliptic curves. Both considered impossible to break. This result directly from the math used in their definitions. Some previous researches have already shown some of their weaknesses, but there is still no solution that would work in every single case. Because of this, it was decided to take a closer look at the weak points of elliptic ciphers, taking into account all the information available to date.

**Keywords:** cryptography, elliptic curves, dictionary attacks, time attacks

DOI: 10.7862/re.2017.17

*Tekst złożono w redakcji: wrzesień 2017*

*Przyjęto do druku: październik 2017*

---

<sup>13</sup> Mateusz Tybura, Politechnika Rzeszowska, adres e-mail: tyburam@hotmail.com