

**Міністерство освіти і науки України
Державний вищий навчальний заклад
«Український державний хіміко-технологічний
університет»**

**МАТЕРІАЛИ
VIII Міжнародної науково-технічної конференції
КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ ТА
ОПТИМІЗАЦІЯ СКЛАДНИХ СИСТЕМ**

**MATERIALS
VIII-th International scientific-technical conference
COMPUTER MODELING AND OPTIMIZATION OF
COMPLEX SYSTEMS**

**1-3 листопада 2023 року
м. Дніпро, Україна**

ЗМІСТ

СЕКЦІЯ 1

ПЕРСПЕКТИВНІ НАПРЯМКИ

МАТЕМАТИЧНОГО МОДЕЛЮВАННЯ12

*Kairov A. S., Yarenko K. Yu.*MATHEMATICAL MODELING OF DYNAMIC DEFORMATION OF LAYERED
COMPOSITE CYLINDRICAL SHELLS UNDER LONGITUDINAL IMPULSE
LOADS.....13*Korotka L. I., Anisimov V. V.*OBJECT-ORIENTED APPROACH IN THE MODELING OF NONLINEAR
DYNAMIC SYSTEMS FOR SOFTWARE DEVELOPMENT15*Makarova L. M., Kaminsky S. S., Bryzgalov M. V.*SOFTWARE DESIGNED TO IDENTIFY MODIFICATIONS MADE TO
EXECUTABLE FILE CODE17*Choudhary N., Strelnikova E., Sierikva O.*COMPUTER SIMULATION OF FREE AND FORCED VIBRATION OF
COMPOUND FUEL TANKS.....19*Ostashko I. O., Nachovny I. I.*SIMULATION OF GAS DYNAMIC MODES OF OPERATION OF THE
GRINDING CHAMBER OF THE CENTRIFUGAL MILL.....20*Hlib Vokhmianin, Oleg Zhulkovskyi, Inna Zhulkovska, Illia Tykhonenko*

USING SIMD ARCHITECTURE IN COMPUTER MODELING TASKS22

*Аушева Н. М., Кардашов О. В.*ЗАСТОСУВАННЯ ГІПЕРКОМПЛЕКСНИХ ЧИСЕЛ ДЛЯ МОДЕЛЮВАННЯ
ГЕОМЕТРИЧНИХ ОБ'ЄКТІВ24*Барташевська Ю. М.*МОДЕЛЮВАННЯ СИСТЕМИ КІБЕРБЕЗПЕКИ ОБ'ЄКТА
ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ.....26*Берлов О. В., Губін О. І., Якубовська З. М.*МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ В ЗАДАЧАХ ПРОГНОЗУВАННЯ
НАСЛІДКІВ ЕКСТРЕМАЛЬНИХ СИТУАЦІЙ.....28*Біляєв М. М., Біляєва В. В., Козачина В. А.*ЧИСЕЛЬНЕ МОДЕЛЮВАННЯ ПРОЦЕСІВ ЗАБРУДНЕННЯ
АТМОСФЕРНОГО ПОВІТРЯ29*Біляєв М. М., Козачина В. В., Коваленко А. С.,**Чірков А. О., Чирва М. В.*МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ПРОЦЕСІВ МАСОПЕРЕНОСУ
ТА ГІДРОДИНАМІКИ30*Біляєва В. В., Машихіна П. Б., Форись С. М.*ЧИСЕЛЬНЕ МОДЕЛЮВАННЯ РАДІОАКТИВНОГО ЗАБРУДНЕННЯ
ПОВІТРЯ У ВИПАДКУ РАПТОВОЇ ЕМІСІЇ НА АЕС.....31*Бомба А. Я., Мороз І. П., Лістєв З. С.*СИСТЕМНИЙ АНАЛІЗ В МАТЕМАТИЧНОМУ ТА ІНФОРМАЦІЙНОМУ
МОДЕЛЮВАННІ НАПІВПРОВІДНИКОВИХ Р-І-N-СТРУКТУР.....32

SOFTWARE DESIGNED TO IDENTIFY MODIFICATIONS MADE TO EXECUTABLE FILE CODE

Makarova L. M., Kaminsky S. S., Bryzgalov M. V.

Admiral Makarov National University of Shipbuilding, Mykolaiv, Ukraine

DisEn is a software tool built on the .NET Framework with a WPF-based UI. It checks executable files for changes [1], disassembles them into assembly code, calculates entropy values [2], and presents results in tables and diagrams. It also saves SHA-1 hashes of files by their names for future comparisons to determine authorship and changes. Using an entropy metric, it assesses assembly code commands to identify code authorship and contributions, with SHA-1 [3] hashes providing extra verification during analysis.

To calculate entropy, the following formula was applied, which is used in information theory:

$$H(i) = -p_i \cdot \log_2(p_i) \quad (1)$$

where: i – possible states,
 p_i – probability of occurrence of the i -th state.

To calculate SHA-1 [4], the following formula was applied, which is used in information theory:

$$\text{HashBlock}_i = f(\text{Block}_i, \text{HashBlock}_{i-1}) \quad (2)$$

where: i – Hash block index.

DisEn provides a number of useful features, among which are:

1. Executable Disassembly: The software can disassemble executable files, utilizing the dumpbin.exe utility, which is included in Microsoft Visual Studio [5]. This process results in a text file containing the program's code.
2. Entropy Calculation: DisEn calculates entropy values for each command found in the disassembled file. The entropy values are determined using formula (1), and all the computed values are saved in a text file.
3. Hashing: The software computes and stores the SHA-1 hash of the current version of the file using formula (2). This hash serves as a unique fingerprint of the file's content.
4. Entropy Threshold Determination: The software determines the entropy threshold for each command within the current file.
5. Entropy Difference Calculation: DisEn calculates the difference in entropy between the current version of the file and a new one.
6. File Comparison: It compares the current version of the file with the new one using a divergence criterion, taking into account both entropy differences and hash comparisons.

The program, DisEn, processes executable files and saves analysis results locally. If a file with the same name is processed again, DisEn will compare it to the previous version (see Figure 1). When a new file with the same name is found, it opens a window displaying the differences between the new and old versions. It then prompts the user to save the analysis results and replaces the old file trace. For example, we utilized a 3D rendering program created by the authors of this article. In version 1, it rendered wireframes, and in version 2, it added triangle rasterization (see Figure 1).

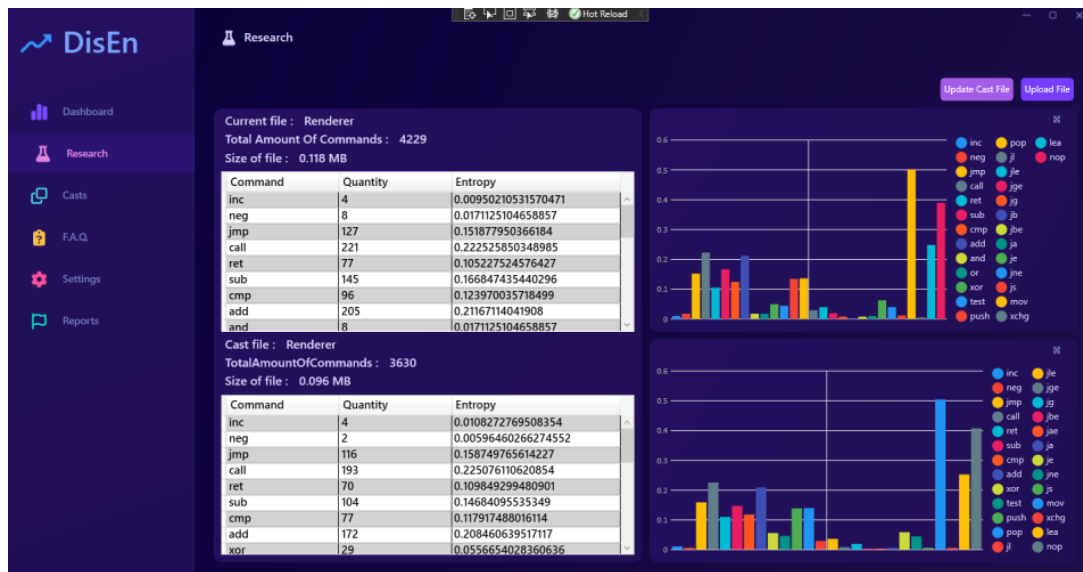


Figure 1 – Difference between two files

DisEn is a useful utility for inspecting executable files and identifying the source of modifications. There are plans to add the capability of customizing disassembly techniques and specifying a set of commands for a more adaptable interaction with the software in the future.

References

1. What is code injection in Windows? [Electronic resource] // Mode of access: <https://www.thefastcode.com/uk-uah/article/what-is-code-injection-on-windows>.
2. Shannon's formula [Electronic resource] // Mode of access: <http://um.co.ua/8/8-16/8-168268.html>.
3. Algorithm development to accelerate file comparison [Electronic resource] // Mode of access: <https://www.inter-nauka.com/uploads/public/14694535994336.pdf/>
4. SHA-1 is a Shambles First Chosen-Prefix Collision on SHA-1 and Application to the PGP Web of Trust, Gaëtan Leurent1 and Thomas Peyrin [Electronic resource] // Mode of access: <https://eprint.iacr.org/2020/014.pdf/>
5. Microsoft Visual Studio disassembler “dumpbin” [Electronic resource] // Mode of access: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4528095/>.