

C.10 RAM: MONITORIZARE ȘI MANIPULARE CU X96DBG

PAUL A. GAGNIUC



Academia Tehnică Militară „Ferdinand I”

PRINCIPALELE PĂRȚI ALE PREZENTĂRII

C.10 Dezasamblare și Patching cu X32dbg / X64dbg:

- 10.1 OPTIMIZARI UTILE IN X32DBG / X64DBG
- 10.2 MEMORIA RAM: HEAP VS STACK
- 10.3 INTERCEPTAREA DATELOR IN MEMORIA RAM
- 10.4 CRIPTAREA DATELOR IN MEMORIA RAM
- 10.5 IDENTIFICAREA PAROLELOR CRIPTATE PE DISC ȘI ÎN RAM
- 10.6 IDENTIFICAREA CENTRULUI DE COMANDĂ & CONTROL, CRIPTAT PE DISC ȘI ÎN RAM
- 10.7 INTERCEPTAREA EXECUȚIEI MALWARE PRIN API
- 10.8 CRIPTAREA INSTRUCTIUNILOR IN SECTIUNEA .TEXT?

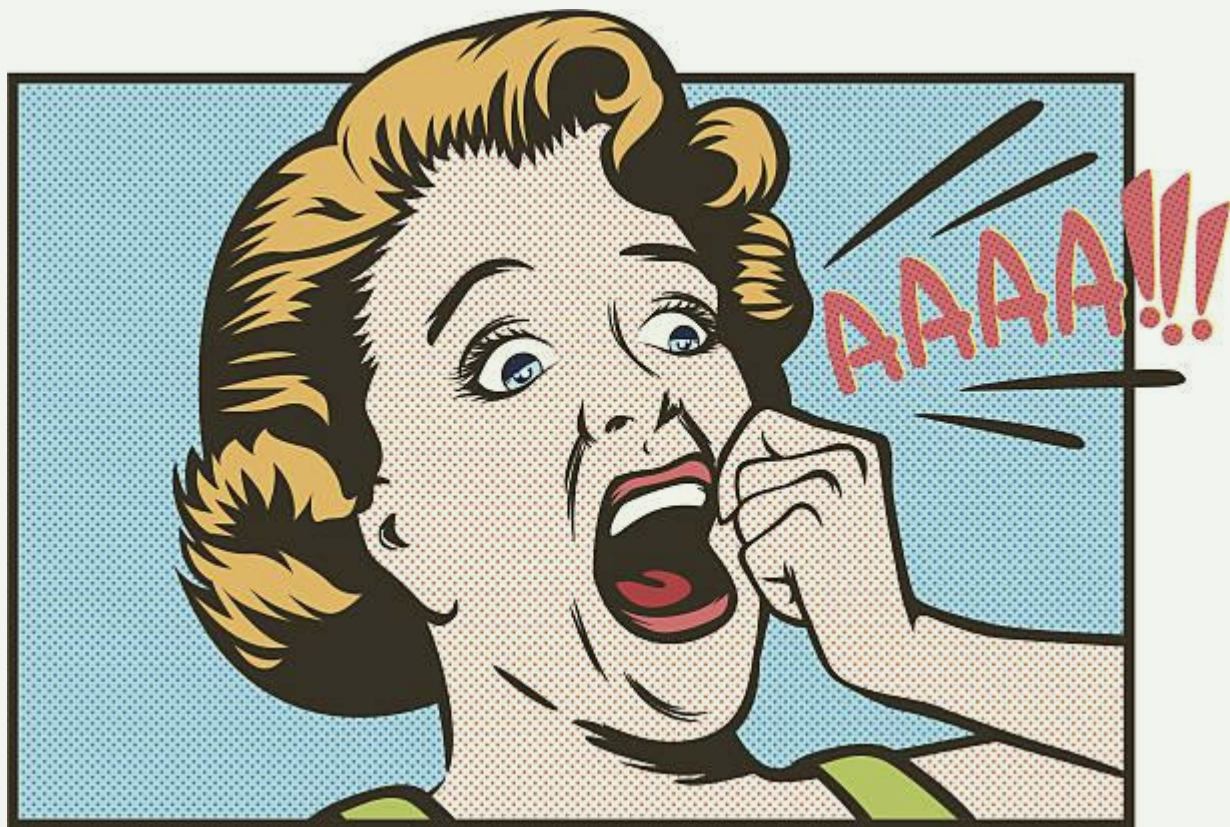


10.1

OPTIMIZARI UTILE IN X32DBG / X64DBG



OPTIMIZARI UTILE IN X32DBG / X64DBG



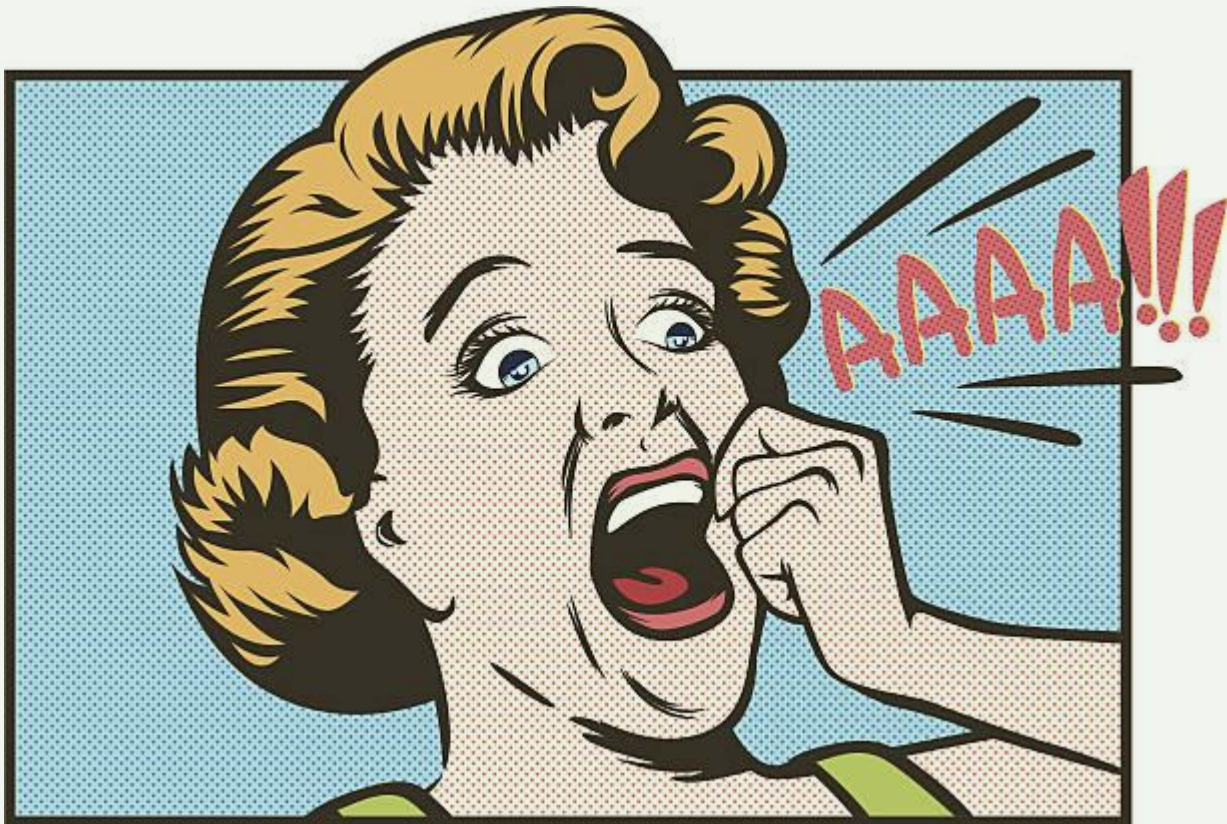
Această parte din prezentare
nu este publică! Este doar
pentru studenții ATM!



10.2 MEMORIA RAM: HEAP VS STACK



MEMORIA RAM: HEAP VS STACK



Această parte din prezentare
nu este publică! Este doar
pentru studenții ATM!



10.3

INTERCEPTAREA DATELOR IN MEMORIA RAM



INTERCEPTAREA DATELOR IN MEMORIA RAM



Această parte din prezentare
nu este publică! Este doar
pentru studenții ATM!

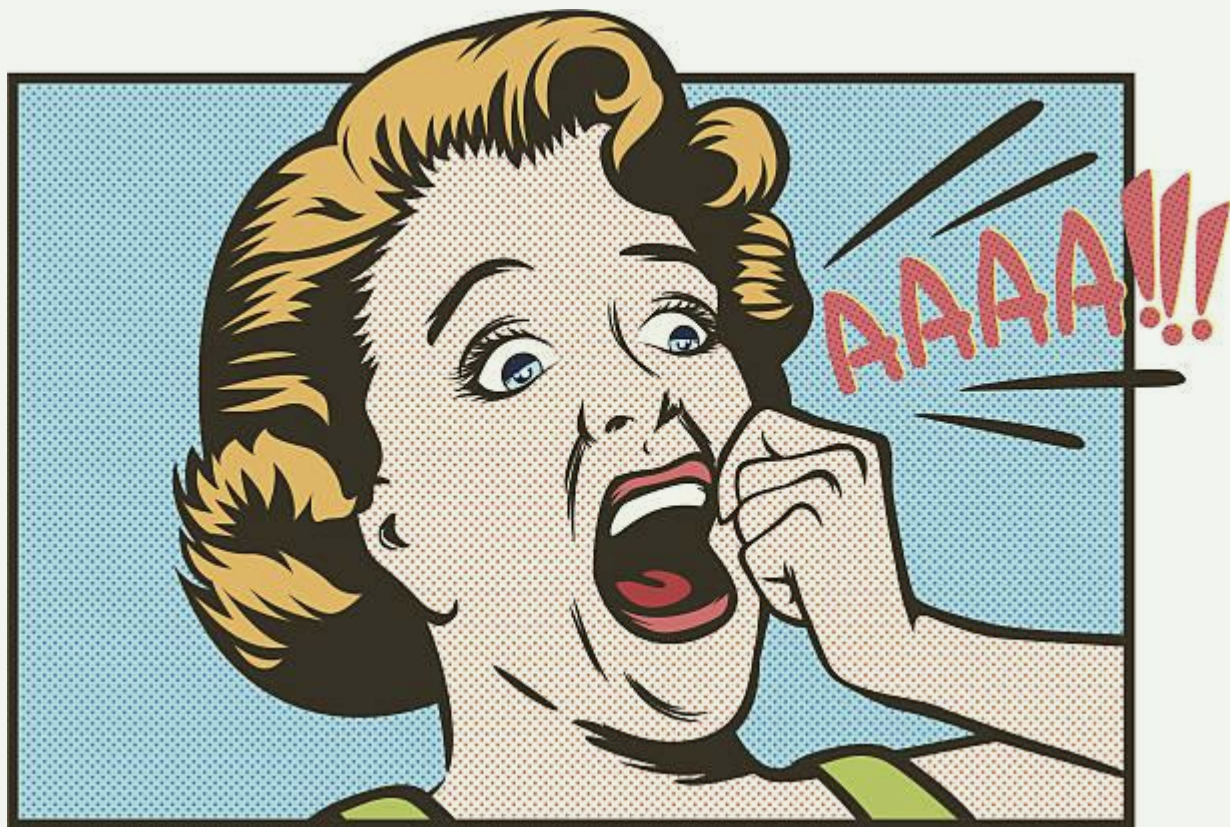


10.4

CRIPTAREA DATELOR IN MEMORIA RAM



CRIPTAREA DATELOR IN MEMORIA RAM



Această parte din prezentare
nu este publică! Este doar
pentru studenții ATM!



10.5

IDENTIFICAREA PAROLELOR CRIPTATE PE DISC ȘI ÎN RAM



IDENTIFICAREA PAROLELOR CRIPTATE PE DISC ȘI ÎN RAM



Această parte din prezentare
nu este publică! Este doar
pentru studenții ATM!

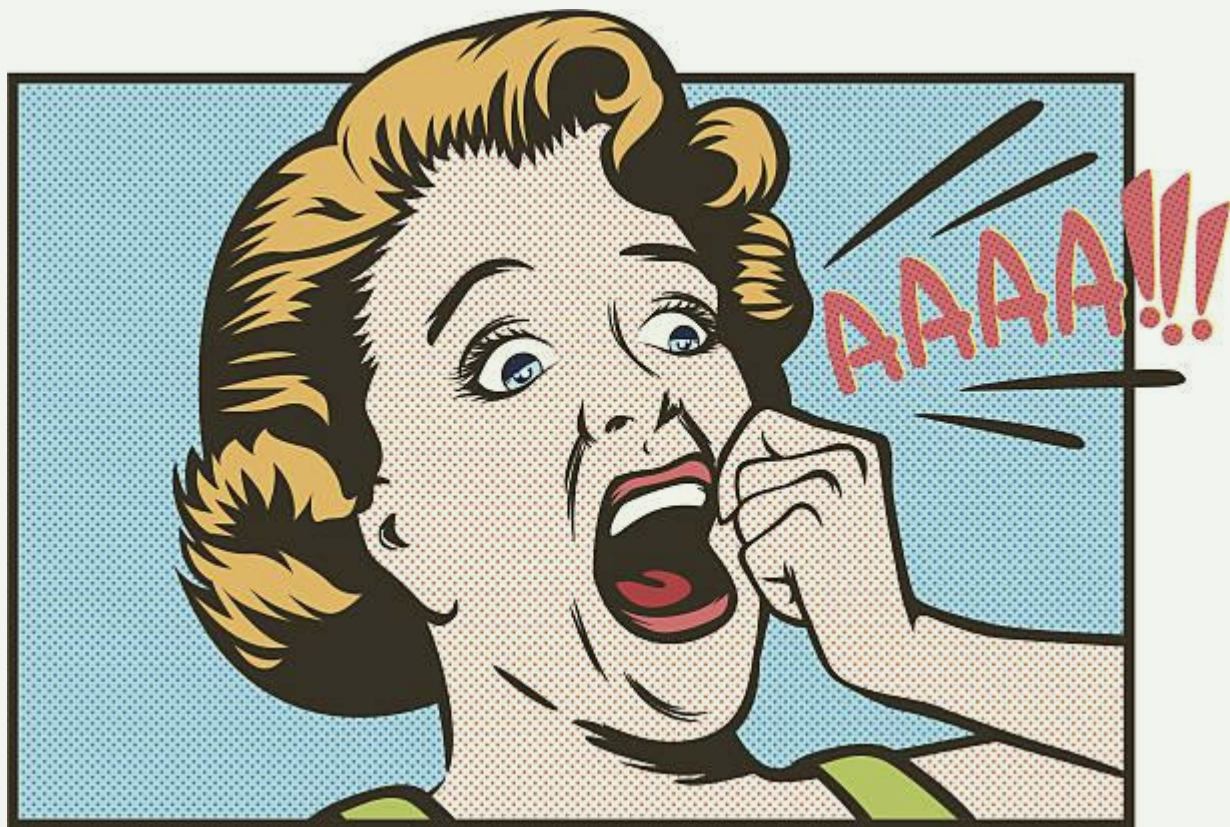


10.6

IDENTIFICAREA CENTRULUI DE COMANDĂ & CONTROL, CRIPTAT PE DISC ȘI ÎN RAM



IDENTIFICAREA CENTRULUI DE COMANDĂ & CONTROL, CRIPTAT PE DISC ȘI ÎN RAM



Această parte din prezentare
nu este publică! Este doar
pentru studenții ATM!

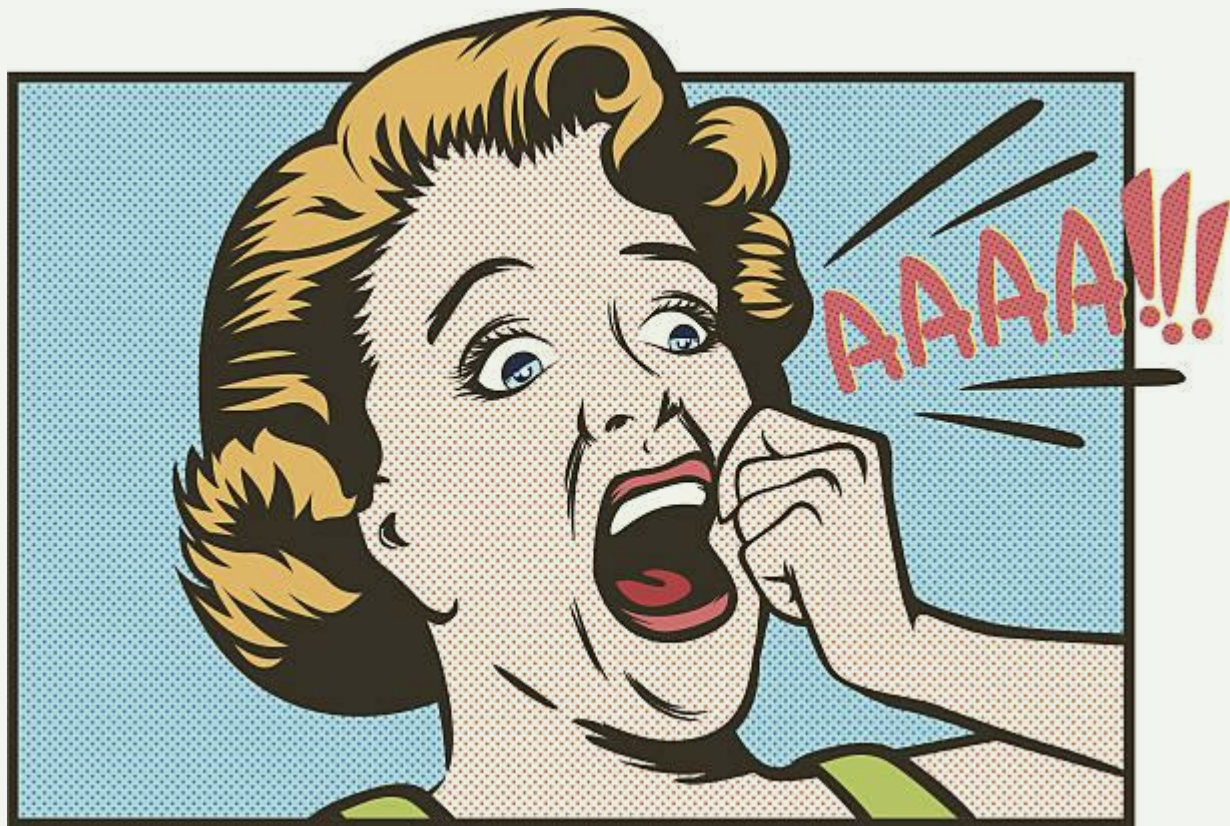


10.7

INTERCEPTAREA EXECUȚIEI MALWARE PRIN API



INTERCEPTAREA EXECUȚIEI MALWARE PRIN API



Această parte din prezentare
nu este publică! Este doar
pentru studenții ATM!

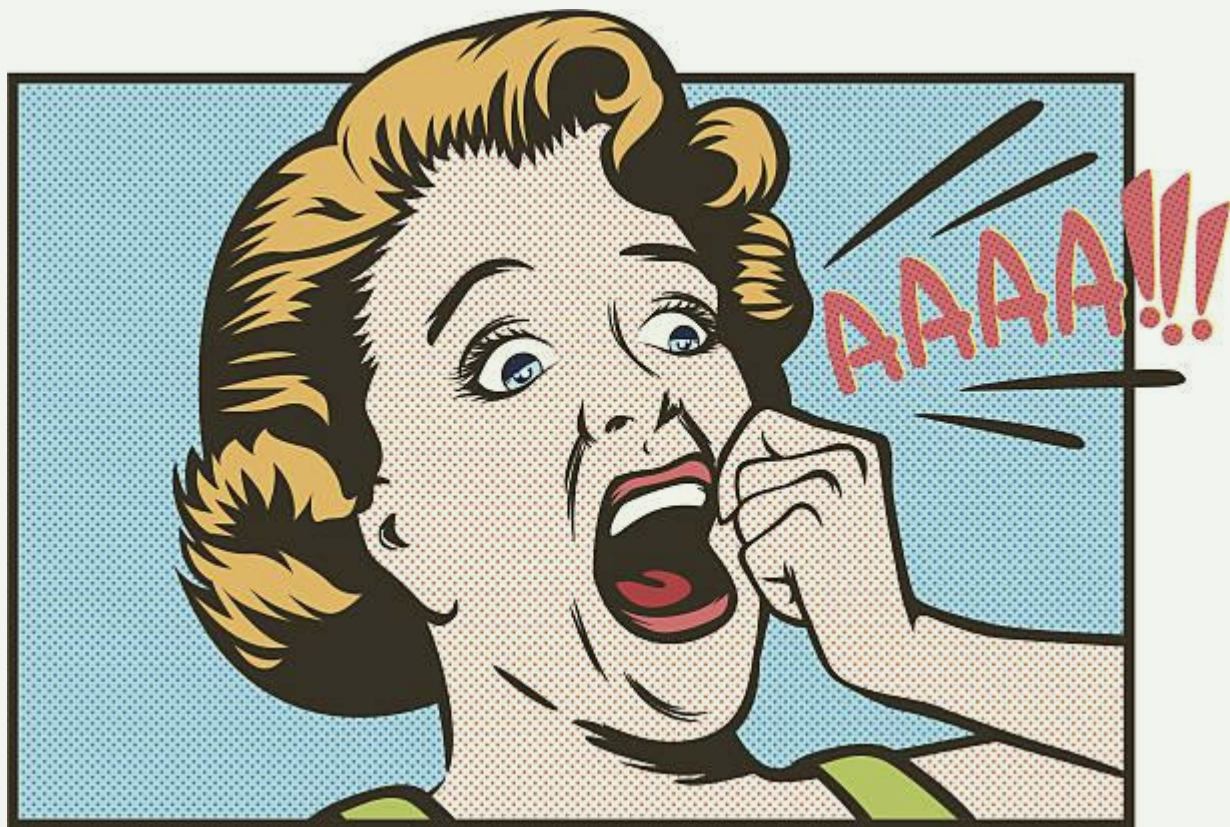


10.8

CRIPTAREA INSTRUCTIUNILOR IN SECTIUNEA .TEXT?



CRIPTAREA INSTRUCȚIUNILOR ÎN SECȚIUNEA .TEXT?



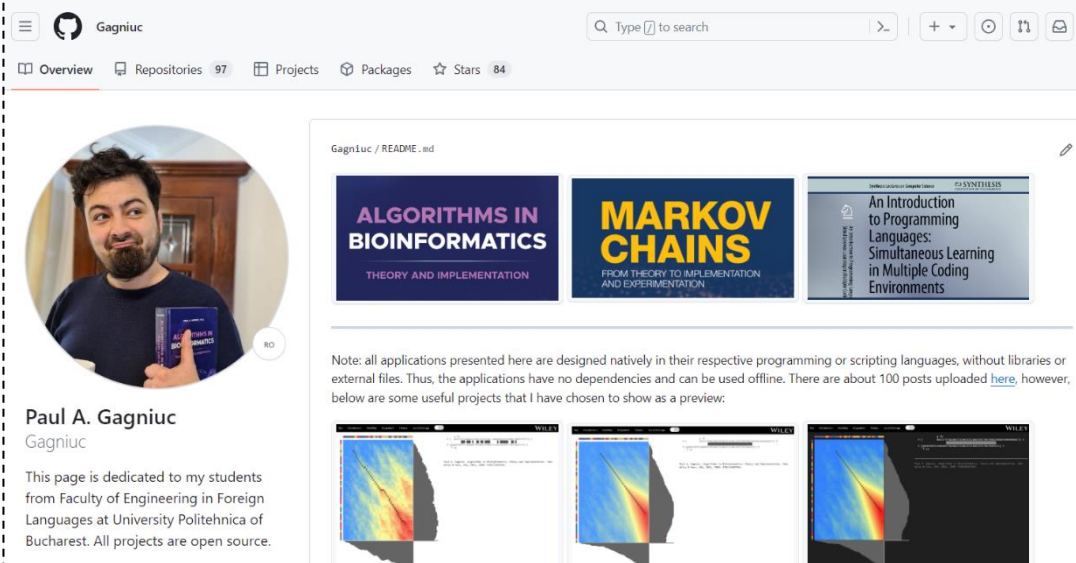
Această parte din prezentare
nu este publică! Este doar
pentru studenții ATM!



BIBLIOGRAFIE / RESURSE

- Paul A. Gagniuc. *Antivirus Engines: From Methods to Innovations, Design, and Applications*. Cambridge, MA: Elsevier Syngress, 2024. pp. 1-656.
- Paul A. Gagniuc. *An Introduction to Programming Languages: Simultaneous Learning in Multiple Coding Environments. Synthesis Lectures on Computer Science*. Springer International Publishing, 2023, pp. 1-280.
- Paul A. Gagniuc. *Coding Examples from Simple to Complex - Applications in MATLAB*, Springer, 2024, pp. 1-255.
- Paul A. Gagniuc. *Coding Examples from Simple to Complex - Applications in Python*, Springer, 2024, pp. 1-245.
- Paul A. Gagniuc. *Coding Examples from Simple to Complex - Applications in Javascript*, Springer, 2024, pp. 1-240.
- Paul A. Gagniuc. *Markov chains: from theory to implementation and experimentation*. Hoboken, NJ, John Wiley & Sons, USA, 2017, ISBN: 978-1-119-38755-8.

<https://github.com/gagniuc>



The screenshot shows the GitHub profile of Gagniuc. The header includes the username 'Gagniuc', a search bar, and navigation links for Overview, Repositories (97), Projects, Packages, Stars (84), and a notification bell. The profile picture shows a man with a beard holding a book. Below the profile picture, the name 'Paul A. Gagniuc' and the handle '@gagniuc' are displayed. A bio states: 'This page is dedicated to my students from Faculty of Engineering in Foreign Languages at University Politehnica of Bucharest. All projects are open source.' The 'Gagniuc / README.md' section features three book covers: 'ALGORITHMS IN BIOINFORMATICS', 'MARKOV CHAINS', and 'An Introduction to Programming Languages: Simultaneous Learning in Multiple Coding Environments'. A note below the books states: 'Note: all applications presented here are designed natively in their respective programming or scripting languages, without libraries or external files. Thus, the applications have no dependencies and can be used offline. There are about 100 posts uploaded [here](#), however, below are some useful projects that I have chosen to show as a preview.' At the bottom, three small images show heatmaps or data visualizations.