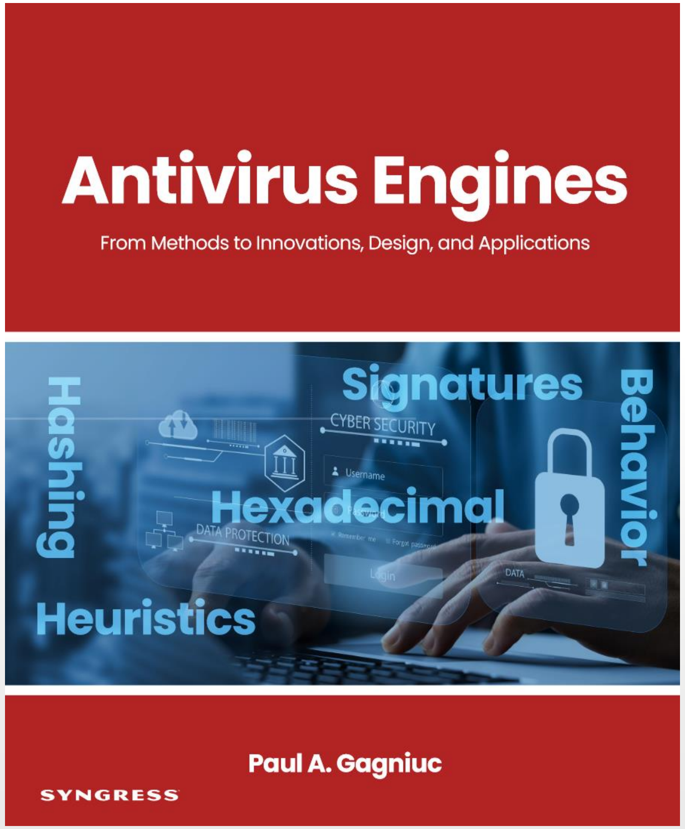
Antivirus engines

Paul A. GAGNIUC

Paul A. Gagniuc. *Antivirus Engines: From Methods to Innovations, Design, and Applications*. Cambridge, MA: Elsevier Syngress, 2024. pp. 1-656.



Antivirus Engines

From Methods to Innovations, Design, and Applications

Paul A. Gagniuc

SYNGRESS

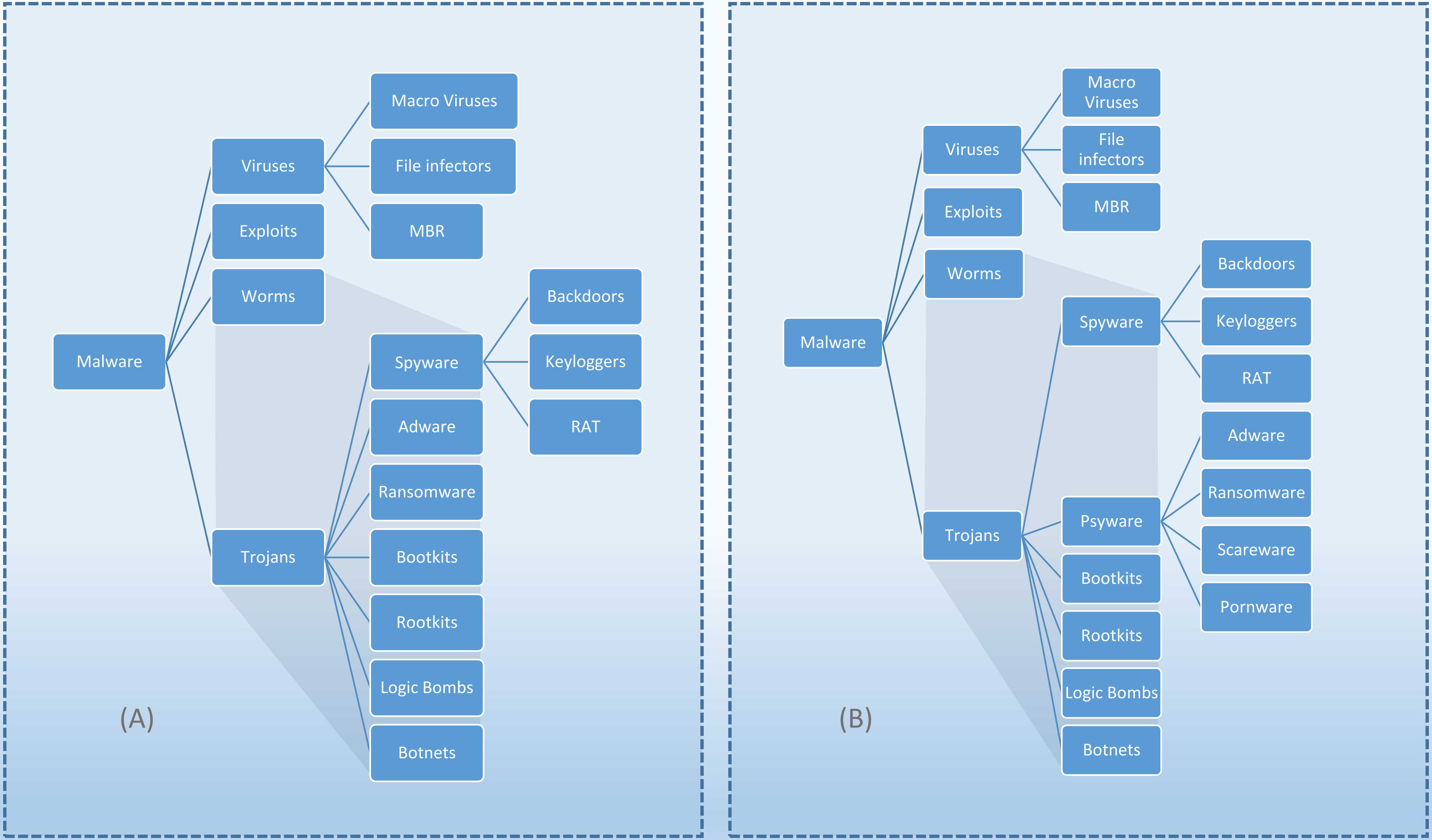
https://github.com/gagniuc/Antivirus-Engines

POLITEHNICA BUCUREȘTI

1818

National University of Science and Technology Politehnica Bucharest

Military Technical Academy "Ferdinand I"



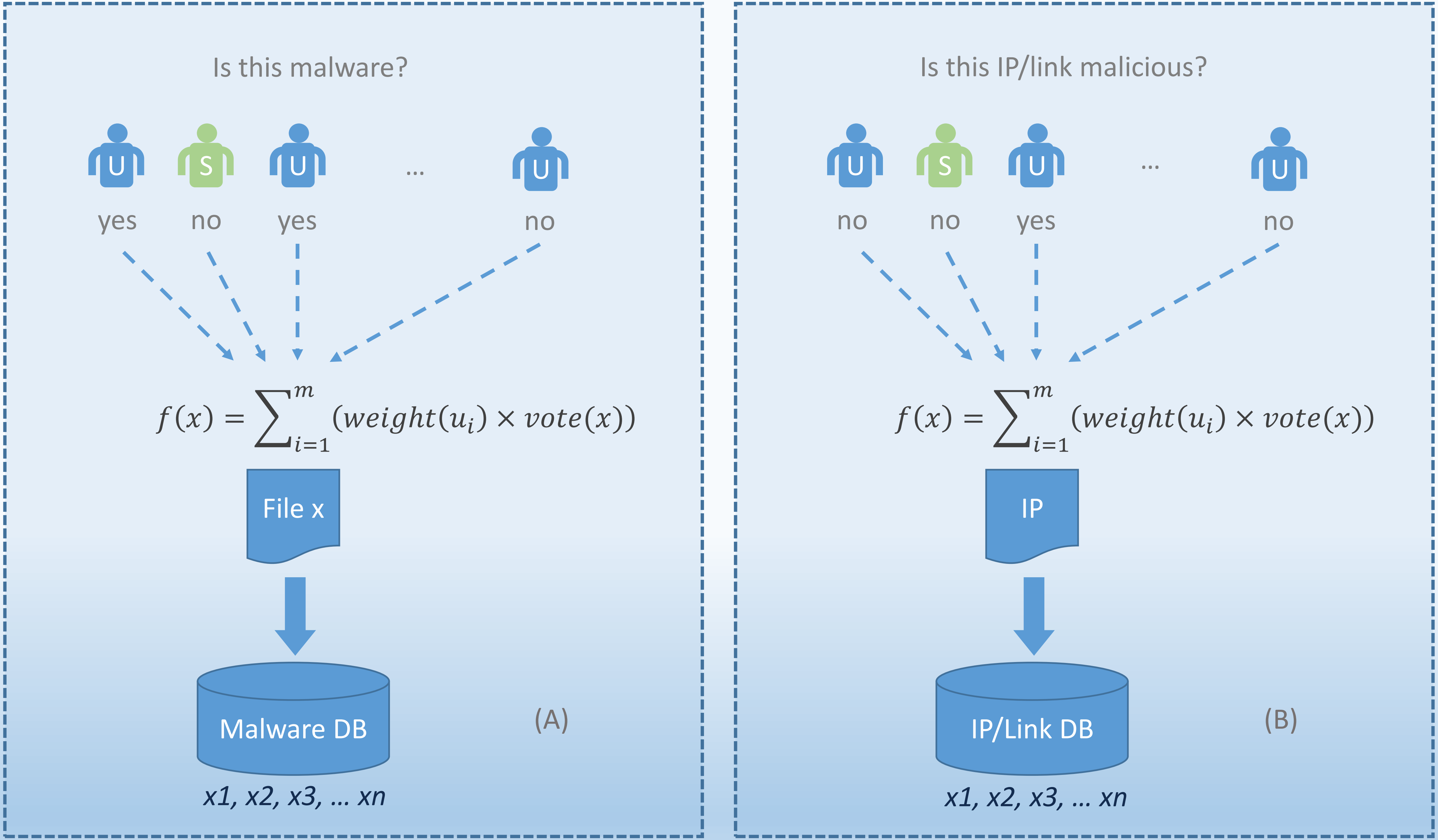
(A)

- Malware
  - Viruses
    - Macro Viruses
    - File infectors
    - MBR
  - Exploits
  - Worms
  - Trojans
    - Spyware
      - Backdoors
      - Keyloggers
      - RAT
    - Adware
    - Ransomware
    - Bootkits
    - Rootkits
    - Logic Bombs
    - Botnets

(B)

- Malware
  - Viruses
    - Macro Viruses
    - File infectors
    - MBR
  - Exploits
  - Worms
  - Trojans
    - Spyware
      - Backdoors
      - Keyloggers
      - RAT
    - Psyware
      - Adware
      - Ransomware
      - Scareware
      - Pornware
    - Bootkits
    - Rootkits
    - Logic Bombs
    - Botnets

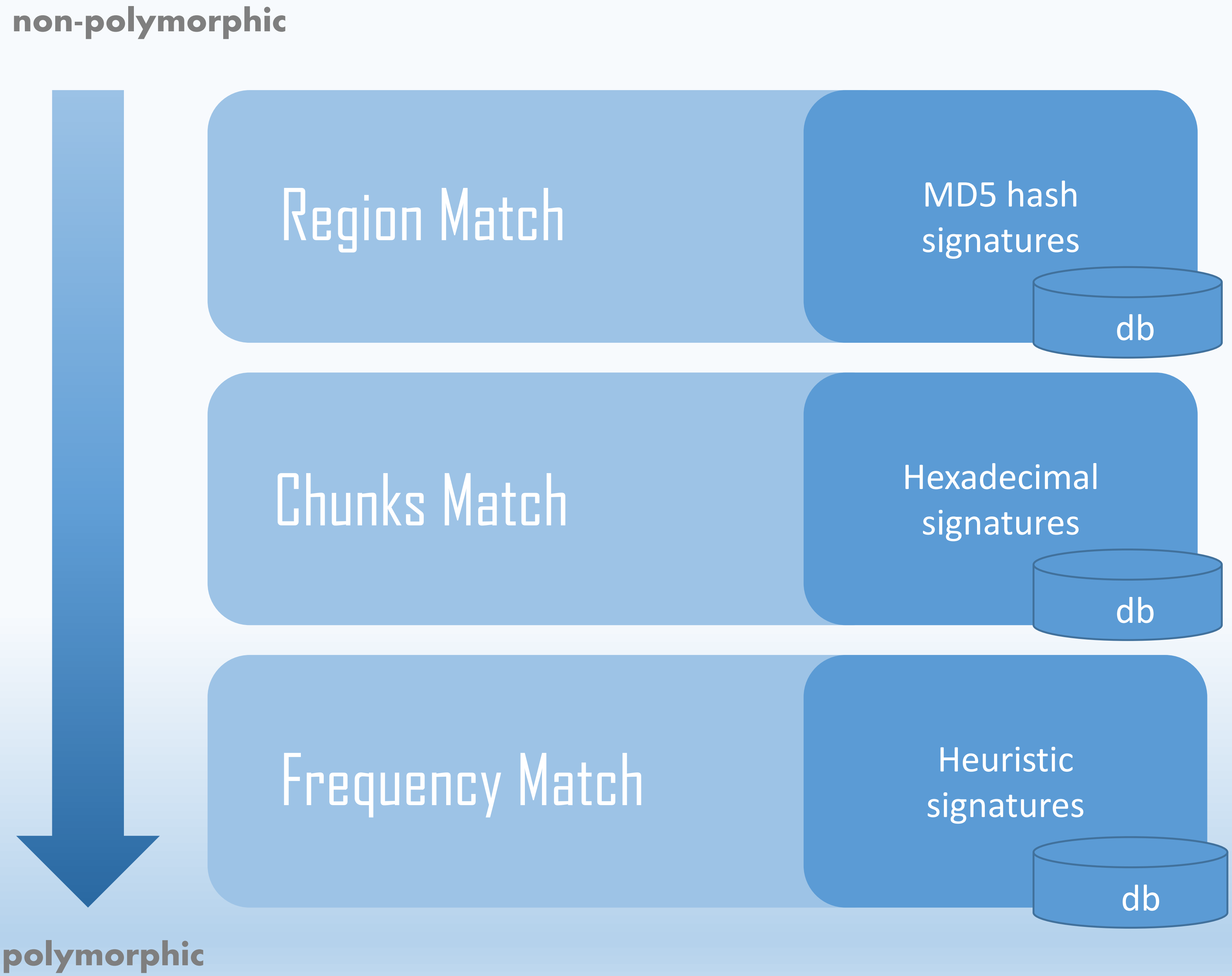
Paul A. Gagniuc. *Antivirus Engines: From Methods to Innovations, Design, and Applications*. Cambridge, MA: Elsevier Syngress, 2024. pp. 1-656.



$$f(x) = \sum_{i=1}^{m} (weight(u_i) \times vote(x))$$

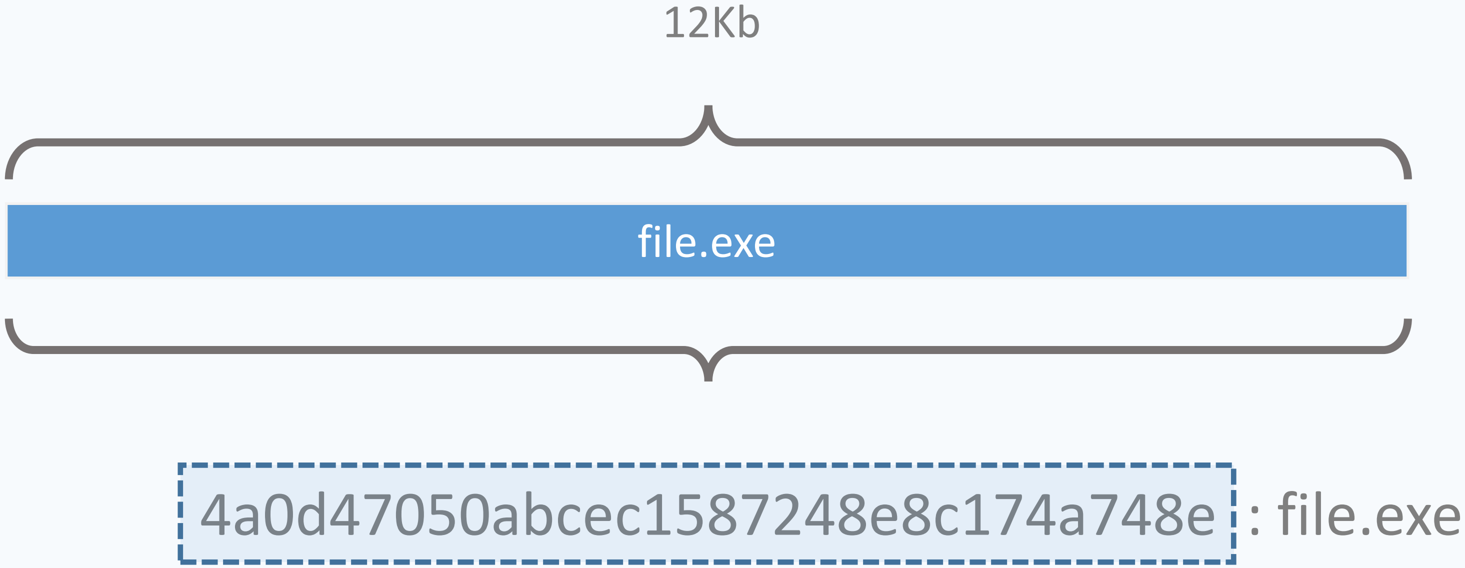
$$f(x) = \sum_{i=1}^{m} (weight(u_i) \times vote(x))$$

Paul A. Gagniuc. *Antivirus Engines: From Methods to Innovations, Design, and Applications*. Cambridge, MA: Elsevier Syngress, 2024. pp. 1-656.



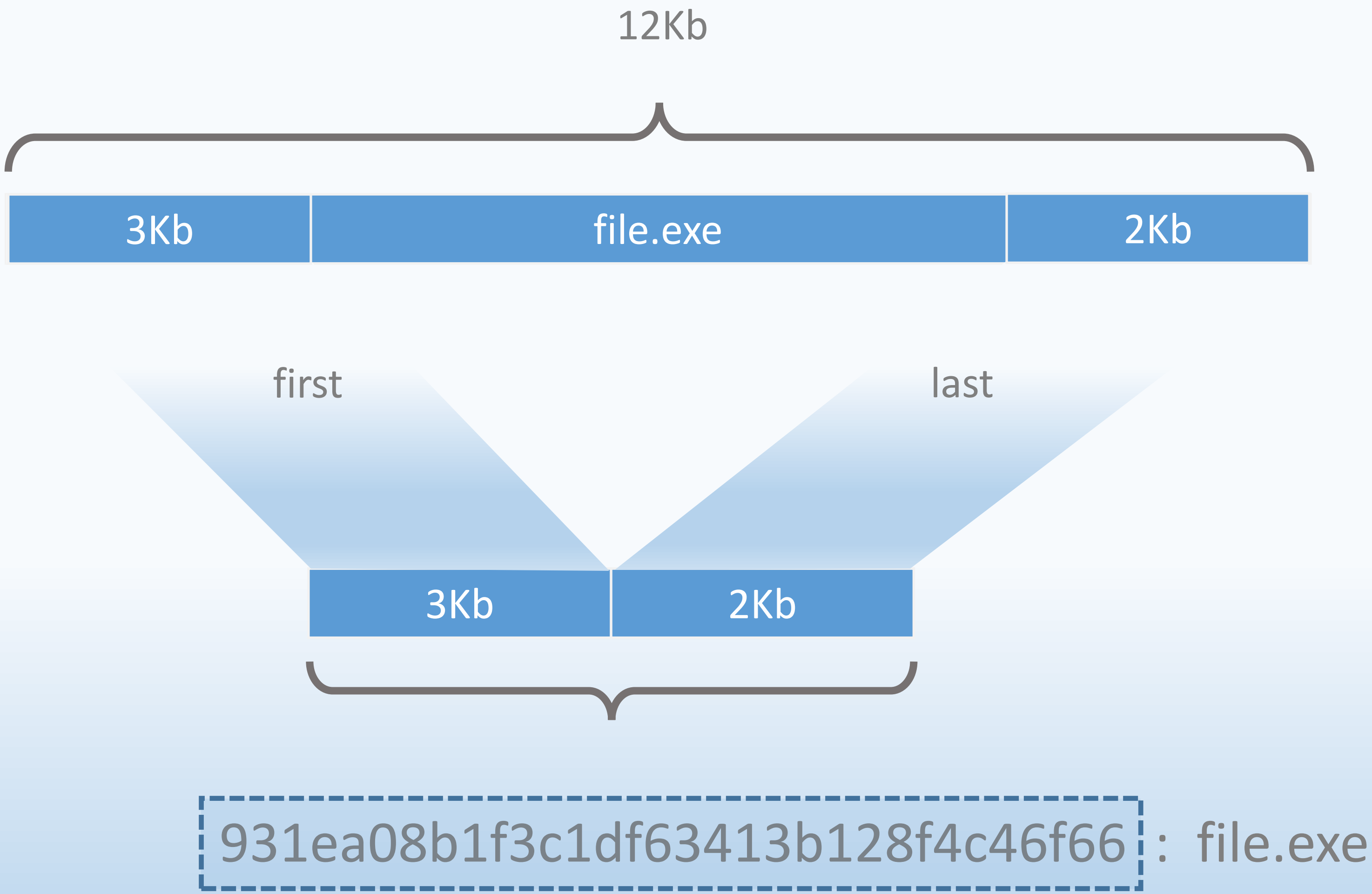
Paul A. Gagniuc. *Antivirus Engines: From Methods to Innovations, Design, and Applications*. Cambridge, MA: Elsevier Syngress, 2024. pp. 1-656.

MD5 signature



Paul A. Gagniuc. *Antivirus Engines: From Methods to Innovations, Design, and Applications*. Cambridge, MA: Elsevier Syngress, 2024. pp. 1-656.

MD5 signature



12Kb

3Kb

file.exe

2Kb

first

last

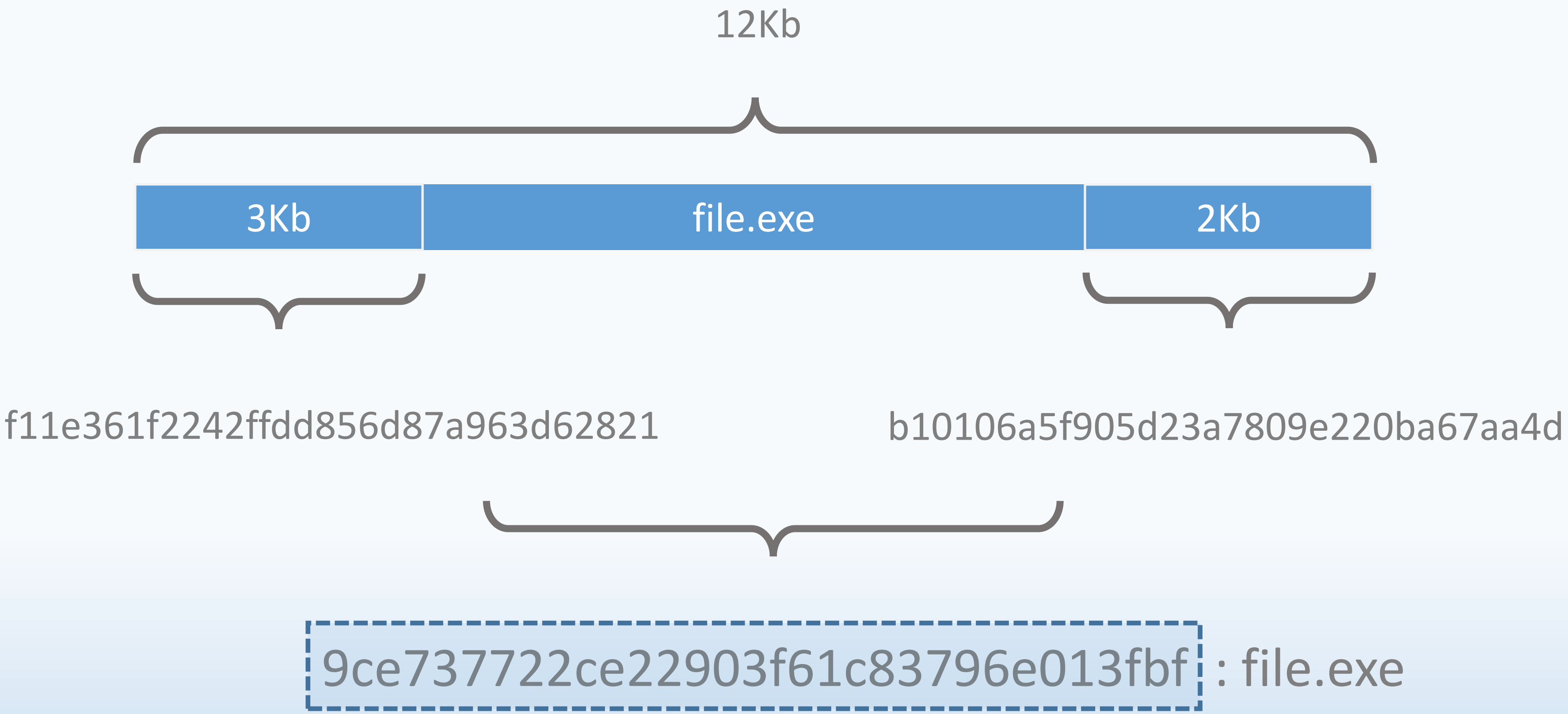
3Kb

2Kb

931ea08b1f3c1df63413b128f4c46f66 : file.exe

Paul A. Gagniuc. *Antivirus Engines: From Methods to Innovations, Design, and Applications*. Cambridge, MA: Elsevier Syngress, 2024. pp. 1-656.

MD5 signature



12Kb

3Kb

file.exe

2Kb

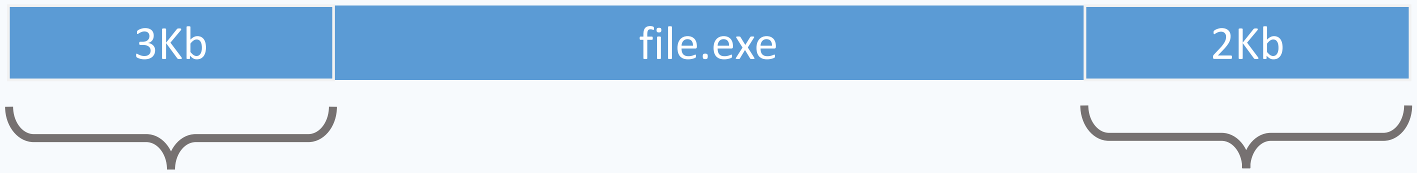
f11e361f2242ffdd856d87a963d62821

b10106a5f905d23a7809e220ba67aa4d

9ce737722ce22903f61c83796e013fbf : file.exe

Paul A. Gagniuc. *Antivirus Engines: From Methods to Innovations, Design, and Applications*. Cambridge, MA: Elsevier Syngress, 2024. pp. 1-656.

MD5 signature

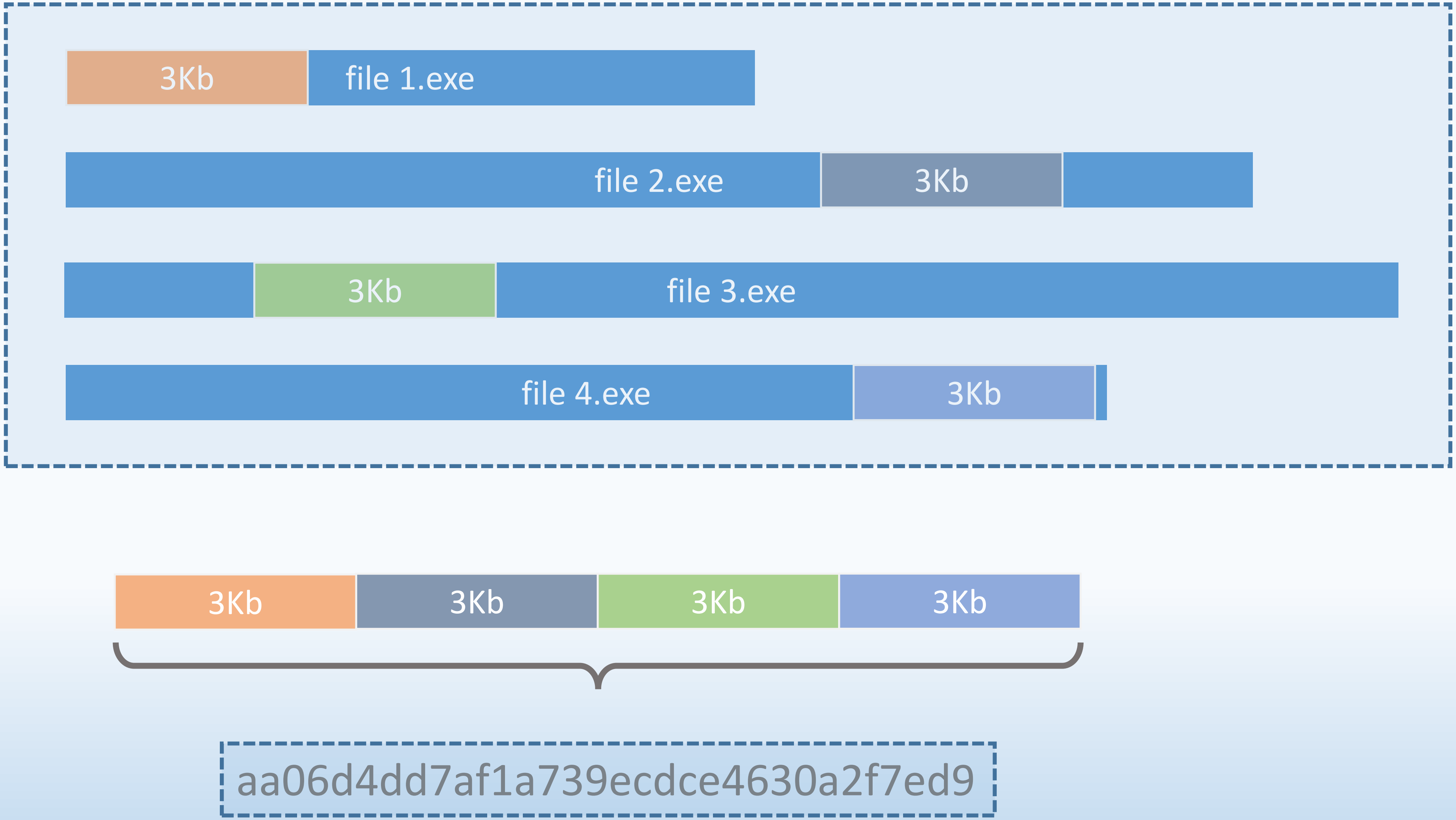


931ea08b1f3c1df63413b128f4c46f66

9ce737722ce22903f61c83796e013fbf

7fa24b9db9b313523977d14b27a7a676 : 9ce737722ce22903f61c83796e013fbf : file.exe

Paul A. Gagniuc. *Antivirus Engines: From Methods to Innovations, Design, and Applications*. Cambridge, MA: Elsevier Syngress, 2024. pp. 1-656.



3Kb

file 1.exe

file 2.exe

3Kb

3Kb

file 3.exe

file 4.exe

3Kb

3Kb

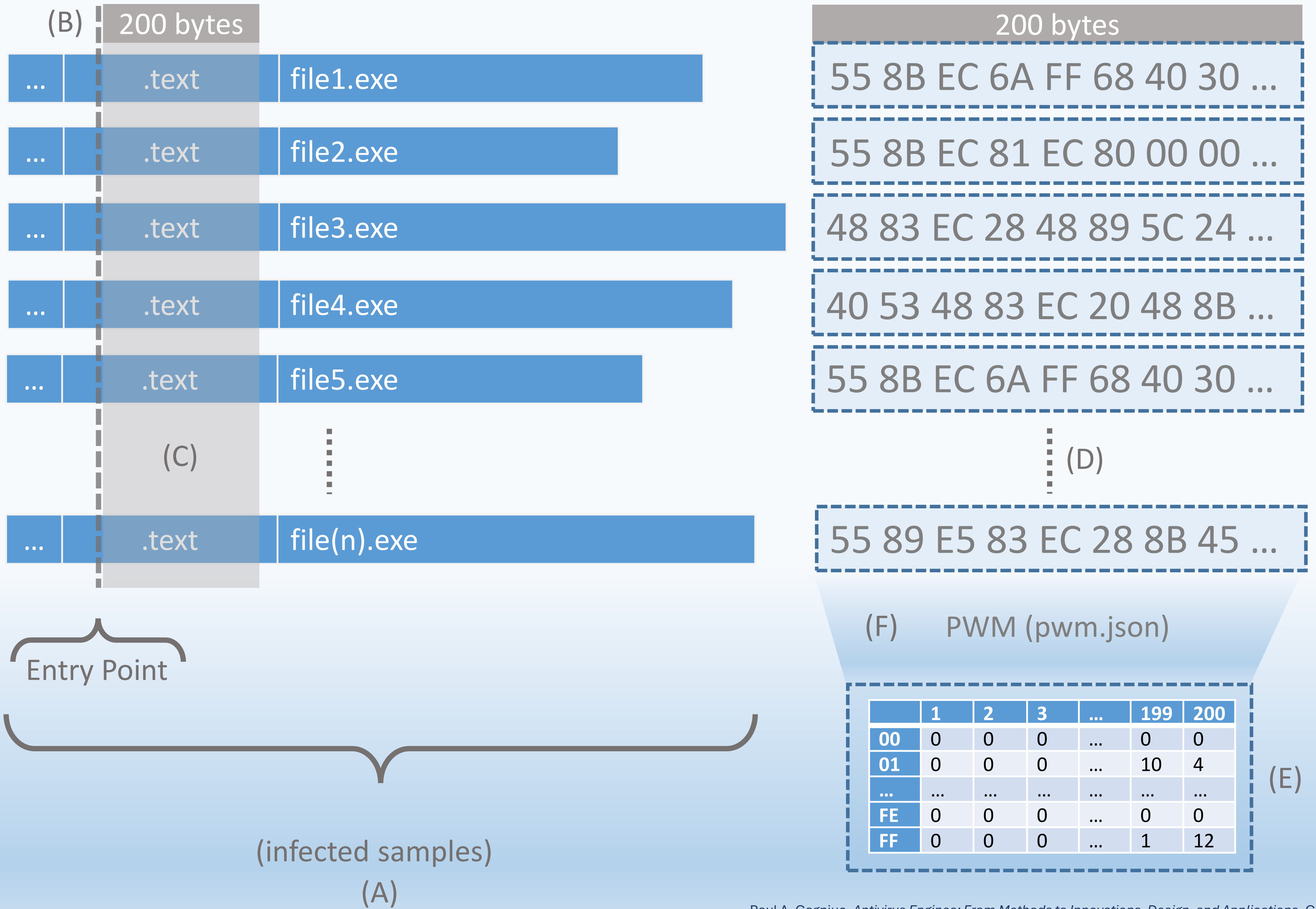
3Kb

3Kb

3Kb

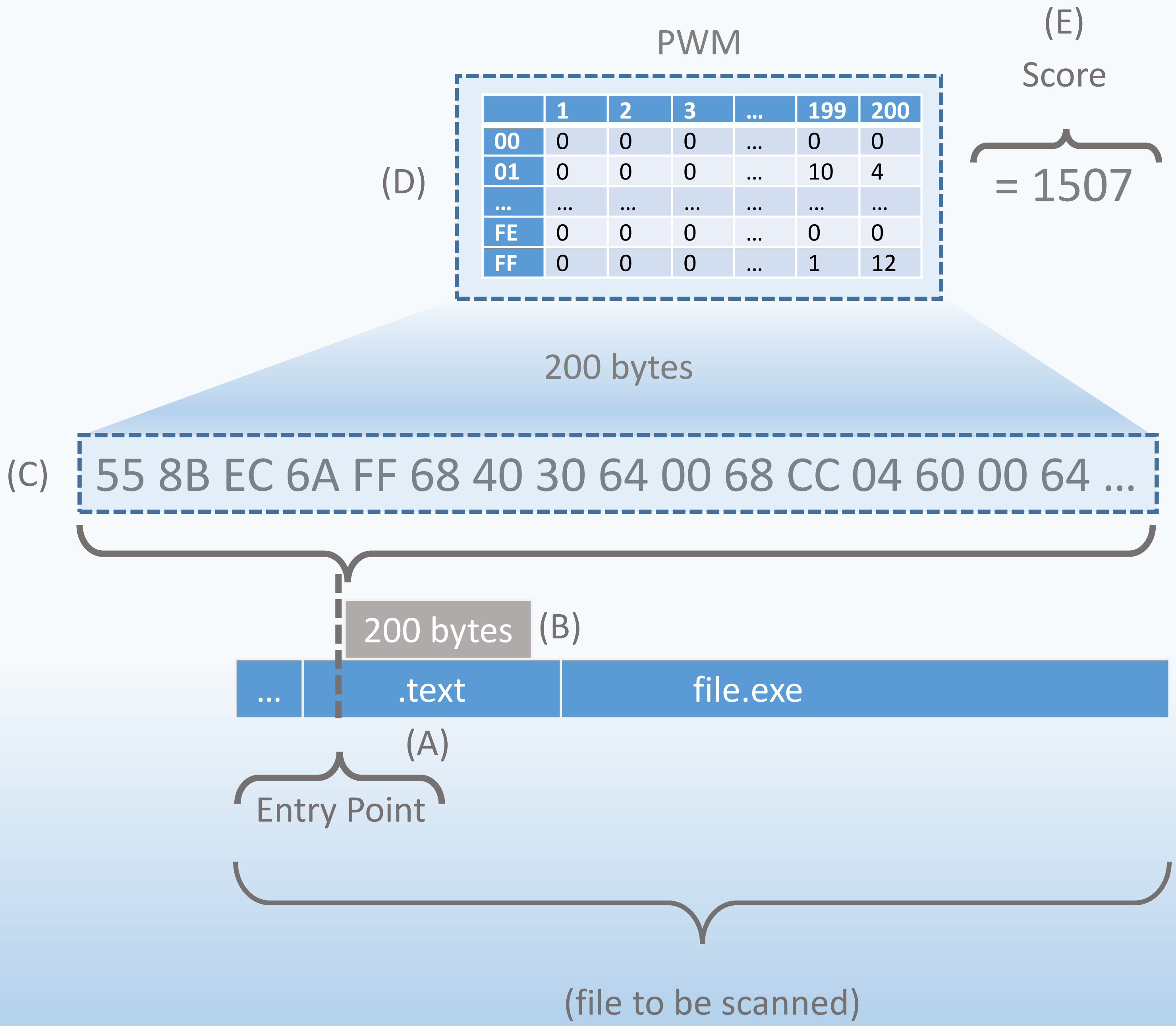
aa06d4dd7af1a739ecdce4630a2f7ed9

Paul A. Gagniuc. *Antivirus Engines: From Methods to Innovations, Design, and Applications*. Cambridge, MA: Elsevier Syngress, 2024. pp. 1-656.



	1	2	3	...	199	200
00	0	0	0	...	0	0
01	0	0	0	...	10	4
...	...	...	...	...	...	...
FE	0	0	0	...	0	0
FF	0	0	0	...	1	12

Paul A. Gagniuc. *Antivirus Engines: From Methods to Innovations, Design, and Applications*. Cambridge, MA: Elsevier Syngress, 2024. pp. 1-656.



PWM

(D)

	1	2	3	...	199	200
00	0	0	0	...	0	0
01	0	0	0	...	10	4
...	...	...	...	...	...	...
FE	0	0	0	...	0	0
FF	0	0	0	...	1	12

(E)

Score

= 1507

200 bytes

(C) 55 8B EC 6A FF 68 40 30 64 00 68 CC 04 60 00 64 ...

200 bytes (B)

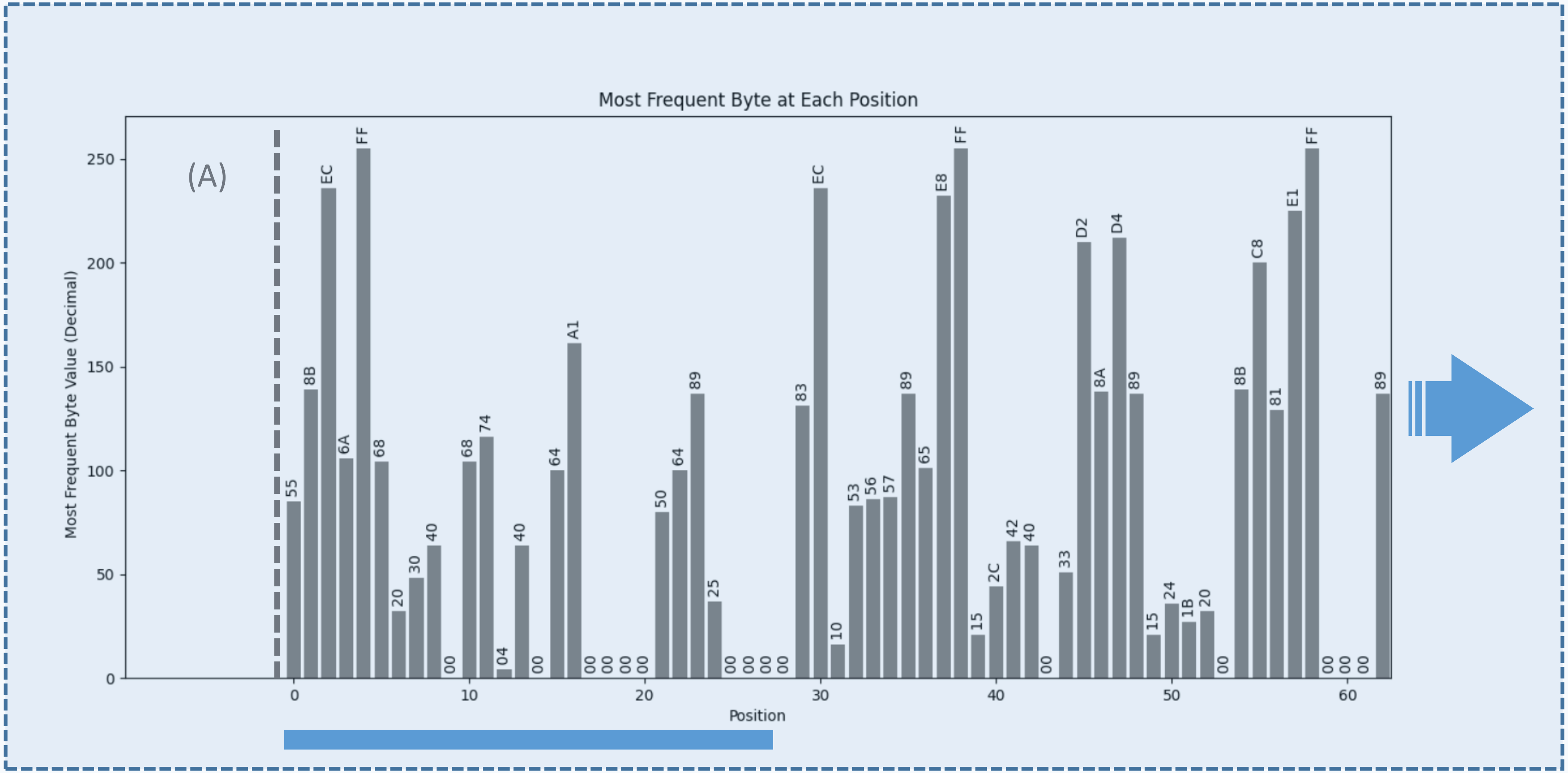
... .text file.exe

(A)

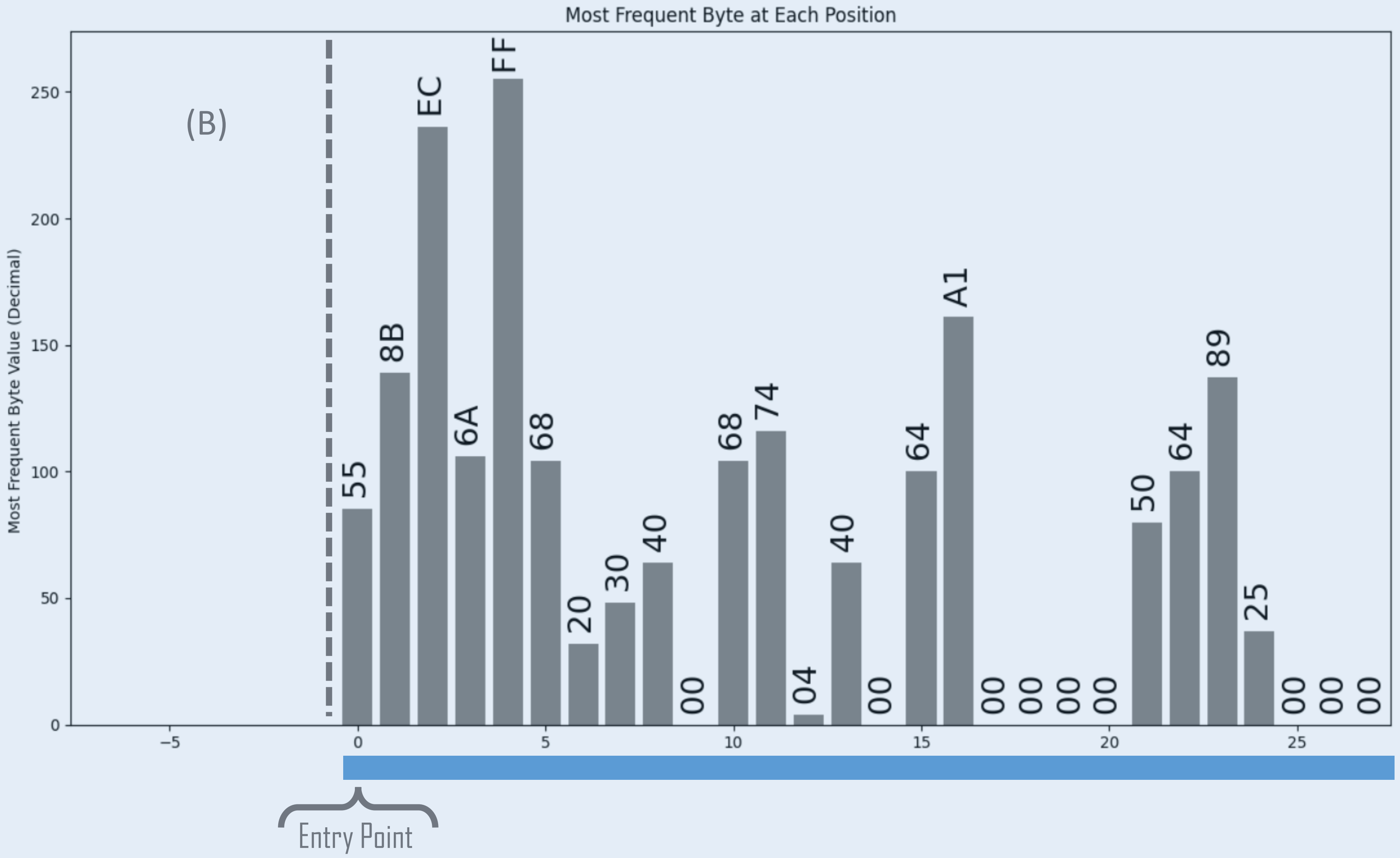
Entry Point

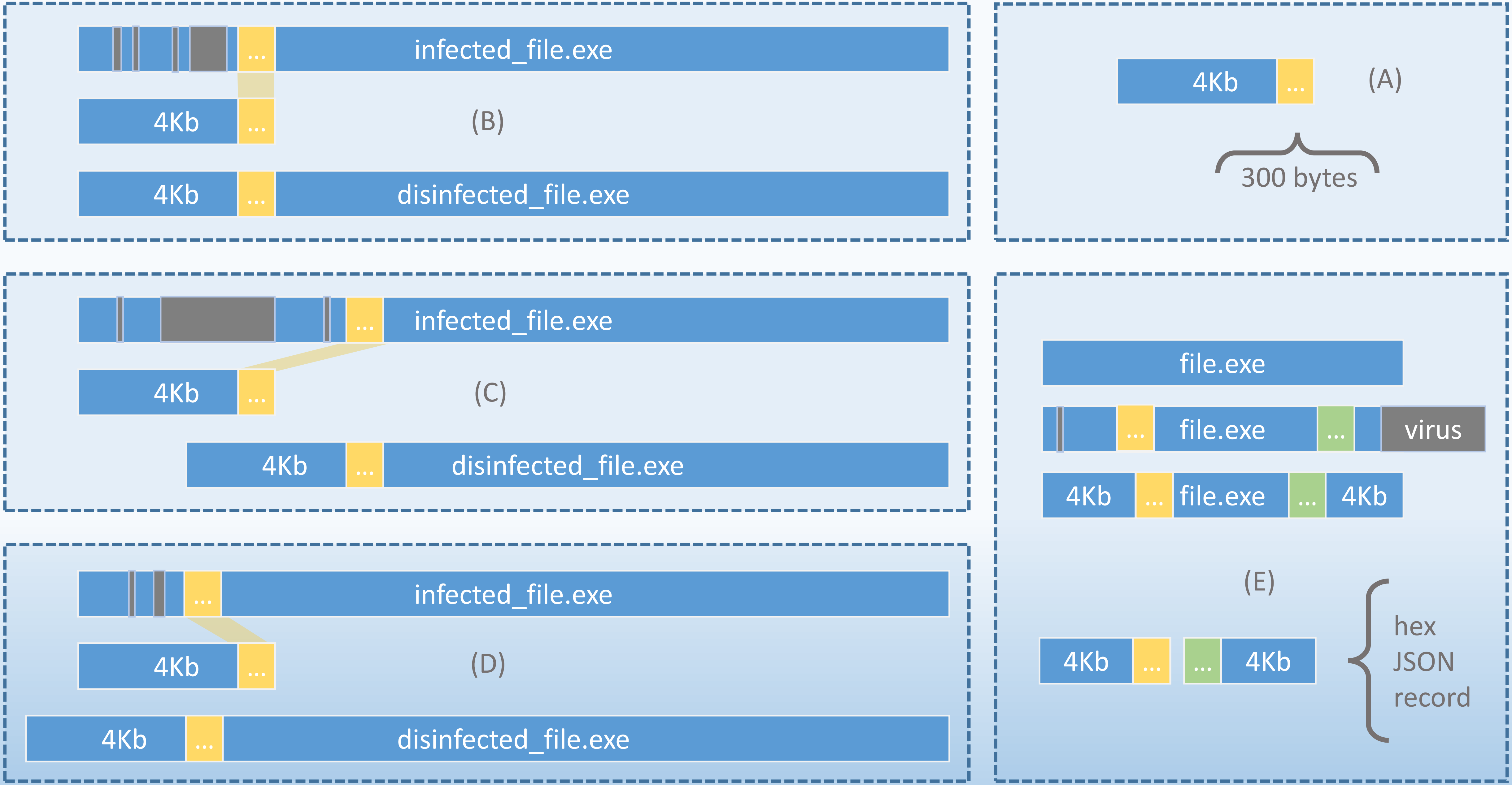
(file to be scanned)

Paul A. Gagniuc. *Antivirus Engines: From Methods to Innovations, Design, and Applications*. Cambridge, MA: Elsevier Syngress, 2024. pp. 1-656.

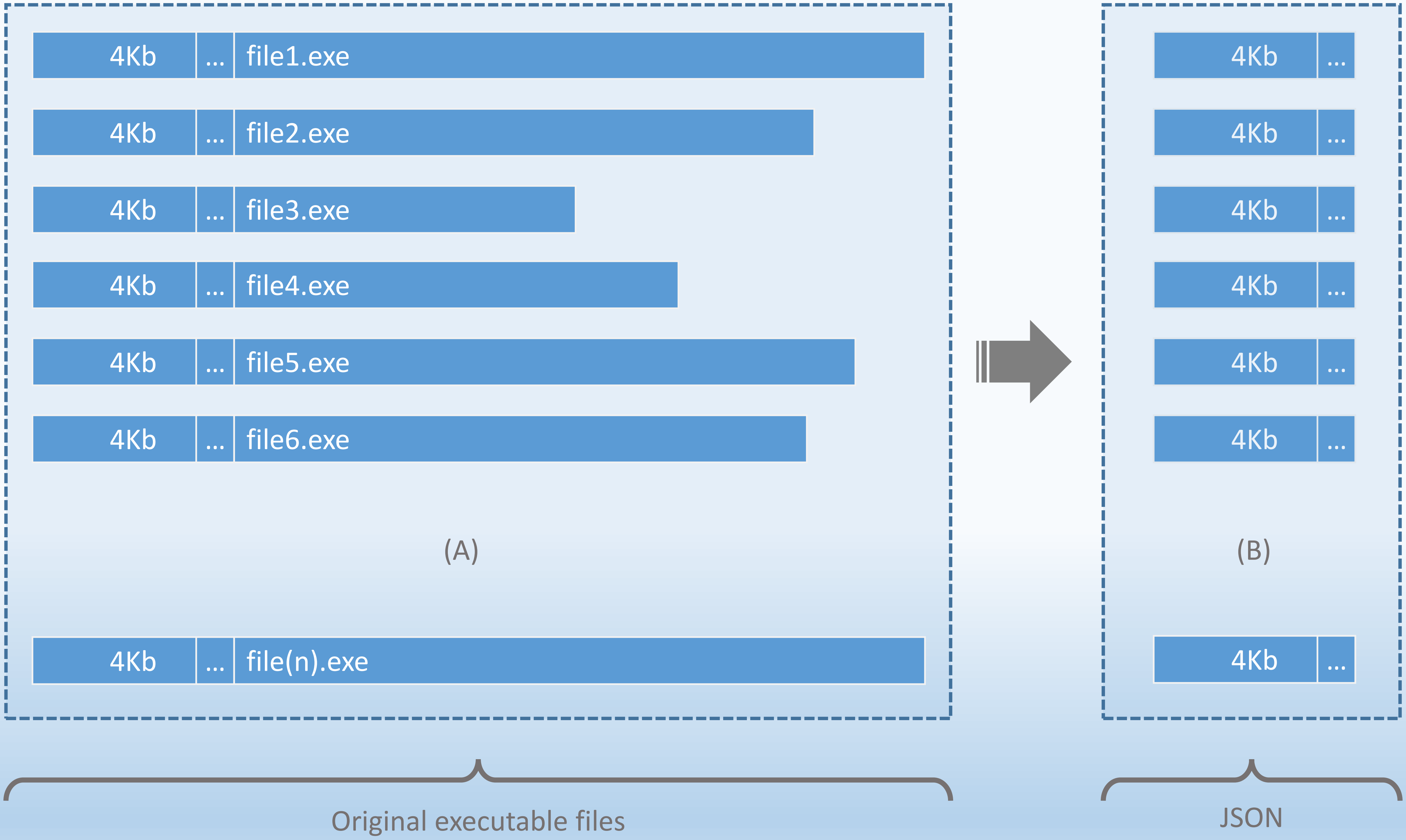

Most Frequent Byte at Each Position
(A)
Most Frequent Byte Value (Decimal)
0
50
100
150
200
250
Position
0
10
20
30
40
50
60
55
8B
EC
6A
FF
68
20
30
40
00
68
74
04
40
00
64
A1
00
00
00
00
50
64
89
25
00
00
00
00
83
EC
10
53
56
57
89
65
E8
FF
15
2C
42
40
00
33
D2
8A
D4
89
15
24
1B
20
00
8B
C8
81
E1
FF
00
00
00
89

Entry Point


Most Frequent Byte at Each Position
(B)
Most Frequent Byte Value (Decimal)
250
200
150
100
50
0
−5
0
5
10
15
20
25
55
8B
EC
6A
FF
68
20
30
40
00
68
74
04
40
00
64
A1
00
00
00
00
50
64
89
25
00
00
00
Entry Point



Paul A. Gagniuc. *Antivirus Engines: From Methods to Innovations, Design, and Applications*. Cambridge, MA: Elsevier Syngress, 2024. pp. 1-656.



4Kb ... file1.exe

4Kb ... file2.exe

4Kb ... file3.exe

4Kb ... file4.exe

4Kb ... file5.exe

4Kb ... file6.exe

(A)

4Kb ... file(n).exe

Original executable files

4Kb ...

4Kb ...

4Kb ...

4Kb ...

4Kb ...

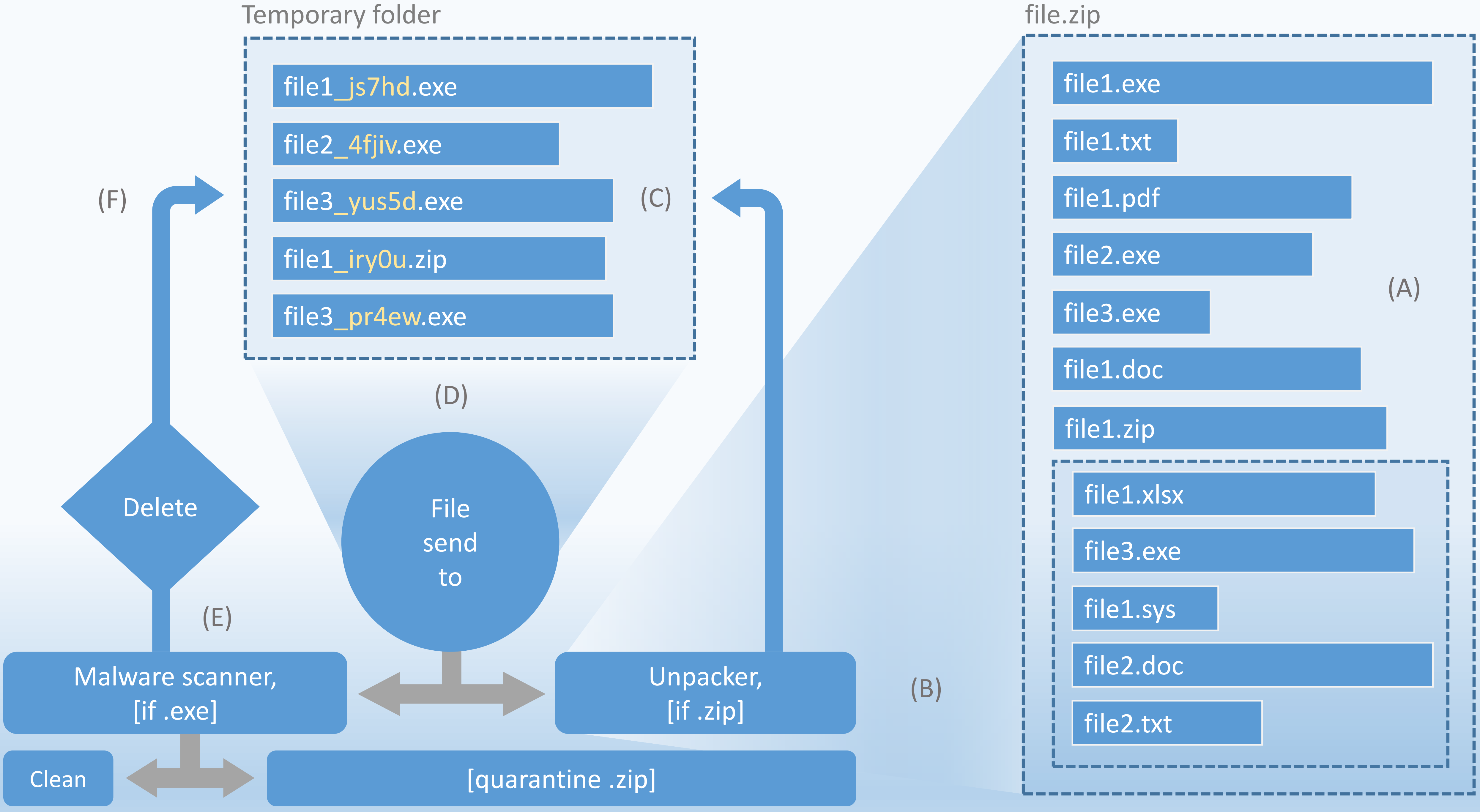
4Kb ...

(B)

4Kb ...

JSON

Paul A. Gagniuc. *Antivirus Engines: From Methods to Innovations, Design, and Applications*. Cambridge, MA: Elsevier Syngress, 2024. pp. 1-656.



Temporary folder

file1_js7hd.exe

file2_4fjiv.exe

file3_yus5d.exe

file1_iry0u.zip

file3_pr4ew.exe

(C)

(F)

(D)

File send to

Delete

(E)

Malware scanner, [if .exe]

Unpacker, [if .zip]

Clean

[quarantine .zip]

(B)

file.zip

file1.exe

file1.txt

file1.pdf

file2.exe

file3.exe

file1.doc

file1.zip

(A)

file1.xlsx

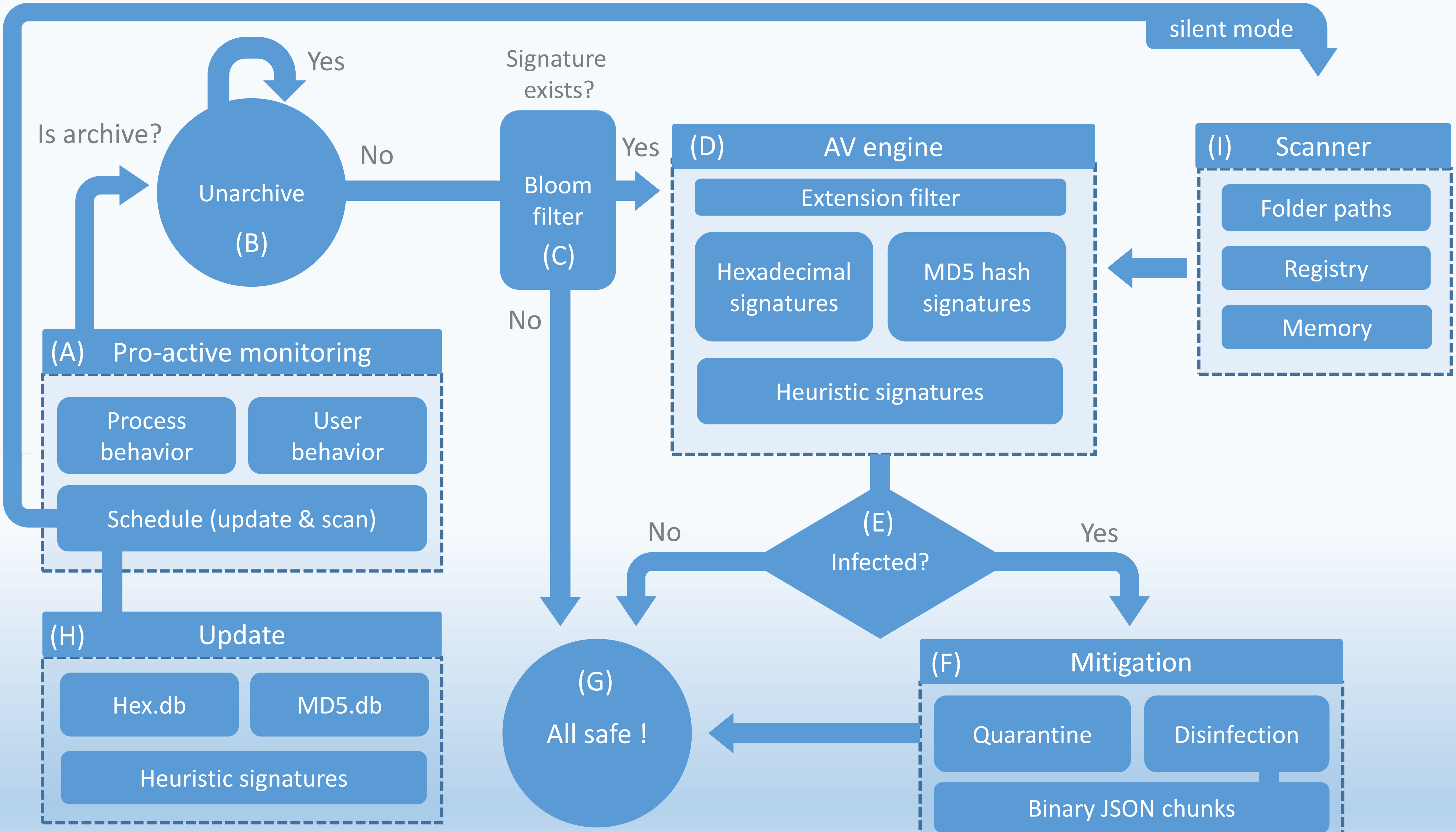
file3.exe

file1.sys

file2.doc

file2.txt

Paul A. Gagniuc. *Antivirus Engines: From Methods to Innovations, Design, and Applications*. Cambridge, MA: Elsevier Syngress, 2024. pp. 1-656.



silent mode

Is archive?

Yes

Unarchive

(B)

No

Signature exists?

Bloom filter

(C)

Yes

No

(D) AV engine

Extension filter

Hexadecimal signatures

MD5 hash signatures

Heuristic signatures

(I) Scanner

Folder paths

Registry

Memory

(A) Pro-active monitoring

Process behavior

User behavior

Schedule (update & scan)

(E)

Infected?

No

Yes

(H) Update

Hex.db

MD5.db

Heuristic signatures

(G)

All safe !

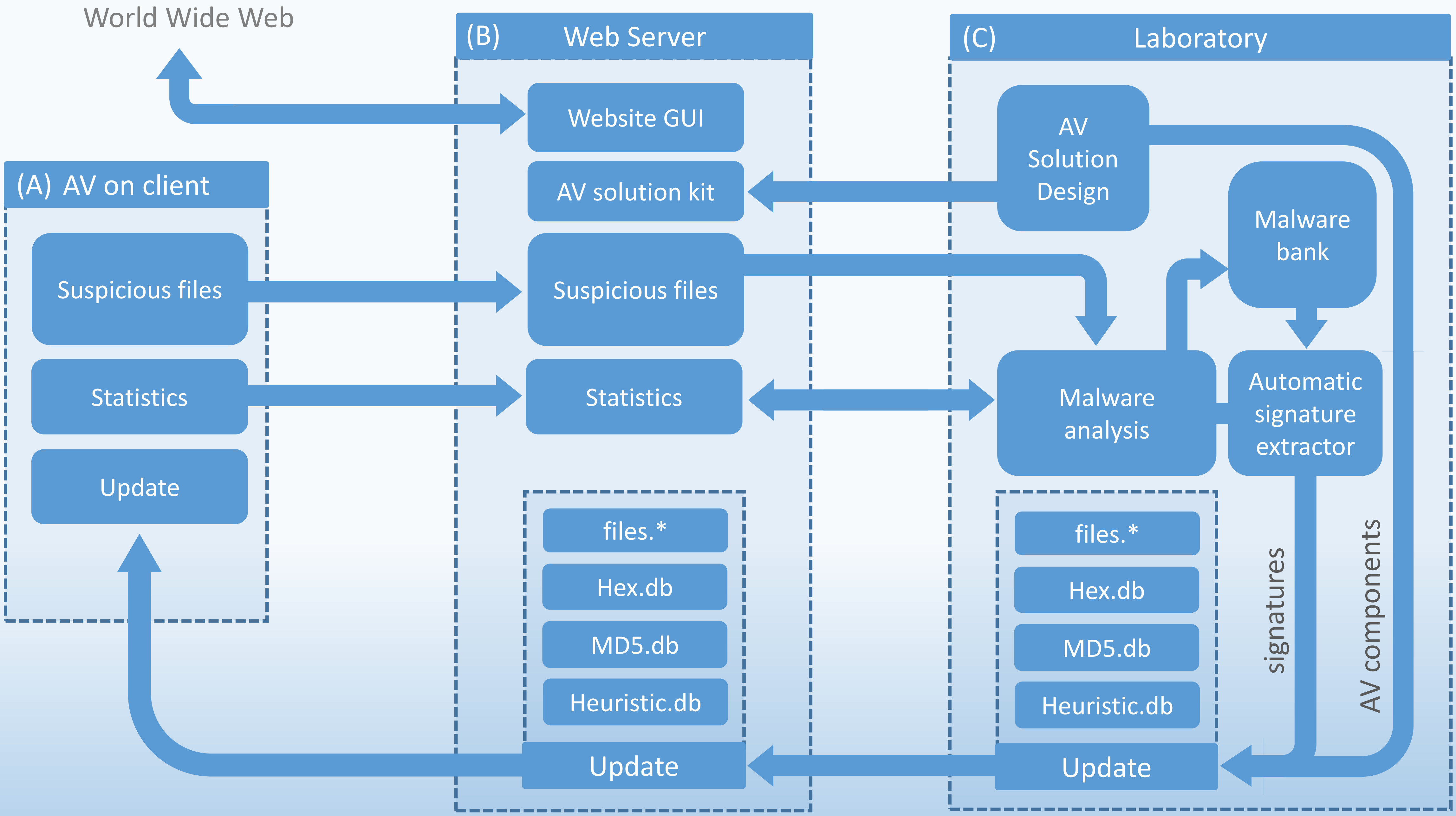
(F) Mitigation

Quarantine

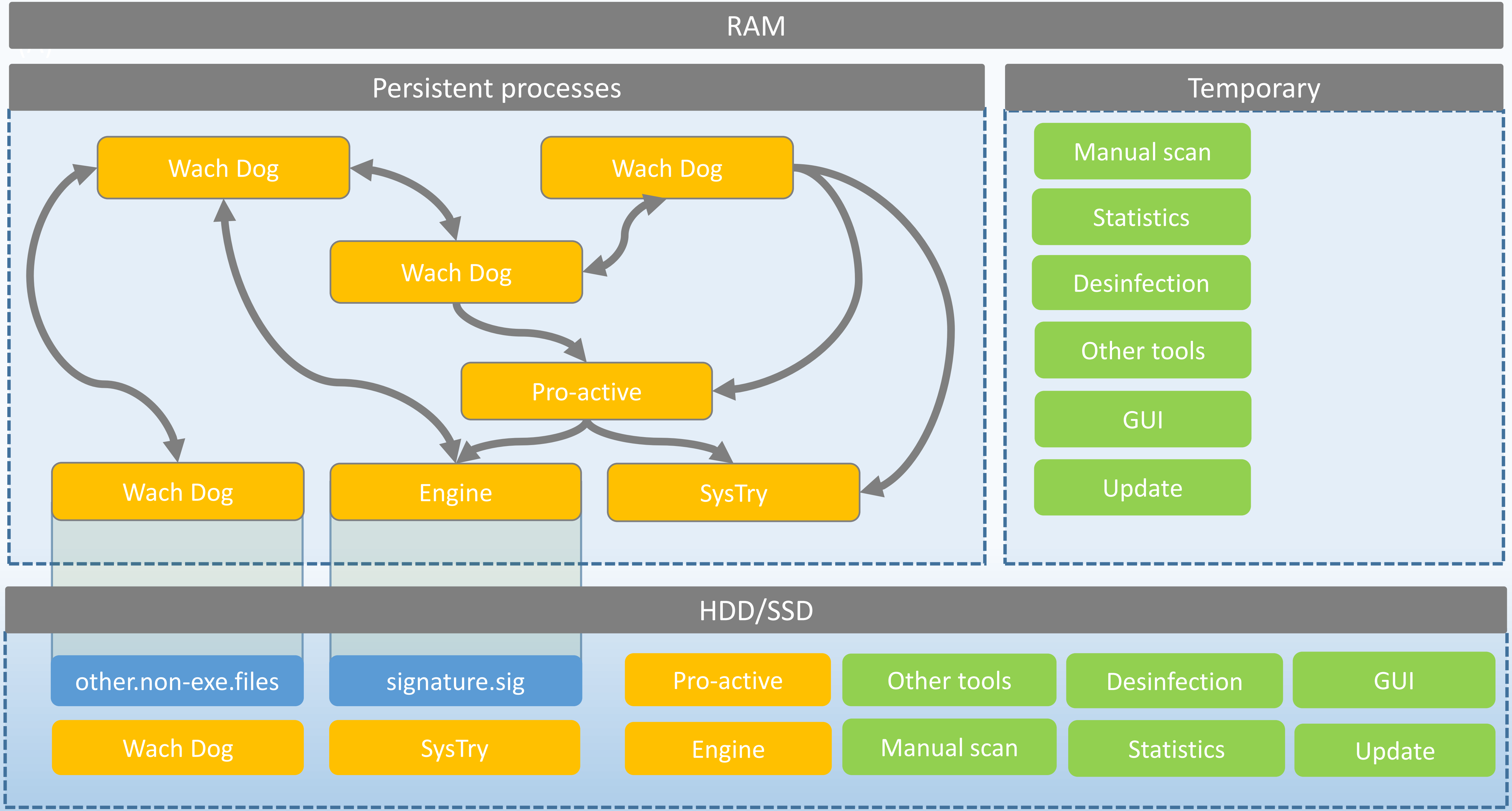
Disinfection

Binary JSON chunks

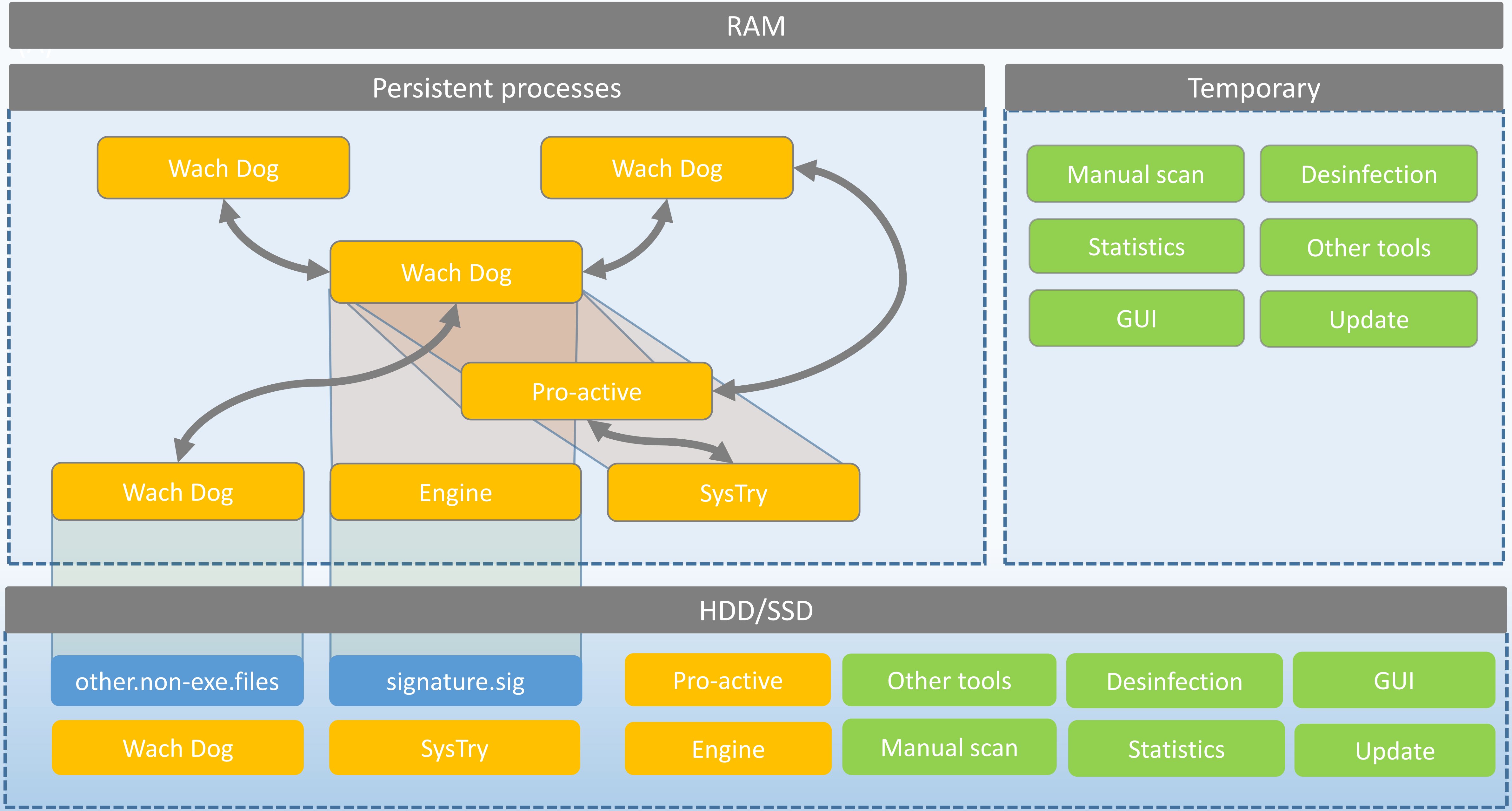
Paul A. Gagniuc. *Antivirus Engines: From Methods to Innovations, Design, and Applications*. Cambridge, MA: Elsevier Syngress, 2024. pp. 1-656.



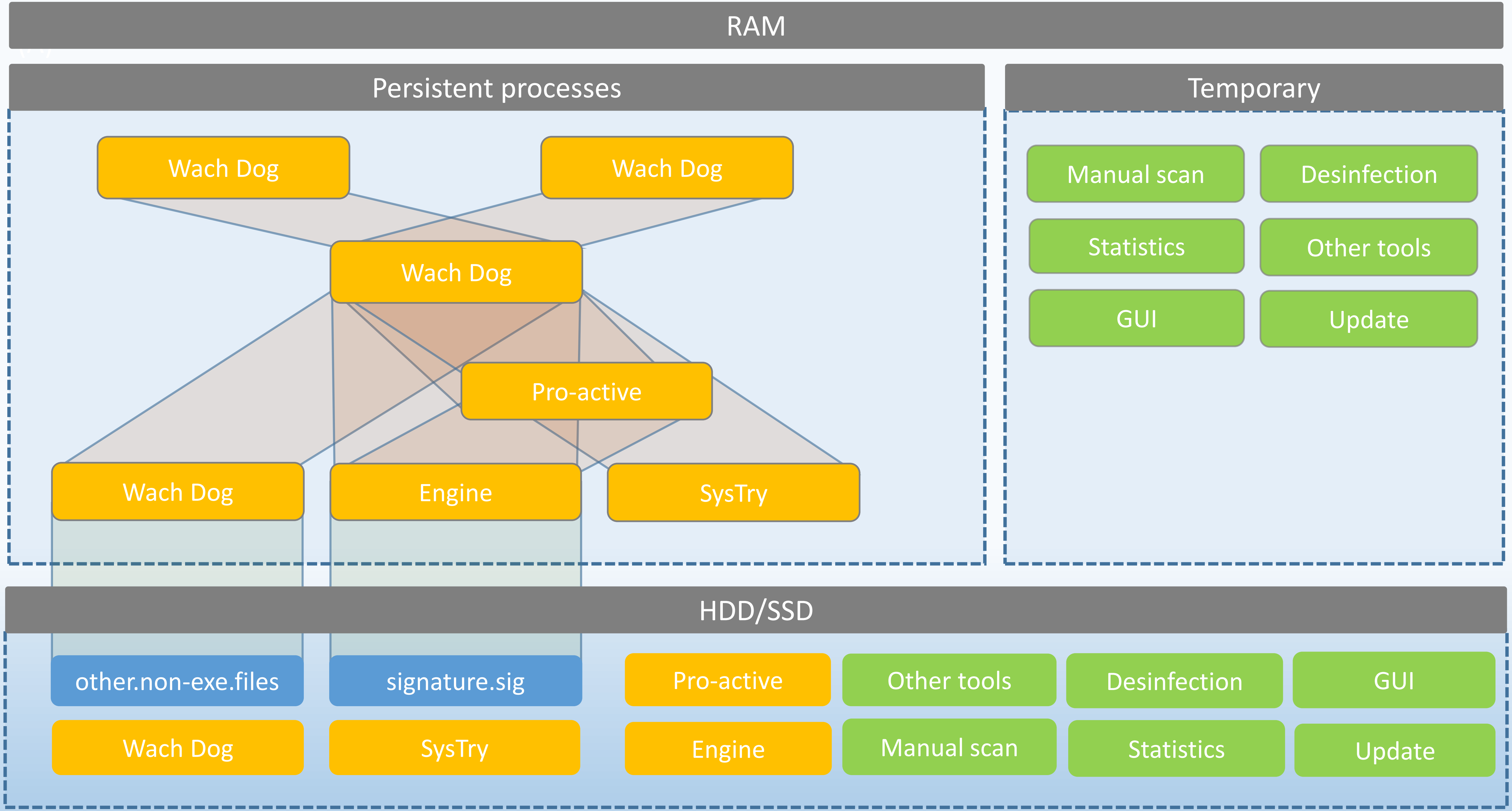
Paul A. Gagniuc. *Antivirus Engines: From Methods to Innovations, Design, and Applications*. Cambridge, MA: Elsevier Syngress, 2024. pp. 1-656.



Paul A. Gagniuc. *Antivirus Engines: From Methods to Innovations, Design, and Applications*. Cambridge, MA: Elsevier Syngress, 2024. pp. 1-656.



Paul A. Gagniuc. *Antivirus Engines: From Methods to Innovations, Design, and Applications*. Cambridge, MA: Elsevier Syngress, 2024. pp. 1-656.



RAM

Persistent processes

Wach Dog

Wach Dog

Wach Dog

Pro-active

Wach Dog

Engine

SysTry

Temporary

Manual scan

Desinfection

Statistics

Other tools

GUI

Update

HDD/SSD

other.non-exe.files

signature.sig

Pro-active

Other tools

Desinfection

GUI

Wach Dog

SysTry

Engine

Manual scan

Statistics

Update

Paul A. Gagniuc. *Antivirus Engines: From Methods to Innovations, Design, and Applications*. Cambridge, MA: Elsevier Syngress, 2024. pp. 1-656.

FILS