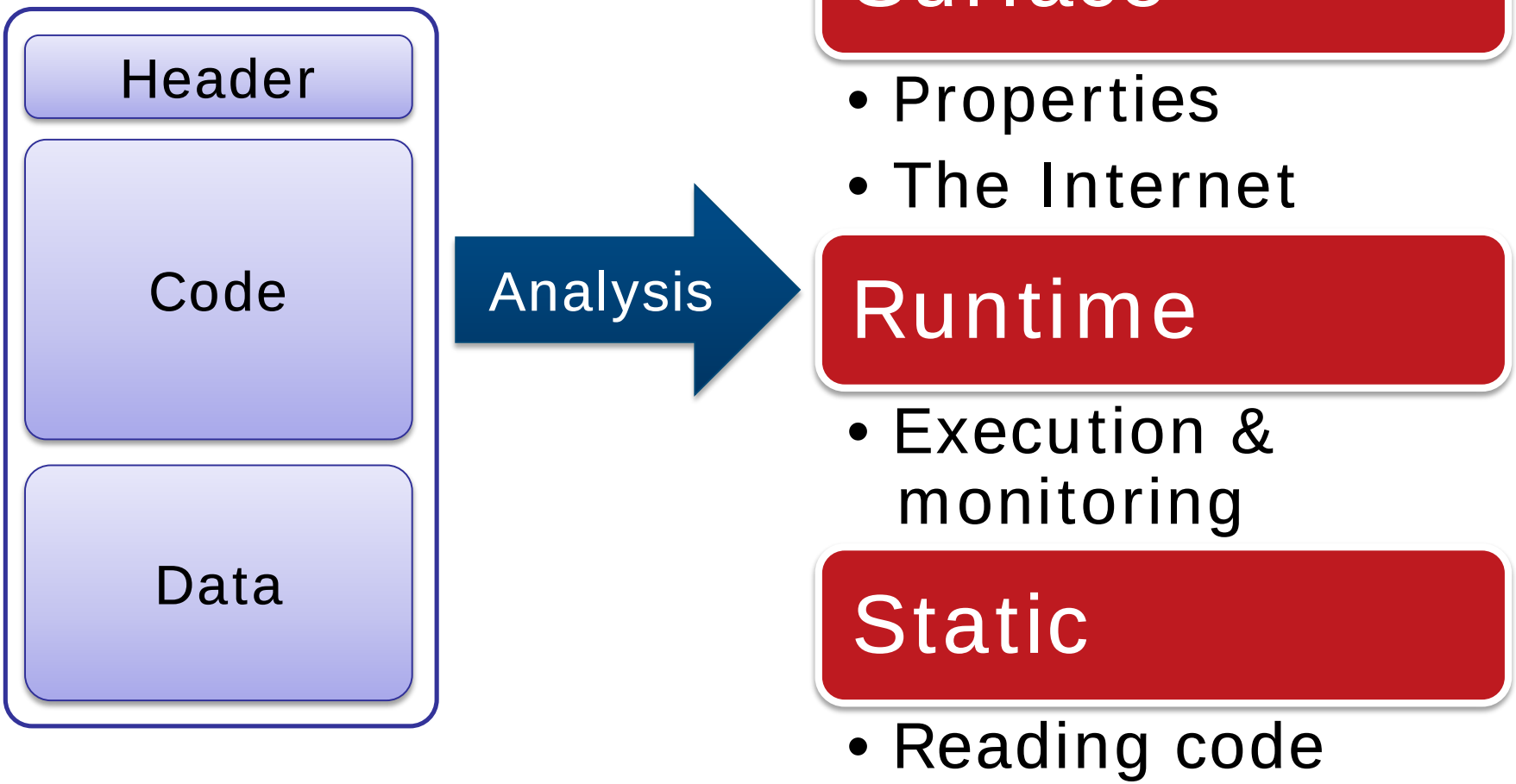
JPCERT CC®

Recommendation of Perfect Unpacking

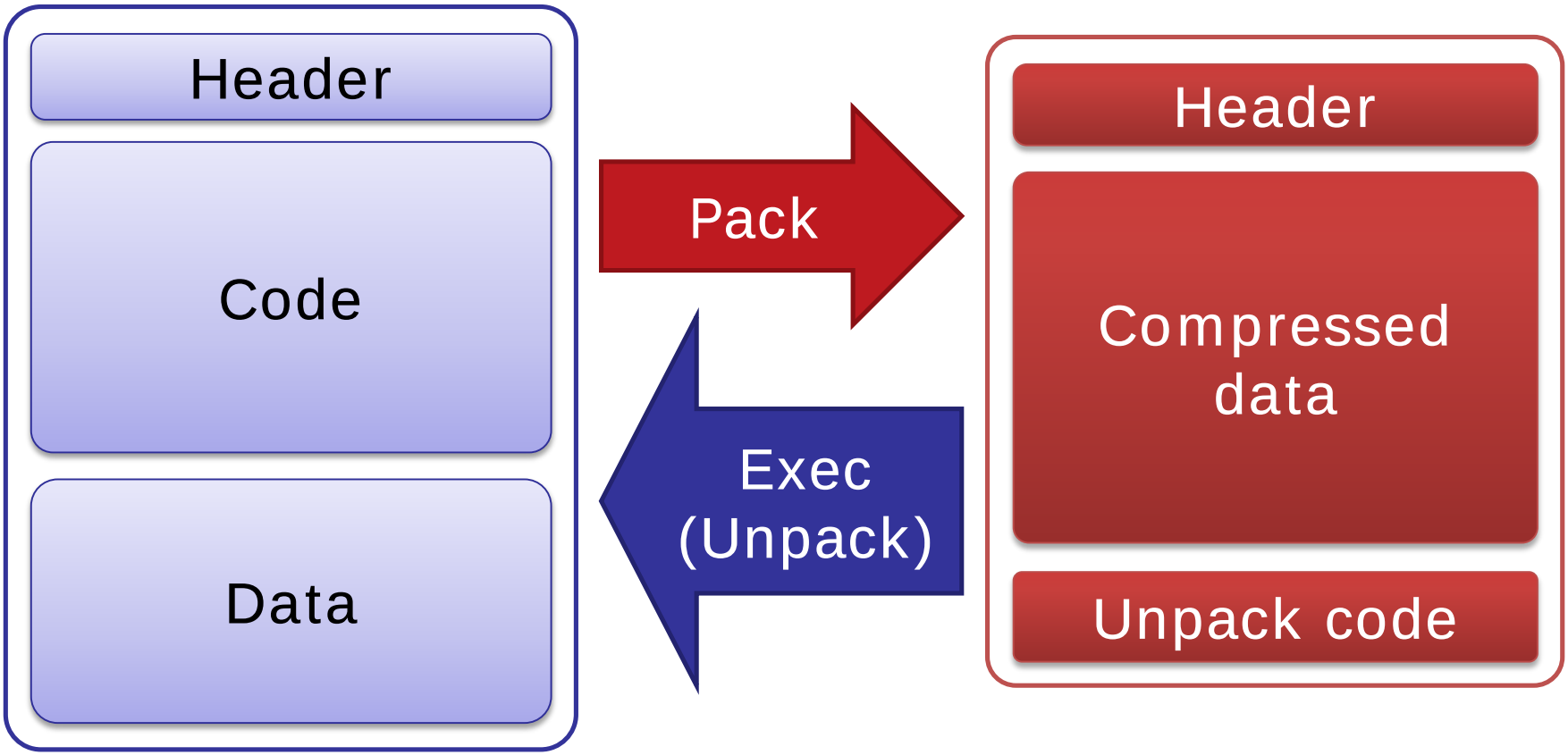
2014/04/24
JPCERT/CC Analysis Center
NAKATSURU You

Windows Malware Analysis

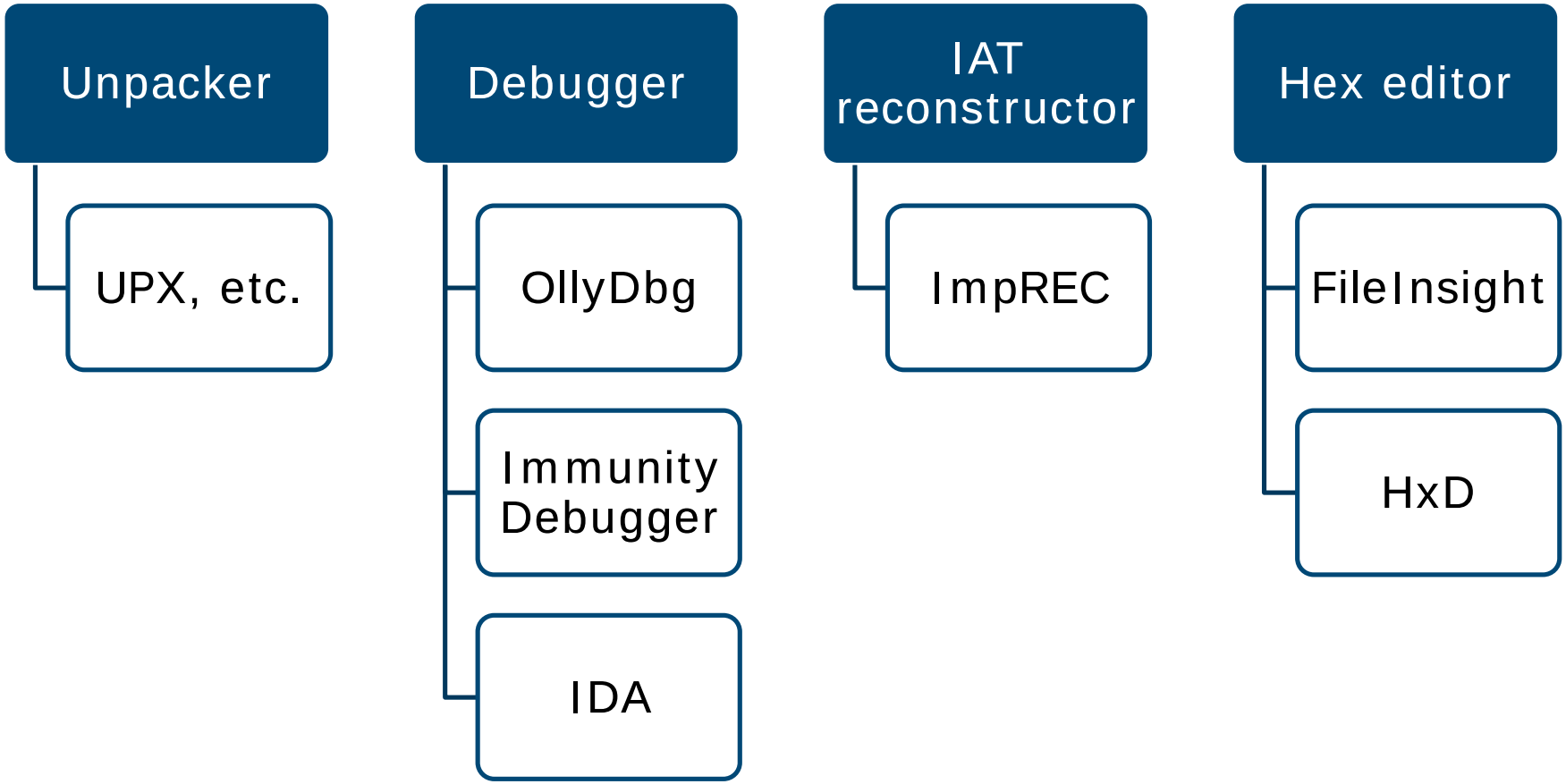


What Packing/Unpacking is

- "Pack" original code for compression/obfuscation

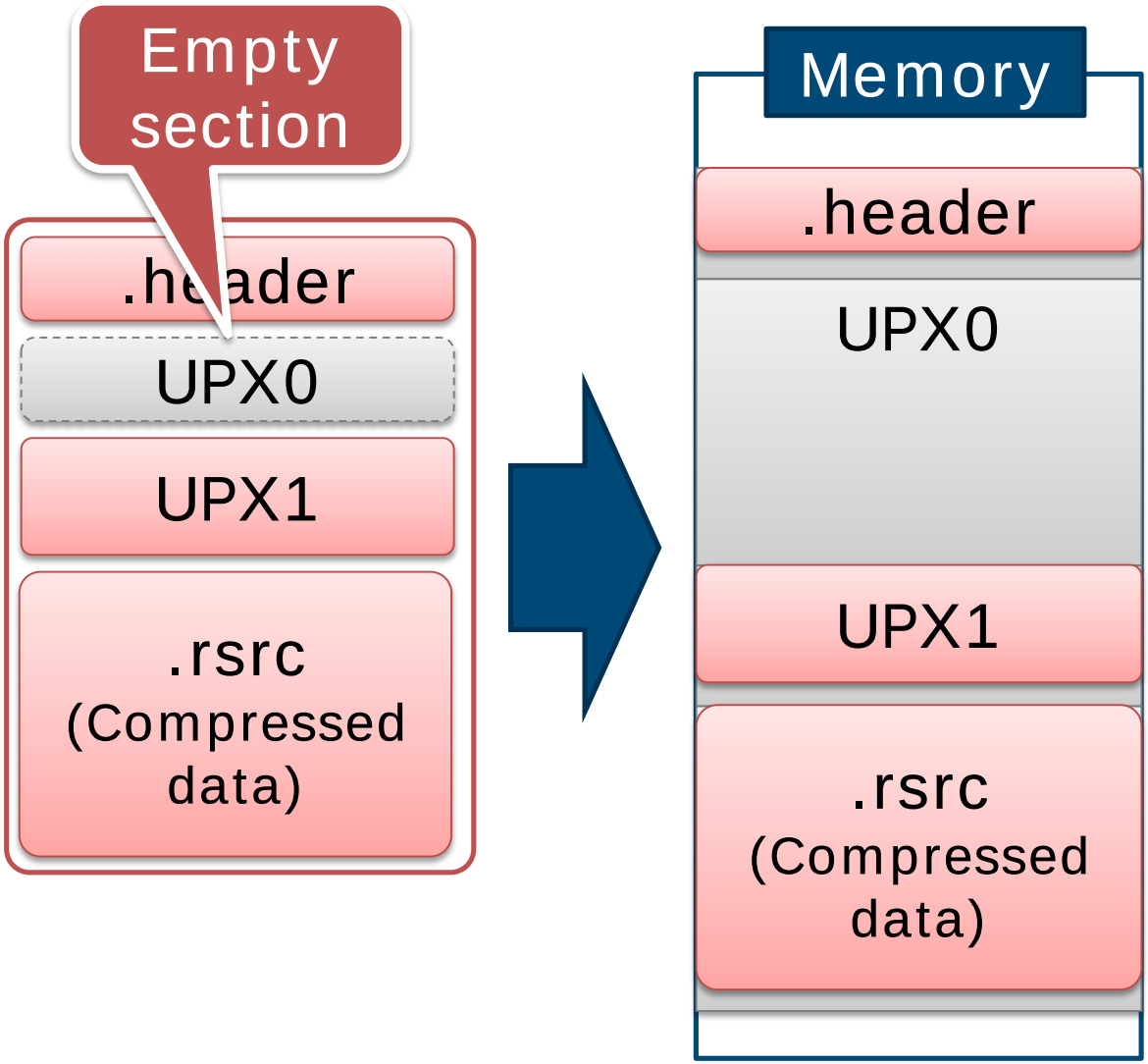


Unpacking Tools

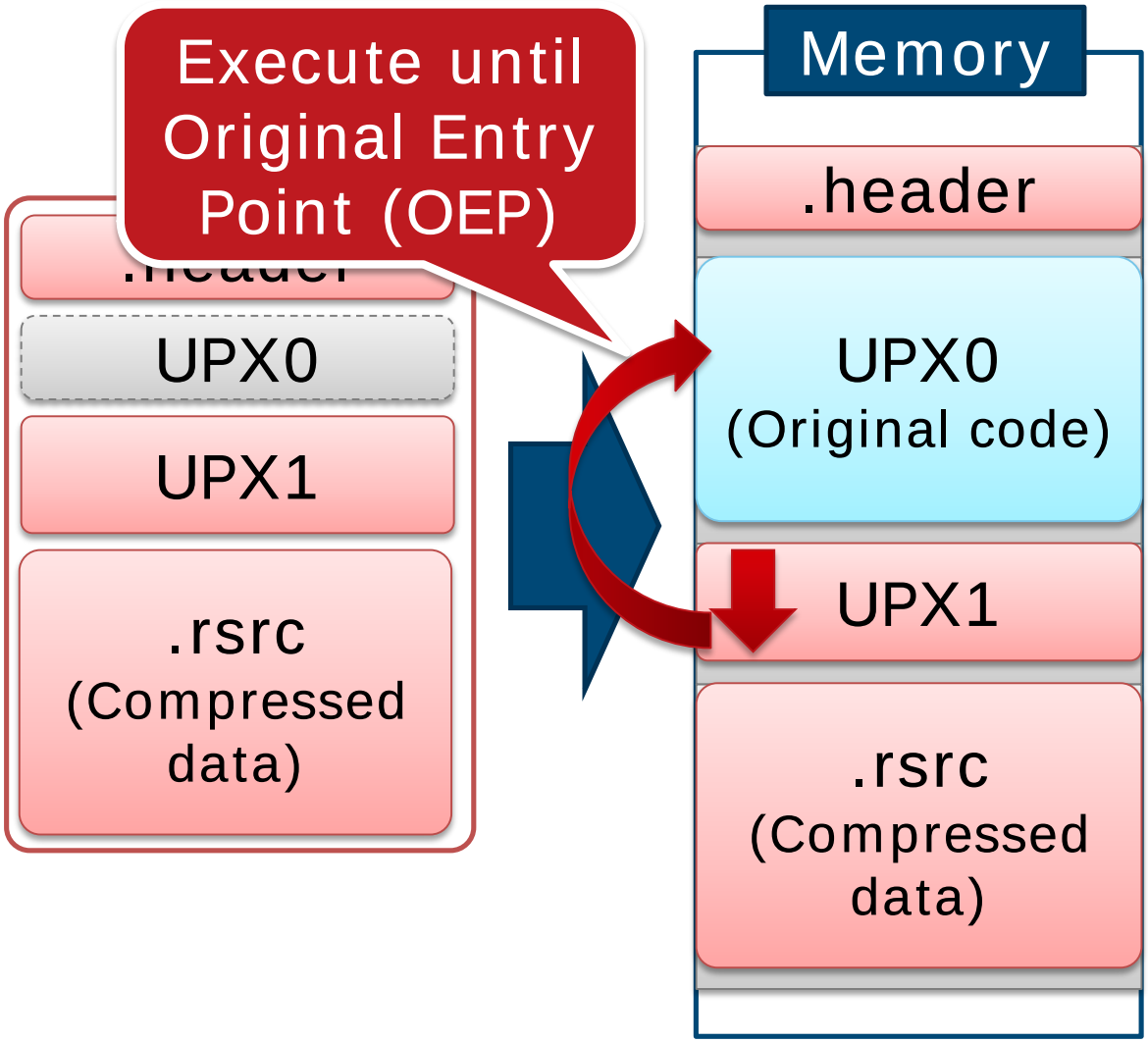


CLASSIC UNPACKING

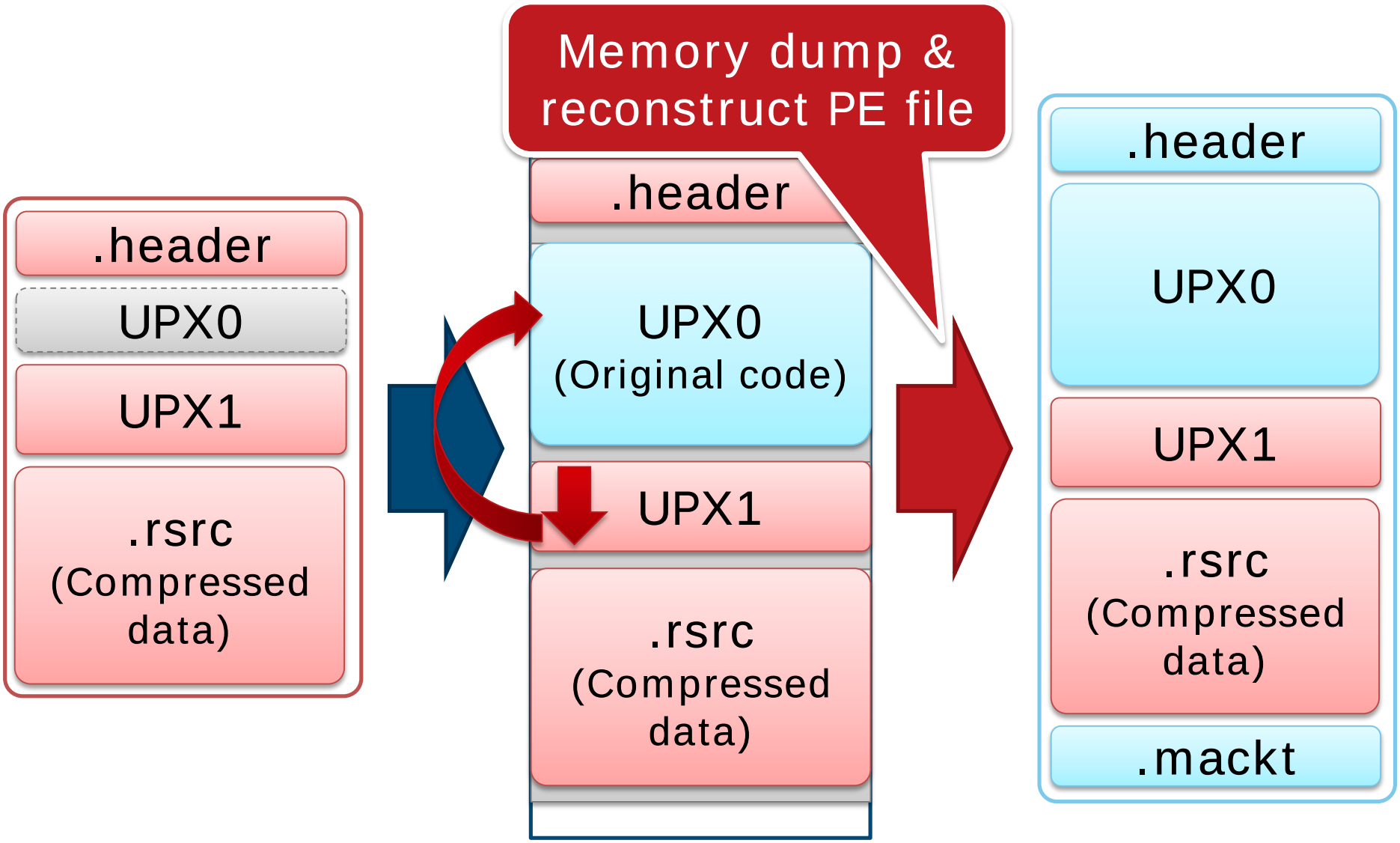
What "Classic Unpacking" is



What "Classic Unpacking" is



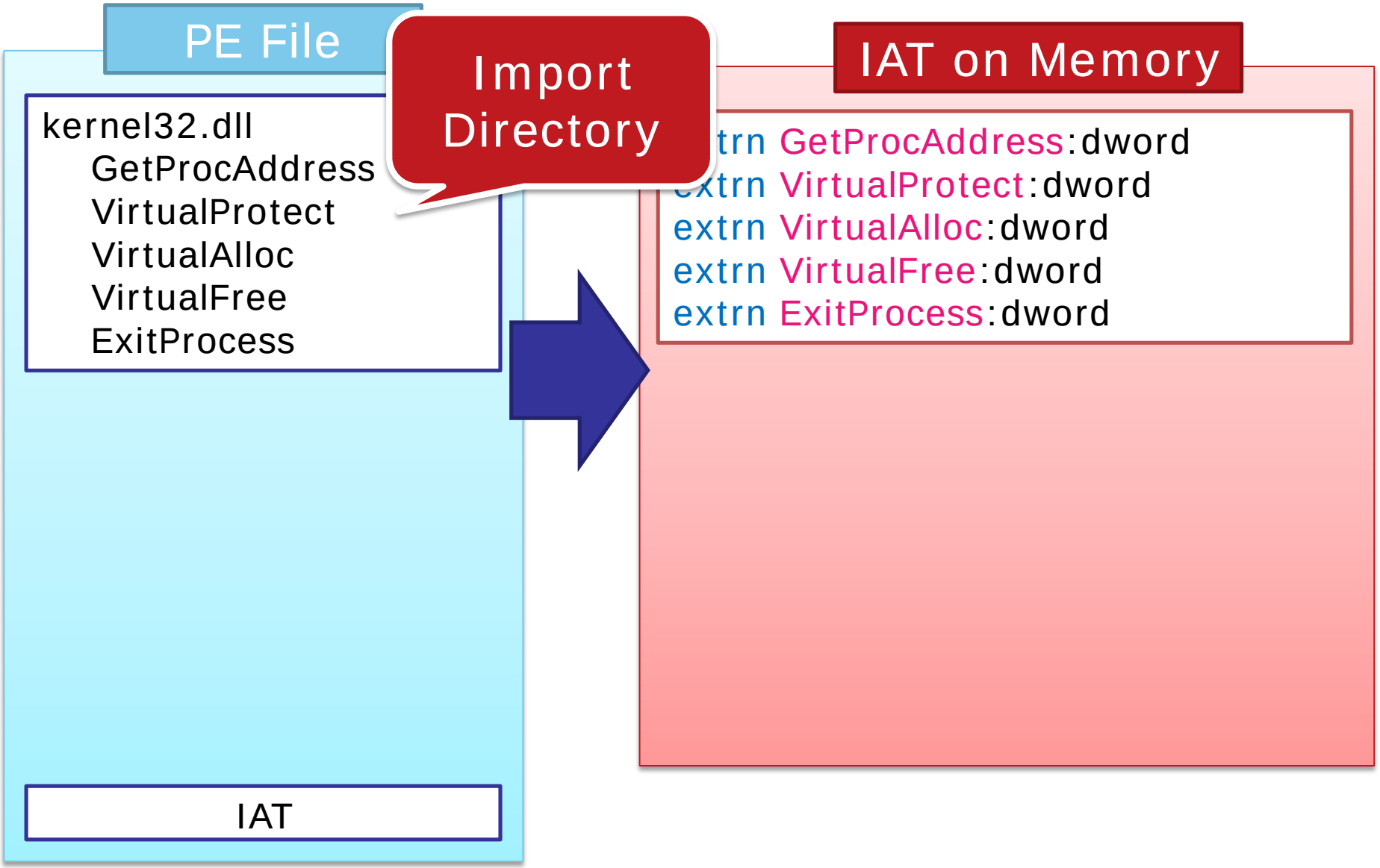
What "Classic Unpacking" is



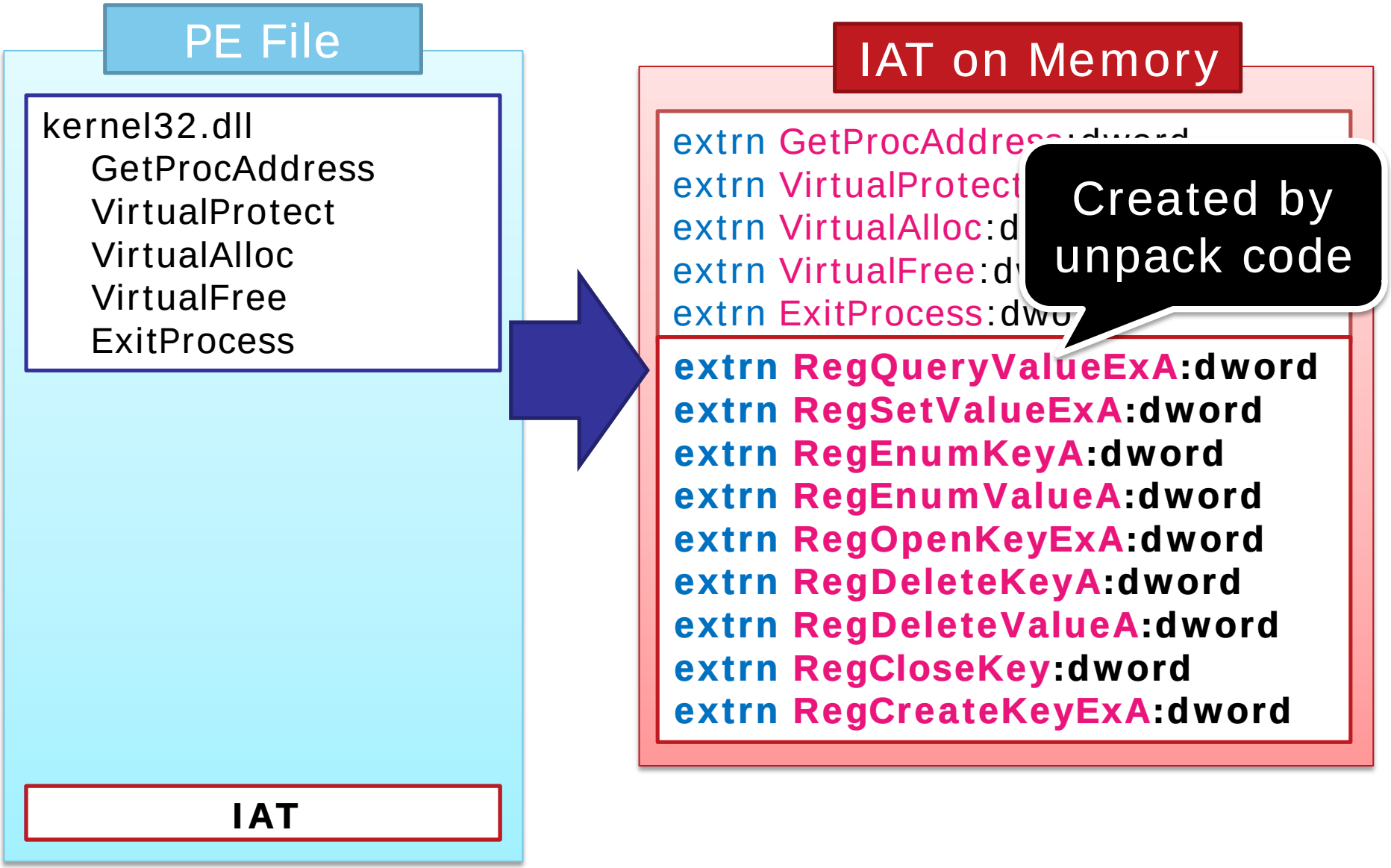
Classic Unpacking Flow

1. Execute unpack code
   - Find OEP
2. Dump as a PE file
   - reconstruct PE header, etc.
3. Reconstruct Import Address Table (IAT)

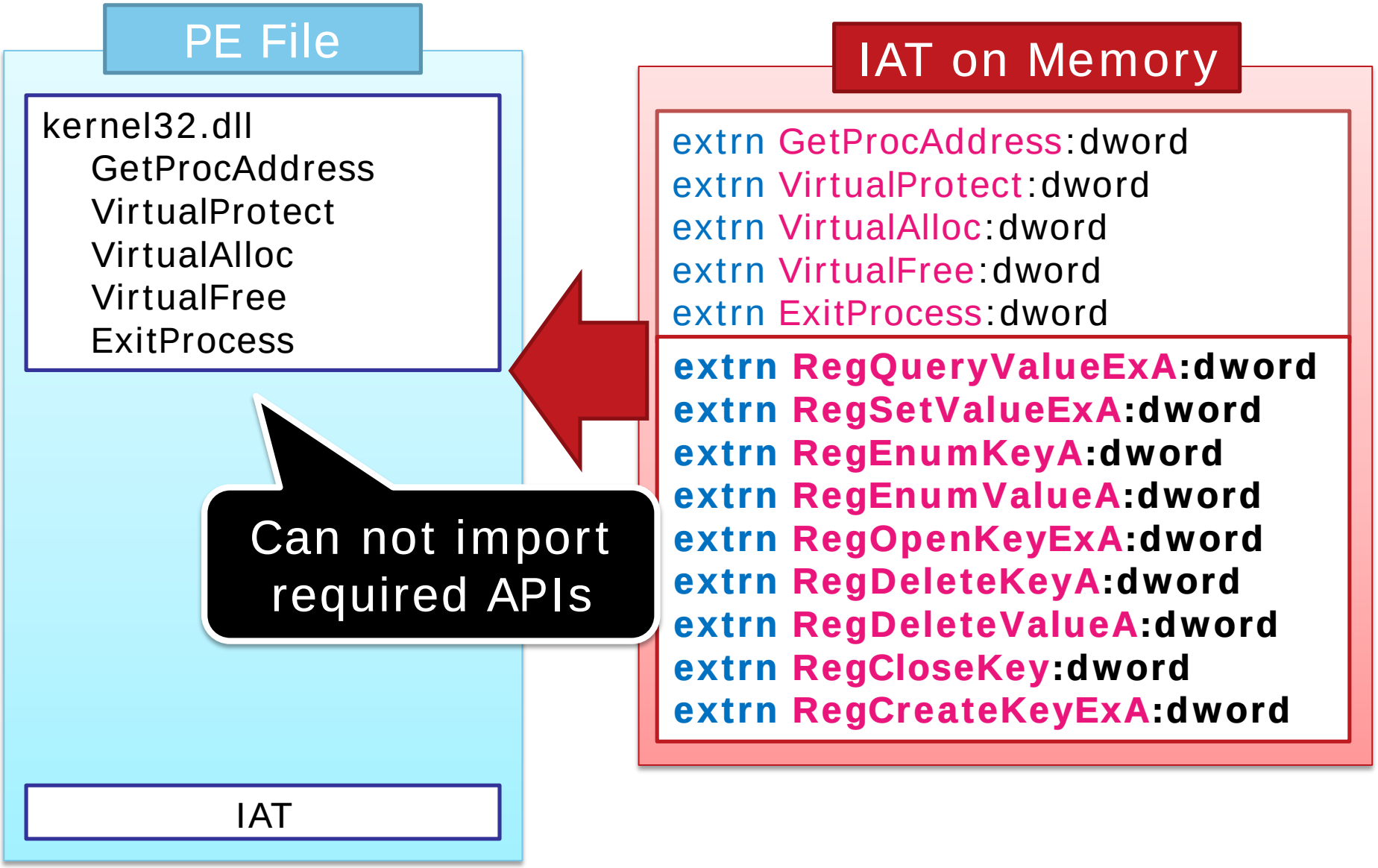
Reconstructing IAT



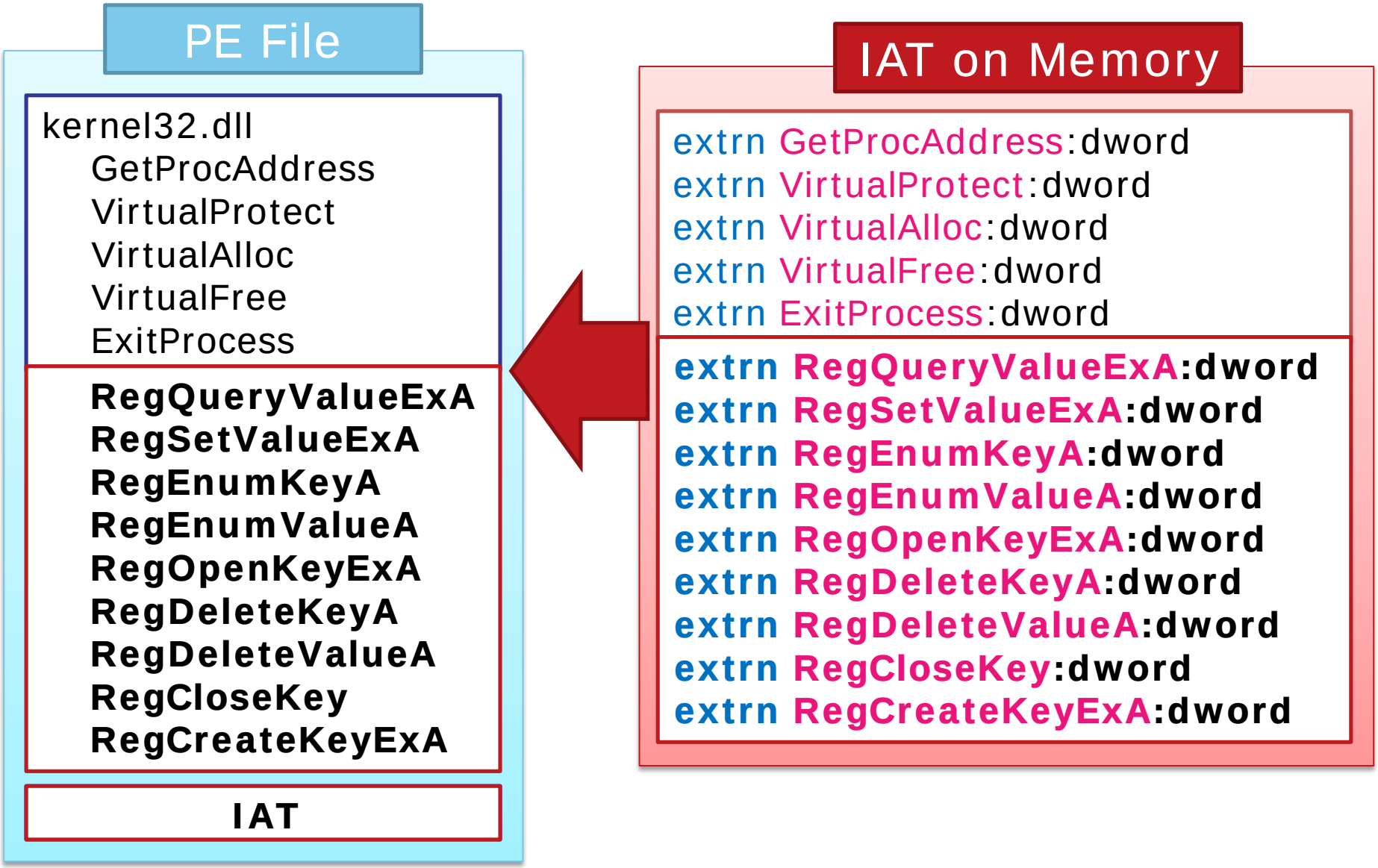
Reconstructing IAT



Reconstructing IAT

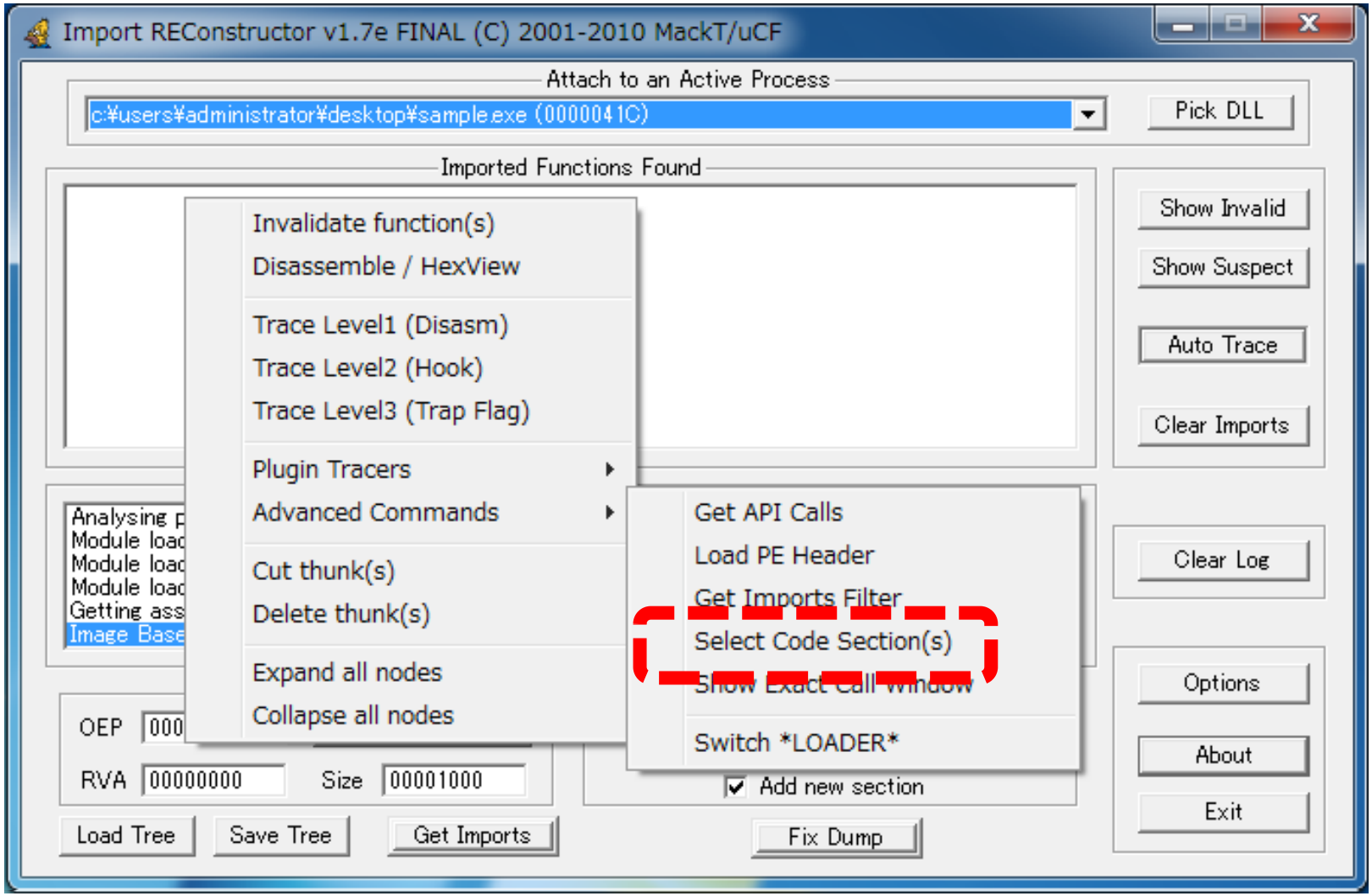


Reconstructing IAT



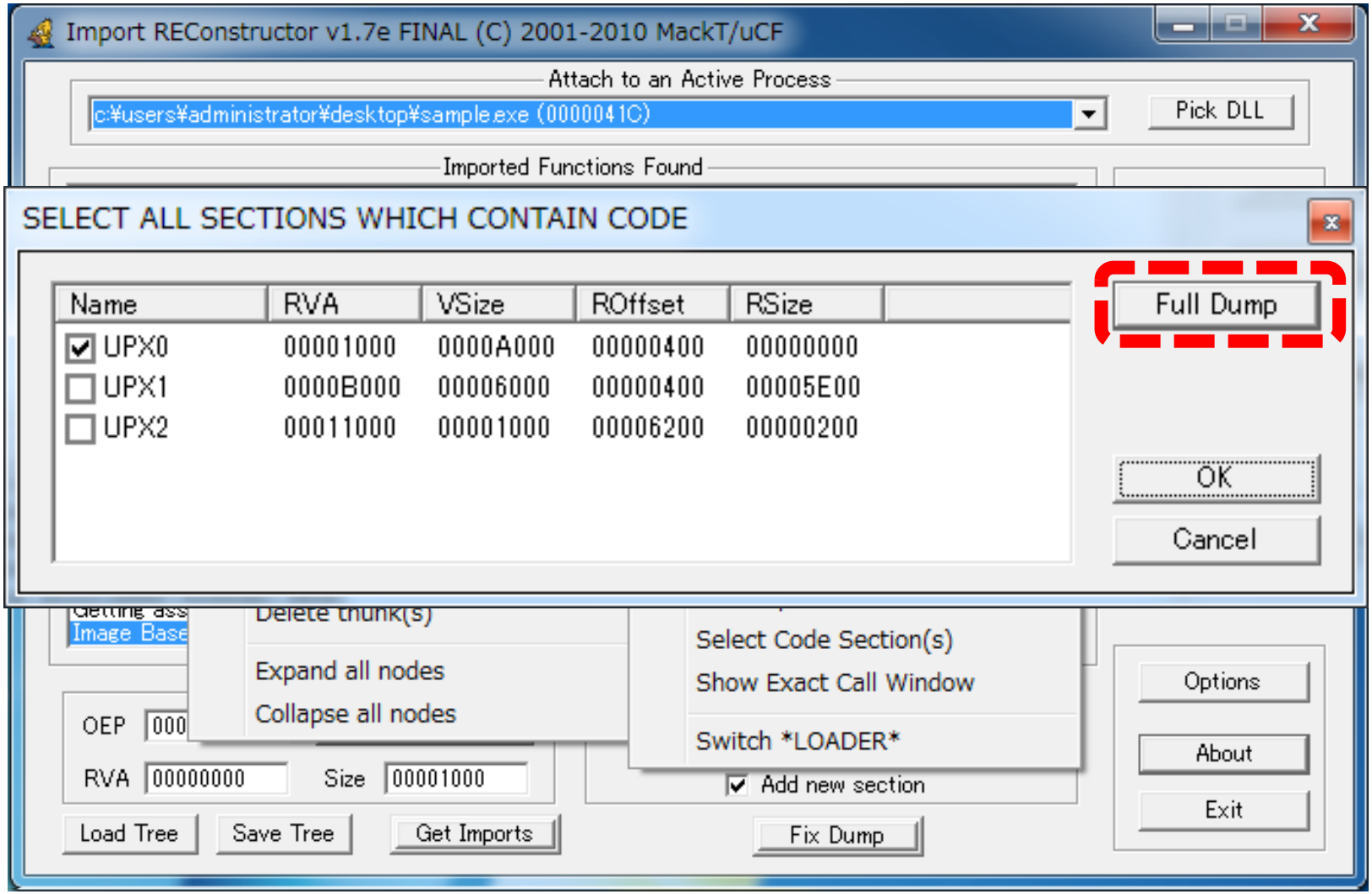
Classic Unpacking

- Reconstruct PE file



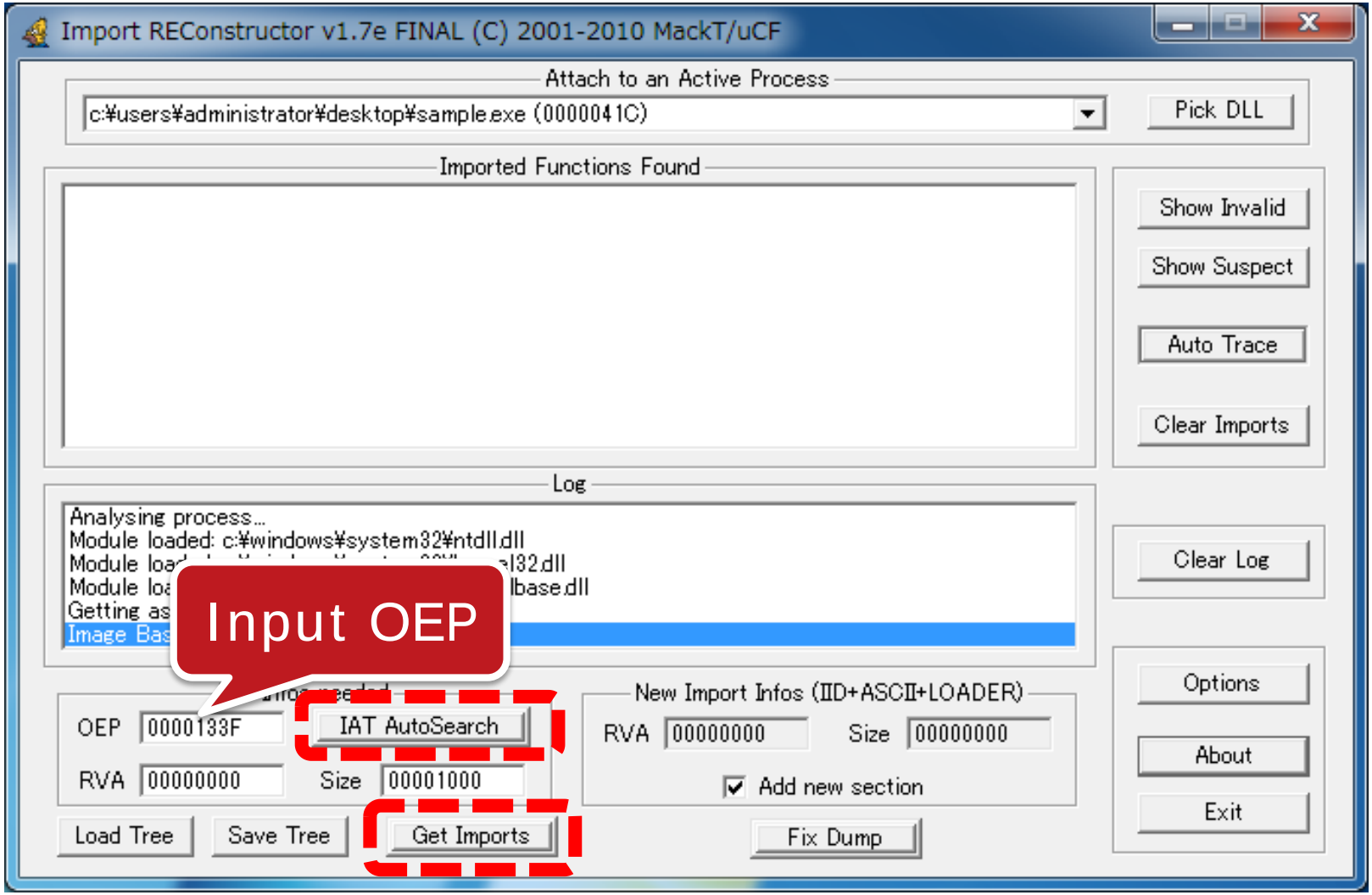
Classic Unpacking

- Reconstruct PE file



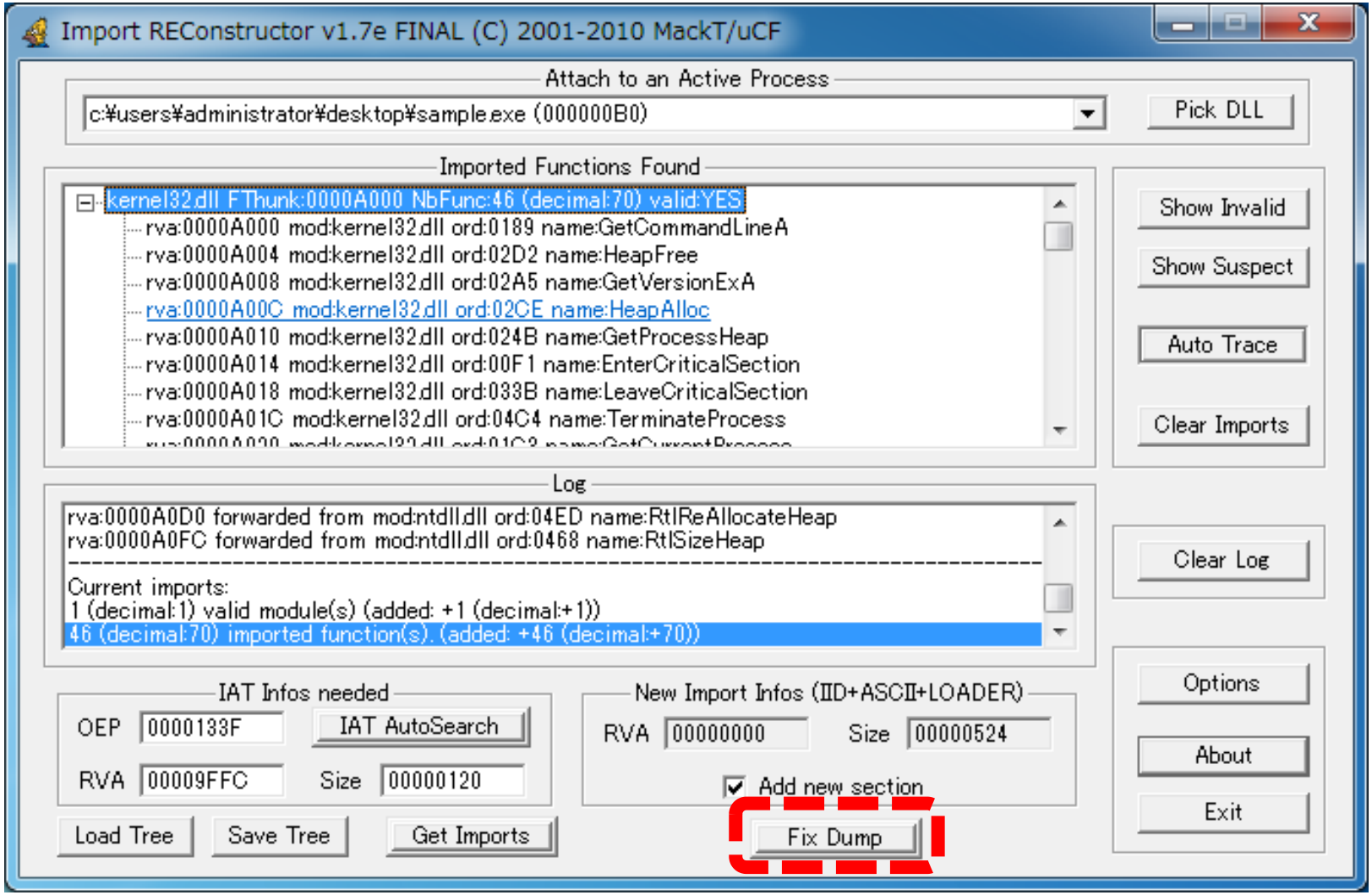
Classic Unpacking

- Reconstruct IAT

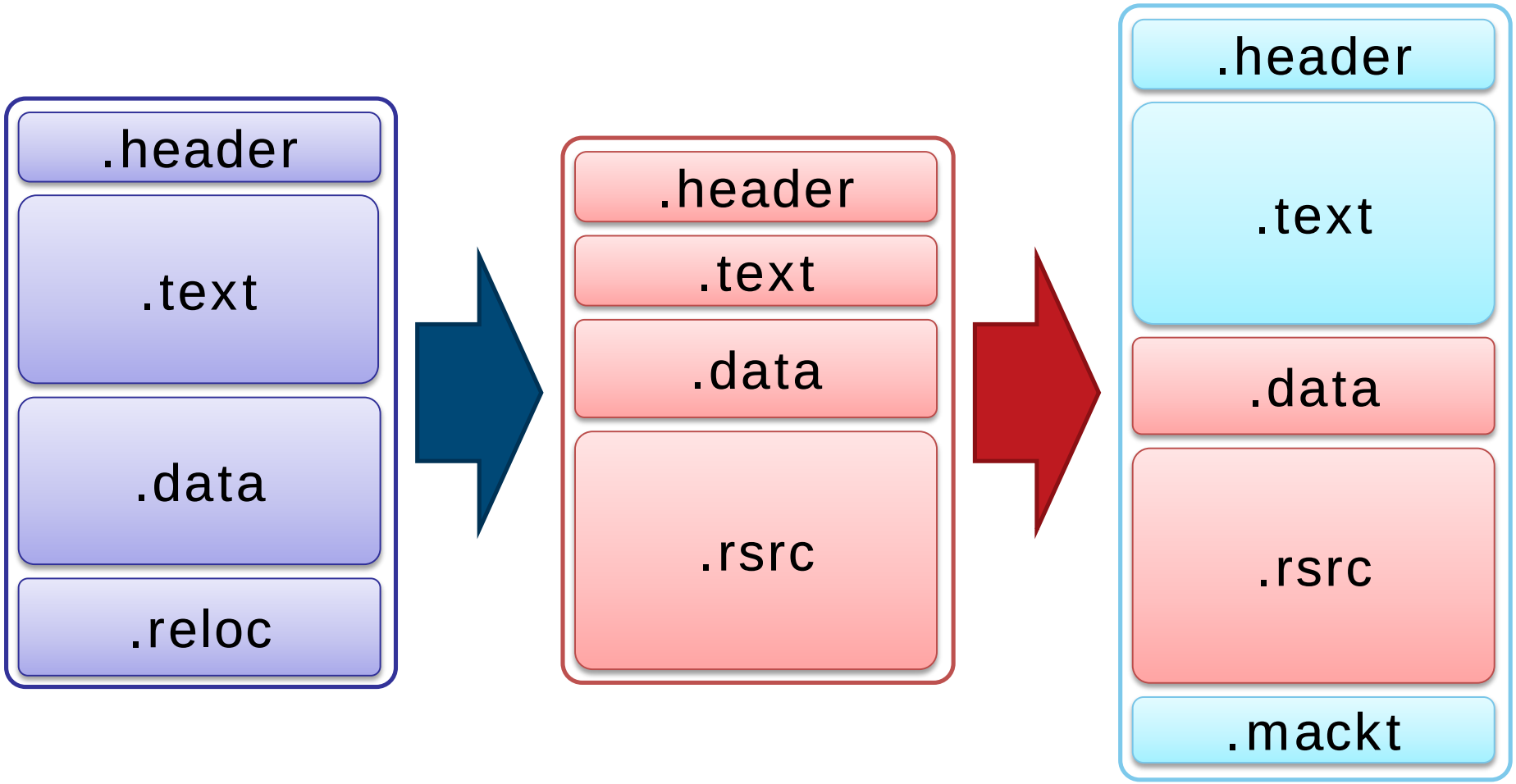


Classic Unpacking

- Reconstruct IAT

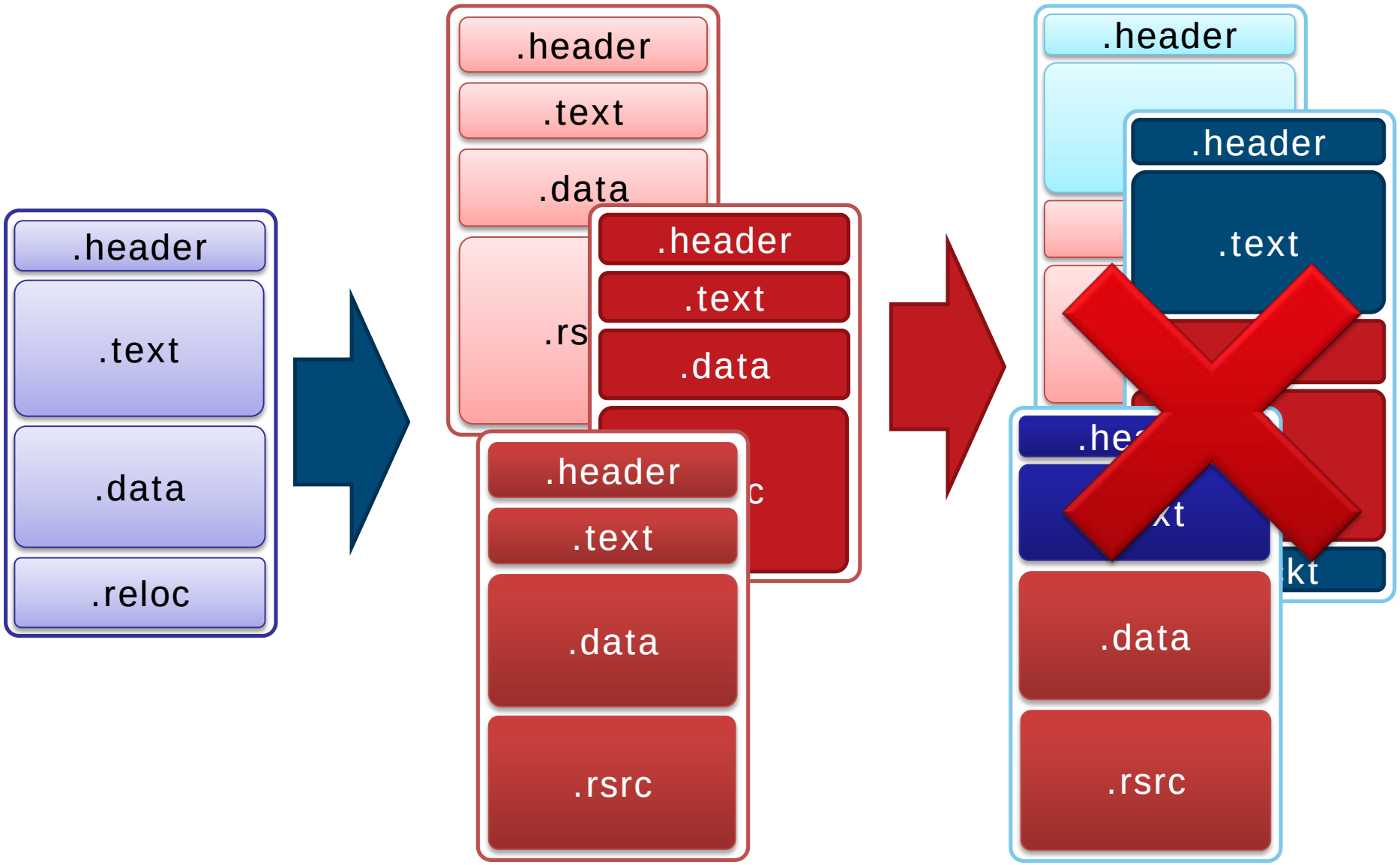


Classic Unpacking Issue



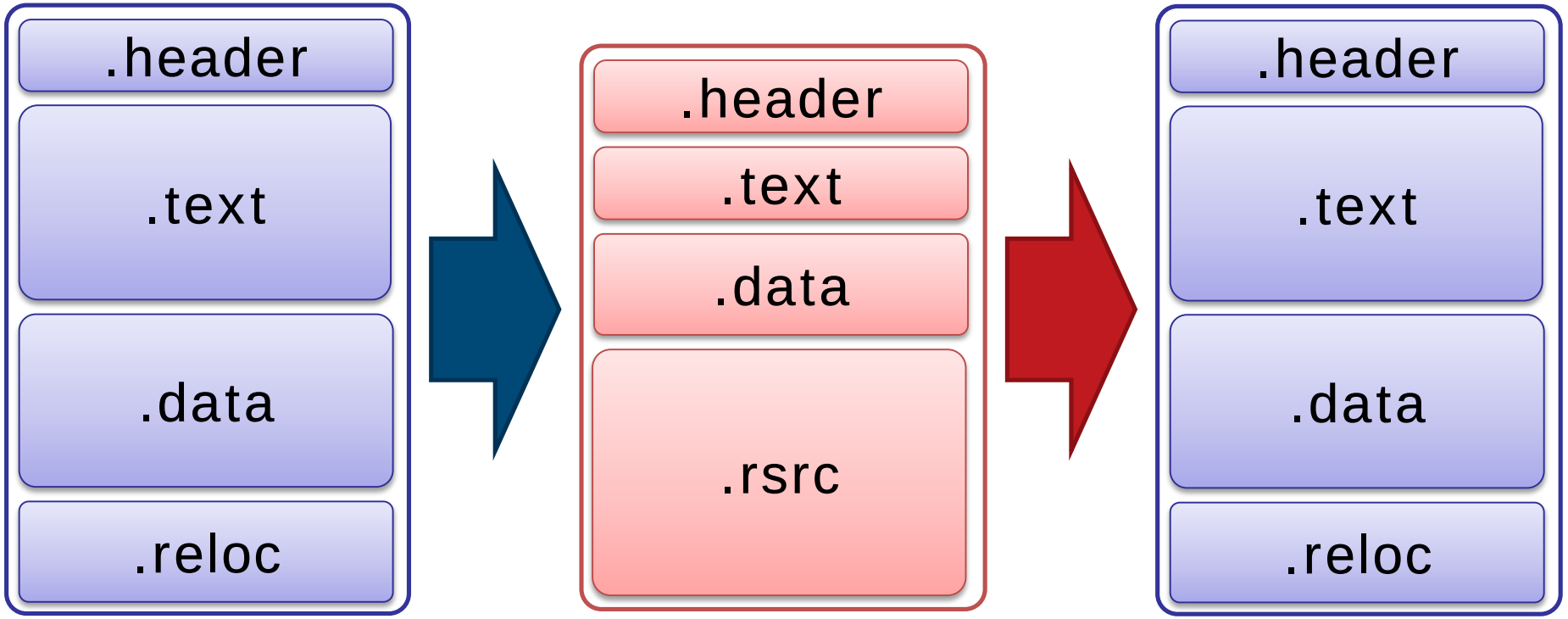
hash("Original") != hash("Unpacked")

Classic Unpacking Issue



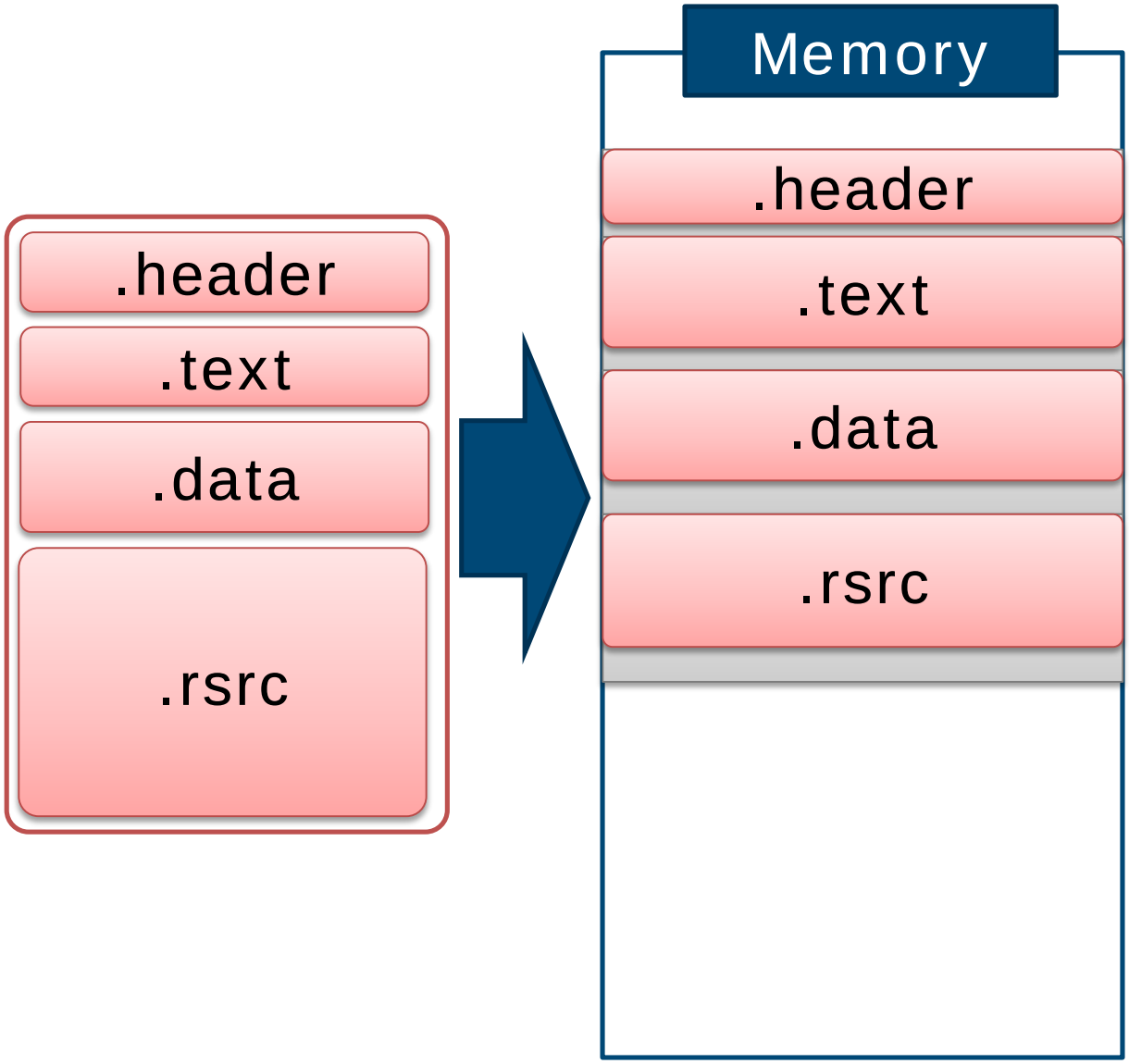
PERFECT UNPACKING

Concept

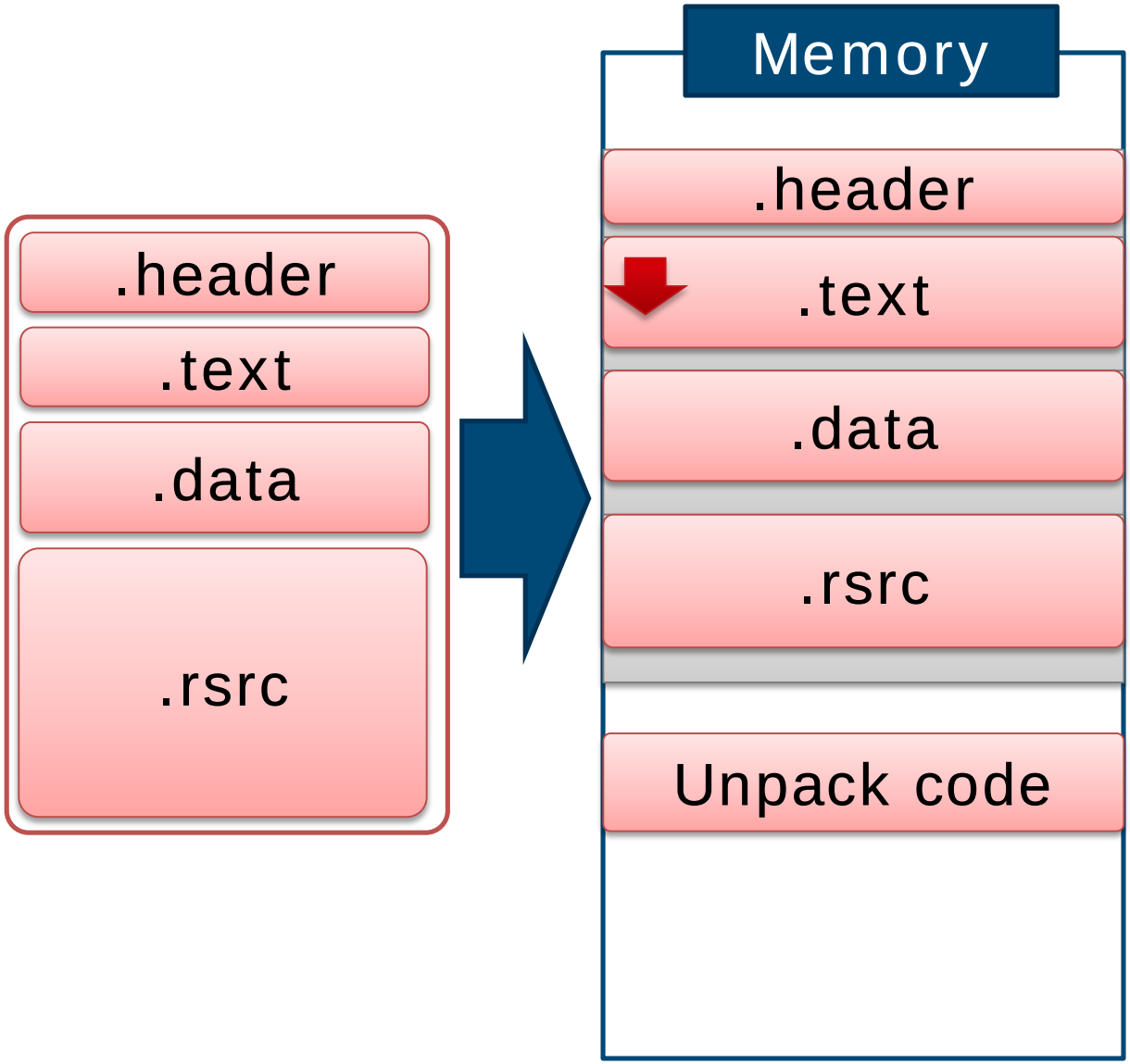


hash("Original") == hash("Unpacked")

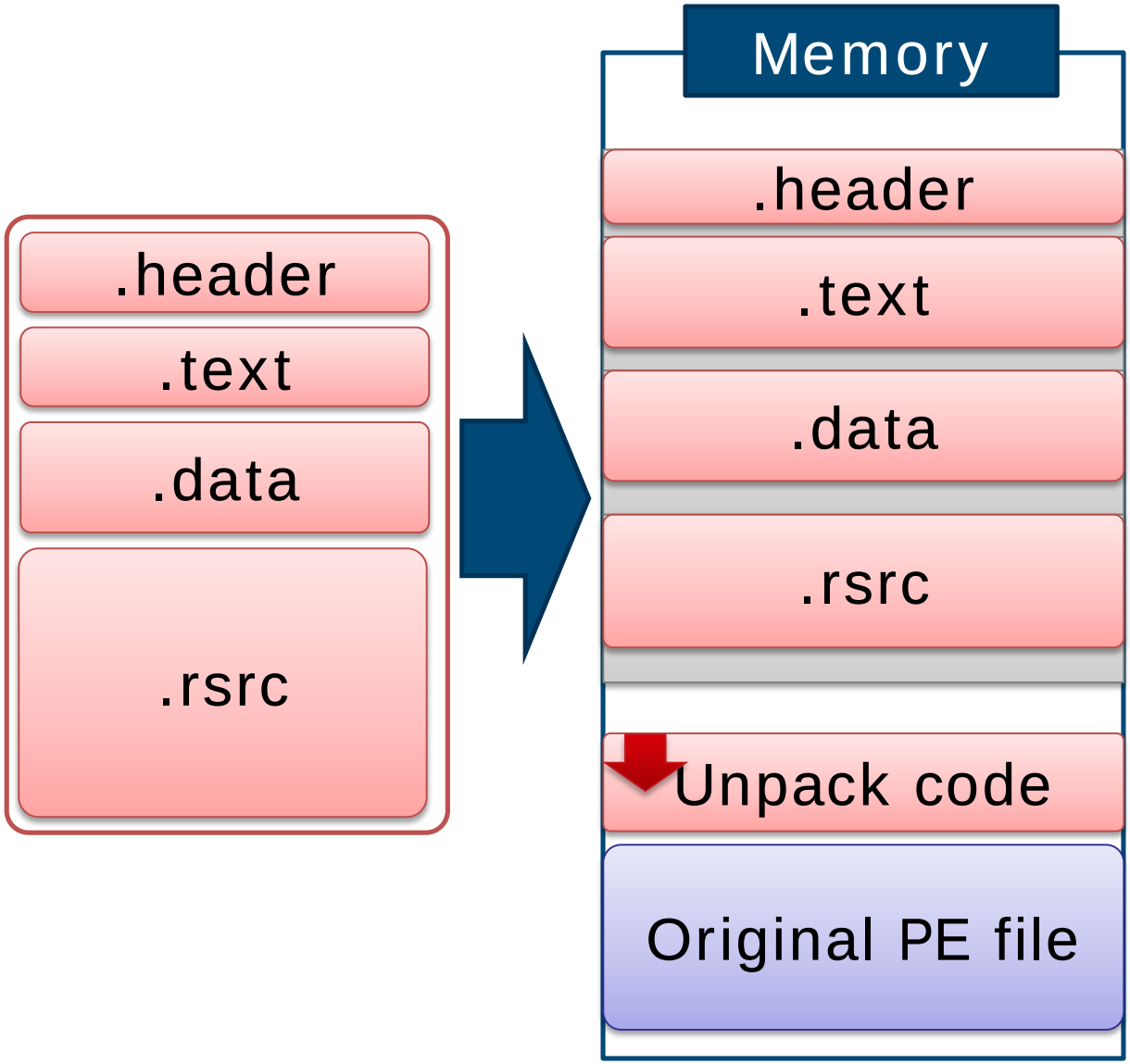
Recent Packer



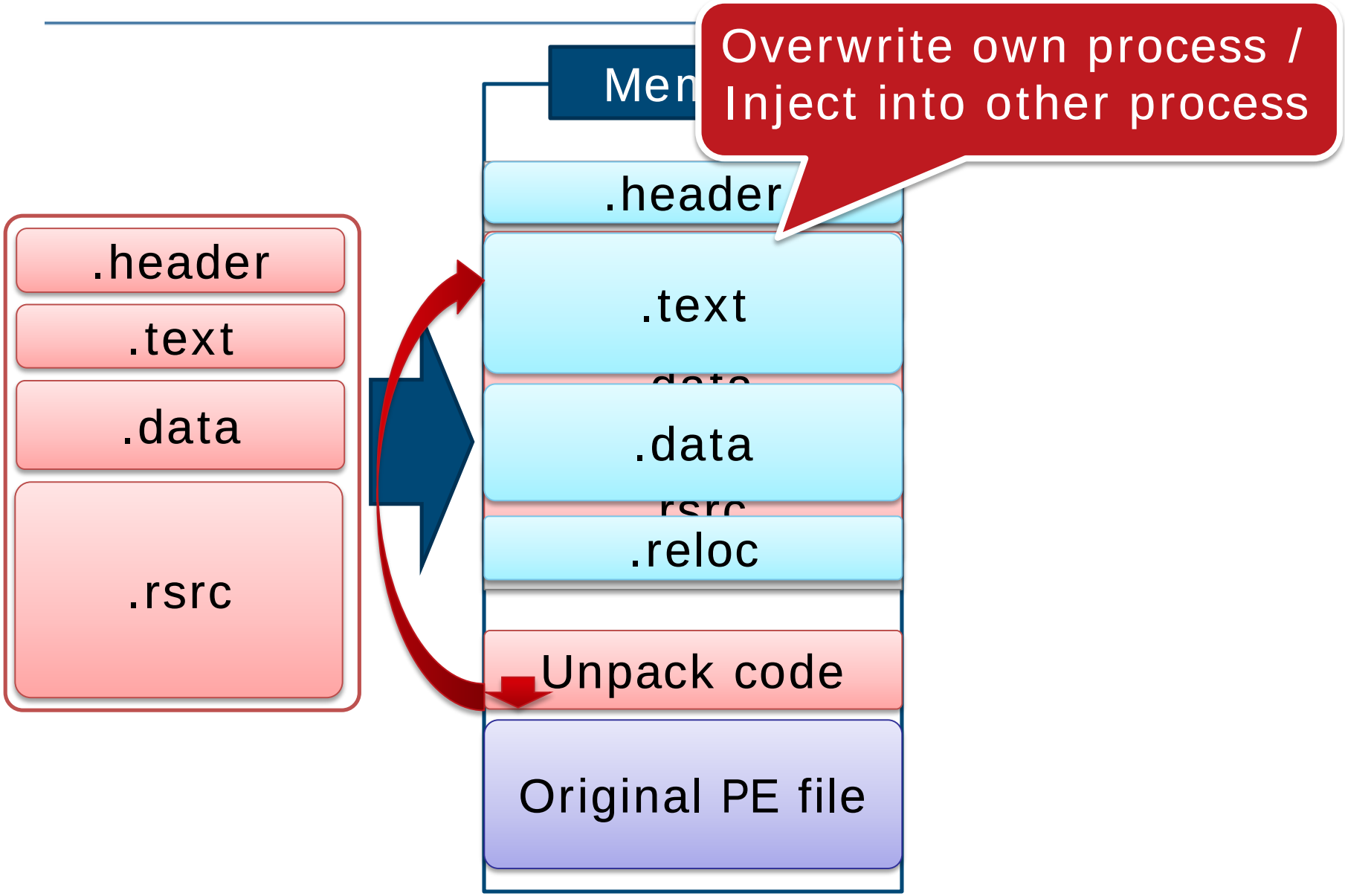
Recent Packer



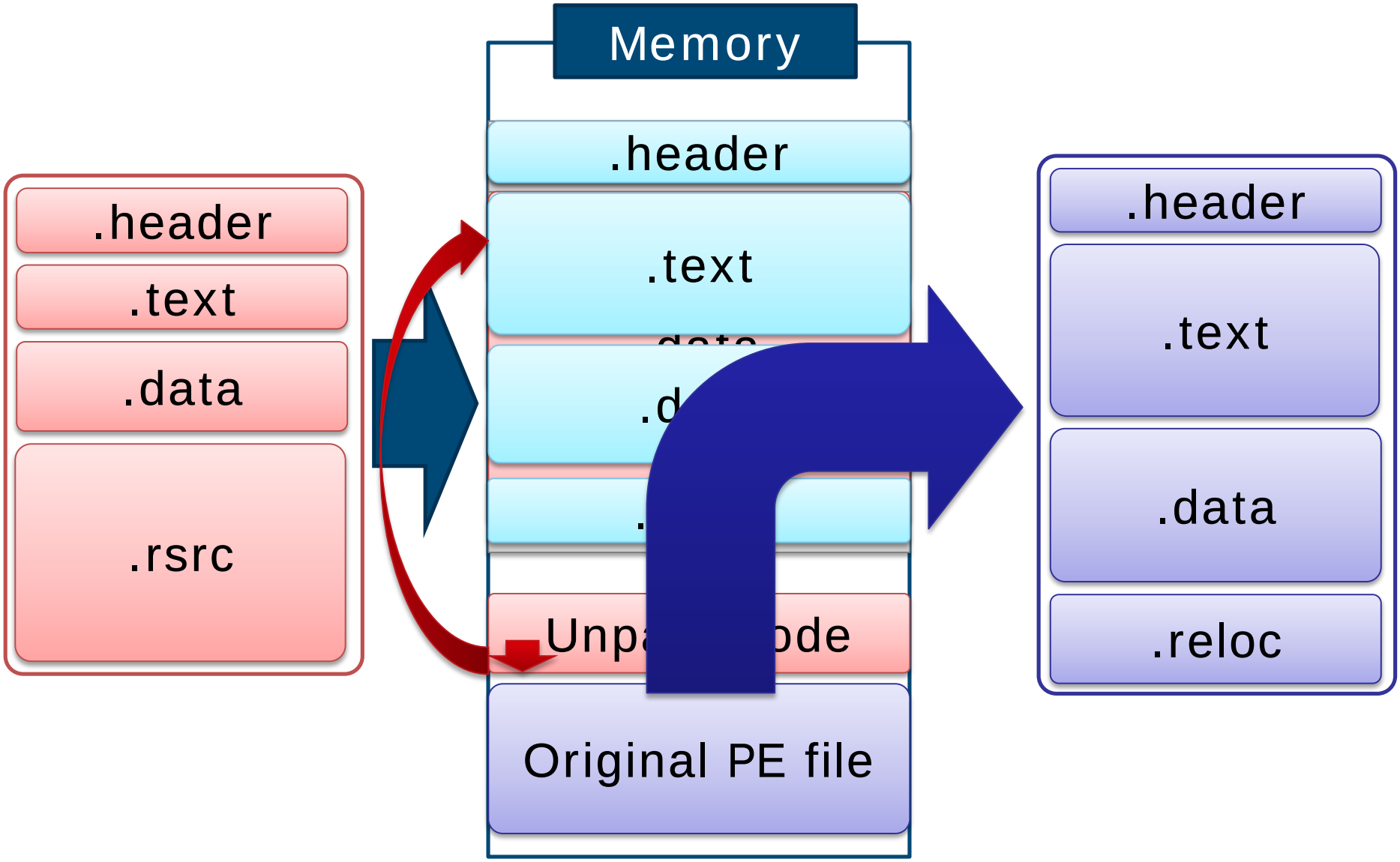
Recent Packer



Recent Packer



Recent Packer



Perfect Unpacking Flow

1. Execute unpack code
   - Let unpack code unpack original PE file

2. Dump memory section contains original PE file

3. Trim PE file

1. Unpack Code Execution

- Set breakpoints on

Windows APIs

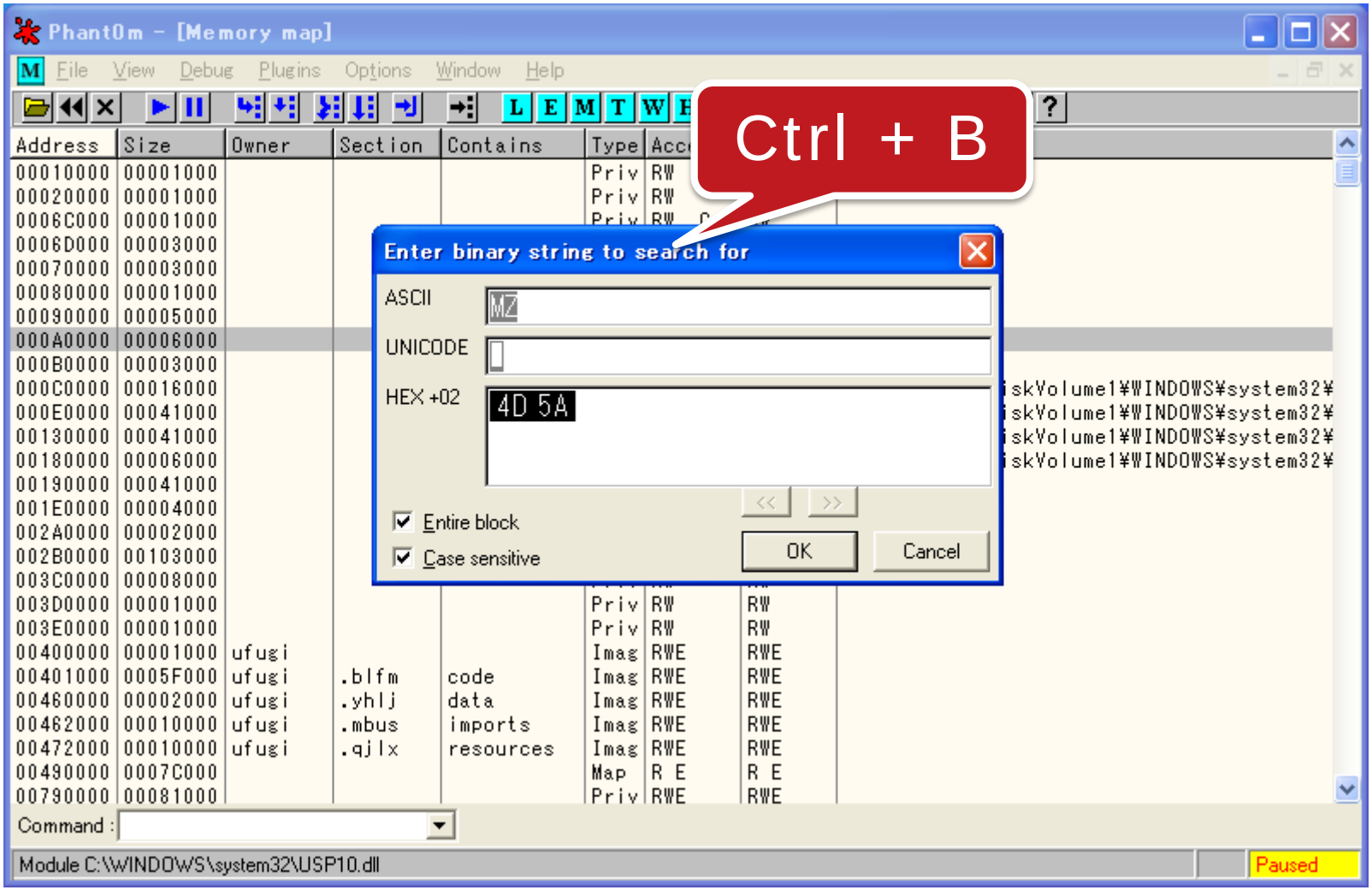
- WriteProcessMemory
- ZwWriteVirtualMemory
- CreateProcessW
- VirtualFree / RtlFreeHeap
- etc.

PE header

- Hardware breakpoint on "M"

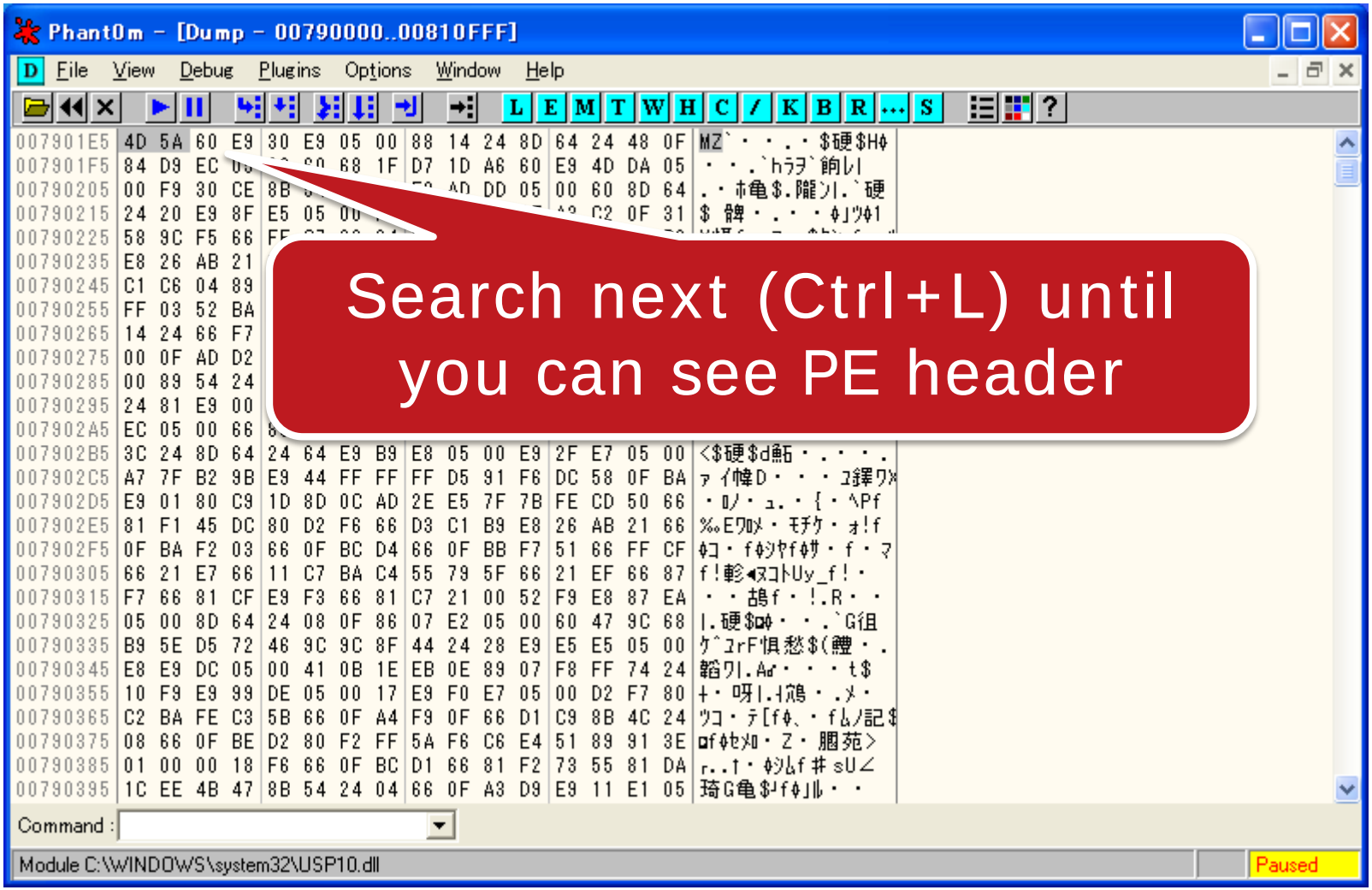
2. Dumping Memory Section

- Search "MZ" string



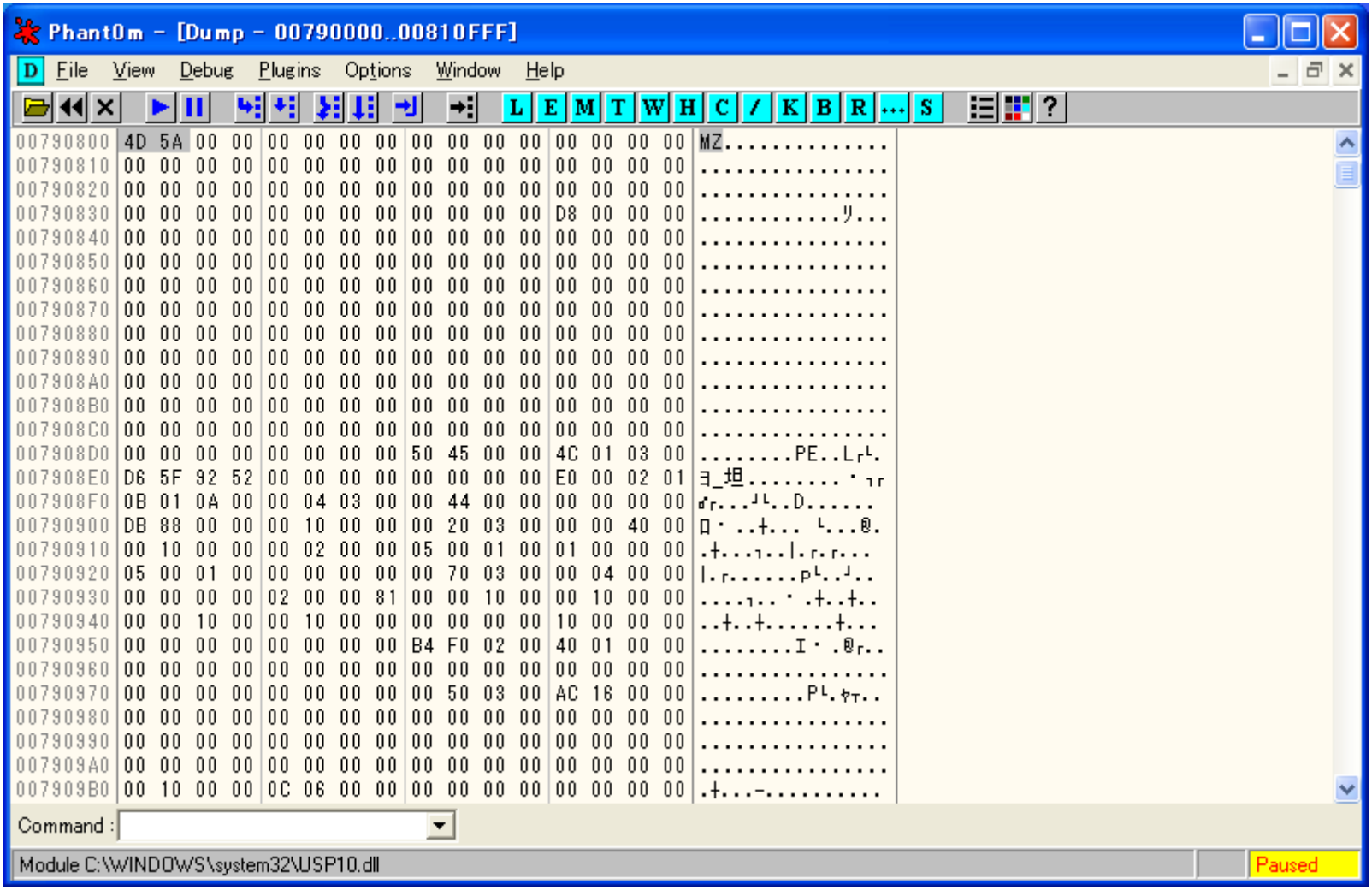
2. Dumping Memory Section

- Search "MZ" string



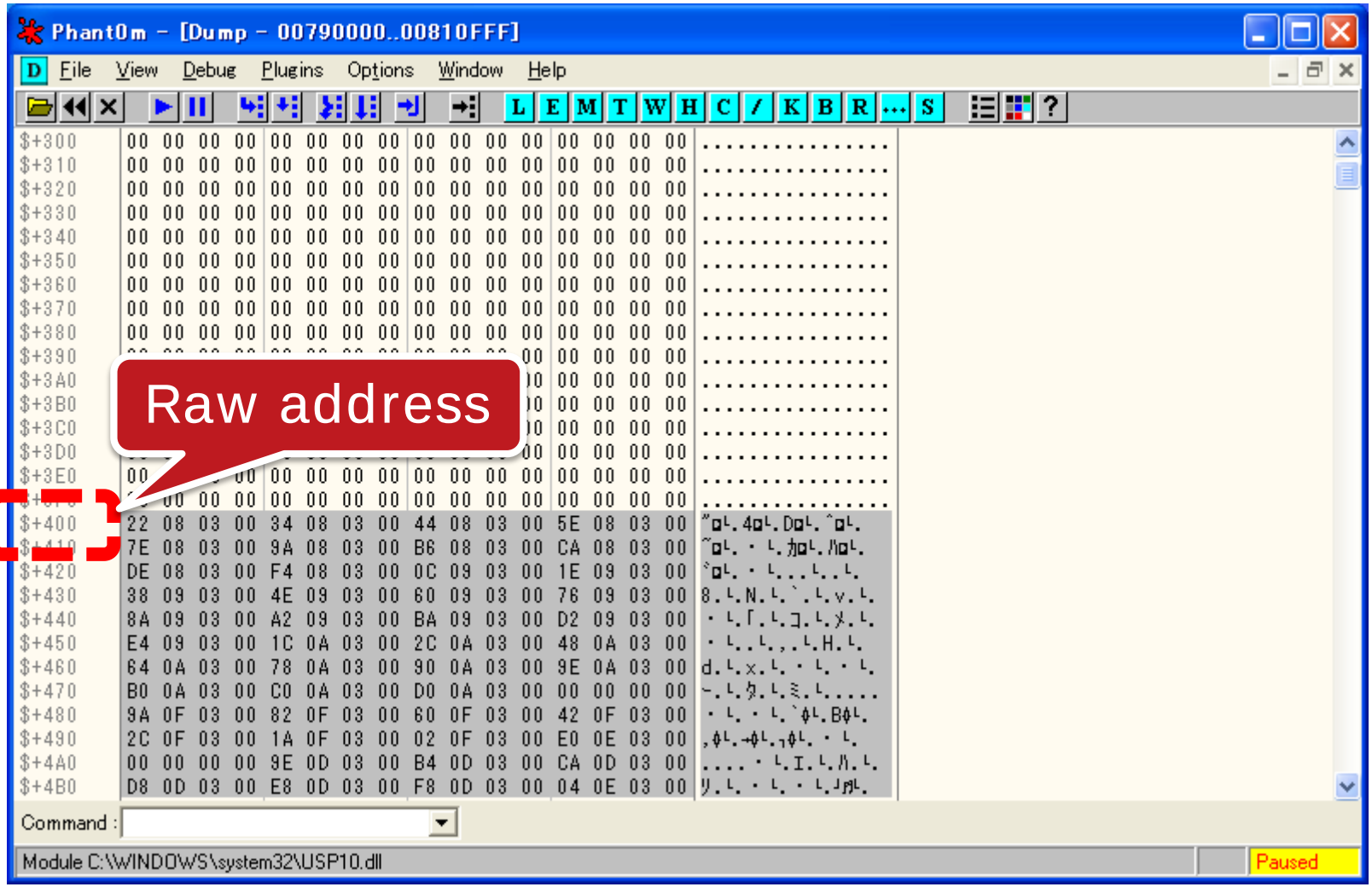
2. Dumping Memory Section

- Search "MZ" string



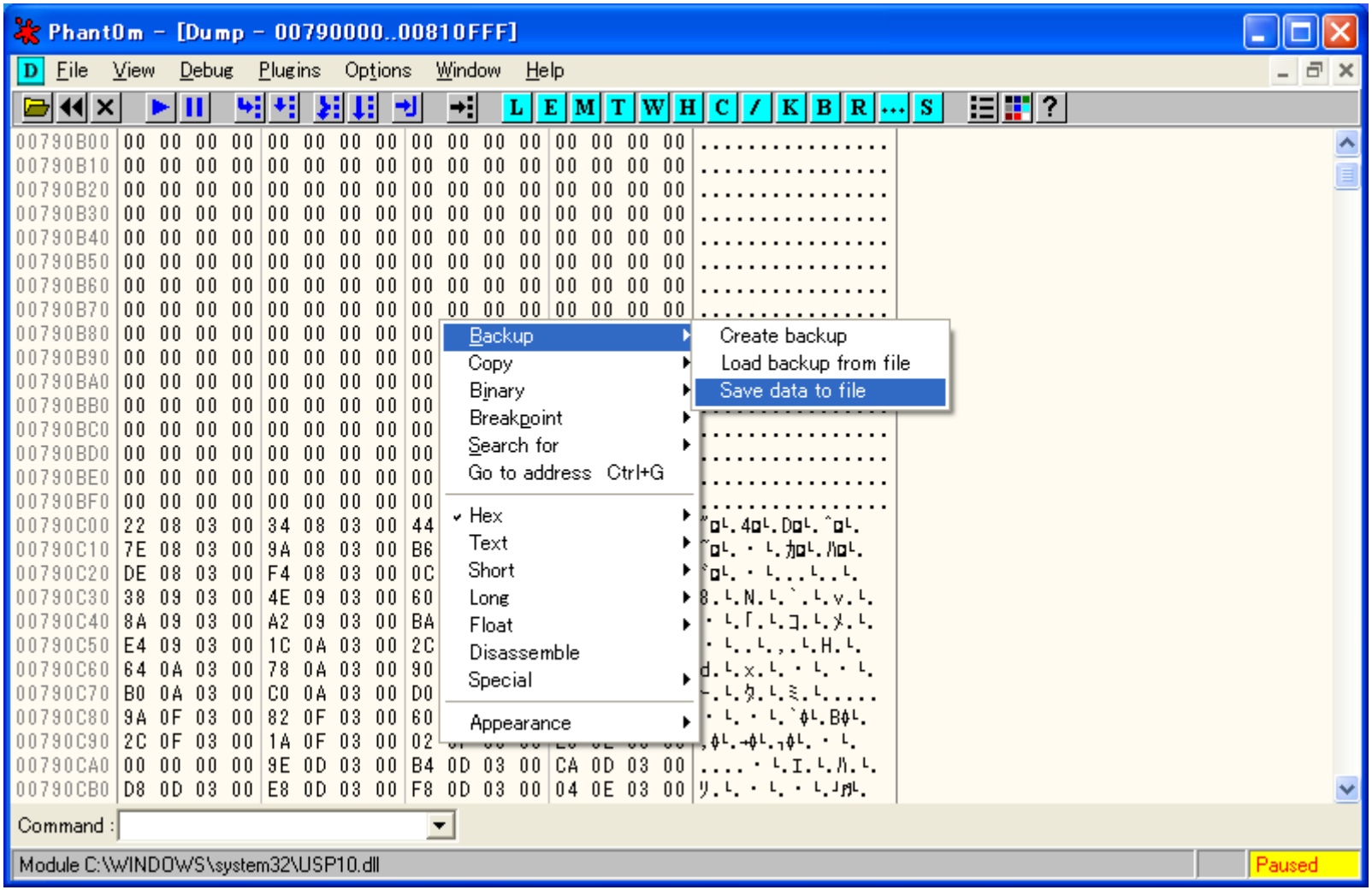
2. Dumping Memory Section

- Search "MZ" string



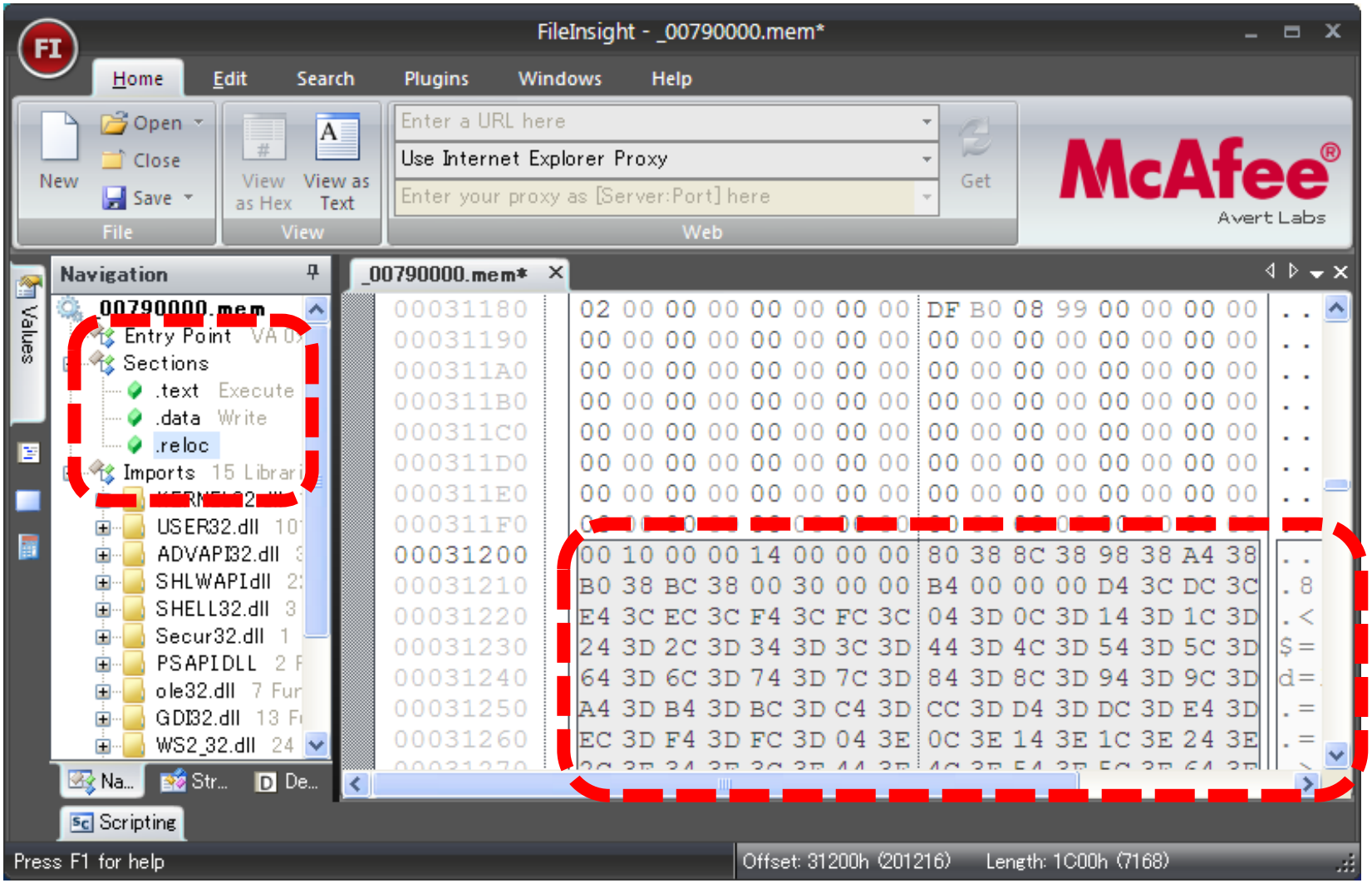
2. Dumping Memory Section

- Dump



3. Trimming PE file

- Parse PE file using FileInsight



Consideration

0. Limited availability

- Depends on packer's implementation

1. Unpacking code execution

- Debugger & VM detection
- **Breakpoint detection**

3. Trimming PE file

- Overlay data
  - Data used by malware
    - e.g. ZeuS variants
  - **Digital signature**

Demo Movie

- Get same original file from different binaries using "Perfect Unpacking"

CONCLUSION

Summary

Classic unpacking issue

- Unpacked file's hash value depends on analyst/tools

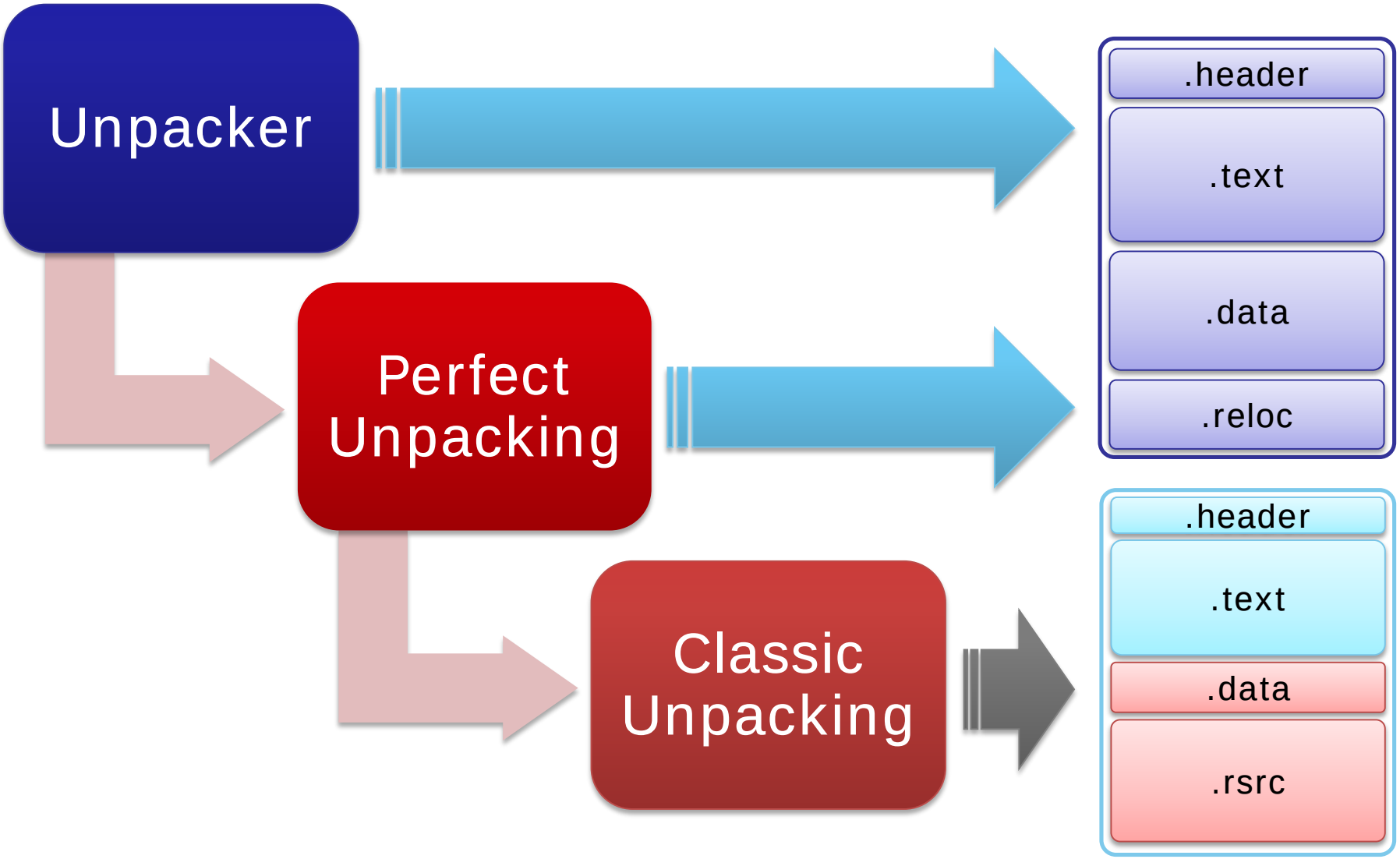
Resent packer implementation

- Packed malware contains original PE file

We have to perform "Perfect Unpacking"

- Dump original PE file from virtual memory

Recommended Unpacking Flow



Thank you!

Contact

- aa-info@jpcert.or.jp
- https://www.jpcert.or.jp

Incident report

- info@jpcert.or.jp
- https://www.jpcert.or.jp/form/