FROD0: Format Reverser Of Data Objects

by Anton Dorfman

HITB 2014, Amsterdam

About me

- Fan of & Fun with Assembly language
- Researcher
- Scientist
- Teach Reverse Engineering since 2001
- Candidate of technical science
- Lecturer at Samara State Technical University and Samara State Aerospace University

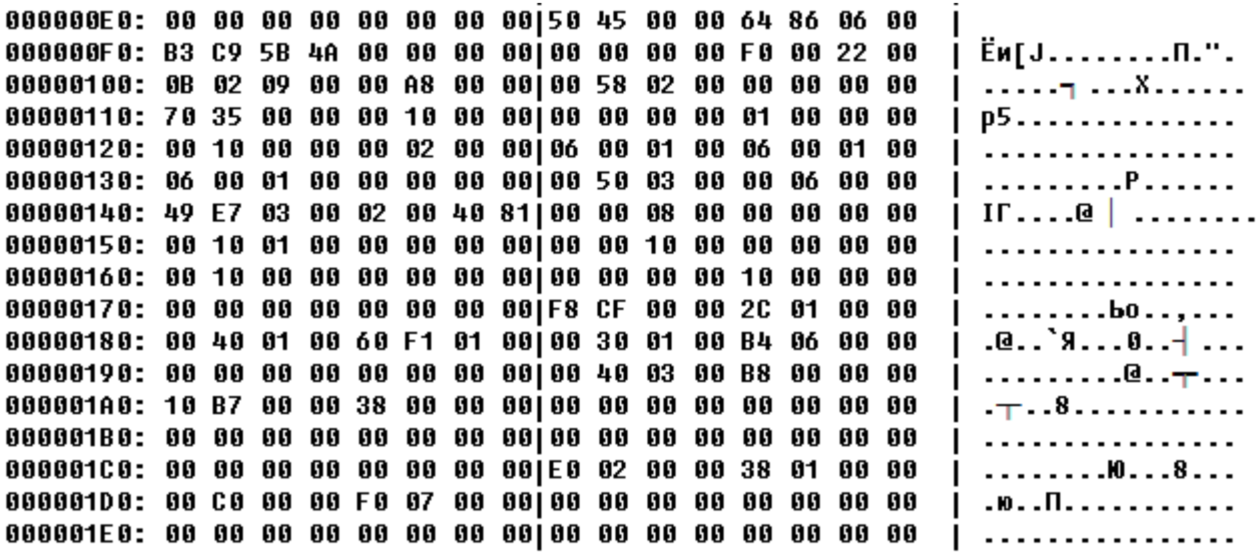
Breaking the rules

- There is the rule RTFM (Read The F**king Manual)
- Nobody likes it
- I’m not exception

- First of all I start my research, and second – try to find related works and analyze them
- After this I generalize ideas from them
- Now I do my best to put all these ideas into the project

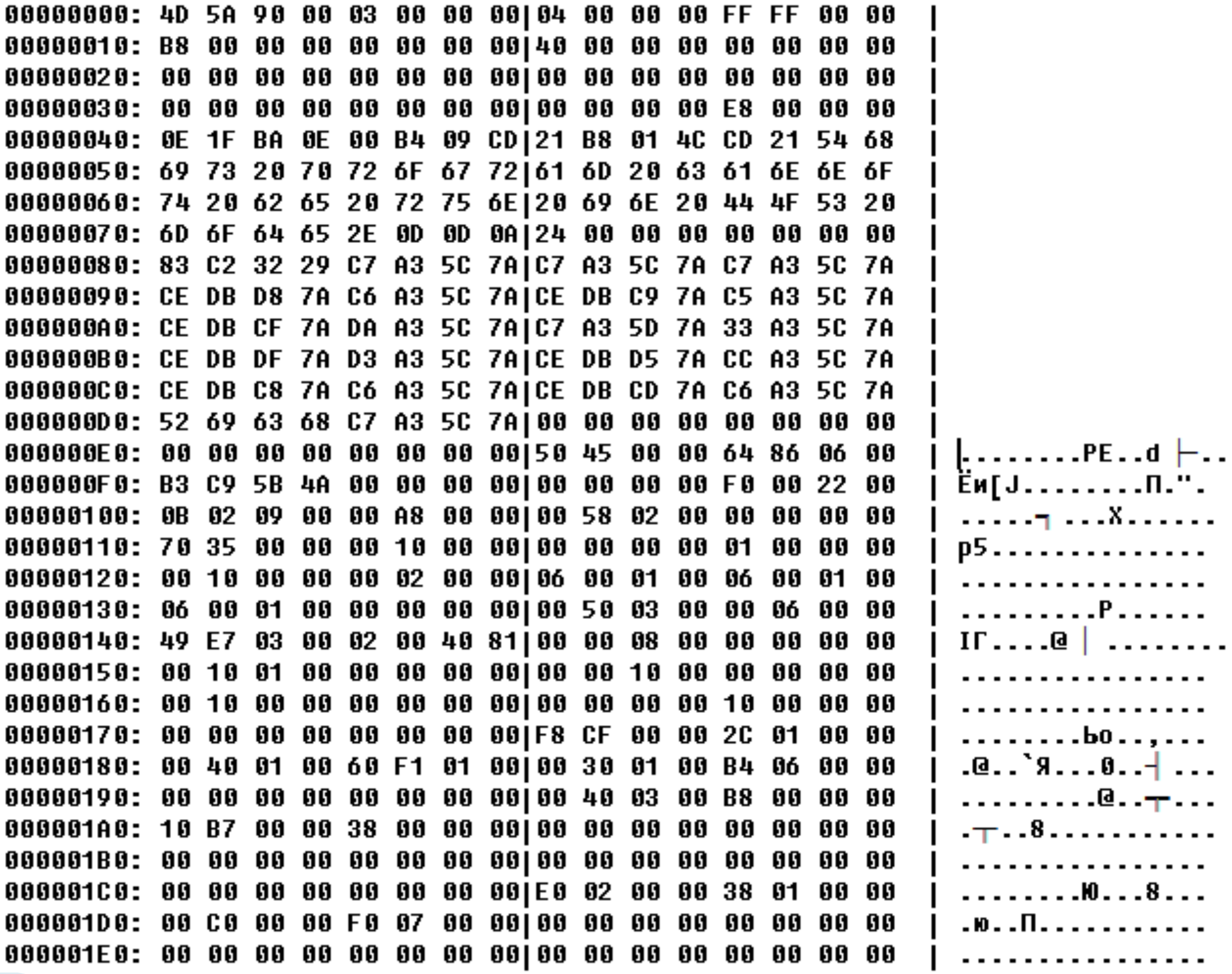
Samples

What is it?



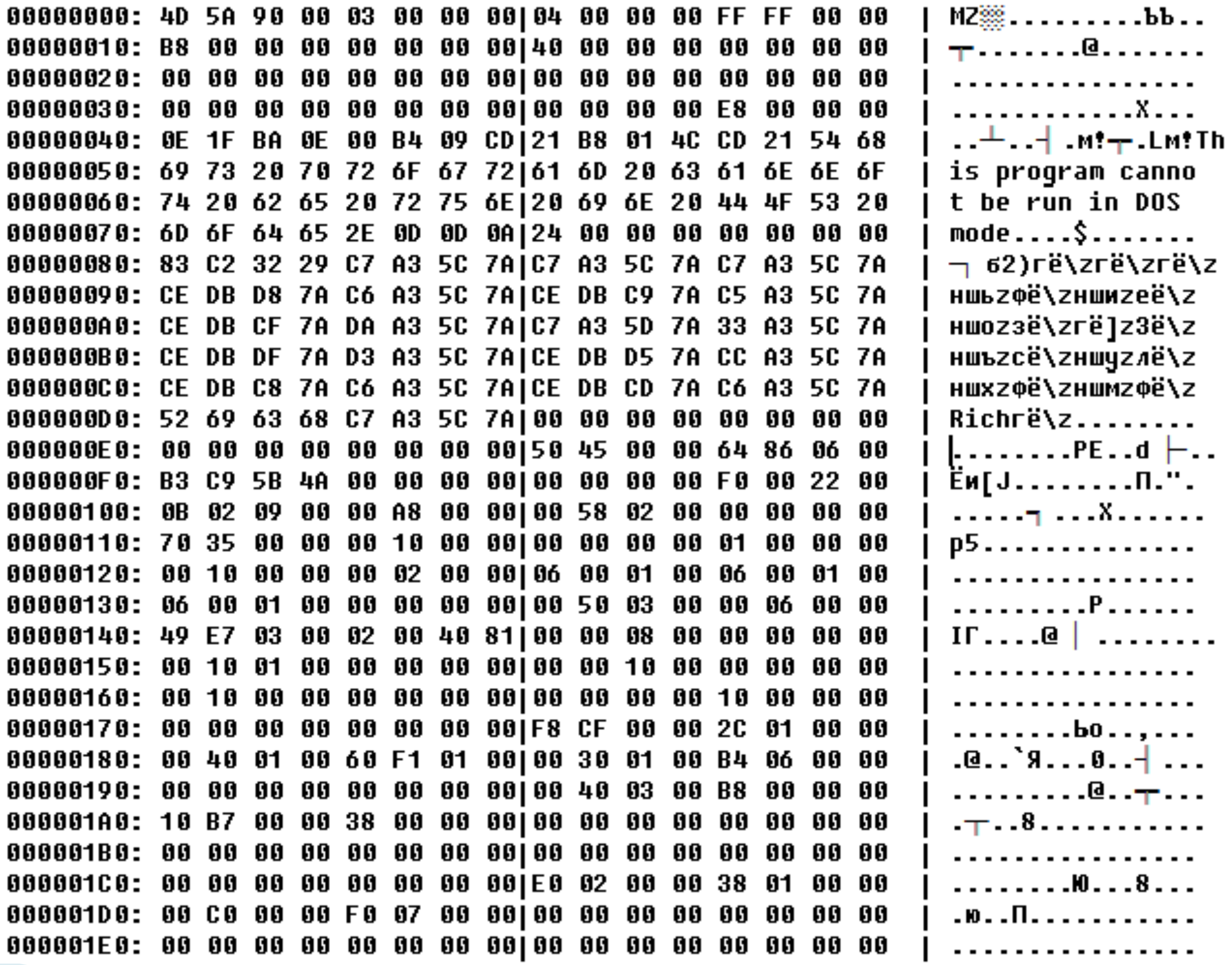
```
000000E0: 00 00 00 00 00 00 00 00|50 45 00 00 64 86 06 00  |
000000F0: B3 C9 5B 4A 00 00 00 00|00 00 00 00 F0 00 22 00  | Ёи[J........П.".
00000100: 0B 02 09 00 00 A8 00 00|00 58 02 00 00 00 00 00  | .....┐...X.......
00000110: 70 35 00 00 00 10 00 00|00 00 00 00 01 00 00 00  | p5..............
00000120: 00 10 00 00 00 02 00 00|06 00 01 00 06 00 01 00  | ................
00000130: 06 00 01 00 00 00 00 00|00 50 03 00 00 06 00 00  | .........P......
00000140: 49 E7 03 00 02 00 40 81|00 00 08 00 00 00 00 00  | IГ....@│........
00000150: 00 10 01 00 00 00 00 00|00 00 10 00 00 00 00 00  | ................
00000160: 00 10 00 00 00 00 00 00|00 00 00 00 10 00 00 00  | ................
00000170: 00 00 00 00 00 00 00 00|F8 CF 00 00 2C 01 00 00  | ........ЬO..,...
00000180: 00 40 01 00 60 F1 01 00|00 30 01 00 B4 06 00 00  | .@..`Я...0..┤...
00000190: 00 00 00 00 00 00 00 00|00 40 03 00 B8 00 00 00  | .........@..┬...
000001A0: 10 B7 00 00 38 00 00 00|00 00 00 00 00 00 00 00  | .┬..8...........
000001B0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
000001C0: 00 00 00 00 00 00 00 00|E0 02 00 00 38 01 00 00  | ........Ю...8...
000001D0: 00 C0 00 00 F0 07 00 00|00 00 00 00 00 00 00 00  | .ю..П...........
000001E0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
```

What is it? Hint 1



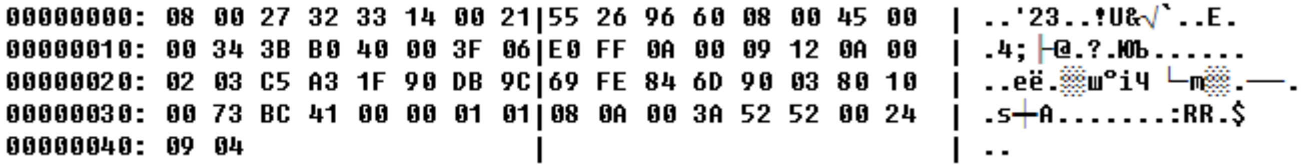
```
00000000: 4D 5A 90 00 03 00 00 00|04 00 00 00 FF FF 00 00  |
00000010: B8 00 00 00 00 00 00 00|40 00 00 00 00 00 00 00  |
00000020: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  |
00000030: 00 00 00 00 00 00 00 00|00 00 00 00 E8 00 00 00  |
00000040: 0E 1F BA 0E 00 B4 09 CD|21 B8 01 4C CD 21 54 68  |
00000050: 69 73 20 70 72 6F 67 72|61 6D 20 63 61 6E 6E 6F  |
00000060: 74 20 62 65 20 72 75 6E|20 69 6E 20 44 4F 53 20  |
00000070: 6D 6F 64 65 2E 0D 0D 0A|24 00 00 00 00 00 00 00  |
00000080: 83 C2 32 29 C7 A3 5C 7A|C7 A3 5C 7A C7 A3 5C 7A  |
00000090: CE DB D8 7A C6 A3 5C 7A|CE DB C9 7A C5 A3 5C 7A  |
000000A0: CE DB CF 7A DA A3 5C 7A|C7 A3 5D 7A 33 A3 5C 7A  |
000000B0: CE DB DF 7A D3 A3 5C 7A|CE DB D5 7A CC A3 5C 7A  |
000000C0: CE DB C8 7A C6 A3 5C 7A|CE DB CD 7A C6 A3 5C 7A  |
000000D0: 52 69 63 68 C7 A3 5C 7A|00 00 00 00 00 00 00 00  |
000000E0: 00 00 00 00 00 00 00 00|50 45 00 00 64 86 06 00  | ........PE..d├..
000000F0: B3 C9 5B 4A 00 00 00 00|00 00 00 00 F0 00 22 00  | Ёи[J........П.".
00000100: 0B 02 09 00 00 A8 00 00|00 58 02 00 00 00 00 00  | .....¬...X.....
00000110: 70 35 00 00 00 10 00 00|00 00 00 00 01 00 00 00  | p5..............
00000120: 00 10 00 00 00 02 00 00|06 00 01 00 06 00 01 00  | ................
00000130: 06 00 01 00 00 00 00 00|00 50 03 00 00 06 00 00  | .........P......
00000140: 49 E7 03 00 02 00 40 81|00 00 08 00 00 00 00 00  | IГ....@│........
00000150: 00 10 01 00 00 00 00 00|00 00 10 00 00 00 00 00  | ................
00000160: 00 10 00 00 00 00 00 00|00 00 00 00 10 00 00 00  | ................
00000170: 00 00 00 00 00 00 00 00|F8 CF 00 00 2C 01 00 00  | ........ьo..,...
00000180: 00 40 01 00 60 F1 01 00|00 30 01 00 B4 06 00 00  | .@..`Я...0..┤...
00000190: 00 00 00 00 00 00 00 00|00 40 03 00 B8 00 00 00  | .........@..╤...
000001A0: 10 B7 00 00 38 00 00 00|00 00 00 00 00 00 00 00  | .┬..8...........
000001B0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
000001C0: 00 00 00 00 00 00 00 00|E0 02 00 00 38 01 00 00  | ........Ю...8...
000001D0: 00 C0 00 00 F0 07 00 00|00 00 00 00 00 00 00 00  | .ю..П...........
000001E0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
```

What is it? Hint 2



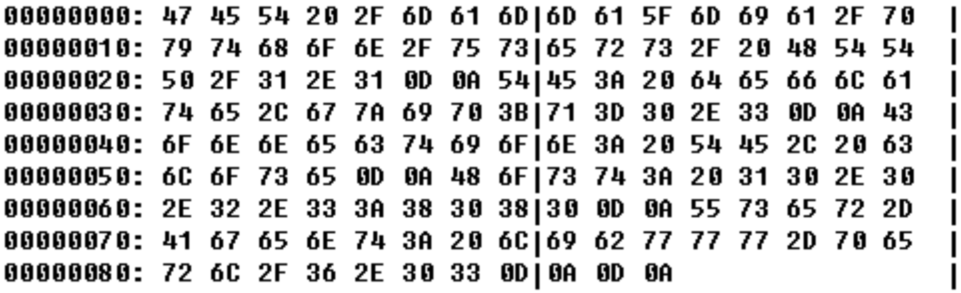
```
00000000: 4D 5A 90 00 03 00 00 00|04 00 00 00 FF FF 00 00  | MZ▒..........ъъ..
00000010: B8 00 00 00 00 00 00 00|40 00 00 00 00 00 00 00  | ┬.......@.......
00000020: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000030: 00 00 00 00 00 00 00 00|00 00 00 00 E8 00 00 00  | ............X...
00000040: 0E 1F BA 0E 00 B4 09 CD|21 B8 01 4C CD 21 54 68  | ..╨..┤.м!┬.Lм!Th
00000050: 69 73 20 70 72 6F 67 72|61 6D 20 63 61 6E 6E 6F  | is program canno
00000060: 74 20 62 65 20 72 75 6E|20 69 6E 20 44 4F 53 20  | t be run in DOS
00000070: 6D 6F 64 65 2E 0D 0D 0A|24 00 00 00 00 00 00 00  | mode....$.......
00000080: 83 C2 32 29 C7 A3 5C 7A|C7 A3 5C 7A C7 A3 5C 7A  | ┐ б2)гё\zгё\zгё\z
00000090: CE DB D8 7A C6 A3 5C 7A|CE DB C9 7A C5 A3 5C 7A  | ншьzфё\zншиzeё\z
000000A0: CE DB CF 7A DA A3 5C 7A|C7 A3 5D 7A 33 A3 5C 7A  | ншozзё\zгё]z3ё\z
000000B0: CE DB DF 7A D3 A3 5C 7A|CE DB D5 7A CC A3 5C 7A  | ншъzсё\zншуzлё\z
000000C0: CE DB C8 7A C6 A3 5C 7A|CE DB CD 7A C6 A3 5C 7A  | ншxzфё\zншмzфё\z
000000D0: 52 69 63 68 C7 A3 5C 7A|00 00 00 00 00 00 00 00  | Richгё\z........
000000E0: 00 00 00 00 00 00 00 00|50 45 00 00 64 86 06 00  | ........PE..d ├..
000000F0: B3 C9 5B 4A 00 00 00 00|00 00 00 00 F0 00 22 00  | Ёи[J........П.".
00000100: 0B 02 09 00 00 A8 00 00|00 58 02 00 00 00 00 00  | .....┐ ...X......
00000110: 70 35 00 00 00 10 00 00|00 00 00 00 01 00 00 00  | p5..............
00000120: 00 10 00 00 00 02 00 00|06 00 01 00 06 00 01 00  | ................
00000130: 06 00 01 00 00 00 00 00|00 50 03 00 00 06 00 00  | .........P......
00000140: 49 E7 03 00 02 00 40 81|00 00 08 00 00 00 00 00  | IГ....@ │ ........
00000150: 00 10 01 00 00 00 00 00|00 00 10 00 00 00 00 00  | ................
00000160: 00 10 00 00 00 00 00 00|00 00 00 00 10 00 00 00  | ................
00000170: 00 00 00 00 00 00 00 00|F8 CF 00 00 2C 01 00 00  | ........ъo..,...
00000180: 00 40 01 00 60 F1 01 00|00 30 01 00 B4 06 00 00  | .@..`Я...0..┤ ...
00000190: 00 00 00 00 00 00 00 00|00 40 03 00 B8 00 00 00  | .........@..┬...
000001A0: 10 B7 00 00 38 00 00 00|00 00 00 00 00 00 00 00  | .┬..8...........
000001B0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
000001C0: 00 00 00 00 00 00 00 00|E0 02 00 00 38 01 00 00  | ........Ю...8...
000001D0: 00 C0 00 00 F0 07 00 00|00 00 00 00 00 00 00 00  | .ю..П...........
000001E0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
```

What is it?



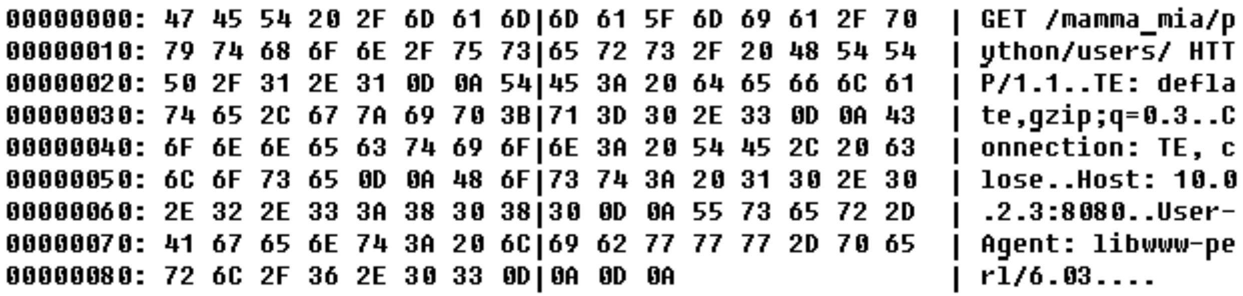
```
00000000: 08 00 27 32 33 14 00 21|55 26 96 60 08 00 45 00  | ..'23..!U&√`..E.
00000010: 00 34 3B B0 40 00 3F 06|E0 FF 0A 00 09 12 0A 00  | .4;├@.?.Юb......
00000020: 02 03 C5 A3 1F 90 DB 9C|69 FE 84 6D 90 03 80 10  | ..eё.▒ш°iЧ └m▒.─.
00000030: 00 73 BC 41 00 00 01 01|08 0A 00 3A 52 52 00 24  | .s┼A........:RR.$
00000040: 09 04                  |                         | ..
```

What is it?



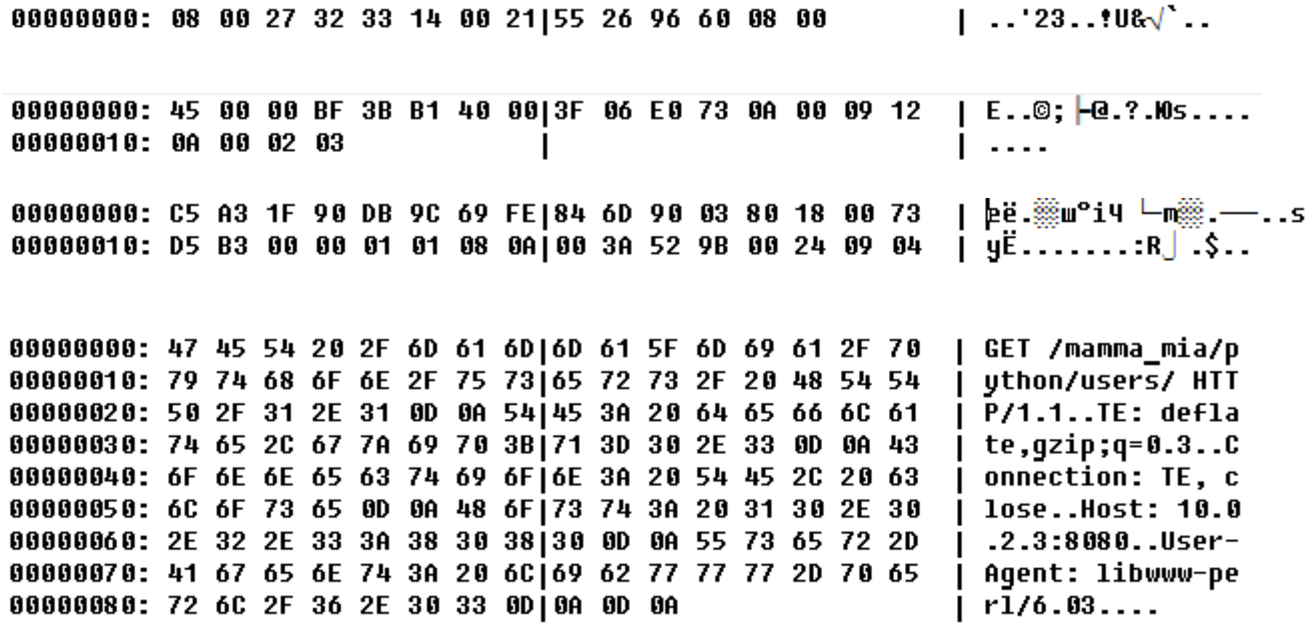
```
00000000: 47 45 54 20 2F 6D 61 6D|6D 61 5F 6D 69 61 2F 70  |
00000010: 79 74 68 6F 6E 2F 75 73|65 72 73 2F 20 48 54 54  |
00000020: 50 2F 31 2E 31 0D 0A 54|45 3A 20 64 65 66 6C 61  |
00000030: 74 65 2C 67 7A 69 70 3B|71 3D 30 2E 33 0D 0A 43  |
00000040: 6F 6E 6E 65 63 74 69 6F|6E 3A 20 54 45 2C 20 63  |
00000050: 6C 6F 73 65 0D 0A 48 6F|73 74 3A 20 31 30 2E 30  |
00000060: 2E 32 2E 33 3A 38 30 38|30 0D 0A 55 73 65 72 2D  |
00000070: 41 67 65 6E 74 3A 20 6C|69 62 77 77 77 2D 70 65  |
00000080: 72 6C 2F 36 2E 30 33 0D|0A 0D 0A                 |
```

What is it? Hint 1



```
00000000: 47 45 54 20 2F 6D 61 6D|6D 61 5F 6D 69 61 2F 70  | GET /mamma_mia/p
00000010: 79 74 68 6F 6E 2F 75 73|65 72 73 2F 20 48 54 54  | ython/users/ HTT
00000020: 50 2F 31 2E 31 0D 0A 54|45 3A 20 64 65 66 6C 61  | P/1.1..TE: defla
00000030: 74 65 2C 67 7A 69 70 3B|71 3D 30 2E 33 0D 0A 43  | te,gzip;q=0.3..C
00000040: 6F 6E 6E 65 63 74 69 6F|6E 3A 20 54 45 2C 20 63  | onnection: TE, c
00000050: 6C 6F 73 65 0D 0A 48 6F|73 74 3A 20 31 30 2E 30  | lose..Host: 10.0
00000060: 2E 32 2E 33 3A 38 30 38|30 0D 0A 55 73 65 72 2D  | .2.3:8080..User-
00000070: 41 67 65 6E 74 3A 20 6C|69 62 77 77 77 2D 70 65  | Agent: libwww-pe
00000080: 72 6C 2F 36 2E 30 33 0D|0A 0D 0A                 | rl/6.03....
```

What is it? Hint 2



```
00000000: 08 00 27 32 33 14 00 21|55 26 96 60 08 00             | ..'23..!U&√`..

00000000: 45 00 00 BF 3B B1 40 00|3F 06 E0 73 0A 00 09 12        | E..©;├@.?.Ю̆s....
00000010: 0A 00 02 03              |                             | ....

00000000: C5 A3 1F 90 DB 9C 69 FE|84 6D 90 03 80 18 00 73        | ╞ë.░ш°i╕ └m░.──..s
00000010: D5 B3 00 00 01 01 08 0A|00 3A 52 9B 00 24 09 04        | yË.......:R┘.$..


00000000: 47 45 54 20 2F 6D 61 6D|6D 61 5F 6D 69 61 2F 70        | GET /mamma_mia/p
00000010: 79 74 68 6F 6E 2F 75 73|65 72 73 2F 20 48 54 54        | ython/users/ HTT
00000020: 50 2F 31 2E 31 0D 0A 54|45 3A 20 64 65 66 6C 61        | P/1.1..TE: defla
00000030: 74 65 2C 67 7A 69 70 3B|71 3D 30 2E 33 0D 0A 43        | te,gzip;q=0.3..C
00000040: 6F 6E 6E 65 63 74 69 6F|6E 3A 20 54 45 2C 20 63        | onnection: TE, c
00000050: 6C 6F 73 65 0D 0A 48 6F|73 74 3A 20 31 30 2E 30        | lose..Host: 10.0
00000060: 2E 32 2E 33 3A 38 30 38|30 0D 0A 55 73 65 72 2D        | .2.3:8080..User-
00000070: 41 67 65 6E 74 3A 20 6C|69 62 77 77 77 2D 70 65        | Agent: libwww-pe
00000080: 72 6C 2F 36 2E 30 33 0D|0A 0D 0A                       | rl/6.03....
```

Intro

What is Data Format?

- File formats – multimedia formats, database formats, internal formats for exchanging between program components and etc.
- Protocols – network protocols, hardware device interaction protocols, protocols of interaction between driver and user space application and etc.
- Structures in memory – OS structures, application structures and etc.

Why RE Data Formats is important?

- Reverse engineering any program
- Reverse engineering undocumented/proprietary file formats, network protocols, structures in memory
- Fuzzing
- Memory forensics
- Examination of protocol implementation
- Vulnerability discovery
- Exploit generation
- Kernel rootkit detection
- Malware classification
- OS kernel fingerprinting
- Replay network interaction
- Zero-day vulnerability signature generation

Standard way

- Hex editor
- Researcher
- Brain (equally important as a hex editor)
- Basic knowledge how data can be organized (in brain)
- Analysis of the executable file that manipulates with data format

- But this way is a hard and challenging task and existing manual approaches tend to be time-consuming, tedious, boring and error-prone. As an example, after numerous trials and errors, it took 12 years for the open-source Samba project to reverse engineer the Microsoft SMB protocol!

Related works analysis

Related works

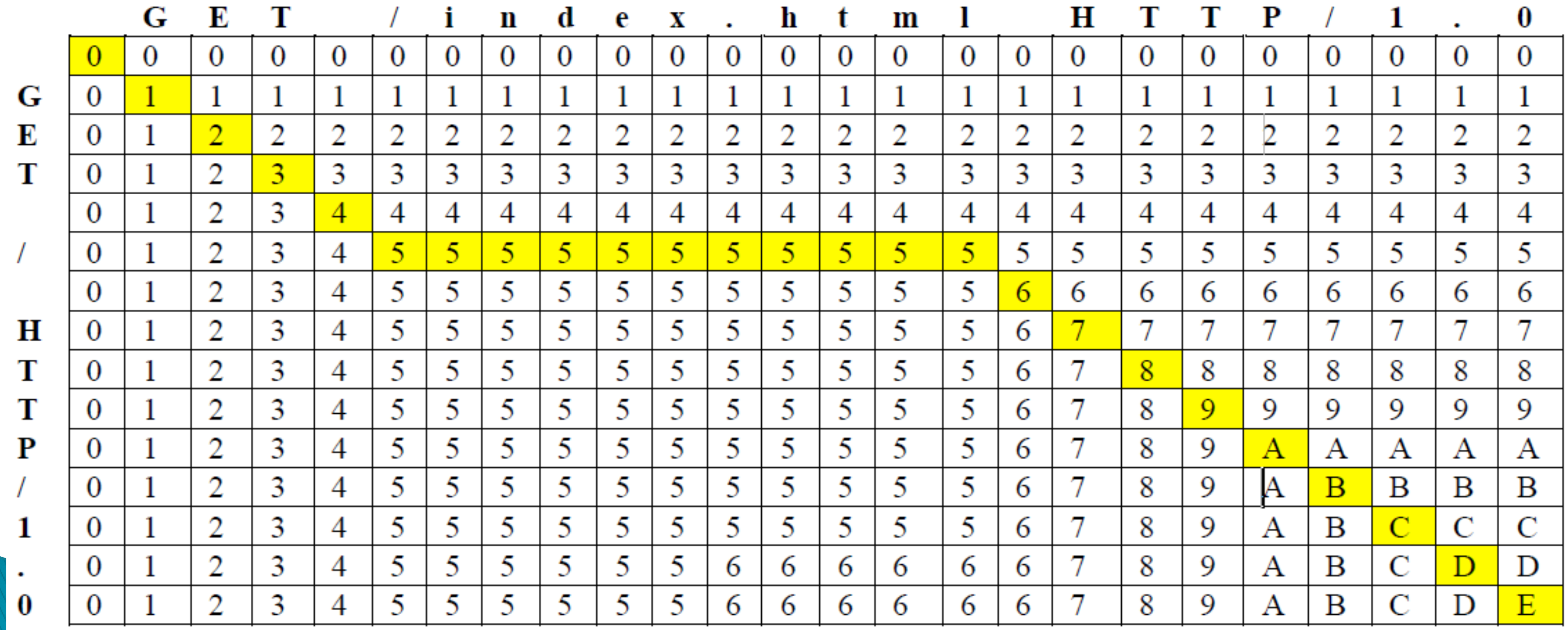
- Protocol Informatics Project – “Network Protocol Analysis using Bioinformatics Algorithms” by Marshall A. Beddoe, 2004
- NoName – “Extracting Output Formats from Executables” by J. Lim, T. Reps, B. Liblit, 2006
- Discoverer – “Discoverer: Automatic Protocol Reverse Engineering from Network Traces” by Weidong Cui, Jayanthkumar Kannan, Helen J. Wang, 2007
- Laika – “Digging For Data Structures” by Anthony Cozzie, Frank Stratton, Hui Xue, and Samuel T. King, 2008
- Tupni – “Tupni: Automatic Reverse Engineering of Input Formats” by Weidong Cui, Marcus Peinado, Karl Chen, Helen J. Wang, Luiz Irun-Briz, 2008
- AutoFormat – “Automatic Protocol Format Reverse Engineering through Context-Aware Monitored Execution” by Zhiqiang Lin, Xuxian Jiang, Dongyan Xu, Xiangyu Zhang, 2008
- REWARDS – “Automatic Reverse Engineering of Data Structures from Binary Execution” by Zhiqiang Lin, Xiangyu Zhang, Dongyan Xu, 2010
- Howard – “Howard: a dynamic excavator for reverse engineering data structures” by Asia Slowinska, Traian Stancescu, Herbert Bos, 2011

3 ways of researching

- Static RE analysis – analyze in static, just using binary file how applications parse and handle data format: NoName
- Dynamic RE analysis – analyze in dynamic how applications parse and handle data format to understand it often uses dynamic taint analysis and dynamic binary instrumentation: Tupni, AutoFormat, REWARDS , Howard
- **Statistic analysis – try to extract header, structures, fields and try to find relationship between data based on some amount of samples and use statistics of changes and ranges of values: Protocol Informatics Project, Discoverer, Laika**

Protocol Informatics Project

- Uses global and local sequence alignment – Needleman Wunsch and Smith Waterman algorithms – with sources

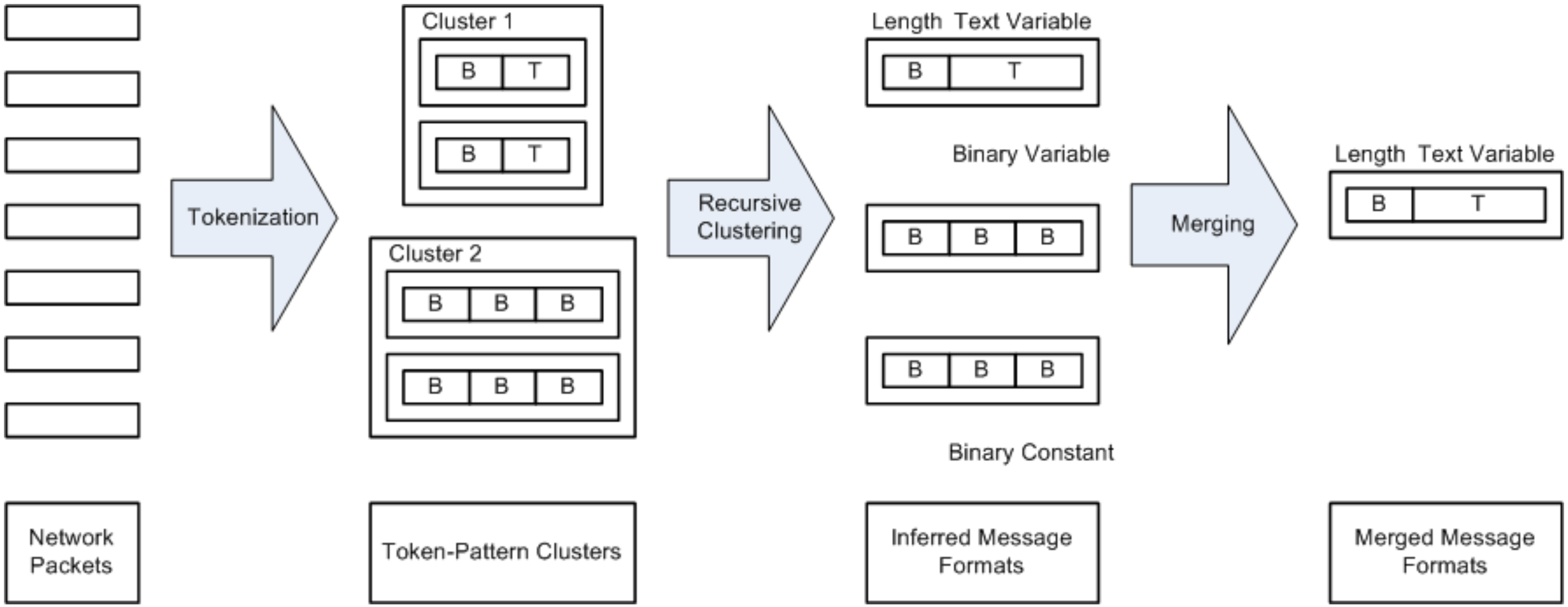


		G	E	T		/	i	n	d	e	x	.	h	t	m	l		H	T	T	P	/	1	.	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
G	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
E	0	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
T	0	1	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
	0	1	2	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
/	0	1	2	3	4	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
	0	1	2	3	4	5	5	5	5	5	5	5	5	5	5	5	6	6	6	6	6	6	6	6	6
H	0	1	2	3	4	5	5	5	5	5	5	5	5	5	5	5	6	7	7	7	7	7	7	7	7
T	0	1	2	3	4	5	5	5	5	5	5	5	5	5	5	5	6	7	8	8	8	8	8	8	8
T	0	1	2	3	4	5	5	5	5	5	5	5	5	5	5	5	6	7	8	9	9	9	9	9	9
P	0	1	2	3	4	5	5	5	5	5	5	5	5	5	5	5	6	7	8	9	A	A	A	A	A
/	0	1	2	3	4	5	5	5	5	5	5	5	5	5	5	5	6	7	8	9	A	B	B	B	B
1	0	1	2	3	4	5	5	5	5	5	5	5	5	5	5	5	6	7	8	9	A	B	C	C	C
.	0	1	2	3	4	5	5	5	5	5	5	6	6	6	6	6	6	7	8	9	A	B	C	D	D
0	0	1	2	3	4	5	5	5	5	5	5	6	6	6	6	6	6	7	8	9	A	B	C	D	E

Discoverer

- A tool for automatically reverse engineering the protocol message formats of an application from its network trace
- A key property of Discoverer is that it operates in a protocol-independent fashion by inferring protocol idioms commonly seen in message formats of many application-level protocols.
- Tested on 1 text protocol – HTTP and 2 binary protocols RPC and CIFS/SMB

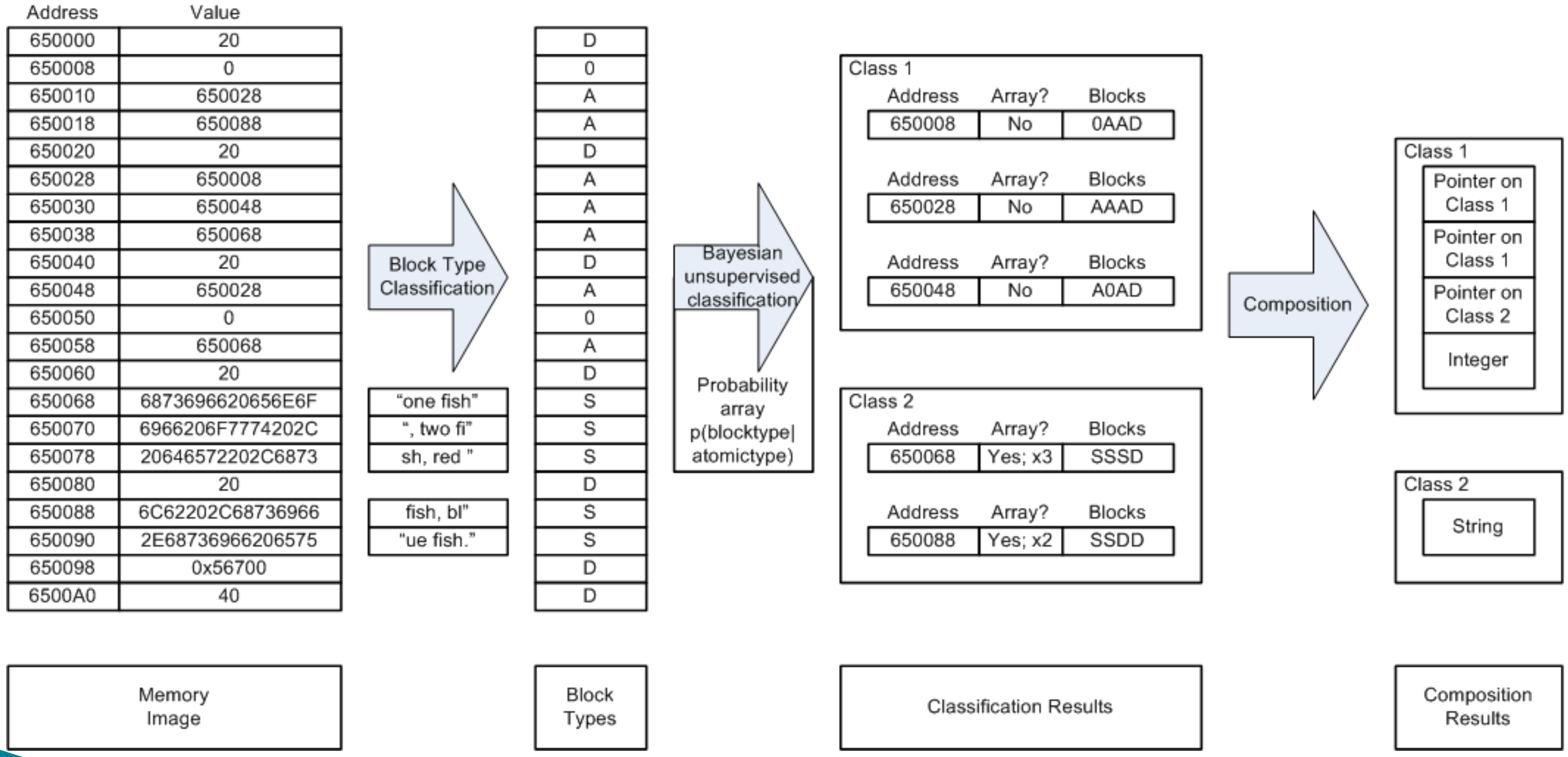
Discoverer


Tokenization
Cluster 1
B
T
B
T
Cluster 2
B
B
B
B
B
B
Recursive Clustering
Length Text Variable
B
T
Binary Variable
B
B
B
B
B
B
Binary Constant
Merging
Length Text Variable
B
T
Network Packets
Token-Pattern Clusters
Inferred Message Formats
Merged Message Formats

Laika

- Detects stuctures in memory using Bayesian unsupervised learning
- For fixed size structures only
- 2 key features: identifying the positions and sizes of objects, and determining which objects are similar based on their byte values.
- Laika identify object positions and sizes by using potential pointers in the image to estimate object positions and sizes.
- The basic block types are address (points into heap/stack), zero, string, and data (everything else)

Laika



Address	Value
650000	20
650008	0
650010	650028
650018	650088
650020	20
650028	650008
650030	650048
650038	650068
650040	20
650048	650028
650050	0
650058	650068
650060	20
650068	6873696620656E6F
650070	6966206F7774202C
650078	20646572202C6873
650080	20
650088	6C62202C68736966
650090	2E68736966206575
650098	0x56700
6500A0	40

Memory Image

“one fish”
“, two fi”
sh, red ”

fish, bl”
“ue fish.”

D
0
A
A
D
A
A
A
D
A
0
A
D
S
S
S
D
S
S
D
D

Block Types

Probability array p(blocktype| atomictype)

Class 1

Address	Array?	Blocks
650008	No	0AAD

Address	Array?	Blocks
650028	No	AAAD

Address	Array?	Blocks
650048	No	A0AD

Class 2

Address	Array?	Blocks
650068	Yes; x3	SSSD

Address	Array?	Blocks
650088	Yes; x2	SSDD

Classification Results

Class 1

- Pointer on Class 1
- Pointer on Class 1
- Pointer on Class 2
- Integer

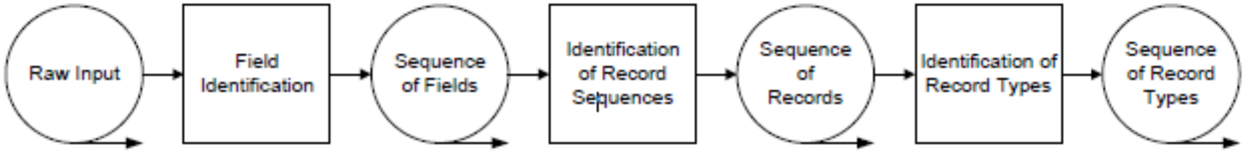
Class 2

- String

Composition Results

Tupni

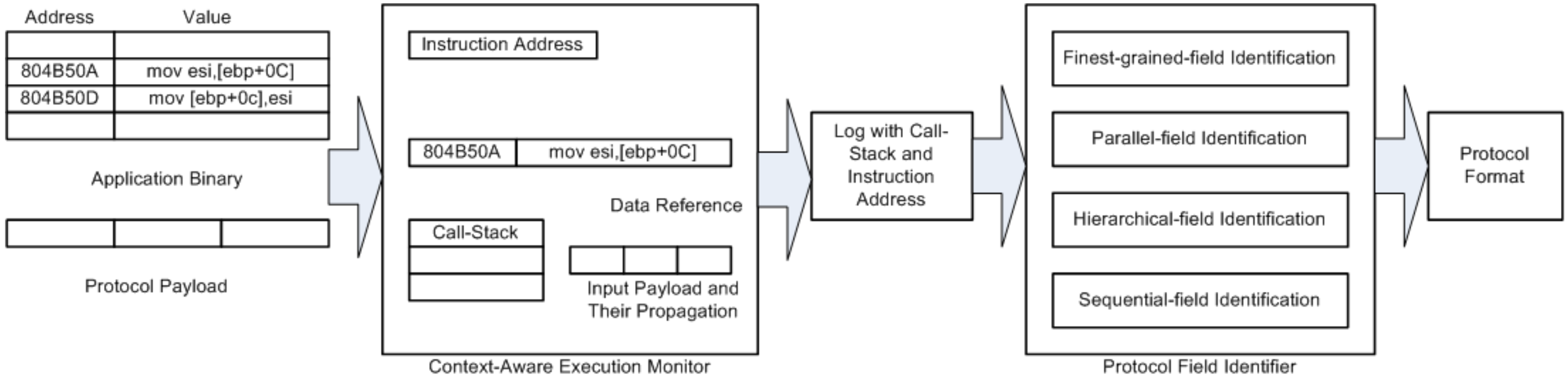
- Based on taint tracking engine
- Tested on WMF, BMP, JPG, PNG, TIF, DNS, RPC, TFTP, HTTP, FTP



AutoFormat

- Application field: 2 text-based HTTP SIP, 3 binary-based DHCP, RIP, OSPF, hybrid (mixed) CIFS/SMB and unknown used by malware structure of the protocol format by revealing possible relations (e.g., sequential, parallel, and hierarchical) among the message fields
- By monitoring the program execution, it collect the execution context information for every message byte (annotated with its offset in the entire message) and cluster them to derive the protocol format

AutoFormat



Address	Value
804B50A	mov esi,[ebp+0C]
804B50D	mov [ebp+0c],esi

804B50A	mov esi,[ebp+0C]

Application Binary
Protocol Payload
Instruction Address
Data Reference
Call-Stack
Input Payload and Their Propagation
Context-Aware Execution Monitor
Log with Call-Stack and Instruction Address
Finest-grained-field Identification
Parallel-field Identification
Hierarchical-field Identification
Sequential-field Identification
Protocol Field Identifier
Protocol Format

FRODO

Main Idea of FRODO

- All programs use data formats
- Data formats are developed by human (not pets or aliens)
- Sometimes looks like that no human works on it…
- Data formats are abstractions of implementation details
- Format developers use common data organization concepts and similar thoughts when creating new data formats
- If we find regularities in data format organization rules we can automate searching of them

Definitions

- Data – information for representing which Data Format is developed
- MetaData – some structure for describing Data Format
- Field – some value used to describe Data Format
- Structure – way for organizing various fields
- Header – most common type of MetaData – structure before data, may contain substructures with fields

FRODO Tasks

- **Data Format analysis – generate specification**
- Format specification checking – the difference between specification and realisation
- Memory dump reconstruction – find various data format structures in memory and links between them

Tasks to solve

- Extract header, separate it from data
- Find field boundaries
- Find value ranges of fields
- Find structures and substructures
- Find types of fields
- Detect bit and byte ordering
- **Determine semantics of fields**

Levels of abstraction

- Bit Order
- Byte Order
- Fields Size
- Field Basic Type
- Field Type
- Structure
- Field Semantics

Types of fields

- Service fields – for describing Data Format (size of structure and etc.)
- Common fields – “fields from life” (time, date and etc.)
- Specific fields – we can find range for that type (bit flags and etc.)

Field Size and Levels of field interpretation

- Commonly field is a byte sequence
- Sometimes field is a bit sequence

- Fixed size in bytes (1, 2, 3, 4, …)
- Fixed size in bits (1, 2, 3, 4, …)
- Variable size in bytes
- Variable size in bits

Basic field types

- Hex value – by default
- Decimal value
- Character value (up to 4 symbols)
- String (ASCII or Unicode)
- Float value

ASCII String

- Usually fixed size, remaining space after text filled with 0
- Variable sized text ended with 0, or there are size of this text field

- Usually text string contain their meanings

Service fields

- ID
- Offset
- Size
- Quantity
- Flag
- Counter

ID

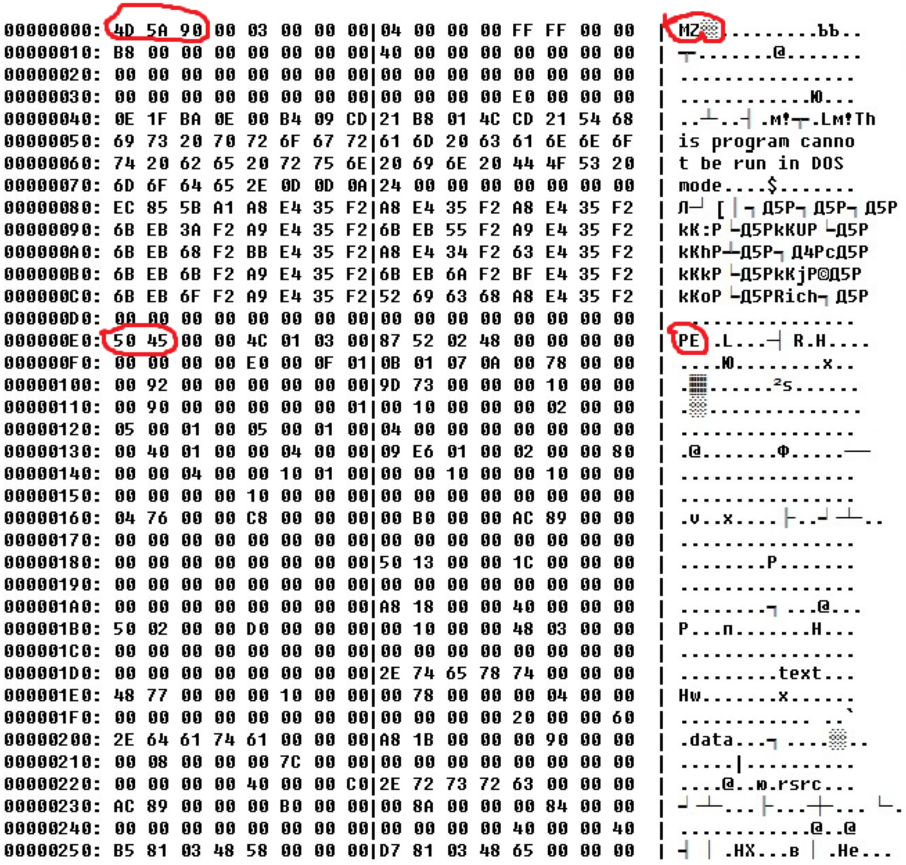
- Common:
- Identifier of data format, also known as «magic number»

- Properties:
- Every copy of data format structure contains the same ID value
- Field size – can be n bytes
- Usually ID of data format – first n bytes of instance
- Often Consist of char symbols – “PE”
- Often Looks like “magic” in hex – BE BA FE CA

- Subtypes:
- ID of data format – exist in all instances of that data format
- ID of structure – exist in all instances of that data structure

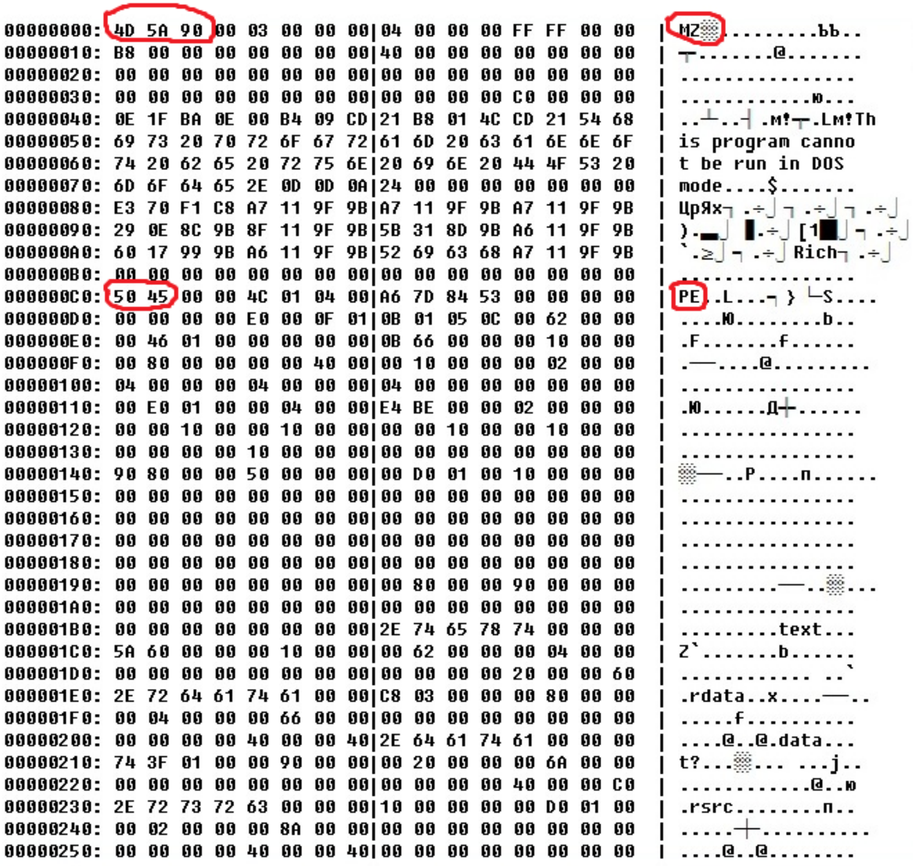
ID

- Notepad.exe



```
00000000: 4D 5A 90 00 03 00 00 00|04 00 00 00 FF FF 00 00  | MZ░.........ьь..
00000010: B8 00 00 00 00 00 00 00|40 00 00 00 00 00 00 00  | ╤.......@.......
00000020: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000030: 00 00 00 00 00 00 00 00|00 00 00 00 E0 00 00 00  | ............Ю...
00000040: 0E 1F BA 0E 00 B4 09 CD|21 B8 01 4C CD 21 54 68  | ..╨..┤.═!╤.L═!Th
00000050: 69 73 20 70 72 6F 67 72|61 6D 20 63 61 6E 6E 6F  | is program canno
00000060: 74 20 62 65 20 72 75 6E|20 69 6E 20 44 4F 53 20  | t be run in DOS
00000070: 6D 6F 64 65 2E 0D 0D 0A|24 00 00 00 00 00 00 00  | mode....$.......
00000080: EC 85 5B A1 A8 E4 35 F2|A8 E4 35 F2 A8 E4 35 F2  | ЛЕ[б╕Д5Р╕Д5Р╕Д5Р
00000090: 6B EB 3A F2 A9 E4 35 F2|6B EB 55 F2 A9 E4 35 F2  | kK:P╘Д5PkKUP╘Д5P
000000A0: 6B EB 68 F2 BB E4 35 F2|A8 E4 34 F2 63 E4 35 F2  | kKhP╗Д5P╕Д4PcД5P
000000B0: 6B EB 6B F2 A9 E4 35 F2|6B EB 6A F2 BF E4 35 F2  | kKkP╘Д5PkKjP©Д5P
000000C0: 6B EB 6F F2 A9 E4 35 F2|52 69 63 68 A8 E4 35 F2  | kKoP╘Д5PRich╕Д5P
000000D0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
000000E0: 50 45 00 00 4C 01 03 00|87 52 02 48 00 00 00 00  | PE..L...┤R.H....
000000F0: 00 00 00 00 E0 00 0F 01|0B 01 07 0A 00 78 00 00  | ....Ю.........x..
00000100: 00 92 00 00 00 00 00 00|9D 73 00 00 00 10 00 00  | .▓......²s......
00000110: 00 90 00 00 00 00 00 01|00 10 00 00 00 02 00 00  | .░..............
00000120: 05 00 01 00 05 00 01 00|04 00 00 00 00 00 00 00  | ................
00000130: 00 40 01 00 00 04 00 00|09 E6 01 00 02 00 00 80  | .@.......Ф.....─
00000140: 00 00 04 00 00 10 01 00|00 00 10 00 00 10 00 00  | ................
00000150: 00 00 00 00 10 00 00 00|00 00 00 00 00 00 00 00  | ................
00000160: 04 76 00 00 C8 00 00 00|00 B0 00 00 AC 89 00 00  | .v..x.....├..┘┴..
00000170: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000180: 00 00 00 00 00 00 00 00|50 13 00 00 1C 00 00 00  | ........P.......
00000190: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
000001A0: 00 00 00 00 00 00 00 00|A8 18 00 00 40 00 00 00  | ........╕...@...
000001B0: 50 02 00 00 D0 00 00 00|00 10 00 00 48 03 00 00  | P...п.......H...
000001C0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
000001D0: 00 00 00 00 00 00 00 00|2E 74 65 78 74 00 00 00  | .........text...
000001E0: 48 77 00 00 00 10 00 00|00 78 00 00 00 04 00 00  | Hw.......x......
000001F0: 00 00 00 00 00 00 00 00|00 00 00 00 20 00 00 60  | ............ ..`
00000200: 2E 64 61 74 61 00 00 00|A8 1B 00 00 00 90 00 00  | .data...╕....░..
00000210: 00 08 00 00 00 7C 00 00|00 00 00 00 00 00 00 00  | .....|..........
00000220: 00 00 00 00 40 00 00 C0|2E 72 73 72 63 00 00 00  | ....@..ю.rsrc...
00000230: AC 89 00 00 00 B0 00 00|00 8A 00 00 00 84 00 00  | ┘┴...├...┼...└.
00000240: 00 00 00 00 00 00 00 00|00 00 00 00 40 00 00 40  | ............@..@
00000250: B5 81 03 48 58 00 00 00|D7 81 03 48 65 00 00 00  | ┤│.HX...в│.He...
```

Frodo.exe



```
00000000: 4D 5A 90 00 03 00 00 00|04 00 00 00 FF FF 00 00  | MZ░.........ьь..
00000010: B8 00 00 00 00 00 00 00|40 00 00 00 00 00 00 00  | ╤.......@.......
00000020: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000030: 00 00 00 00 00 00 00 00|00 00 00 00 C0 00 00 00  | ............ю...
00000040: 0E 1F BA 0E 00 B4 09 CD|21 B8 01 4C CD 21 54 68  | ..╨..┤.═!╤.L═!Th
00000050: 69 73 20 70 72 6F 67 72|61 6D 20 63 61 6E 6E 6F  | is program canno
00000060: 74 20 62 65 20 72 75 6E|20 69 6E 20 44 4F 53 20  | t be run in DOS
00000070: 6D 6F 64 65 2E 0D 0D 0A|24 00 00 00 00 00 00 00  | mode....$.......
00000080: E3 70 F1 C8 A7 11 9F 9B|A7 11 9F 9B A7 11 9F 9B  | ЦрЯх╖.÷┘╖.÷┘╖.÷┘
00000090: 29 0E 8C 9B 8F 11 9F 9B|5B 31 8D 9B A6 11 9F 9B  | ).▄┘▐.÷┘[1█┘╢.÷┘
000000A0: 60 17 99 9B A6 11 9F 9B|52 69 63 68 A7 11 9F 9B  | `.≥┘╢.÷┘Rich╖.÷┘
000000B0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
000000C0: 50 45 00 00 4C 01 04 00|A6 7D 84 53 00 00 00 00  | PE..L...╢}└S....
000000D0: 00 00 00 00 E0 00 0F 01|0B 01 05 0C 00 62 00 00  | ....Ю.........b..
000000E0: 00 46 01 00 00 00 00 00|0B 66 00 00 00 10 00 00  | .F.......f......
000000F0: 00 80 00 00 00 00 40 00|00 10 00 00 00 02 00 00  | .─.....@.........
00000100: 04 00 00 00 04 00 00 00|04 00 00 00 00 00 00 00  | ................
00000110: 00 E0 01 00 00 04 00 00|E4 BE 00 00 02 00 00 00  | .Ю......Д┼......
00000120: 00 00 10 00 00 10 00 00|00 00 10 00 00 10 00 00  | ................
00000130: 00 00 00 00 10 00 00 00|00 00 00 00 00 00 00 00  | ................
00000140: 90 80 00 00 50 00 00 00|00 D0 01 00 10 00 00 00  | ░─..P....п......
00000150: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000160: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000170: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000180: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000190: 00 00 00 00 00 00 00 00|00 80 00 00 90 00 00 00  | .........─..░...
000001A0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
000001B0: 00 00 00 00 00 00 00 00|2E 74 65 78 74 00 00 00  | .........text...
000001C0: 5A 60 00 00 00 10 00 00|00 62 00 00 00 04 00 00  | Z`.......b......
000001D0: 00 00 00 00 00 00 00 00|00 00 00 00 20 00 00 60  | ............ ..`
000001E0: 2E 72 64 61 74 61 00 00|C8 03 00 00 00 80 00 00  | .rdata..x....─..
000001F0: 00 04 00 00 00 66 00 00|00 00 00 00 00 00 00 00  | .....f..........
00000200: 00 00 00 00 40 00 00 40|2E 64 61 74 61 00 00 00  | ....@..@.data...
00000210: 74 3F 01 00 00 90 00 00|00 20 00 00 00 6A 00 00  | t?...░... ...j..
00000220: 00 00 00 00 00 00 00 00|00 00 00 00 40 00 00 C0  | ............@..ю
00000230: 2E 72 73 72 63 00 00 00|10 00 00 00 00 D0 01 00  | .rsrc.........п..
00000240: 00 02 00 00 00 8A 00 00|00 00 00 00 00 00 00 00  | .....┼..........
00000250: 00 00 00 00 40 00 00 40|00 00 00 00 00 00 00 00  | ....@..@........
```

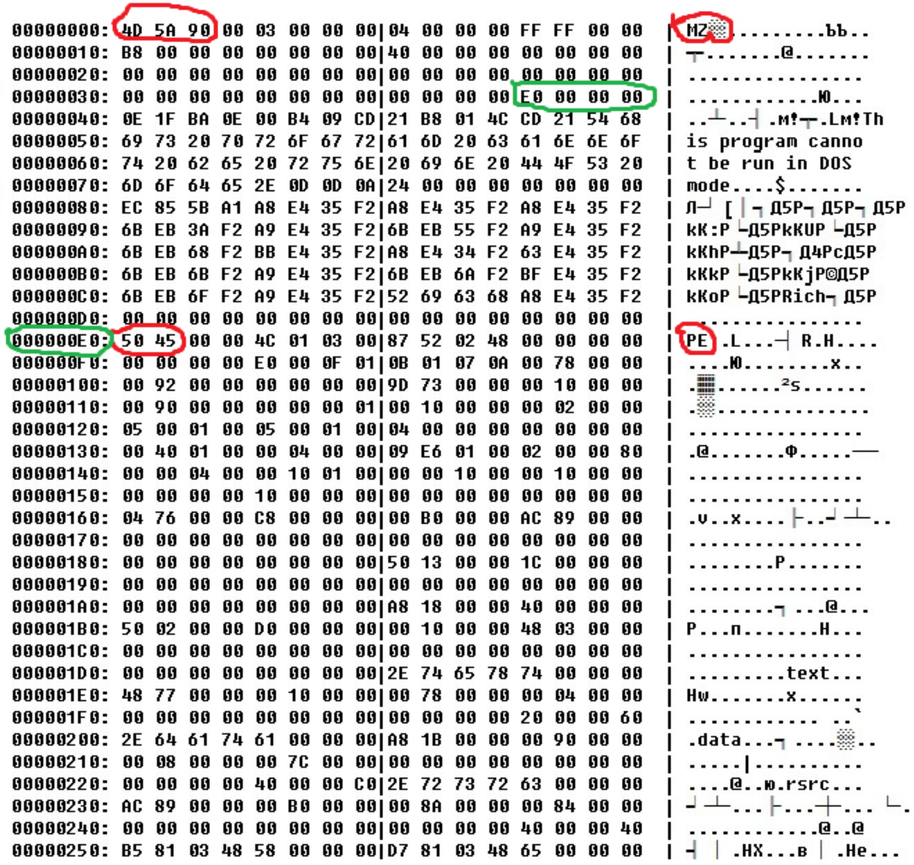
Offset

- Properties:
- Offset pointed inside instance of data format
- Offset pointed inside concerned block
- Depends on it can be absolute or relative
- Field size – depends on architecture – 2, 4, 8 and etc bytes

- Subtypes:
- Offset to data
- Offset to another field
- Offset to another structure
- Offset to the instance of the same structure (next or previous in linked list)

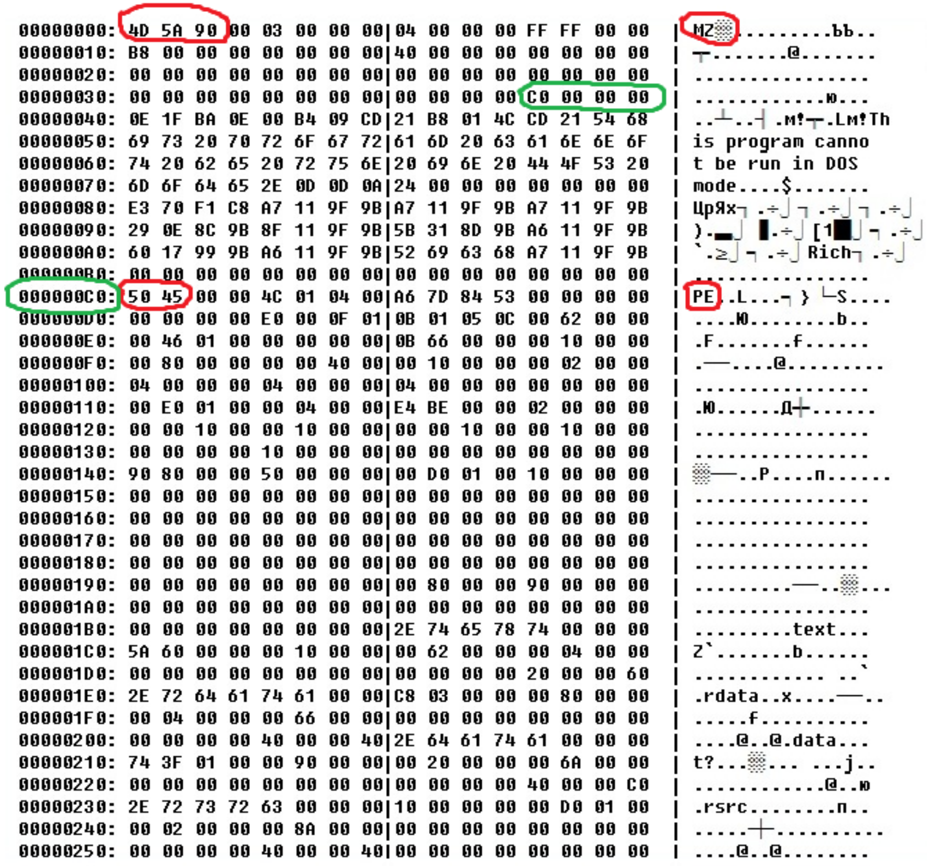
Offset

- Notepad.exe



```
00000000: 4D 5A 90 00 03 00 00 00|04 00 00 00 FF FF 00 00  | MZ░.........ЪЪ..
00000010: B8 00 00 00 00 00 00 00|40 00 00 00 00 00 00 00  | ┬.......@.......
00000020: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000030: 00 00 00 00 00 00 00 00|00 00 00 00 E0 00 00 00  | ............Ю...
00000040: 0E 1F BA 0E 00 B4 09 CD|21 B8 01 4C CD 21 54 68  | ..╨..┤.═!┬.L═!Th
00000050: 69 73 20 70 72 6F 67 72|61 6D 20 63 61 6E 6E 6F  | is program canno
00000060: 74 20 62 65 20 72 75 6E|20 69 6E 20 44 4F 53 20  | t be run in DOS 
00000070: 6D 6F 64 65 2E 0D 0D 0A|24 00 00 00 00 00 00 00  | mode....$.......
00000080: EC 85 5B A1 A8 E4 35 F2|A8 E4 35 F2 A8 E4 35 F2  | ьЕ[б╕д5Є╕д5Є╕д5Є
00000090: 6B EB 3A F2 A9 E4 35 F2|6B EB 55 F2 A9 E4 35 F2  | kы:Є╣д5ЄkыUЄ╣д5Є
000000A0: 6B EB 68 F2 BB E4 35 F2|A8 E4 34 F2 63 E4 35 F2  | kыhЄ╗д5Є╕д4Єcд5Є
000000B0: 6B EB 6B F2 A9 E4 35 F2|6B EB 6A F2 BF E4 35 F2  | kыkЄ╣д5ЄkыjЄ┐д5Є
000000C0: 6B EB 6F F2 A9 E4 35 F2|52 69 63 68 A8 E4 35 F2  | kыoЄ╣д5ЄRich╕д5Є
000000D0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
000000E0: 50 45 00 00 4C 01 03 00|87 52 02 48 00 00 00 00  | PE..L...ЗR.H....
000000F0: 00 00 00 00 E0 00 0F 01|0B 01 07 0A 00 78 00 00  | ....Ю........x..
00000100: 00 92 00 00 00 00 00 00|9D 73 00 00 00 10 00 00  | .Т......Эs......
00000110: 00 90 00 00 00 00 00 01|00 10 00 00 00 02 00 00  | .Р..............
00000120: 05 00 01 00 05 00 01 00|04 00 00 00 00 00 00 00  | ................
00000130: 00 40 01 00 00 04 00 00|09 E6 01 00 02 00 00 80  | .@.......ц.....А
00000140: 00 00 04 00 00 10 01 00|00 00 10 00 00 10 00 00  | ................
00000150: 00 00 00 00 10 00 00 00|00 00 00 00 00 00 00 00  | ................
00000160: 04 76 00 00 C8 00 00 00|00 B0 00 00 AC 89 00 00  | .v..╚....░..мЙ..
00000170: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000180: 00 00 00 00 00 00 00 00|50 13 00 00 1C 00 00 00  | ........P.......
00000190: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
000001A0: 00 00 00 00 00 00 00 00|A8 18 00 00 40 00 00 00  | ........╕...@...
000001B0: 50 02 00 00 D0 00 00 00|00 10 00 00 48 03 00 00  | P...╨.......H...
000001C0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
000001D0: 00 00 00 00 00 00 00 00|2E 74 65 78 74 00 00 00  | .........text...
000001E0: 48 77 00 00 00 10 00 00|00 78 00 00 00 04 00 00  | Hw.......x......
000001F0: 00 00 00 00 00 00 00 00|00 00 00 00 20 00 00 60  | ............ ..`
00000200: 2E 64 61 74 61 00 00 00|A8 1B 00 00 00 90 00 00  | .data...╕....Р..
00000210: 00 08 00 00 00 7C 00 00|00 00 00 00 00 00 00 00  | .....|..........
00000220: 00 00 00 00 40 00 00 C0|2E 72 73 72 63 00 00 00  | ....@..└.rsrc...
00000230: AC 89 00 00 00 B0 00 00|00 8A 00 00 00 84 00 00  | мЙ...░...К...Д..
00000240: 00 00 00 00 00 00 00 00|00 00 00 00 40 00 00 40  | ............@..@
00000250: B5 81 03 48 58 00 00 00|D7 81 03 48 65 00 00 00  | ╡Б.HX...╫Б.He...
```

Frodo.exe



```
00000000: 4D 5A 90 00 03 00 00 00|04 00 00 00 FF FF 00 00  | MZ░.........ЪЪ..
00000010: B8 00 00 00 00 00 00 00|40 00 00 00 00 00 00 00  | ┬.......@.......
00000020: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000030: 00 00 00 00 00 00 00 00|00 00 00 00 C0 00 00 00  | ............└...
00000040: 0E 1F BA 0E 00 B4 09 CD|21 B8 01 4C CD 21 54 68  | ..╨..┤.═!┬.L═!Th
00000050: 69 73 20 70 72 6F 67 72|61 6D 20 63 61 6E 6E 6F  | is program canno
00000060: 74 20 62 65 20 72 75 6E|20 69 6E 20 44 4F 53 20  | t be run in DOS 
00000070: 6D 6F 64 65 2E 0D 0D 0A|24 00 00 00 00 00 00 00  | mode....$.......
00000080: E3 70 F1 C8 A7 11 9F 9B|A7 11 9F 9B A7 11 9F 9B  | ЦрЯx╖.Я Ы╖.ЯЫ╖.ЯЫ
00000090: 29 0E 8C 9B 8F 11 9F 9B|5B 31 8D 9B A6 11 9F 9B  | ).МЫП.ЯЫ[1НЫж.ЯЫ
000000A0: 60 17 99 9B A6 11 9F 9B|52 69 63 68 A7 11 9F 9B  | `.ЩЫж.ЯЫRich╖.ЯЫ
000000B0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
000000C0: 50 45 00 00 4C 01 04 00|A6 7D 84 53 00 00 00 00  | PE..L...ж}ДS....
000000D0: 00 00 00 00 E0 00 0F 01|0B 01 05 0C 00 62 00 00  | ....Ю........b..
000000E0: 00 46 01 00 00 00 00 00|0B 66 00 00 00 10 00 00  | .F.......f......
000000F0: 00 80 00 00 00 00 40 00|00 10 00 00 00 02 00 00  | .А....@.........
00000100: 04 00 00 00 04 00 00 00|04 00 00 00 00 00 00 00  | ................
00000110: 00 E0 01 00 00 04 00 00|E4 BE 00 00 02 00 00 00  | .Ю......д╛......
00000120: 00 00 10 00 00 10 00 00|00 00 10 00 00 10 00 00  | ................
00000130: 00 00 00 00 10 00 00 00|00 00 00 00 00 00 00 00  | ................
00000140: 90 80 00 00 50 00 00 00|00 D0 01 00 10 00 00 00  | РА..P....╨......
00000150: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000160: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000170: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000180: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000190: 00 00 00 00 00 00 00 00|00 80 00 00 90 00 00 00  | .........А..Р...
000001A0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
000001B0: 00 00 00 00 00 00 00 00|2E 74 65 78 74 00 00 00  | .........text...
000001C0: 5A 60 00 00 00 10 00 00|00 62 00 00 00 04 00 00  | Z`.......b......
000001D0: 00 00 00 00 00 00 00 00|00 00 00 00 20 00 00 60  | ............ ..`
000001E0: 2E 72 64 61 74 61 00 00|C8 03 00 00 00 80 00 00  | .rdata..╚....А..
000001F0: 00 04 00 00 00 66 00 00|00 00 00 00 00 00 00 00  | .....f..........
00000200: 00 00 00 00 40 00 00 40|2E 64 61 74 61 00 00 00  | ....@..@.data...
00000210: 74 3F 01 00 00 90 00 00|00 20 00 00 00 6A 00 00  | t?...Р... ...j..
00000220: 00 00 00 00 00 00 00 00|00 00 00 00 40 00 00 C0  | ............@..└
00000230: 2E 72 73 72 63 00 00 00|10 00 00 00 00 D0 01 00  | .rsrc........╨..
00000240: 00 02 00 00 00 8A 00 00|00 00 00 00 00 00 00 00  | .....К..........
00000250: 00 00 00 00 40 00 00 40|00 00 00 00 00 00 00 00  | ....@..@........
```

Size

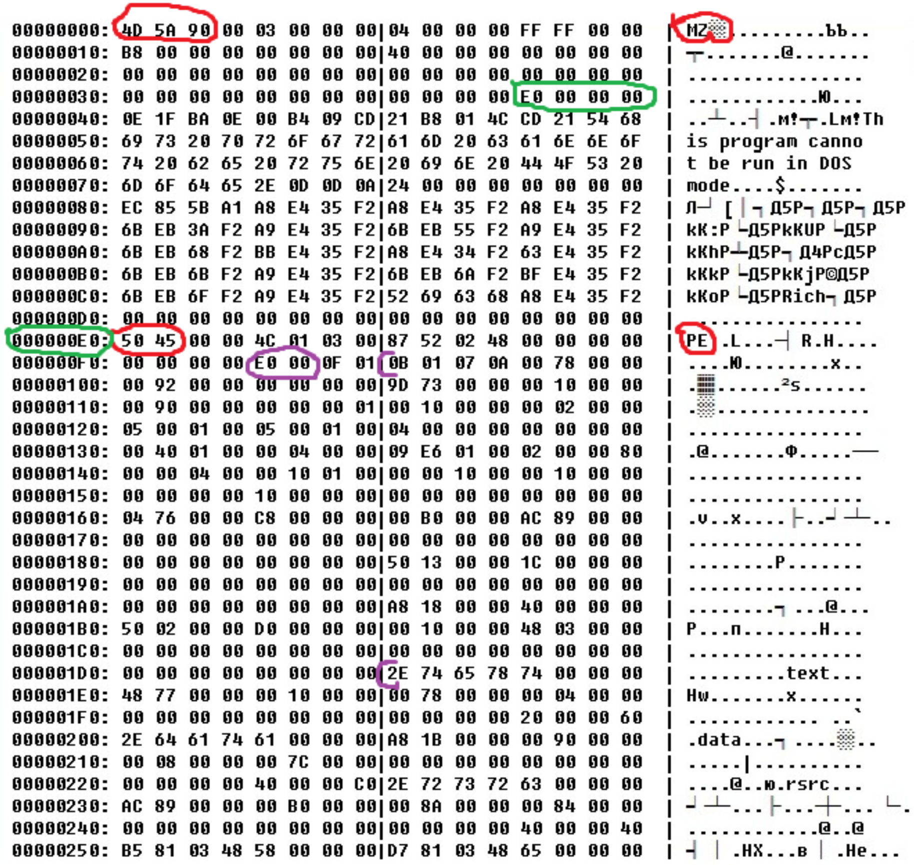
- Common:
- Size of metadata or data in data format

- Properties:
- Can’t be more then concerned block
- Measured in bytes

- Subtypes:
- Size of data
- Size of metadata
- Size of structure
- Size of field

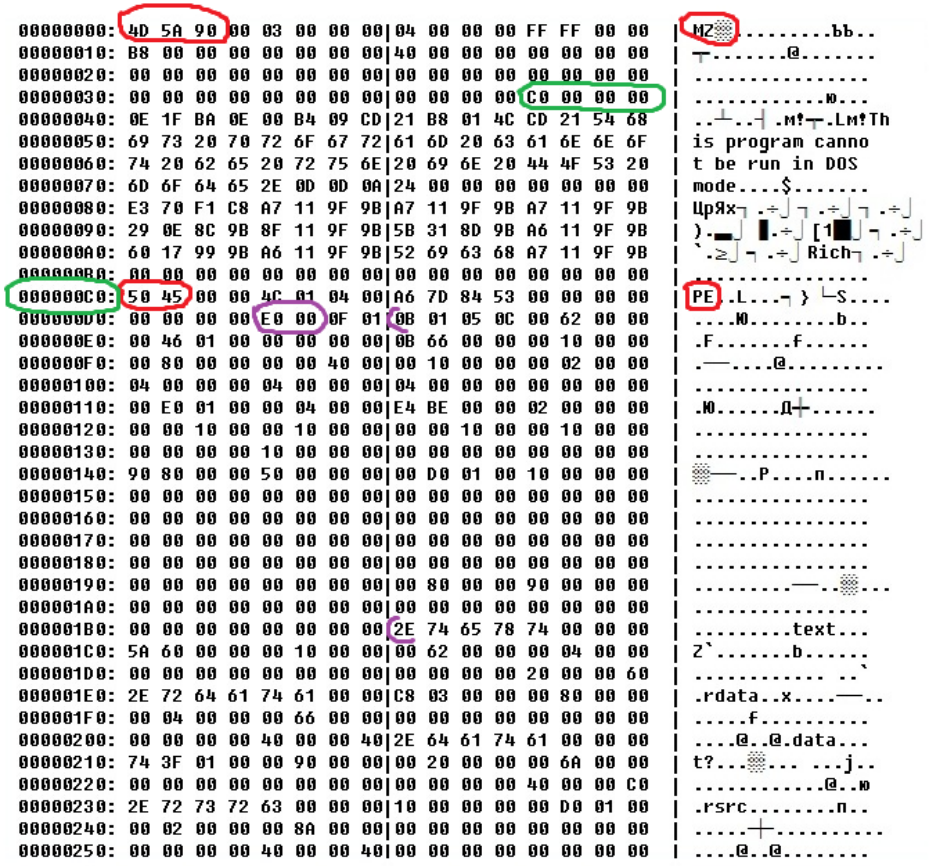
Size

- Notepad.exe



```
00000000: 4D 5A 90 00 03 00 00 00|04 00 00 00 FF FF 00 00  | MZ▒.........ьь..
00000010: B8 00 00 00 00 00 00 00|40 00 00 00 00 00 00 00  | ┬.......@.......
00000020: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000030: 00 00 00 00 00 00 00 00|00 00 00 00 E0 00 00 00  | ............Ю...
00000040: 0E 1F BA 0E 00 B4 09 CD|21 B8 01 4C CD 21 54 68  | ..┴..┤.═!┬.L═!Th
00000050: 69 73 20 70 72 6F 67 72|61 6D 20 63 61 6E 6E 6F  | is program canno
00000060: 74 20 62 65 20 72 75 6E|20 69 6E 20 44 4F 53 20  | t be run in DOS 
00000070: 6D 6F 64 65 2E 0D 0D 0A|24 00 00 00 00 00 00 00  | mode....$.......
00000080: EC 85 5B A1 A8 E4 35 F2|A8 E4 35 F2 A8 E4 35 F2  | л┘ [│┐Д5Р┐Д5Р┐Д5Р
00000090: 6B EB 3A F2 A9 E4 35 F2|6B EB 55 F2 A9 E4 35 F2  | kК:Р└Д5PkKUP└Д5P
000000A0: 6B EB 68 F2 BB E4 35 F2|A8 E4 34 F2 63 E4 35 F2  | kKhP┴Д5P┐Д4PcД5P
000000B0: 6B EB 6B F2 A9 E4 35 F2|6B EB 6A F2 BF E4 35 F2  | kKkP└Д5PkKjP©Д5P
000000C0: 6B EB 6F F2 A9 E4 35 F2|52 69 63 68 A8 E4 35 F2  | kKoP└Д5PRich┐Д5P
000000D0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
000000E0: 50 45 00 00 4C 01 03 00|87 52 02 48 00 00 00 00  | PE..L...┤R.H....
000000F0: 00 00 00 00 E0 00 0F 01|0B 01 07 0A 00 78 00 00  | ....Ю........x..
00000100: 00 92 00 00 00 00 00 00|9D 73 00 00 00 10 00 00  | .▓......²s......
00000110: 00 90 00 00 00 00 00 01|00 10 00 00 00 02 00 00  | .▒..............
00000120: 05 00 01 00 05 00 01 00|04 00 00 00 00 00 00 00  | ................
00000130: 00 40 01 00 00 04 00 00|09 E6 01 00 02 00 00 80  | .@.......Ф.....─
00000140: 00 00 04 00 00 10 01 00|00 00 10 00 00 10 00 00  | ................
00000150: 00 00 00 00 10 00 00 00|00 00 00 00 00 00 00 00  | ................
00000160: 04 76 00 00 C8 00 00 00|00 B0 00 00 AC 89 00 00  | .v..x....├..┘┴..
00000170: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000180: 00 00 00 00 00 00 00 00|50 13 00 00 1C 00 00 00  | ........P.......
00000190: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
000001A0: 00 00 00 00 00 00 00 00|A8 18 00 00 40 00 00 00  | ........┐...@...
000001B0: 50 02 00 00 D0 00 00 00|00 10 00 00 48 03 00 00  | P...п.......H...
000001C0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
000001D0: 00 00 00 00 00 00 00 00|2E 74 65 78 74 00 00 00  | .........text...
000001E0: 48 77 00 00 00 10 00 00|00 78 00 00 00 04 00 00  | Hw.......x......
000001F0: 00 00 00 00 00 00 00 00|00 00 00 00 20 00 00 60  | ............ ..`
00000200: 2E 64 61 74 61 00 00 00|A8 1B 00 00 00 90 00 00  | .data...┐....▒..
00000210: 00 08 00 00 00 7C 00 00|00 00 00 00 00 00 00 00  | .....|..........
00000220: 00 00 00 00 40 00 00 C0|2E 72 73 72 63 00 00 00  | ....@..ю.rsrc...
00000230: AC 89 00 00 00 B0 00 00|00 8A 00 00 00 84 00 00  | ┘┴...├...┼...└.
00000240: 00 00 00 00 00 00 00 00|00 00 00 00 40 00 00 40  | ............@..@
00000250: B5 81 03 48 58 00 00 00|D7 81 03 48 65 00 00 00  | ┤│.HX...в│.He...
```

Frodo.exe



```
00000000: 4D 5A 90 00 03 00 00 00|04 00 00 00 FF FF 00 00  | MZ▒.........ьь..
00000010: B8 00 00 00 00 00 00 00|40 00 00 00 00 00 00 00  | ┬.......@.......
00000020: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000030: 00 00 00 00 00 00 00 00|00 00 00 00 C0 00 00 00  | ............ю...
00000040: 0E 1F BA 0E 00 B4 09 CD|21 B8 01 4C CD 21 54 68  | ..┴..┤.═!┬.L═!Th
00000050: 69 73 20 70 72 6F 67 72|61 6D 20 63 61 6E 6E 6F  | is program canno
00000060: 74 20 62 65 20 72 75 6E|20 69 6E 20 44 4F 53 20  | t be run in DOS 
00000070: 6D 6F 64 65 2E 0D 0D 0A|24 00 00 00 00 00 00 00  | mode....$.......
00000080: E3 70 F1 C8 A7 11 9F 9B|A7 11 9F 9B A7 11 9F 9B  | ЦрЯx┐.÷┘┐.÷┘┐.÷┘
00000090: 29 0E 8C 9B 8F 11 9F 9B|5B 31 8D 9B A6 11 9F 9B  | ).▄┘▐.÷┘[1█┘┐.÷┘
000000A0: 60 17 99 9B A6 11 9F 9B|52 69 63 68 A7 11 9F 9B  | `.≥┘┐.÷┘Rich┐.÷┘
000000B0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
000000C0: 50 45 00 00 4C 01 04 00|A6 7D 84 53 00 00 00 00  | PE..L...┐}└S....
000000D0: 00 00 00 00 E0 00 0F 01|0B 01 05 0C 00 62 00 00  | ....Ю........b..
000000E0: 00 46 01 00 00 00 00 00|0B 66 00 00 00 10 00 00  | .F.......f......
000000F0: 00 80 00 00 00 00 40 00|00 10 00 00 00 02 00 00  | .─....@.........
00000100: 04 00 00 00 04 00 00 00|04 00 00 00 00 00 00 00  | ................
00000110: 00 E0 01 00 00 04 00 00|E4 BE 00 00 02 00 00 00  | .Ю......Д┼......
00000120: 00 00 10 00 00 10 00 00|00 00 10 00 00 10 00 00  | ................
00000130: 00 00 00 00 10 00 00 00|00 00 00 00 00 00 00 00  | ................
00000140: 90 80 00 00 50 00 00 00|00 D0 01 00 10 00 00 00  | ▒─..P....п......
00000150: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000160: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000170: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000180: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000190: 00 00 00 00 00 00 00 00|00 80 00 00 90 00 00 00  | .........─..▒...
000001A0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
000001B0: 00 00 00 00 00 00 00 00|2E 74 65 78 74 00 00 00  | .........text...
000001C0: 5A 60 00 00 00 10 00 00|00 62 00 00 00 04 00 00  | Z`.......b......
000001D0: 00 00 00 00 00 00 00 00|00 00 00 00 20 00 00 60  | ............ ..`
000001E0: 2E 72 64 61 74 61 00 00|C8 03 00 00 00 80 00 00  | .rdata..x....─..
000001F0: 00 04 00 00 00 66 00 00|00 00 00 00 00 00 00 00  | .....f..........
00000200: 00 00 00 00 40 00 00 40|2E 64 61 74 61 00 00 00  | ....@..@.data...
00000210: 74 3F 01 00 00 90 00 00|00 20 00 00 00 6A 00 00  | t?...▒... ...j..
00000220: 00 00 00 00 00 00 00 00|00 00 00 00 40 00 00 C0  | ............@..ю
00000230: 2E 72 73 72 63 00 00 00|10 00 00 00 00 D0 01 00  | .rsrc........п..
00000240: 00 02 00 00 00 8A 00 00|00 00 00 00 00 00 00 00  | .....┼..........
00000250: 00 00 00 00 40 00 00 40|00 00 00 00 00 00 00 00  | ....@..@........
```

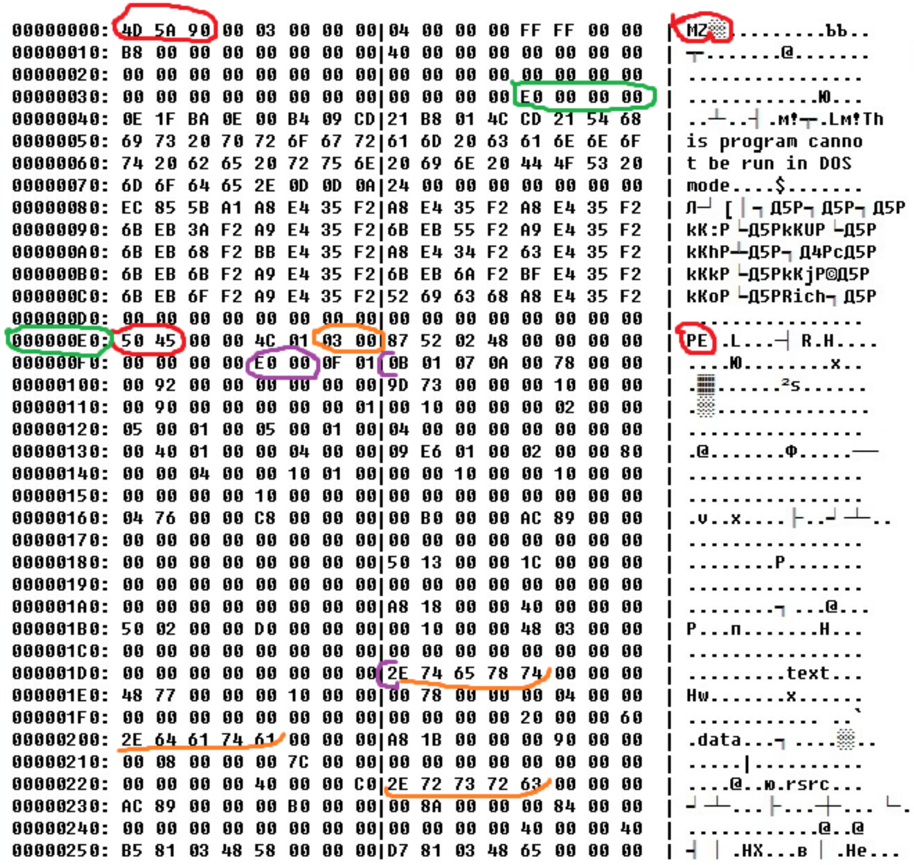
Quantity

- Properties:
- Quantity of structures of some type in data format
- Quantity can be concerned as size of same type elements array
- Elements size – more then 1 byte – word (2 byte), double word, paragraph (16 byte) and etc.
- Quantity multiplied by the size can’t be more then concerned block

- Subtypes:
- Quantity of same type structures
- Quantity of same type fields

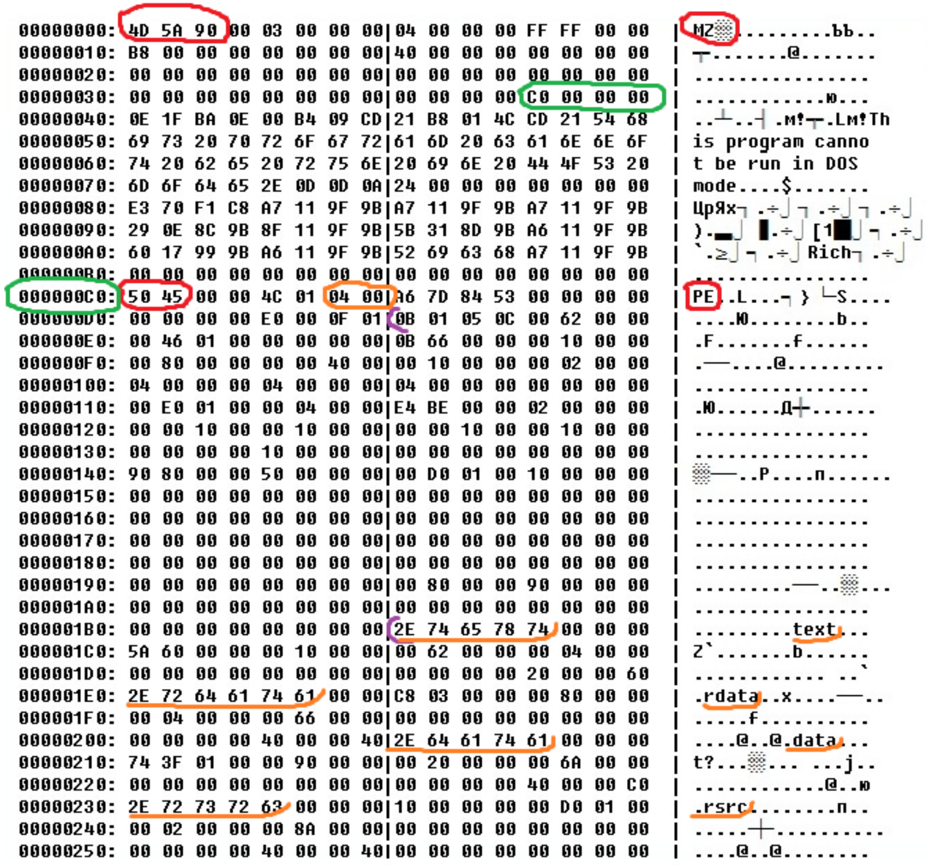
Quantity

- Notepad.exe



```
00000000: 4D 5A 90 00 03 00 00 00|04 00 00 00 FF FF 00 00  | MZ░.........bb..
00000010: B8 00 00 00 00 00 00 00|40 00 00 00 00 00 00 00  | ┬.......@.......
00000020: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000030: 00 00 00 00 00 00 00 00|00 00 00 00 E0 00 00 00  | ............Ю...
00000040: 0E 1F BA 0E 00 B4 09 CD|21 B8 01 4C CD 21 54 68  | ..┴..┤.═!╕.L═!Th
00000050: 69 73 20 70 72 6F 67 72|61 6D 20 63 61 6E 6E 6F  | is program canno
00000060: 74 20 62 65 20 72 75 6E|20 69 6E 20 44 4F 53 20  | t be run in DOS 
00000070: 6D 6F 64 65 2E 0D 0D 0A|24 00 00 00 00 00 00 00  | mode....$.......
00000080: EC 85 5B A1 A8 E4 35 F2|A8 E4 35 F2 A8 E4 35 F2  | Л┘[│┐Д5P┐Д5P┐Д5P
00000090: 6B EB 3A F2 A9 E4 35 F2|6B EB 55 F2 A9 E4 35 F2  | kK:P└Д5PkKUP└Д5P
000000A0: 6B EB 68 F2 BB E4 35 F2|A8 E4 34 F2 63 E4 35 F2  | kKhP╗Д5P┐Д4PcД5P
000000B0: 6B EB 6B F2 A9 E4 35 F2|6B EB 6A F2 BF E4 35 F2  | kKkP└Д5PkKjP©Д5P
000000C0: 6B EB 6F F2 A9 E4 35 F2|52 69 63 68 A8 E4 35 F2  | kKoP└Д5PRich┐Д5P
000000D0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
000000E0: 50 45 00 00 4C 01 03 00|87 52 02 48 00 00 00 00  | PE..L...┤R.H....
000000F0: 00 00 00 00 E0 00 0F 01|0B 01 07 0A 00 78 00 00  | ....Ю........x..
00000100: 00 92 00 00 00 00 00 00|9D 73 00 00 00 10 00 00  | .▓......²s......
00000110: 00 90 00 00 00 00 00 01|00 10 00 00 00 02 00 00  | .░..............
00000120: 05 00 01 00 05 00 01 00|04 00 00 00 00 00 00 00  | ................
00000130: 00 40 01 00 00 04 00 00|09 E6 01 00 02 00 00 80  | .@.......Ф.....─
00000140: 00 00 04 00 00 10 01 00|00 00 10 00 00 10 00 00  | ................
00000150: 00 00 00 00 10 00 00 00|00 00 00 00 00 00 00 00  | ................
00000160: 04 76 00 00 C8 00 00 00|00 B0 00 00 AC 89 00 00  | .v..x.....├..┘┴..
00000170: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000180: 00 00 00 00 00 00 00 00|50 13 00 00 1C 00 00 00  | ........P.......
00000190: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
000001A0: 00 00 00 00 00 00 00 00|A8 18 00 00 40 00 00 00  | ........┐...@...
000001B0: 50 02 00 00 D0 00 00 00|00 10 00 00 48 03 00 00  | P...п.......H...
000001C0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
000001D0: 00 00 00 00 00 00 00 00|2E 74 65 78 74 00 00 00  | .........text...
000001E0: 48 77 00 00 00 10 00 00|00 78 00 00 00 04 00 00  | Hw.......x......
000001F0: 00 00 00 00 00 00 00 00|00 00 00 00 20 00 00 60  | ............ ..`
00000200: 2E 64 61 74 61 00 00 00|A8 1B 00 00 00 90 00 00  | .data...┐....░..
00000210: 00 08 00 00 00 7C 00 00|00 00 00 00 00 00 00 00  | .....|..........
00000220: 00 00 00 00 40 00 00 C0|2E 72 73 72 63 00 00 00  | ....@..ю.rsrc...
00000230: AC 89 00 00 00 B0 00 00|00 8A 00 00 00 84 00 00  | ┘┴...├...┼...└.
00000240: 00 00 00 00 00 00 00 00|00 00 00 00 40 00 00 40  | ............@..@
00000250: B5 81 03 48 58 00 00 00|D7 81 03 48 65 00 00 00  | ┤│.HX...в│.He...
```

Frodo.exe



```
00000000: 4D 5A 90 00 03 00 00 00|04 00 00 00 FF FF 00 00  | MZ░.........bb..
00000010: B8 00 00 00 00 00 00 00|40 00 00 00 00 00 00 00  | ┬.......@.......
00000020: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000030: 00 00 00 00 00 00 00 00|00 00 00 00 C0 00 00 00  | ............ю...
00000040: 0E 1F BA 0E 00 B4 09 CD|21 B8 01 4C CD 21 54 68  | ..┴..┤.═!╕.L═!Th
00000050: 69 73 20 70 72 6F 67 72|61 6D 20 63 61 6E 6E 6F  | is program canno
00000060: 74 20 62 65 20 72 75 6E|20 69 6E 20 44 4F 53 20  | t be run in DOS 
00000070: 6D 6F 64 65 2E 0D 0D 0A|24 00 00 00 00 00 00 00  | mode....$.......
00000080: E3 70 F1 C8 A7 11 9F 9B|A7 11 9F 9B A7 11 9F 9B  | ЦpЯx┐.÷┘┐.÷┘┐.÷┘
00000090: 29 0E 8C 9B 8F 11 9F 9B|5B 31 8D 9B A6 11 9F 9B  | ).▄┘▌.÷┘[1█┘┐.÷┘
000000A0: 60 17 99 9B A6 11 9F 9B|52 69 63 68 A7 11 9F 9B  | `.≥┘┐.÷┘Rich┐.÷┘
000000B0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
000000C0: 50 45 00 00 4C 01 04 00|A6 7D 84 53 00 00 00 00  | PE..L...┐}└S....
000000D0: 00 00 00 00 E0 00 0F 01|0B 01 05 0C 00 62 00 00  | ....Ю........b..
000000E0: 00 46 01 00 00 00 00 00|0B 66 00 00 00 10 00 00  | .F.......f......
000000F0: 00 80 00 00 00 00 40 00|00 10 00 00 00 02 00 00  | .─.....@........
00000100: 04 00 00 00 04 00 00 00|04 00 00 00 00 00 00 00  | ................
00000110: 00 E0 01 00 00 04 00 00|E4 BE 00 00 02 00 00 00  | .Ю......Д┼......
00000120: 00 00 10 00 00 10 00 00|00 00 10 00 00 10 00 00  | ................
00000130: 00 00 00 00 10 00 00 00|00 00 00 00 00 00 00 00  | ................
00000140: 90 80 00 00 50 00 00 00|00 D0 01 00 10 00 00 00  | ░─..P....п......
00000150: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000160: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000170: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000180: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000190: 00 00 00 00 00 00 00 00|00 80 00 00 90 00 00 00  | .........─..░...
000001A0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
000001B0: 00 00 00 00 00 00 00 00|2E 74 65 78 74 00 00 00  | .........text...
000001C0: 5A 60 00 00 00 10 00 00|00 62 00 00 00 04 00 00  | Z`.......b......
000001D0: 00 00 00 00 00 00 00 00|00 00 00 00 20 00 00 60  | ............ ..`
000001E0: 2E 72 64 61 74 61 00 00|C8 03 00 00 00 80 00 00  | .rdata..x....─..
000001F0: 00 04 00 00 00 66 00 00|00 00 00 00 00 00 00 00  | .....f..........
00000200: 00 00 00 00 40 00 00 40|2E 64 61 74 61 00 00 00  | ....@..@.data...
00000210: 74 3F 01 00 00 90 00 00|00 20 00 00 00 6A 00 00  | t?...░... ...j..
00000220: 00 00 00 00 00 00 00 00|00 00 00 00 40 00 00 C0  | ............@..ю
00000230: 2E 72 73 72 63 00 00 00|10 00 00 00 00 D0 01 00  | .rsrc........п..
00000240: 00 02 00 00 00 8A 00 00|00 00 00 00 00 00 00 00  | .....┼..........
00000250: 00 00 00 00 40 00 00 40|00 00 00 00 00 00 00 00  | ....@..@........
```

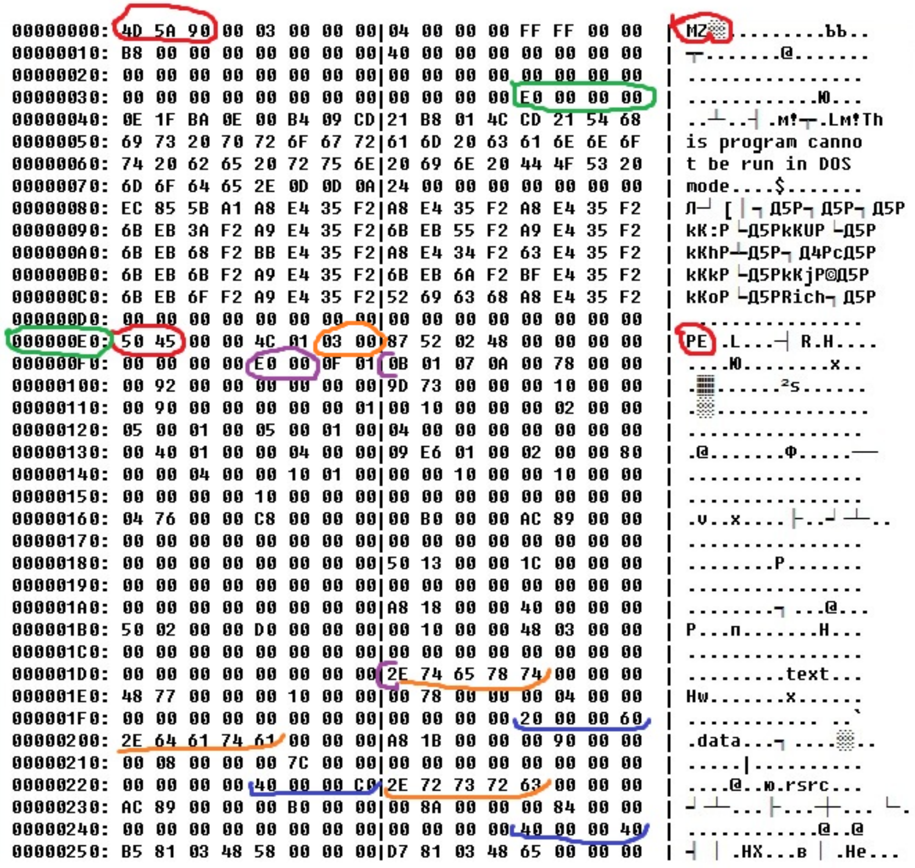
Flag

- Properties:
- Usually this field – combination of bit values
- Data range of this field nave limited values

- Subtypes:
- Bit Flag
- Enum value flag
- Bool value flag

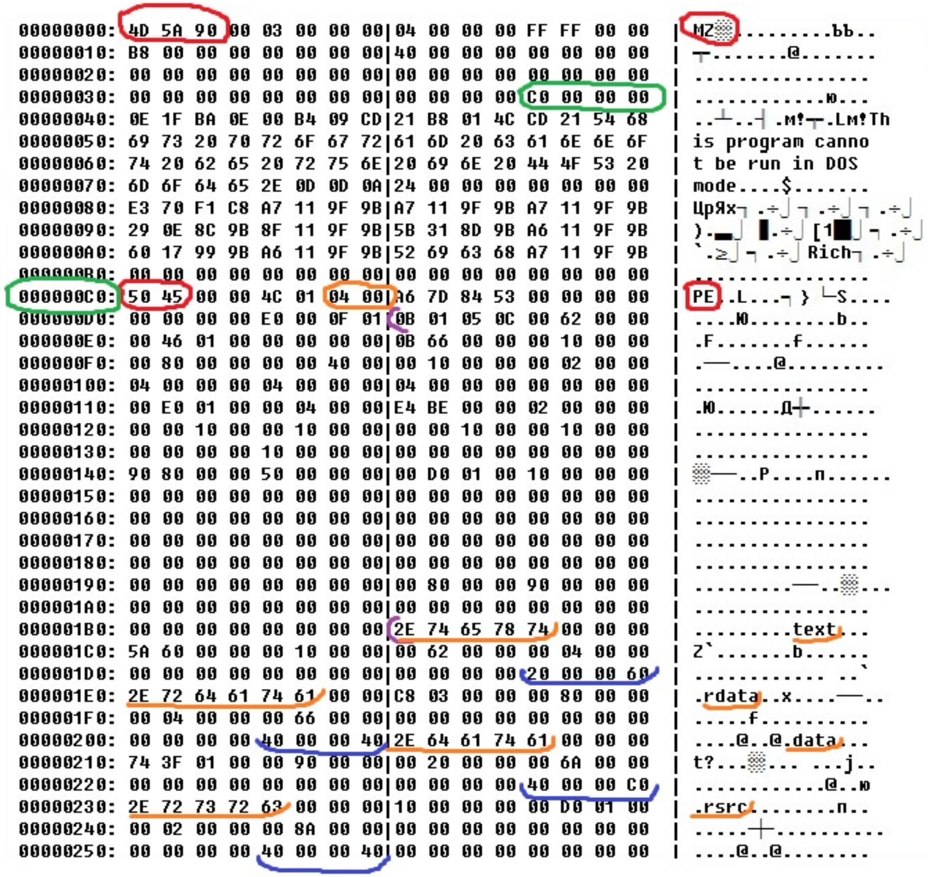
Flag

- Notepad.exe



```
00000000: 4D 5A 90 00 03 00 00 00|04 00 00 00 FF FF 00 00  | MZ░.........ьь..
00000010: B8 00 00 00 00 00 00 00|40 00 00 00 00 00 00 00  | ┬.......@.......
00000020: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000030: 00 00 00 00 00 00 00 00|00 00 00 00 E0 00 00 00  | ............Ю...
00000040: 0E 1F BA 0E 00 B4 09 CD|21 B8 01 4C CD 21 54 68  | ..┴..┤.м!┬.Lм!Th
00000050: 69 73 20 70 72 6F 67 72|61 6D 20 63 61 6E 6E 6F  | is program canno
00000060: 74 20 62 65 20 72 75 6E|20 69 6E 20 44 4F 53 20  | t be run in DOS
00000070: 6D 6F 64 65 2E 0D 0D 0A|24 00 00 00 00 00 00 00  | mode....$.......
00000080: EC 85 5B A1 A8 E4 35 F2|A8 E4 35 F2 A8 E4 35 F2  | л┘ [│┐Д5P┐Д5P┐Д5P
00000090: 6B EB 3A F2 A9 E4 35 F2|6B EB 55 F2 A9 E4 35 F2  | kK:P └Д5PkKUP └Д5P
000000A0: 6B EB 68 F2 BB E4 35 F2|A8 E4 34 F2 63 E4 35 F2  | kKhP┴Д5P┐Д4PcД5P
000000B0: 6B EB 6B F2 A9 E4 35 F2|6B EB 6A F2 BF E4 35 F2  | kKkP └Д5PkKjP©Д5P
000000C0: 6B EB 6F F2 A9 E4 35 F2|52 69 63 68 A8 E4 35 F2  | kKoP └Д5PRich┐Д5P
000000D0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
000000E0: 50 45 00 00 4C 01 03 00|87 52 02 48 00 00 00 00  | PE..L...┤ R.H....
000000F0: 00 00 00 00 E0 00 0F 01|0B 01 07 0A 00 78 00 00  | ....Ю.........x..
00000100: 00 92 00 00 00 00 00 00|9D 73 00 00 00 10 00 00  | .▓......²s......
00000110: 00 90 00 00 00 00 00 01|00 10 00 00 00 02 00 00  | .░..............
00000120: 05 00 01 00 05 00 01 00|04 00 00 00 00 00 00 00  | ................
00000130: 00 40 01 00 00 04 00 00|09 E6 01 00 02 00 00 80  | .@.......Ф.....─
00000140: 00 00 04 00 00 10 01 00|00 00 10 00 00 10 00 00  | ................
00000150: 00 00 00 00 10 00 00 00|00 00 00 00 00 00 00 00  | ................
00000160: 04 76 00 00 C8 00 00 00|00 B0 00 00 AC 89 00 00  | .v..x....├..┘┴..
00000170: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000180: 00 00 00 00 00 00 00 00|50 13 00 00 1C 00 00 00  | ........P.......
00000190: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
000001A0: 00 00 00 00 00 00 00 00|A8 18 00 00 40 00 00 00  | ........┐...@...
000001B0: 50 02 00 00 D0 00 00 00|00 10 00 00 48 03 00 00  | P...п.......H...
000001C0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
000001D0: 00 00 00 00 00 00 00 00|2E 74 65 78 74 00 00 00  | .........text...
000001E0: 48 77 00 00 00 10 00 00|00 78 00 00 00 04 00 00  | Hw.......x......
000001F0: 00 00 00 00 00 00 00 00|00 00 00 00 20 00 00 60  | ............ ..`
00000200: 2E 64 61 74 61 00 00 00|A8 1B 00 00 00 90 00 00  | .data...┐....░..
00000210: 00 08 00 00 00 7C 00 00|00 00 00 00 00 00 00 00  | .....|..........
00000220: 00 00 00 00 40 00 00 C0|2E 72 73 72 63 00 00 00  | ....@..ю.rsrc...
00000230: AC 89 00 00 00 B0 00 00|00 8A 00 00 00 84 00 00  | ┘┴...├...┼... └.
00000240: 00 00 00 00 00 00 00 00|00 00 00 00 40 00 00 40  | ............@..@
00000250: B5 81 03 48 58 00 00 00|D7 81 03 48 65 00 00 00  | ┤│.HX...в│.He...
```

Frodo.exe



```
00000000: 4D 5A 90 00 03 00 00 00|04 00 00 00 FF FF 00 00  | MZ░.........ьь..
00000010: B8 00 00 00 00 00 00 00|40 00 00 00 00 00 00 00  | ┬.......@.......
00000020: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000030: 00 00 00 00 00 00 00 00|00 00 00 00 C0 00 00 00  | ............ю...
00000040: 0E 1F BA 0E 00 B4 09 CD|21 B8 01 4C CD 21 54 68  | ..┴..┤.м!┬.Lм!Th
00000050: 69 73 20 70 72 6F 67 72|61 6D 20 63 61 6E 6E 6F  | is program canno
00000060: 74 20 62 65 20 72 75 6E|20 69 6E 20 44 4F 53 20  | t be run in DOS
00000070: 6D 6F 64 65 2E 0D 0D 0A|24 00 00 00 00 00 00 00  | mode....$.......
00000080: E3 70 F1 C8 A7 11 9F 9B|A7 11 9F 9B A7 11 9F 9B  | ЦрЯx┐.÷┘┐.÷┘┐.÷┘
00000090: 29 0E 8C 9B 8F 11 9F 9B|5B 31 8D 9B A6 11 9F 9B  | ).▄┘ ▌.÷┘[1█┘┐.÷┘
000000A0: 60 17 99 9B A6 11 9F 9B|52 69 63 68 A7 11 9F 9B  | `.≥┘┐.÷┘Rich┐.÷┘
000000B0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
000000C0: 50 45 00 00 4C 01 04 00|A6 7D 84 53 00 00 00 00  | PE..L...┐}└S....
000000D0: 00 00 00 00 E0 00 0F 01|0B 01 05 0C 00 62 00 00  | ....Ю.........b..
000000E0: 00 46 01 00 00 00 00 00|0B 66 00 00 00 10 00 00  | .F.......f......
000000F0: 00 80 00 00 00 00 40 00|00 10 00 00 00 02 00 00  | .─....@.........
00000100: 04 00 00 00 04 00 00 00|04 00 00 00 00 00 00 00  | ................
00000110: 00 E0 01 00 00 04 00 00|E4 BE 00 00 02 00 00 00  | .Ю......Д┼......
00000120: 00 00 10 00 00 10 00 00|00 00 10 00 00 10 00 00  | ................
00000130: 00 00 00 00 10 00 00 00|00 00 00 00 00 00 00 00  | ................
00000140: 90 80 00 00 50 00 00 00|00 D0 01 00 10 00 00 00  | ░─..P....п......
00000150: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000160: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000170: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000180: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000190: 00 00 00 00 00 00 00 00|00 80 00 00 90 00 00 00  | .........─..░...
000001A0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
000001B0: 00 00 00 00 00 00 00 00|2E 74 65 78 74 00 00 00  | .........text...
000001C0: 5A 60 00 00 00 10 00 00|00 62 00 00 00 04 00 00  | Z`.......b......
000001D0: 00 00 00 00 00 00 00 00|00 00 00 00 20 00 00 60  | ............ ..`
000001E0: 2E 72 64 61 74 61 00 00|C8 03 00 00 00 80 00 00  | .rdata..x....─..
000001F0: 00 04 00 00 00 66 00 00|00 00 00 00 00 00 00 00  | .....f..........
00000200: 00 00 00 00 40 00 00 40|2E 64 61 74 61 00 00 00  | ....@..@.data...
00000210: 74 3F 01 00 00 90 00 00|00 20 00 00 00 6A 00 00  | t?...░... ...j..
00000220: 00 00 00 00 00 00 00 00|00 00 00 00 40 00 00 C0  | ............@..ю
00000230: 2E 72 73 72 63 00 00 00|10 00 00 00 00 D0 01 00  | .rsrc........п..
00000240: 00 02 00 00 00 8A 00 00|00 00 00 00 00 00 00 00  | .....┼..........
00000250: 00 00 00 00 40 00 00 40|00 00 00 00 00 00 00 00  | ....@..@........
```

Counter

- Properties:
- Sequence number of the packet in the protocol communication, or sequence number of the frame in multimedia format
- Usually counter is incremented by 1

- Subtypes:
- Incremented counter
- Decremented counter
- Starts with 0
- Begins with another value
- Changes by 1
- Changes by another value

Common fields

- Time
- Date
- Protect

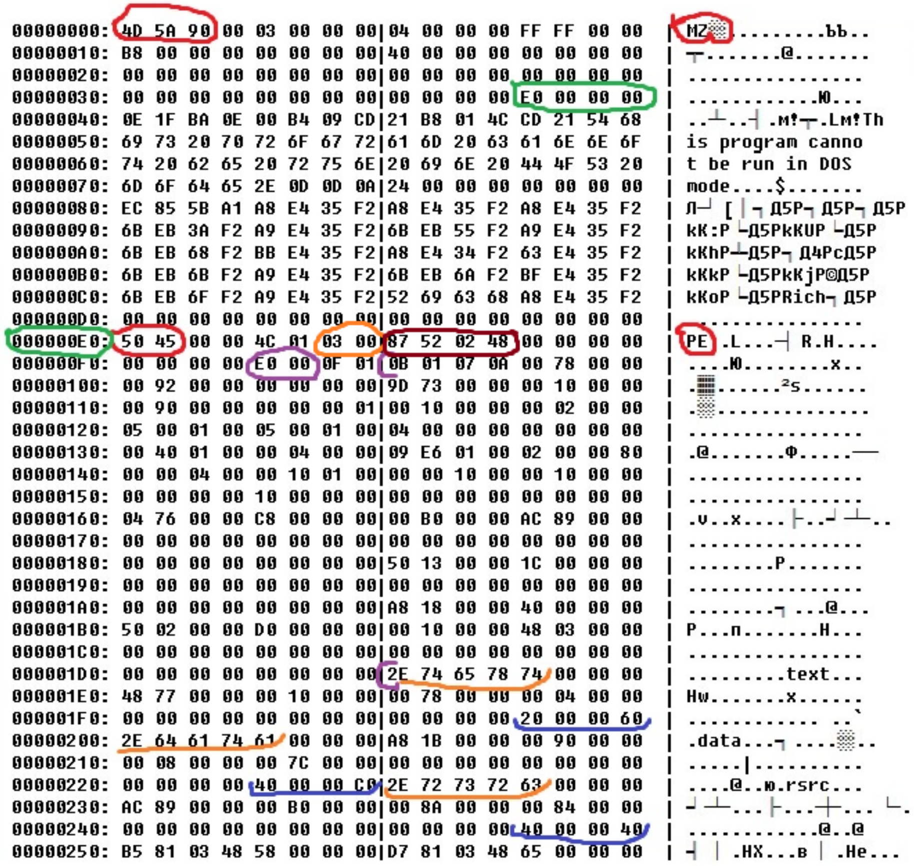
- Etc.

Time and Date

- Storing format
- Resolution
- Moment of beginning
- Range

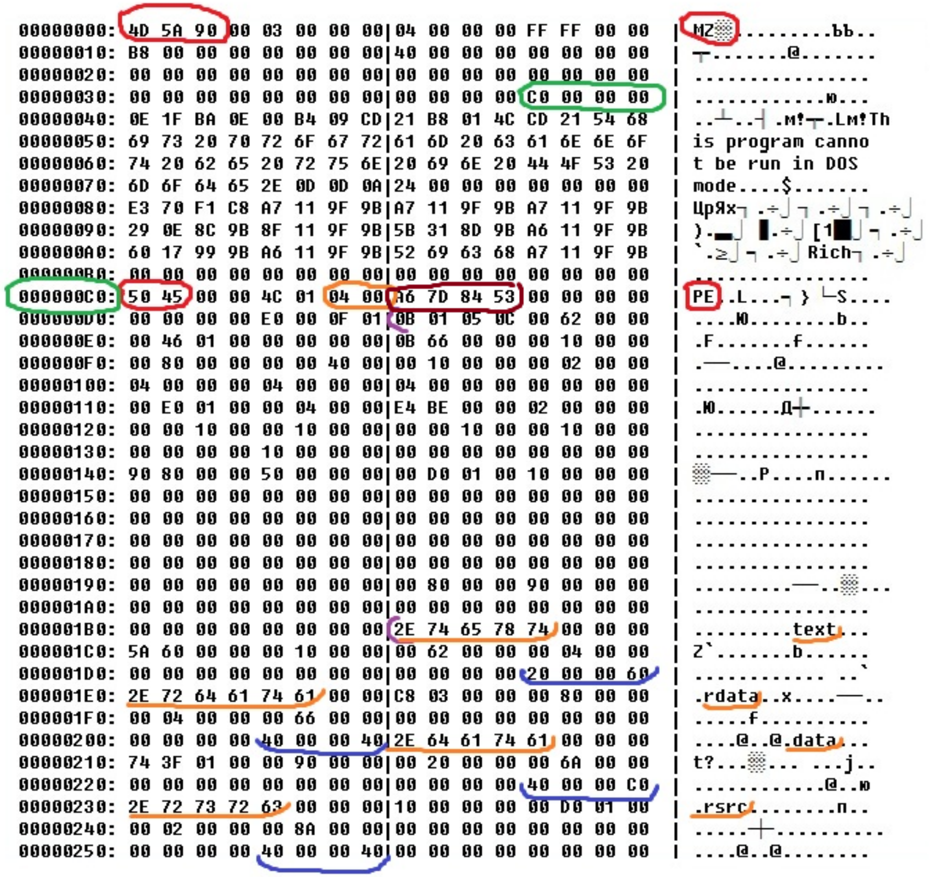
Time and Date

- Notepad.exe



```
00000000: 4D 5A 90 00 03 00 00 00|04 00 00 00 FF FF 00 00  | MZ░.........bb..
00000010: B8 00 00 00 00 00 00 00|40 00 00 00 00 00 00 00  | ┬.......@.......
00000020: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000030: 00 00 00 00 00 00 00 00|00 00 00 00 E0 00 00 00  | ............Ю...
00000040: 0E 1F BA 0E 00 B4 09 CD|21 B8 01 4C CD 21 54 68  | ..┴..┤.м!┬.Lм!Th
00000050: 69 73 20 70 72 6F 67 72|61 6D 20 63 61 6E 6E 6F  | is program canno
00000060: 74 20 62 65 20 72 75 6E|20 69 6E 20 44 4F 53 20  | t be run in DOS 
00000070: 6D 6F 64 65 2E 0D 0D 0A|24 00 00 00 00 00 00 00  | mode....$.......
00000080: EC 85 5B A1 A8 E4 35 F2|A8 E4 35 F2 A8 E4 35 F2  | лЕ[б┐ф5Є┐ф5Є┐ф5Є
00000090: 6B EB 3A F2 A9 E4 35 F2|6B EB 55 F2 A9 E4 35 F2  | kK:P└Д5PkKUP└Д5P
000000A0: 6B EB 68 F2 BB E4 35 F2|A8 E4 34 F2 63 E4 35 F2  | kKhP┴Д5P┐Д4PcД5P
000000B0: 6B EB 6B F2 A9 E4 35 F2|6B EB 6A F2 BF E4 35 F2  | kKkP└Д5PkKjP©Д5P
000000C0: 6B EB 6F F2 A9 E4 35 F2|52 69 63 68 A8 E4 35 F2  | kKoP└Д5PRich┐Д5P
000000D0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
000000E0: 50 45 00 00 4C 01 03 00|87 52 02 48 00 00 00 00  | PE..L...┤R.H....
000000F0: 00 00 00 00 E0 00 0F 01|0B 01 07 0A 00 78 00 00  | ....Ю........x..
00000100: 00 92 00 00 00 00 00 00|9D 73 00 00 00 10 00 00  | .▓......²s......
00000110: 00 90 00 00 00 00 00 01|00 10 00 00 00 02 00 00  | .░..............
00000120: 05 00 01 00 05 00 01 00|04 00 00 00 00 00 00 00  | ................
00000130: 00 40 01 00 00 04 00 00|09 E6 01 00 02 00 00 80  | .@.......Ф.....─
00000140: 00 00 04 00 00 10 01 00|00 00 10 00 00 10 00 00  | ................
00000150: 00 00 00 00 10 00 00 00|00 00 00 00 00 00 00 00  | ................
00000160: 04 76 00 00 C8 00 00 00|00 B0 00 00 AC 89 00 00  | .v..x....├..┘┴..
00000170: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000180: 00 00 00 00 00 00 00 00|50 13 00 00 1C 00 00 00  | ........P.......
00000190: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
000001A0: 00 00 00 00 00 00 00 00|A8 18 00 00 40 00 00 00  | ........┐...@...
000001B0: 50 02 00 00 D0 00 00 00|00 10 00 00 48 03 00 00  | P...п.......H...
000001C0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
000001D0: 00 00 00 00 00 00 00 00|2E 74 65 78 74 00 00 00  | .........text...
000001E0: 48 77 00 00 00 10 00 00|00 78 00 00 00 04 00 00  | Hw.......x......
000001F0: 00 00 00 00 00 00 00 00|00 00 00 00 20 00 00 60  | ............ ..`
00000200: 2E 64 61 74 61 00 00 00|A8 1B 00 00 00 90 00 00  | .data...┐....░..
00000210: 00 08 00 00 00 7C 00 00|00 00 00 00 00 00 00 00  | .....|..........
00000220: 00 00 00 00 40 00 00 C0|2E 72 73 72 63 00 00 00  | ....@..ю.rsrc...
00000230: AC 89 00 00 00 B0 00 00|00 8A 00 00 00 84 00 00  | ┘┴...├...┼...└.
00000240: 00 00 00 00 00 00 00 00|00 00 00 00 40 00 00 40  | ............@..@
00000250: B5 81 03 48 58 00 00 00|D7 81 03 48 65 00 00 00  | ┤│.HX...в│.He...
```

Frodo.exe



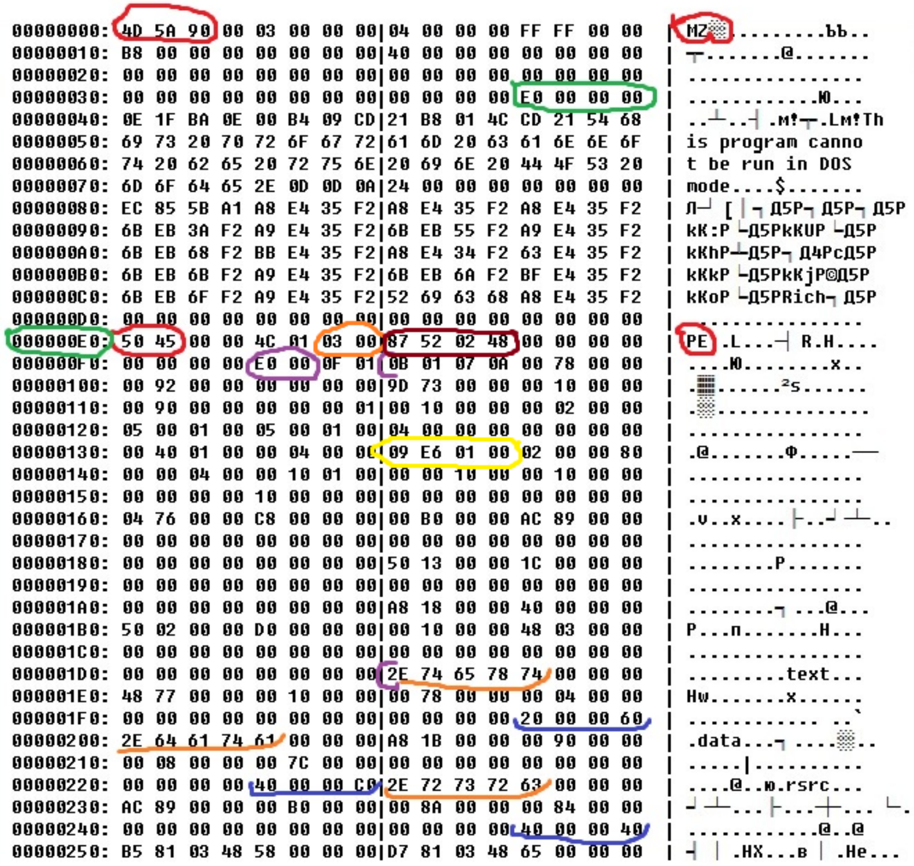
```
00000000: 4D 5A 90 00 03 00 00 00|04 00 00 00 FF FF 00 00  | MZ░.........bb..
00000010: B8 00 00 00 00 00 00 00|40 00 00 00 00 00 00 00  | ┬.......@.......
00000020: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000030: 00 00 00 00 00 00 00 00|00 00 00 00 C0 00 00 00  | ............ю...
00000040: 0E 1F BA 0E 00 B4 09 CD|21 B8 01 4C CD 21 54 68  | ..┴..┤.м!┬.Lм!Th
00000050: 69 73 20 70 72 6F 67 72|61 6D 20 63 61 6E 6E 6F  | is program canno
00000060: 74 20 62 65 20 72 75 6E|20 69 6E 20 44 4F 53 20  | t be run in DOS 
00000070: 6D 6F 64 65 2E 0D 0D 0A|24 00 00 00 00 00 00 00  | mode....$.......
00000080: E3 70 F1 C8 A7 11 9F 9B|A7 11 9F 9B A7 11 9F 9B  | ЦрЯх┐.÷┘┐.÷┘┐.÷┘
00000090: 29 0E 8C 9B 8F 11 9F 9B|5B 31 8D 9B A6 11 9F 9B  | ).▄┘▌.÷┘[1█┘┐.÷┘
000000A0: 60 17 99 9B A6 11 9F 9B|52 69 63 68 A7 11 9F 9B  | `.≥┘┐.÷┘Rich┐.÷┘
000000B0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
000000C0: 50 45 00 00 4C 01 04 00|A6 7D 84 53 00 00 00 00  | PE..L...┐}└S....
000000D0: 00 00 00 00 E0 00 0F 01|0B 01 05 0C 00 62 00 00  | ....Ю........b..
000000E0: 00 46 01 00 00 00 00 00|0B 66 00 00 00 10 00 00  | .F.......f......
000000F0: 00 80 00 00 00 00 40 00|00 10 00 00 00 02 00 00  | .─....@.........
00000100: 04 00 00 00 04 00 00 00|04 00 00 00 00 00 00 00  | ................
00000110: 00 E0 01 00 00 04 00 00|E4 BE 00 00 02 00 00 00  | .Ю......Д┼......
00000120: 00 00 10 00 00 10 00 00|00 00 10 00 00 10 00 00  | ................
00000130: 00 00 00 00 10 00 00 00|00 00 00 00 00 00 00 00  | ................
00000140: 90 80 00 00 50 00 00 00|00 D0 01 00 10 00 00 00  | ░─..P....п......
00000150: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000160: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000170: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000180: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000190: 00 00 00 00 00 00 00 00|00 80 00 00 90 00 00 00  | .........─..░...
000001A0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
000001B0: 00 00 00 00 00 00 00 00|2E 74 65 78 74 00 00 00  | .........text...
000001C0: 5A 60 00 00 00 10 00 00|00 62 00 00 00 04 00 00  | Z`.......b......
000001D0: 00 00 00 00 00 00 00 00|00 00 00 00 20 00 00 60  | ............ ..`
000001E0: 2E 72 64 61 74 61 00 00|C8 03 00 00 00 80 00 00  | .rdata..x....─..
000001F0: 00 04 00 00 00 66 00 00|00 00 00 00 00 00 00 00  | .....f..........
00000200: 00 00 00 00 40 00 00 40|2E 64 61 74 61 00 00 00  | ....@..@.data...
00000210: 74 3F 01 00 00 90 00 00|00 20 00 00 00 6A 00 00  | t?...░... ...j..
00000220: 00 00 00 00 00 00 00 00|00 00 00 00 40 00 00 C0  | ............@..ю
00000230: 2E 72 73 72 63 00 00 00|10 00 00 00 00 D0 01 00  | .rsrc........п..
00000240: 00 02 00 00 00 8A 00 00|00 00 00 00 00 00 00 00  | .....┼..........
00000250: 00 00 00 00 40 00 00 40|00 00 00 00 00 00 00 00  | ....@..@........
```

Protect

- CRC value of whole block
- CRC value of data
- CRC value of metadata
- CRC value of structure
- Various Hash functions and etc.

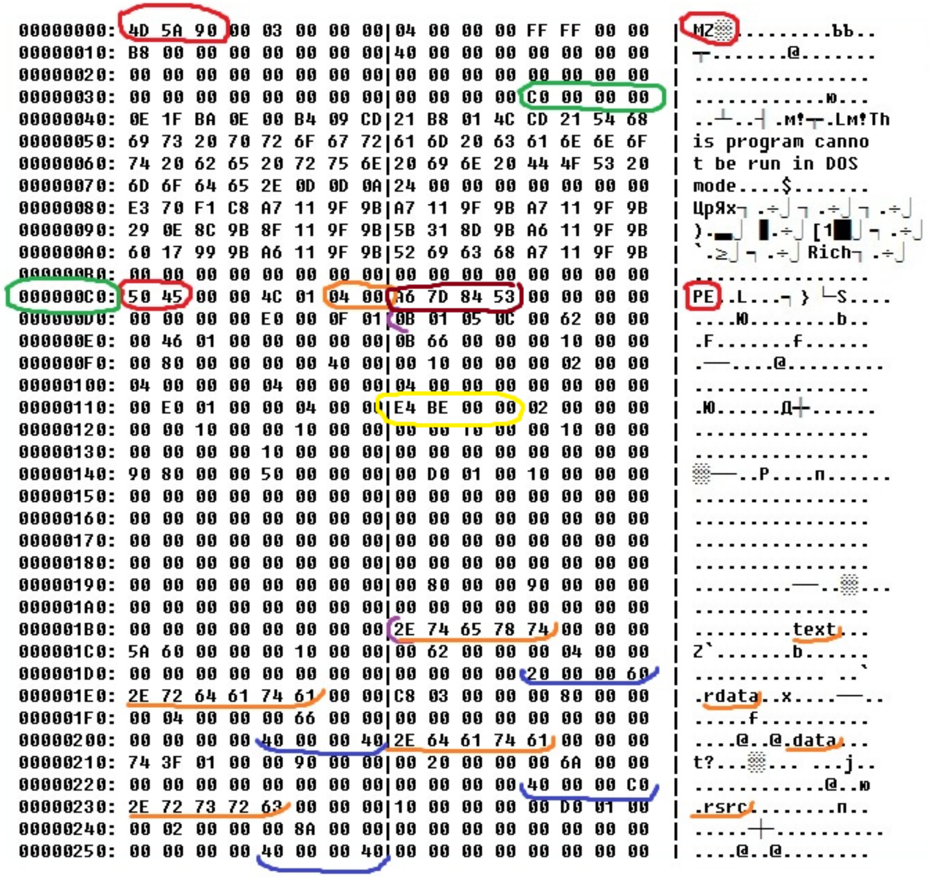
Protect

- Notepad.exe



```
00000000: 4D 5A 90 00 03 00 00 00|04 00 00 00 FF FF 00 00  | MZ░.........ьь..
00000010: B8 00 00 00 00 00 00 00|40 00 00 00 00 00 00 00  | ┬.......@.......
00000020: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000030: 00 00 00 00 00 00 00 00|00 00 00 00 E0 00 00 00  | ............ю...
00000040: 0E 1F BA 0E 00 B4 09 CD|21 B8 01 4C CD 21 54 68  | ..╨..┤.═!╕.L═!Th
00000050: 69 73 20 70 72 6F 67 72|61 6D 20 63 61 6E 6E 6F  | is program canno
00000060: 74 20 62 65 20 72 75 6E|20 69 6E 20 44 4F 53 20  | t be run in DOS 
00000070: 6D 6F 64 65 2E 0D 0D 0A|24 00 00 00 00 00 00 00  | mode....$.......
00000080: EC 85 5B A1 A8 E4 35 F2|A8 E4 35 F2 A8 E4 35 F2  | ьЕ[б╕ф5Є╕ф5Є╕ф5Є
00000090: 6B EB 3A F2 A9 E4 35 F2|6B EB 55 F2 A9 E4 35 F2  | kы:Є╣ф5ЄkыUЄ╣ф5Є
000000A0: 6B EB 68 F2 BB E4 35 F2|A8 E4 34 F2 63 E4 35 F2  | kыhЄ╗ф5Є╕ф4Єcф5Є
000000B0: 6B EB 6B F2 A9 E4 35 F2|6B EB 6A F2 BF E4 35 F2  | kыkЄ╣ф5ЄkыjЄ┐ф5Є
000000C0: 6B EB 6F F2 A9 E4 35 F2|52 69 63 68 A8 E4 35 F2  | kыoЄ╣ф5ЄRich╕ф5Є
000000D0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
000000E0: 50 45 00 00 4C 01 03 00|87 52 02 48 00 00 00 00  | PE..L...ЗR.H....
000000F0: 00 00 00 00 E0 00 0F 01|0B 01 07 0A 00 78 00 00  | ....ю........x..
00000100: 00 92 00 00 00 00 00 00|9D 73 00 00 00 10 00 00  | .Т......Эs......
00000110: 00 90 00 00 00 00 00 01|00 10 00 00 00 02 00 00  | .Р..............
00000120: 05 00 01 00 05 00 01 00|04 00 00 00 00 00 00 00  | ................
00000130: 00 40 01 00 00 04 00 00|09 E6 01 00 02 00 00 80  | .@.......ц.....А
00000140: 00 00 04 00 00 10 01 00|00 00 10 00 00 10 00 00  | ................
00000150: 00 00 00 00 10 00 00 00|00 00 00 00 00 00 00 00  | ................
00000160: 04 76 00 00 C8 00 00 00|00 B0 00 00 AC 89 00 00  | .v..╚....░..мЙ..
00000170: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000180: 00 00 00 00 00 00 00 00|50 13 00 00 1C 00 00 00  | ........P.......
00000190: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
000001A0: 00 00 00 00 00 00 00 00|A8 18 00 00 40 00 00 00  | ........╕...@...
000001B0: 50 02 00 00 D0 00 00 00|00 10 00 00 48 03 00 00  | P...╨.......H...
000001C0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
000001D0: 00 00 00 00 00 00 00 00|2E 74 65 78 74 00 00 00  | .........text...
000001E0: 48 77 00 00 00 10 00 00|00 78 00 00 00 04 00 00  | Hw.......x......
000001F0: 00 00 00 00 00 00 00 00|00 00 00 00 20 00 00 60  | ............ ..`
00000200: 2E 64 61 74 61 00 00 00|A8 1B 00 00 00 90 00 00  | .data...╕....Р..
00000210: 00 08 00 00 00 7C 00 00|00 00 00 00 00 00 00 00  | .....|..........
00000220: 00 00 00 00 40 00 00 C0|2E 72 73 72 63 00 00 00  | ....@..ю.rsrc...
00000230: AC 89 00 00 00 B0 00 00|00 8A 00 00 00 84 00 00  | мЙ...░...К...Д..
00000240: 00 00 00 00 00 00 00 00|00 00 00 00 40 00 00 40  | ............@..@
00000250: B5 81 03 48 58 00 00 00|D7 81 03 48 65 00 00 00  | ╡Б.HX...╫Б.He...
```

Frodo.exe



```
00000000: 4D 5A 90 00 03 00 00 00|04 00 00 00 FF FF 00 00  | MZ░.........ьь..
00000010: B8 00 00 00 00 00 00 00|40 00 00 00 00 00 00 00  | ┬.......@.......
00000020: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000030: 00 00 00 00 00 00 00 00|00 00 00 00 C0 00 00 00  | ............ю...
00000040: 0E 1F BA 0E 00 B4 09 CD|21 B8 01 4C CD 21 54 68  | ..╨..┤.═!╕.L═!Th
00000050: 69 73 20 70 72 6F 67 72|61 6D 20 63 61 6E 6E 6F  | is program canno
00000060: 74 20 62 65 20 72 75 6E|20 69 6E 20 44 4F 53 20  | t be run in DOS 
00000070: 6D 6F 64 65 2E 0D 0D 0A|24 00 00 00 00 00 00 00  | mode....$.......
00000080: E3 70 F1 C8 A7 11 9F 9B|A7 11 9F 9B A7 11 9F 9B  | ЦрЯх╖.÷╛╖.÷╛╖.÷╛
00000090: 29 0E 8C 9B 8F 11 9F 9B|5B 31 8D 9B A6 11 9F 9B  | ).▄╛▌.÷╛[1█╛╢.÷╛
000000A0: 60 17 99 9B A6 11 9F 9B|52 69 63 68 A7 11 9F 9B  | `.≥╛╢.÷╛Rich╖.÷╛
000000B0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
000000C0: 50 45 00 00 4C 01 04 00|A6 7D 84 53 00 00 00 00  | PE..L...╢}└S....
000000D0: 00 00 00 00 E0 00 0F 01|0B 01 05 0C 00 62 00 00  | ....ю........b..
000000E0: 00 46 01 00 00 00 00 00|0B 66 00 00 00 10 00 00  | .F.......f......
000000F0: 00 80 00 00 00 00 40 00|00 10 00 00 00 02 00 00  | .─....@.........
00000100: 04 00 00 00 04 00 00 00|04 00 00 00 00 00 00 00  | ................
00000110: 00 E0 01 00 00 04 00 00|E4 BE 00 00 02 00 00 00  | .ю......Д┼......
00000120: 00 00 10 00 00 10 00 00|00 00 10 00 00 10 00 00  | ................
00000130: 00 00 00 00 10 00 00 00|00 00 00 00 00 00 00 00  | ................
00000140: 90 80 00 00 50 00 00 00|00 D0 01 00 10 00 00 00  | ░─..P....п......
00000150: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000160: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000170: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000180: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
00000190: 00 00 00 00 00 00 00 00|00 80 00 00 90 00 00 00  | .........─..░...
000001A0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  | ................
000001B0: 00 00 00 00 00 00 00 00|2E 74 65 78 74 00 00 00  | .........text...
000001C0: 5A 60 00 00 00 10 00 00|00 62 00 00 00 04 00 00  | Z`.......b......
000001D0: 00 00 00 00 00 00 00 00|00 00 00 00 20 00 00 60  | ............ ..`
000001E0: 2E 72 64 61 74 61 00 00|C8 03 00 00 00 80 00 00  | .rdata..x....─..
000001F0: 00 04 00 00 00 66 00 00|00 00 00 00 00 00 00 00  | .....f..........
00000200: 00 00 00 00 40 00 00 40|2E 64 61 74 61 00 00 00  | ....@..@.data...
00000210: 74 3F 01 00 00 90 00 00|00 20 00 00 00 6A 00 00  | t?...░... ...j..
00000220: 00 00 00 00 00 00 00 00|00 00 00 00 40 00 00 C0  | ............@..ю
00000230: 2E 72 73 72 63 00 00 00|10 00 00 00 00 D0 01 00  | .rsrc........п..
00000240: 00 02 00 00 00 8A 00 00|00 00 00 00 00 00 00 00  | .....┼..........
00000250: 00 00 00 00 40 00 00 40|00 00 00 00 00 00 00 00  | ....@..@........
```

Methods of FRODO

- Range checking
- Value substraction
- Hamming distance
- Entropy of blocks checking
- Some heuristics

FRODO Summary

- Written in Assembler x86
- Executable file size – 35840 bytes – many internal
- Fast and furious!
- Testing is on its active phase now

Thank you! Questions? ;-)

- dorfmananton@gmail.com