

Malware Analysis with Reverse Engineering Hands-on

Matjaž Rihtar

Ljubljana, March 2018

Making Everything Easier!™

5th Edition

Reverse Engineering FOR **DUMMIES**® A Nobrainer

Learn to:

- Defend against the latest Windows® 10 and Linux® hacks
- Develop an effective security testing plan
- Protect web applications, databases, laptops, servers, and smartphones
- Use the latest testing tools and techniques

Matjaž Rihtar

Independent information security consultant



Example

- What does this code do?

... 0F 31 66 BB FF 00 66 F7 F3 ...

- Disassembly

```
rdtsc  
mov    bx, 0xFF  
div    bx
```

- Explanation - a random generator

```
rdtsc          ; CPU time stamp counter → EDX:EAX  
mov    bx, 0xFF ; 255 → BX  
div    bx      ; DX:AX % BX → DX (random [0..254])
```



Code patterns

- Recognizing
 - Architecture
 - Compiler
 - Language
 - Functions
 - Arguments
 - Results of functions
 - System calls

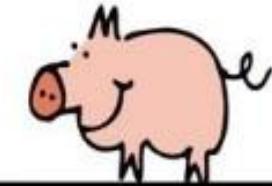
Spelling difficult words

I	C	S	T	O	E	B	I	S	C	U	I	T	B
O	E	E	D	N	E	H	C	A	N	I	P	S	M
U	L	Y	E	I	G	O	Y	U	G	W	I	U	A
C	E	L	L	O	A	A	O	E	R	S	N	U	N
O	R	P	I	N	S	C	L	P	I	E	E	I	G
T	Y	N	C	A	U	F	K	E	A	O	S	S	O
A	H	O	I	R	A	S	P	B	E	R	R	Y	E
T	C	M	O	T	S	L	A	S	A	G	N	E	S
O	I	M	U	N	R	B	E	G	A	B	B	A	C
P	W	I	S	N	A	L	M	O	N	D	P	P	E
L	D	S	P	A	E	I	N	I	H	C	C	U	Z
S	N	R	B	P	U	M	P	K	I	N	G	D	N
S	A	E	T	I	T	E	P	P	A	E	C	U	N
N	S	P	R	E	W	O	L	F	I	L	U	A	C

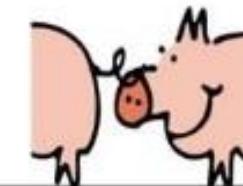
RASPBERRY
DELICIOUS
CABBAGE
PUMPKIN
BISCUIT
POTATO
YOLK
SPINACH
APPETITE
ZUCCHINI
CAULIFLOWER
CELERY
SANDWICH
SAUSAGE
ALMOND
PERSIMMON
MANGOES
LASAGNE
ONION

Important fundamentals

- Data structures and storage
 - Memory: byte/word/long/long long
 - CPU registers
 - Logical operators AND/OR/XOR
 - Endianness
 - Intel is little-endian
- CPU instructions
 - 32-bit/64-bit
 - Special: SSE/AVX/...



BIG-ENDIAN



LITTLE-ENDIAN

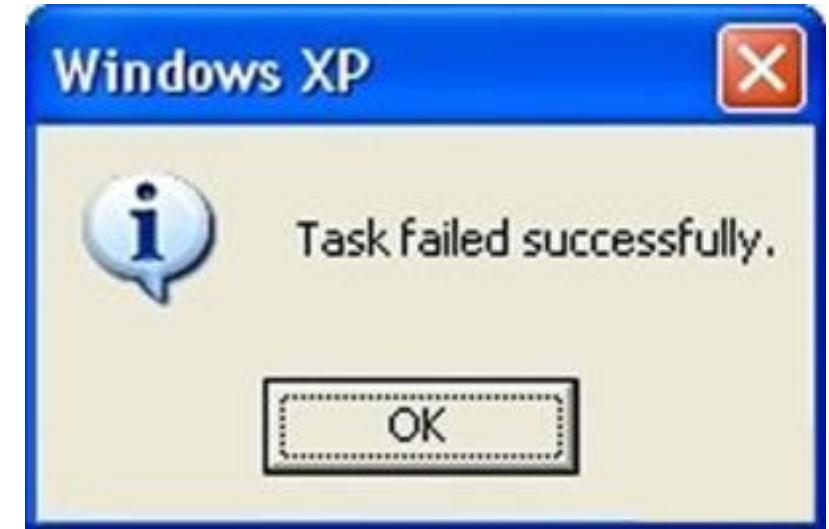
Finding interesting stuff in the code

- Analysis of executables
 - EXE header
 - Imported DLLs
 - LoadLibrary
 - Strings
 - ASCII and Unicode
 - Constants
 - Precomputed values
CRC32, MD5, ...
 - Magic numbers
 - MZ for EXE/DLL files
 - Dates



OS Specifics

- Argument passing
 - Via stack and registers
 - cdecl, stdcall, fastcall
- Returning values
 - Modifying arguments on stack
 - Via pointers
 - Via registers
- Windows NT
 - CRT → main
 - GUI → WinMain



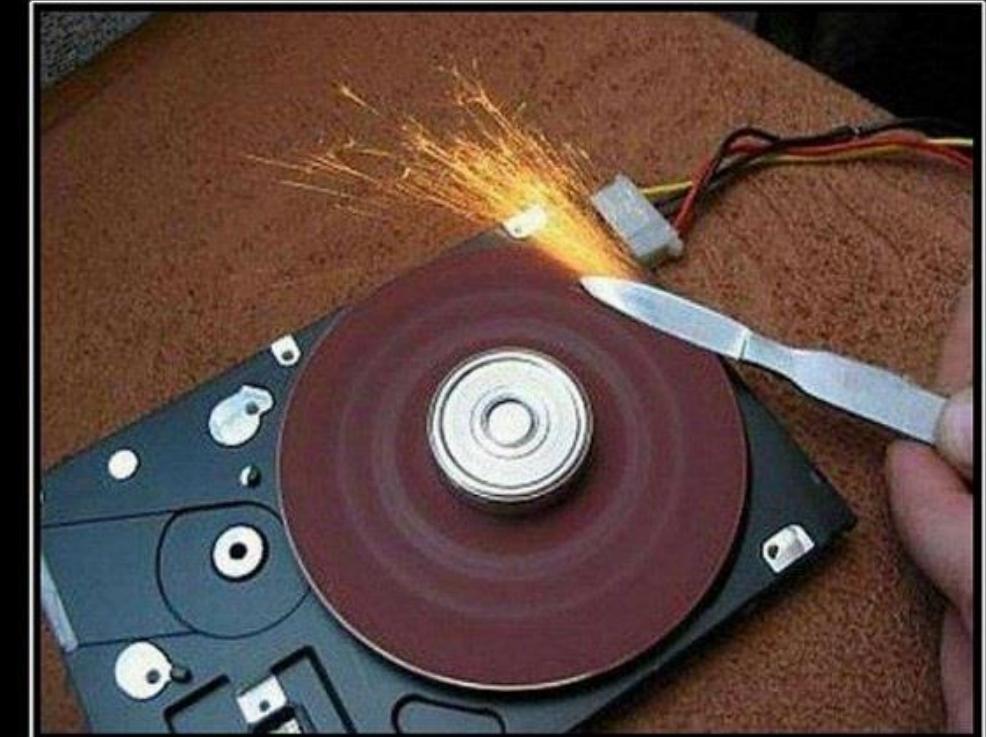
API Function hooks

- Microsoft Detours
 - Pro (x64) version: 10000 USD
- Others
 - madCodeHook
 - PolyHook
- Sandbox isolation
 - Sandboxie
 - Cameyo, Shade Sandbox, Shadow Defender, Cuckoo Sandbox, ...
- Virtual machines
 - VMware Workstation, VirtualBox



Tools

- Disassemblers
 - IDA Pro
- Decompilers
 - Hex-Rays
- Debuggers
 - OllyDbg, WinDbg, Radare, x64dbg, ...
- System calls tracing
 - Sysinternals' Process Monitor
- Other tools
 - Hex editor, Wireshark, QEMU, calculator



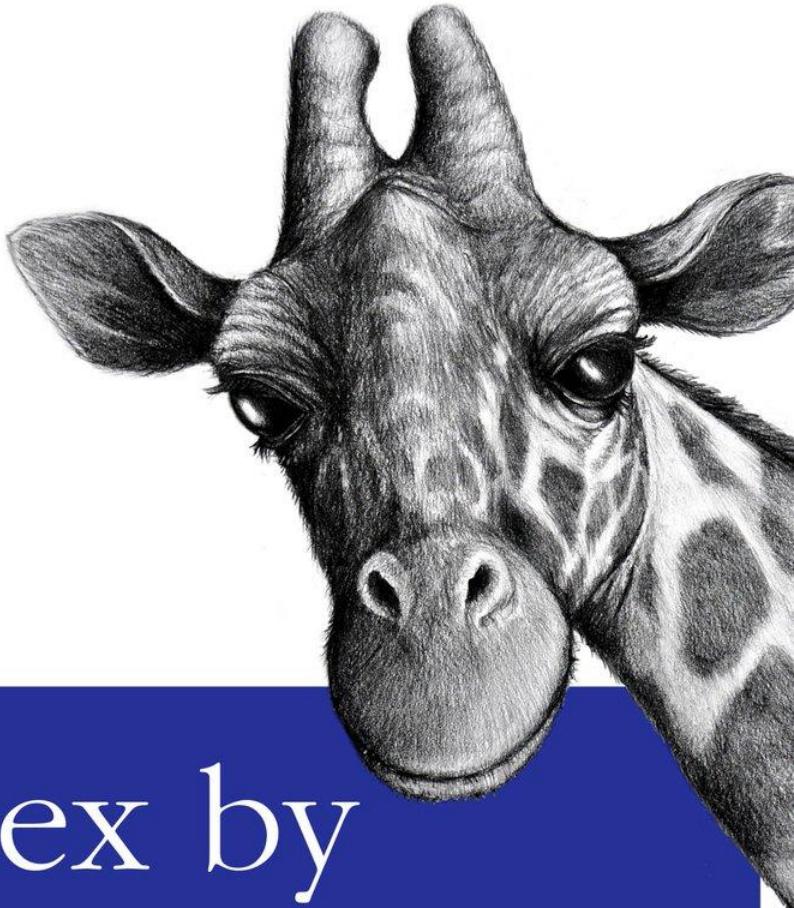
Low-Level Format Tool

Example in practice

- Regex Match Tracer
 - IDA Pro
 - OllyDbg
 - Hex editor
 - Process Monitor

Expert

Regex by
Trial and Error



Complications

- Code obfuscation
 - Hiding text strings
 - Inserting garbage code
- EXE packers/crypters
 - Armadillo, ASPack, PECompact, UPX, ...
 - Packer detectors: PEiD, DIE (Detect It Easy), RDG Packer Detector, ...
- Code virtualization
 - Reversed code is virtual machine's byte code
- Anti-debugging measures
 - IsDebuggerPresent, FindWindow, CsrGetProcessId, ...
 - TitanHide (kernel driver)

The chalkboard contains several mathematical equations and formulas:

- $\Delta = \frac{P}{\lambda}$
- $E(\Delta) = E\left(\frac{\lambda P}{\sum k}\right) = \int_0^{\infty} \frac{1}{\Gamma(\lambda P)} \times \frac{\lambda^m}{C(\lambda P)} e^{-\lambda P} d\lambda = \frac{1}{\Gamma(\lambda P)} \int_0^{\infty} (\lambda P)^2 e^{-\lambda P} d\lambda = \frac{\Gamma(\lambda P - 1)}{\Gamma(\lambda P)}$
- $P(\lambda P) = C(\lambda P - 1) \Rightarrow \frac{\Gamma(\lambda P - 1)}{\Gamma(\lambda P)} = \frac{(\lambda P - 2)!}{(\lambda P - 1)!} = \frac{1}{\lambda P - 1} \Rightarrow E\Delta = \frac{1}{\lambda P - 1} \lambda P = \frac{\lambda P}{\lambda P - 1}$
- $K_m E\Delta = \left(m \frac{\lambda P}{\lambda P - 1}\right) \Delta = \lambda P$
- $\text{Var } \Delta = E\Delta^2 - (E\Delta)^2 = \frac{(\lambda P)^2}{(\lambda P - 1)(\lambda P - 2)} - \frac{(\lambda P)^2}{(\lambda P - 1)^2} = \frac{\lambda P^2}{(\lambda P - 1)^2}$
- $(\lambda P)^2 \left[(\lambda P - 1) - (\lambda P - 2) \right] = \lambda P^2$
- $F(\epsilon) = P\left[T \leq \epsilon\right] = P\left[\frac{t}{\lambda P} \leq \epsilon\right] = P\left[t \leq \lambda P \epsilon\right]$
- $F(t) = \int_0^t \frac{u^{t-1}}{\lambda^m} du = \frac{1}{\lambda^m} \left[\frac{u^t}{t} \right]_0^t = \frac{1}{\lambda^m} t^{\lambda P}$
- $P\{X_{\lambda P} \leq t\} = \left[\lambda P F(t) \right]^{\lambda P} = \frac{P}{\lambda P} t^{\lambda P}$
- $E(T_2) = E(\bar{X}) = \frac{2}{\lambda} E(2X) = \frac{2}{\lambda} \beta = \beta \times \frac{2}{\lambda}$

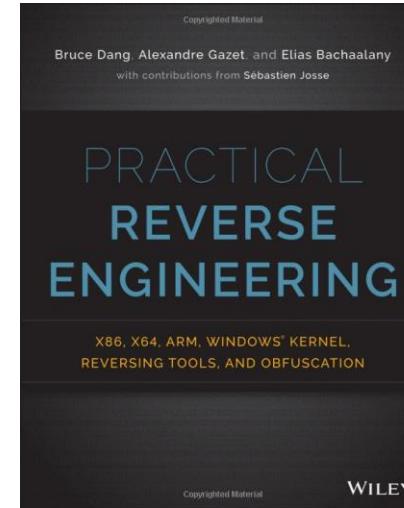
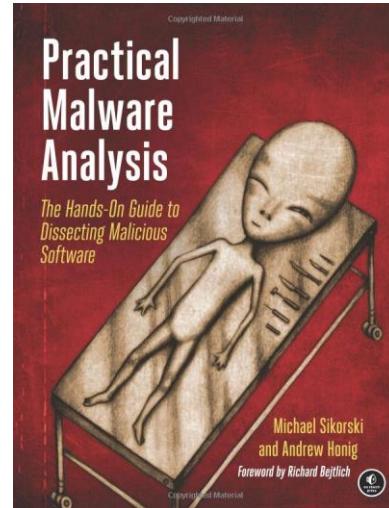
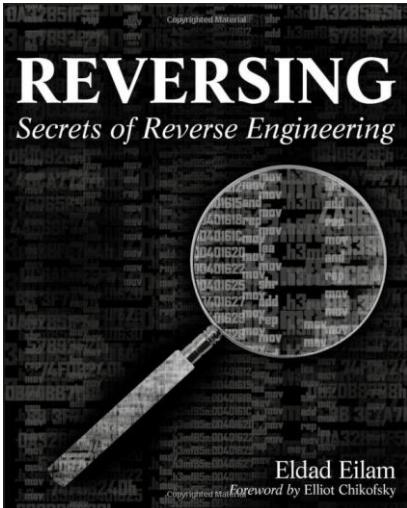
A hand-drawn diagram of a right-angled triangle ABC is shown, with the right angle at vertex C. The vertical leg is labeled 'a', the horizontal leg is labeled 'b', and the hypotenuse is labeled 'c'. The angle at vertex A is labeled 'A'.

Pythagorean theorem formulas are written on the board:

- $a^2 + b^2 = c^2, c = \sqrt{a^2 + b^2}$
- $c^2 - a^2 = b^2, c^2 - b^2 = a^2$
- $\frac{a}{c} = \frac{HB}{AB}$
- $ac = c \times HB \text{ and } bc = c \times AB$
- $a^2 + b^2 = c \times HB + c \times AB$
- $\sin A = \frac{a}{c}$
- $\log c = \frac{a}{b}$

Literature

- Reversing - Secrets of Reverse Engineering (Eilam, 2005)
- Practical Malware Analysis (Sikorski, 2012)
- Practical Reverse Engineering (Dang, 2014)
- Reverse Engineering for Beginners (Yurichev, 2018)



Reverse Engineering for
Beginners



Dennis Yurichev

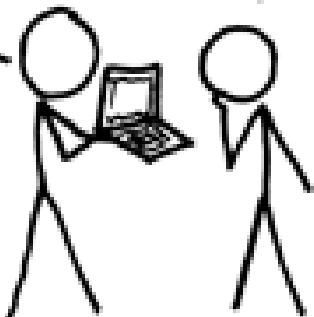
Questions?

A CRYPTO NERD'S
IMAGINATION:

HIS LAPTOP'S ENCRYPTED.
LET'S BUILD A MILLION-DOLLAR
CLUSTER TO CRACK IT.

NO GOOD! IT'S
4096-BIT RSA!

BLAST! OUR
EVIL PLAN
IS FOILED!



WHAT WOULD
ACTUALLY HAPPEN:

HIS LAPTOP'S ENCRYPTED.
DRUG HIM AND HIT HIM WITH
THIS \$5 WRENCH UNTIL
HE TELLS US THE PASSWORD.

GOT IT.

