

Binary Analysis Course

MAX 'LIBRA' KERSTEN

What is it?

- A public and free [course](#) providing step-by-step insights
 - It provides conceptual insights with the help of practical cases
 - Fully focused on free and open-source software
- The course contains
 - Background information
 - Conceptual explanations
 - Practical cases
 - Malware analysis
 - Automation scripts
 - Report writing tips

1. Introduction to the course
 1. Practical case: Secura Grand Slam CTF "Easy Reverse"
 2. The workstation
 3. Basic CPU architecture
 4. Compilers and (dis)assemblers
2. Assembly basics
 1. Conditions and loops
 2. Practical case: Patch Me 0x01
 3. Methods and macros: the call stack
 4. Practical case: Buffer Overflow 0x01
 5. Crash course
 6. Practical case: Crack Me 0x01
 7. Practical case: Crack Me 0x02
 8. Practical case: Crack Me 0x03
3. Assembly code
 1. Hello World
 2. Universal Product Code calculator
 3. Debugging code
4. Binary types
 1. Dot Net
 2. Java
 3. Android
 4. Browser plug-in
5. Common techniques
 1. General techniques
 2. Analysing scripts
 3. Debugging Dot Net binaries
 4. Analysing high level languages
 5. Analysing low level languages
 6. Dealing with obfuscation
6. Malware analysis
 1. Dot Net RAT
 2. Android SMS Stealer
 3. LNK & ISESteroids Powershell dropper
 4. Emotet droppers
 5. Magecart
 6. Corona DDoS bot
 7. Azorult loader stages
 8. Emotet JavaScript downloader
 9. Corona Locker
 10. ReZer0v4 loader
 11. Dumping WhisperGate's wiper from an Eazfuscator obfuscated loader
7. Analysis scripts
 1. PowerShell string formatting deobfuscation
 2. JavaScript string concatenation deobfuscation
 3. Automatic ReZer0 payload and configuration extraction
 4. Ghidra script to decrypt strings in Amadey 1.09
 5. Ghidra script to decrypt a string array in XOR DDoS
 6. Ghidra script to handle stack strings
8. Obtaining samples
 1. Searching samples
 2. Trapping spam e-mails
 3. Setting up a honeypot
9. Documentation
 1. Article structure
10. Resources
11. F.A.Q.
12. Miscellaneous
 1. A year in review: 2018-2019
 2. A year in review: 2019-2020
 3. A year in review: 2020-2021

Console - Scripting

```
TalismanStackStringDecryption.java> Running...
TalismanStackStringDecryption.java> Stack string starting at 0x10002401
TalismanStackStringDecryption.java> Stack string ended, since no suitable scalar value could be found at 0x10002460!
TalismanStackStringDecryption.java> -----
TalismanStackStringDecryption.java> US-ASCII: Global\DelSelf(%8.8X)
TalismanStackStringDecryption.java> ISO-LATIN-1: Global\DelSelf(%8.8X)
TalismanStackStringDecryption.java> UTF-16BE: 認難漿戀做難耐騎攀難勻攀難的 一畝「畝堀」
TalismanStackStringDecryption.java> UTF-16LE: Global\DelSelf(%8.8X)
TalismanStackStringDecryption.java> UTF-8: Global\DelSelf(%8.8X)
TalismanStackStringDecryption.java> Length in bytes: 46
TalismanStackStringDecryption.java> -----
TalismanStackStringDecryption.java> Finished!
```

Console - Scripting

```
xorddos_array_decryption.java> Running...
xorddos_array_decryption.java> cat resolv.conf
xorddos_array_decryption.java> sh
xorddos_array_decryption.java> bash
xorddos_array_decryption.java> su
xorddos_array_decryption.java> ps -ef
xorddos_array_decryption.java> ls
xorddos_array_decryption.java> ls -la
xorddos_array_decryption.java> top
xorddos_array_decryption.java> netstat -an
xorddos_array_decryption.java> netstat -antop
xorddos_array_decryption.java> grep "A"
xorddos_array_decryption.java> sleep 1
xorddos_array_decryption.java> cd /etc
xorddos_array_decryption.java> echo "find"
xorddos_array_decryption.java> ifconfig eth0
xorddos_array_decryption.java> ifconfig
xorddos_array_decryption.java> route -n
xorddos_array_decryption.java> gnome-terminal
xorddos_array_decryption.java> id
xorddos_array_decryption.java> who
xorddos_array_decryption.java> whoami
xorddos_array_decryption.java> pwd
xorddos_array_decryption.java> uptime
xorddos_array_decryption.java> Finished!
```

```
2 undefined __Z8aCheckAVv(void)
3
4 {
5     bool bVar1;
6     char *pcVar2;
7     undefined uVar3;
8
9     pcVar2 = __Z8aDecryptPc(&_aAV00);
10    bVar1 = __Z7aPathAVPc(pcVar2);
11    uVar3 = bVar1 != false;
12    pcVar2 = __Z8aDecryptPc(&_aAV01);
13    bVar1 = __Z7aPathAVPc(pcVar2);
14    if (bVar1 != false) {
15        uVar3 = 0x2;
16    }
17    pcVar2 = __Z8aDecryptPc(&_aAV02);
18    bVar1 = __Z7aPathAVPc(pcVar2);
19    if (bVar1 != false) {
20        uVar3 = 0x3;
21    }
22    pcVar2 = __Z8aDecryptPc(&_aAV03);
23    bVar1 = __Z7aPathAVPc(pcVar2);
24    if (bVar1 != false) {
25        uVar3 = 0x4;
26    }
27    pcVar2 = __Z8aDecryptPc(&_aAV04);
28    bVar1 = __Z7aPathAVPc(pcVar2);
29    if (bVar1 != false) {
30        uVar3 = 0x5;
31    }
}
```

```
2 undefined __Z8aCheckAVv(void)
3
4 {
5     bool bVar1;
6     char *pcVar2;
7     undefined uVar3;
8
9     /* Decrypted value: "AVAST Software" */
10    pcVar2 = __Z8aDecryptPc(&_aAV00);
11    bVar1 = __Z7aPathAVPc(pcVar2);
12    uVar3 = bVar1 != false;
13    /* Decrypted value: "Avira" */
14    pcVar2 = __Z8aDecryptPc(&_aAV01);
15    bVar1 = __Z7aPathAVPc(pcVar2);
16    if (bVar1 != false) {
17        uVar3 = 0x2;
18    }
19    /* Decrypted value: "Kaspersky Lab" */
20    pcVar2 = __Z8aDecryptPc(&_aAV02);
21    bVar1 = __Z7aPathAVPc(pcVar2);
22    if (bVar1 != false) {
23        uVar3 = 0x3;
24    }
25    /* Decrypted value: "ESET" */
26    pcVar2 = __Z8aDecryptPc(&_aAV03);
27    bVar1 = __Z7aPathAVPc(pcVar2);
28    if (bVar1 != false) {
29        uVar3 = 0x4;
30    }
31    /* Decrypted value: "Panda Security" */
32    pcVar2 = __Z8aDecryptPc(&_aAV04);
33    bVar1 = __Z7aPathAVPc(pcVar2);
34    if (bVar1 != false) {
35        uVar3 = 0x5;
36    }
}
```

Where can I find it?

- On my website: maxkersten.nl/binary-analysis-course/
- If you have questions, suggestions, or simply want to state you dislike Java
 - [@Libranalysis](https://twitter.com/Libranalysis) on Twitter
 - [/in/ThisIsLibra](https://www.linkedin.com/company/thisislibra/) on LinkedIn
 - @ThisIsLibra on Telegram