Malware Analysis

MuhamaD.B

Contact us:

پێشەکی

- بۆچی مالوێر ئەنالسیس ؟
- دروستکردنی ناوەندێکی سەلامەت بۆ مالوێر ئەنالسیس.

- Static Analysis تەکنیکی
- Dynamic Analysis تەکنیکی
- Packing

- دۆزینەوەی مالوێر.

بۆچی مالوێر ئنالسیس ؟

بە گشتی:

- هەر کۆدێك کە هەڵبستێ بە ئەنجامدانی کارێکی خراپ، کە لە ئێستادا ئەمە زۆر باوە.
- هەر فەرمانێ هەڵسێ بە ئەنجامدانی کارێکی نەزانراو، جێگیرببێت لەناو سیستەمێك،وەك:

- Viruses
- Worms
- Intrusion Tools
- Spyware
- Rootkits

بۆچی مالوێر ئنالسیس ؟

- بۆ زانینی زیانەکە.
- بۆ ڕێککەوتن لەنێوان هەردولادا.
- بۆ دیاریکردنی ئاستی ئەم کەسەی کە هەڵساوە بە دروستکردنی.
- بۆ زانینی ئاستی فایلەکە.
- بۆ دۆزینەوەی ئەو کەسەی کە ئەم کارەی ئەنجامداوە.
- بۆ وەلامدانەوەی پرسیارەکان.
- نیشاندانی نێت؟
- نیشاندانی شوێنی هۆستەکە؟
- بەردەوام چۆن کارئەکا؟

بۆچی مالوێر ئنالسیس ؟

- بۆ ماوەی چەند ئەمێنێتەوە؟
- ئایا ئەمە بلاوئەبێتەوە بۆ ئامێرەکانیتر؟
- چۆن بتوانم لەنێو ئامێرەکانیتر بیدۆزمەوە؟
- چۆن ڕێگری لێبکەم لەوەی کە لە داهاتوودا ڕووئەدات؟
- ئەم مالوێرە ئەنجامی چییە؟
- چۆن هاتە ناو کۆمپیوتەر؟
- کێ ئەنجامی داوە، وە ئاستی چۆنە؟
- چۆن لەوە ڕزگارمبێ؟
- چی شتێك ئەدزێت؟
- بەردەوام چۆن کارئەکا؟
- کاتی دروستکردنی؟

بۆچی مالوێر ئنالسیس ؟

- بە چی زمانێك نوسراوە؟
- ئایا پارێزراوە؟
- ئایا ئەمە ئامادە کراوە بۆ بەرپێچی کردن لە ئنالسیس؟
- ئایا هیچ فەرمانێکی رووتکێتی تیایە؟
- کاتی دامەزراندنی؟

دروستکردنی ناوەندێکی سەلامەت بۆ مالوێر ئنالسیس.

- هیچ کاتێك مالوێر لەنێو کۆمپیوتەرەکەت مەکەوە.
- هەوڵبە کۆمپیوتەرەکەت لە ژورەکەی خۆتبێ نەوەك لەبەردەست ئەندامانی خێزانەکەت دابێت، وە داتاکانت لەنێو هاردێکدا هەڵبگرە بۆ هەر ئەگەرێکی نەخوازراو.
- ئەتوانیت کار لەسەر ئەمانە بکەیت،

ویندۆز وەهمی بەکاربهێنە بۆ ئەوەی کارەکانت بە سەلامەتی ئەنجامبدەیت.

- VMware Workstation
- Parallels
- Microsoft Virtual PC
- Xen

کەمکردنەوەی مەترسی

- ئەگەر بکرێت ستاتیك ئنالسیس لە سیستەمێکیتر ئەنجامبدرێ بۆ ئەوەی مەترسیەکەی کەمبکرێتەوە.
- خۆ دورخستنەوە لە دەبڵ کلیك کردن لە

- کارکرن بەشێوازێکی زیرەکانە.

دروستکردنی ناوچەیەکی سەلامەت.

- ئەمە ئاسانە بۆ ئەو کە دەست بەسەر هەموو شتێکت دابگرێت.
- لەوانەیە ڕەوشتی هێرشبەرەکە بگۆڕێت،چۆن؟!

بەڕێگادان بە هێرشبەرەکە بۆ ئەوەی کە دەستبگرێت بەسەر سێرفەرەکە، لەو کاتەیە ئەچیتە نێو جەنگێکی ڕاستەقینە لەگەڵ مرۆڤێك تا ئەوەی دەست بگرێت بەسەر ئامێرەکەت.

- هەوڵبە براوسەری تۆڕ بەکاربهێنیت.
- لەوانەی بەهۆی تۆوە زیان بە خەڵکی تریش بگەیەنێت.

دروستکردنی ناوچەیەکی سەلامەت.

- بە دڵنیاییەوە ئێمە نامانەوێ تۆ ڕێگە بە مالوێرەکە بەیت بۆ ئەوەی دەستکاری ئینتەرنێتە دروستەکە بکات.
- تەنیا هۆست-ئۆنڵی بەکاربهێنە لە ڤیرتوالیزاشن (ویندۆز وەهمی).
- دانانی (دنس،وێب،هتد...) لەسەر ڤیرتوالیزاشن (ویندۆز وەهمی).
- بەکارهێنانی بەرنامەی نێت کەت (ئەتوانن لە گوڵگ دایگرن).
- دروستکردنی سێرڤەر تایبەت بەخۆت(ئەمە بۆ کەسانێکە کە لە ئاستێکی بەرزدابن نەوەك بۆ ئەوانەی کە لە سەرەتان).

ڕێکخستنی ڤیرتوالیزاشن (ویندۆز وەهمی)

- پێویستی بە شارەزاییەکی کەم هەیە.
- بەکارهێنانی (هۆست-ئۆنڵی).
- گرنگی مەدە بەشێوازی ویندۆزەکە.
- پێویست ناکا هیچ شتێکی شەخصی لەنێو ویندۆزەکە دابنێیت.
- هیچ ئەکاونتێکی شەخصی لەنێو وینۆزەکە بەکاربهێنە.

ئەنجامدانی مالوێر ئنالیسیس لەسەر ویندۆز

Static vs. Dynamic Analysis

Static Analysis:

- گرنگی بە کۆد نادرێت.
- یاخود کار لەسەر ئەو کۆدانە ئەکرێت کە وەك مردوو وان.

Dynamic Analysis:

- گرنگی بە کۆد ئەدرێو ڕاستەوخۆ کاری لەسەر ئەکرێت.
- شێوەکەی وەك ناوچەی مێرولە وایە.

ئەی باشترین و خێراترین ڕێگا چیە؟

- باشترین ڕێگا ئەوەیە کە کار لەسەر هەردوو ڕێگاکە بکەین بۆ ئەوەی بگەین بە ئامانجەکەمان.

Static Analysis

- وەك ووتمان لێرەیا زۆر گرنگی بە کۆد نادەین.
- وە گرنگی بە (سەلامەتی) کردن نادەین کاتێك لەسەر ویندۆز کارئەکەین.

Static Code Analysis

فایلی شوێن پەنجە(پەنجە مۆر)

- یەکەم ڕێگا تاقیکردنەوە لەسەر فایلی پەنجە مۆر(شوێن پەنجە) ئەکەین، وە وا ئەزانیت ئەگەر لەکاتی ئنالسیس دا بگۆڕێت.
- بەکارهێنانی

md5deep, md5deep, md5sum, Hex, etc...

وەک ئەم نمونەی خوارەوە،

```
krk@ws ~> md5sum hello* > md5sum_hello_files.txt
krk@ws ~> cat md5sum_hello_files.txt
611957bd6a2ad96420279 04a65f3638e  hello
7ab03b44ac6a20b0fa0cc80b636b0f51  hello.c
bef5bfe7ddf597c8ea86eecb2cbf52a3  hello_debug
38e85544dd4349c523430923eafc86ac  hello_static
```

- کاتێک لە کارەکە تەواوبوویت واتا ئنالسیس، وە لە نرخەکان دڵنیابوویت، ئەگەڕێیتە دواوە بۆ ئەوەی دڵنیابیت کە نرخی نەگۆڕاوەو وەک خۆیەتی.

```
krk@ws ~> md5sum -c md5sum_hello_files.txt
```

Virus Scan

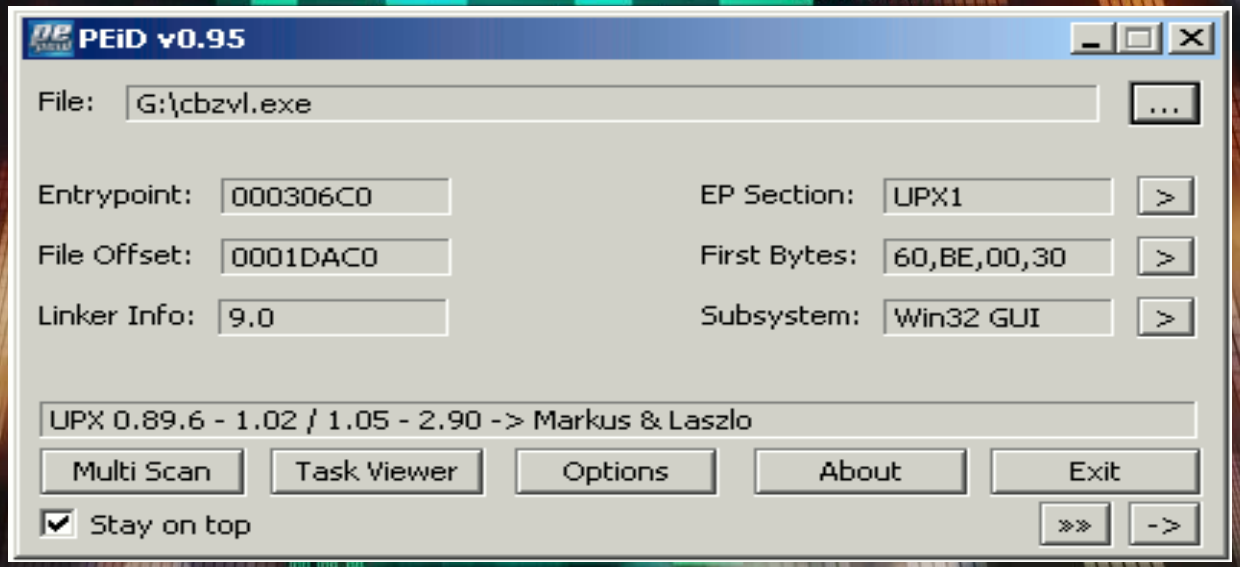
- هەمووکات پشکنین بۆ مالوێرێکی نوێ بکە بە ئەنتیڤایرۆسێك کە ئەپدەیتی نوێ بێت.
- لەوانەیە کەسێکی تر ئەو بەرنامەیەی دۆزیبێتەوەو تاقیکردنەوەی لەسەر کردبێت کە تۆ کاری لەسەر دەکەیت.
- ئەگەر دوای ئەم رێگایەنەش هەستت بە شتێك کردوو دڵنیانەبویت ئەتوانیت لە

http://www.virustotal.com

پشکنینی بۆ بکەیت.

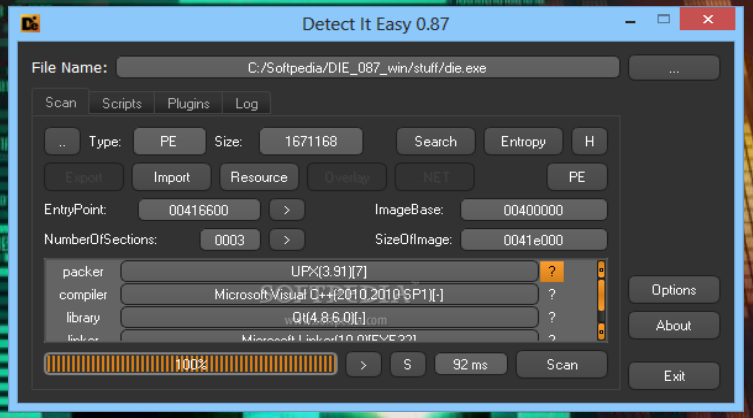
PEiD

- بەرنامەیەکی بەخۆراییە کە زانیاریت لەسەر ئەم بەرنامەی پێ ئەدات.
- وە پێت ئەڵێت کە ئەم بەرنامەیە بە چی پاك کراوە (پارێزراوە لە ئەنپاك کردن) وە پێت ئەڵێ چۆن ئەنپاکی بکەیت(ئەگەر بکرێت).

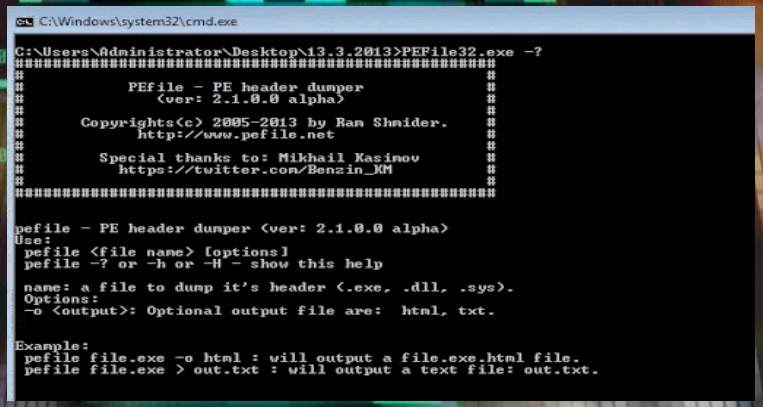


ئەمانەش هەمان کاری ئەم بەرنامانەی سەرەوە ئەکەن،

Detect It Easy



pefile



Strings

- هەندێکجار شتەکان ئاسانن.
- سەیرێکی وێنەکە بکە هەندێکجار وا ئاشکرایە.

```
$ strings unknown2.exe
...
 <host> <port>
 -install <host> <port>
 -remove
EC.1
EC.2
cmd.exe
connect thread started!
...
```

Strings, Bintext, Hex Workshop, IDAPro

- بەلام ئاگاداری کۆدەکانبە.

Strings

C:\analysis> strings
Strings v2.1
Copyright (C)1999-2003 Mark Russinovich
Systems Internals - www.sysinternals.com
usage: strings [-s] [-n length] [-a] [-u] [-q] <file or directory>

-s Recurse subdirectories

-n کەمترین ڕێژە (ئاسایی 3یە)

-a گەران بەدوای Ascii

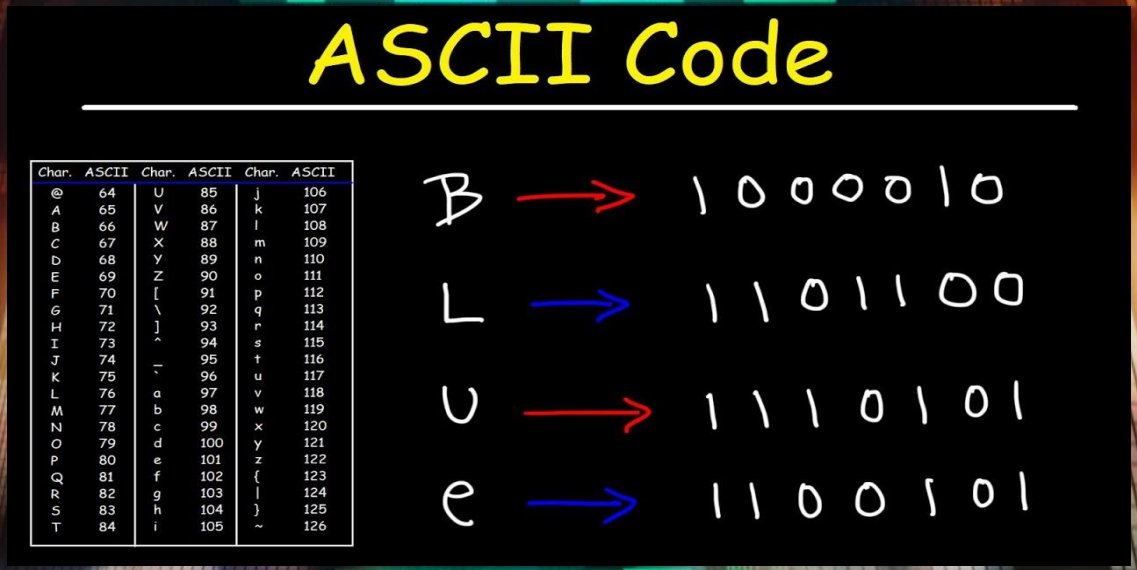
-u گەران بەدوای Unicode

-q دەرچون

UNICODE

```
┌─[root@parrot]─[/home/pentest/Malware Analysis/Samples/Malware/Maldoc]
└──╼ #cat Unicode
u00e8u0000u5d00uc583ub914u018bu0000u3db0u4530u4500u7549uebf9uad00uadaduadaduadadud4adu3dc1u3d3du5962u0
b0ub641u0155ucab6u3957ud564u3db2u3d3duc4dfu5255u3d53u553du4f48u5051uc269ub62bud5d5u3d44u3d3dueab6ubd7a
b63du6ce1u6e6fu3955u3d3cuc23du316bu6467u6f6cu3fb6u7e6eu06bdu483dubcc7uc146u5813u5845u3e48ud6beub435ufa
du6a6euc26du2d6buc5beu483du573bu6e3cu6bc2u6739ube64u39ffubd7cu3d07u8948u6bc2u6c35ub66bu0148u49b6u4513u
549uf6fcu3e30u7de7uccd6u2206uda48ub663u1963ue03eub65bu7631u63b6u3e21ub6e0ub639uf83eu6396ufe64uc2d5uc2c
u6c77u3d4eu4955u4d49u1207u0412u130fu0f0bu0c13u0d0du0b13u120bu505fu0212u0055u5c04u3d58u5a5eu0254u0405u5
04u0b0du0d0du0d0du0d0du0d0du0f0du0c5eu0d08u0c0eu0e04u0d0du0c0du090du040du0d0du0d0du0d0du0d0du0a0cu3d0d
┌─[root@parrot]─[/home/pentest/Malware Analysis/Samples/Malware/Maldoc]
└──╼ #
```

ASCII



Char.	ASCII	Char.	ASCII	Char.	ASCII
@	64	U	85	j	106
A	65	V	86	k	107
B	66	W	87	l	108
C	67	X	88	m	109
D	68	Y	89	n	110
E	69	Z	90	o	111
F	70	[	91	p	112
G	71	\	92	q	113
H	72	]	93	r	114
I	73	^	94	s	115
J	74	_	95	t	116
K	75	`	96	u	117
L	76	a	97	v	118
M	77	b	98	w	119
N	78	c	99	x	120
O	79	d	100	y	121
P	80	e	101	z	122
Q	81	f	102	{	123
R	82	g	103	|	124
S	83	h	104	}	125
T	84	i	105	~	126

Recurse subdirectories

```
        public function shcEnCry($key, $locate) {
            $data      = file_get_contents($locate);
            $iv        = mcrypt_create_iv(mcrypt_get_iv_size(MCRYPT_RIJNDAEL_128, MCRYPT_MODE_CBC), MCRYPT_DEV_URANDOM);
            $encrypted = base64_encode($iv . mcrypt_encrypt(MCRYPT_RIJNDAEL_128, hash('sha256', $key, true), $data, MCRYPT_MODE_CBC, $iv));
            if(file_put_contents($locate, $encrypted)) {
                echo '<i class="fa fa-lock"
aria-hidden="true"></i> <font
color="#00BCD4">Locked</font> (<font
color="#40CE08">Success</font>) <font
color="#FF9800">|</font> <font
color="#2196F3">' . $locate . '</font> <br>';
            } else {
                echo '<i class="fa fa-lock"
aria-hidden="true"></i> <font
color="#00BCD4">Locked</font> (<font
color="red">Failed</font>) <font
color="#FF9800">|</font> ' . $locate . ' <br>';
            }
        }
```

Encryption

```
        public function shcDeCry($key, $locate) {
            $data      = base64_decode(file_get_contents($locate));
            $iv        = substr($data, 0, mcrypt_get_iv_size(MCRYPT_RIJNDAEL_128, MCRYPT_MODE_CBC));
            $decrypted = rtrim(mcrypt_decrypt(MCRYPT_RIJNDAEL_128, hash('sha256', $key, true), substr($data, mcrypt_get_iv_size(MCRYPT_RIJNDAEL_128,
                MCRYPT_MODE_CBC)), MCRYPT_MODE_CBC, $iv), "\0");
            if(file_put_contents($locate, $decrypted)) {
                echo '<i class="fa fa-unlock"
aria-hidden="true"></i> <font
color="#FFEB3B">Unlock</font> (<font
color="#40CE08">Success</font>) <font
color="#FF9800">|</font> <font
color="#2196F3">' . $locate . '</font> <br>';
            } else {
                echo '<i class="fa fa-unlock"
aria-hidden="true"></i> <font
color="#FFEB3B">Unlock</font> (<font
color="red">Failed</font>) <font
color="#FF9800">|</font> <font
color="#2196F3">' . $locate . '</font> <br>';
            }
        }
        public function kecuali($ext, $name) {
            $re = "/({$name})/";
            preg_match($re, $ext, $matches);
            if($matches[1]) {
                return false;
            }
            return true;
        }
```

Decryption

Strings

- بە وریاییەوە کاربکە.
- هیچ شتێك نییە کە هێرشبەرەکە بوەستێنێ لە هەڵخەلاتندنی شیکەرەوەکە (ئنالسیس).
- ستڕینگ بۆ سەرەتا شتێکی باشە، وە ئەتوانی بۆ دەستکەوتنی زانیاریش سودی لێببینیت.

```
rem barok -loveletter(vbe) <i hate go to school>
rem by: spyder / ispyder@mail.com / \
        @GRAMMERSoft Group / Manila,Philippines
On Error Resume Next
dim fso,dirsystem,dirwin,dirtemp,eq,ctr,file,
    vbscopy,dow eq="" ctr=0
Set fso = CreateObject("Scripting.FileSystemObject")
set file = fso.OpenTextFile(WScript.ScriptFullname,1)
```

سوود وەرگرتن لە گەرانی ئینتەرنێتدا.

- زانیاری لەسەر ستڕینگ پەیدابکە، وە ئاگاداری ئیمەیڵ،نێتوۆرك بە.
- گەران لە ئینتەرنێت بۆ کۆکردنەوەی زانیاری یاخود ئاگاداربون لە هەواڵە نوێیەکان.
- هەوڵبە فێری زمانی ئینگلیزی،ڕوسی،چینی ببیت بۆ ئەمەش ئەتوانیت سوود لە گوگڵ وەربگریت.

https://translate.google.com/

- بەلام ئەبێ ئاگاداربیت چونکە ئەتوانێت سەیرت بکات.

بەکارنەهێنانی ستڕینگ

- ئەتوانیت تەنیا سوود لە packers وەربگریت.
- بۆ وەرگرتنی زانیاری لەسەر ئەم بەرنامەیە یاخود بەچی پاڕێزراوە.
- کارەکانت بۆ ئاسان ئەکا.

دواتر بە درێژی باسی packers ئەکەین.

PE Format

زانیاریەکان لەسەر PE:

- بۆ ویندۆز

https://docs.microsoft.com/en-us/windows/win32/debug/pe-format

- بۆ لینۆکس:

www.skyfree.org/linux/references/ELF_Format.pdf

- چەند زانیاریەکی بەسود کە ئەم کارانە ئەکا،

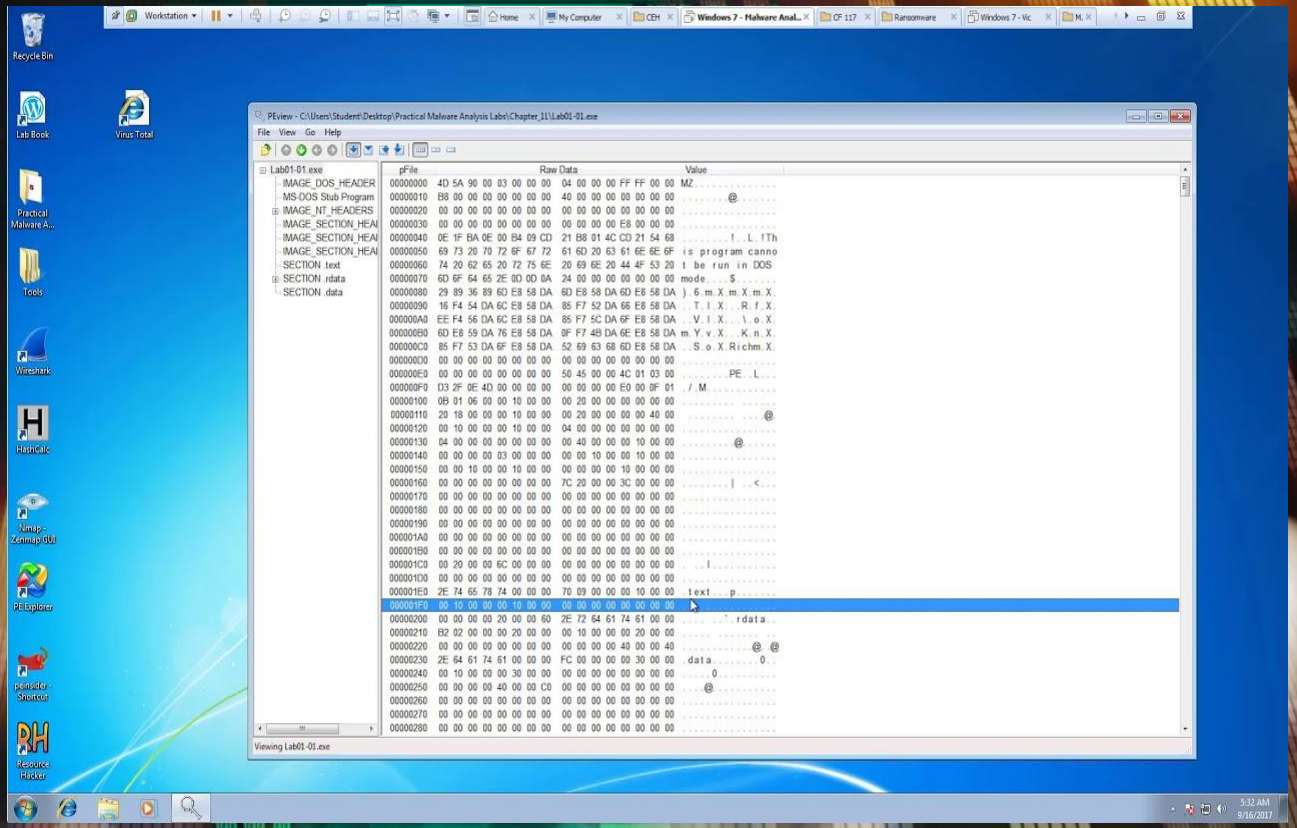
- Imports
- Exports
- Metadata
- Resources

PE Format

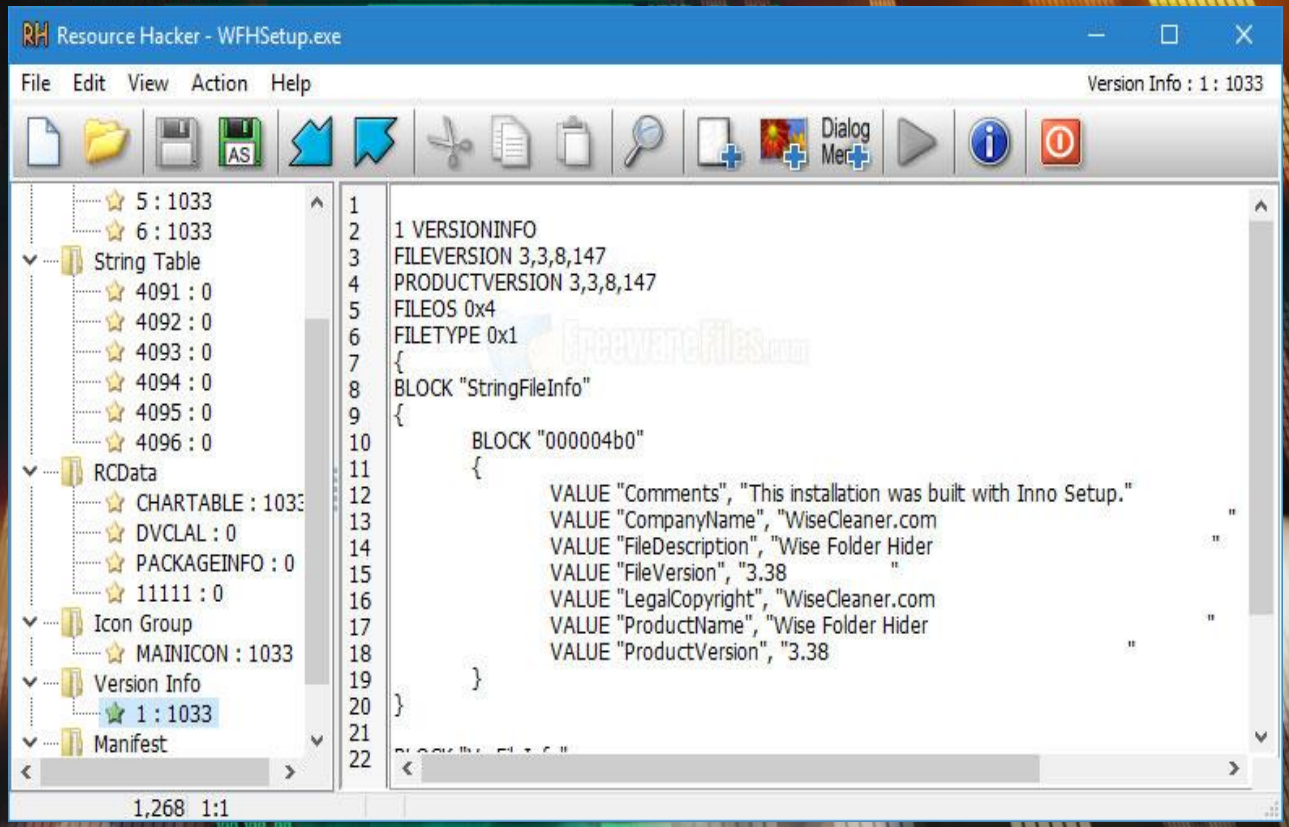
- بەرنامەکان:

- PEview- Wayne Radburn:
  http://www.magma.ca/~wir/
- PEBrowse Professional – Russ Osterlund:
  http://www.smidgeonsoft.com
- Objdump-Cygwin:
  http://www.cygwin.com
- IDA Pro –DataRescue:
  http://www.datarescue.be
- Resource Hacker –Angus Johnson:
  http://www.angusj.com/resourcehacker/

PEview


PEview - C:\Users\Student\Desktop\Practical Malware Analysis Labs\Chapter_11\Lab01-01.exe
File View Go Help
Lab01-01.exe
IMAGE_DOS_HEADER
MS-DOS Stub Program
IMAGE_NT_HEADERS
IMAGE_SECTION_HEAI
IMAGE_SECTION_HEAI
IMAGE_SECTION_HEAI
SECTION .text
SECTION .rdata
SECTION .data
pFile
Raw Data
Value
Viewing Lab01-01.exe

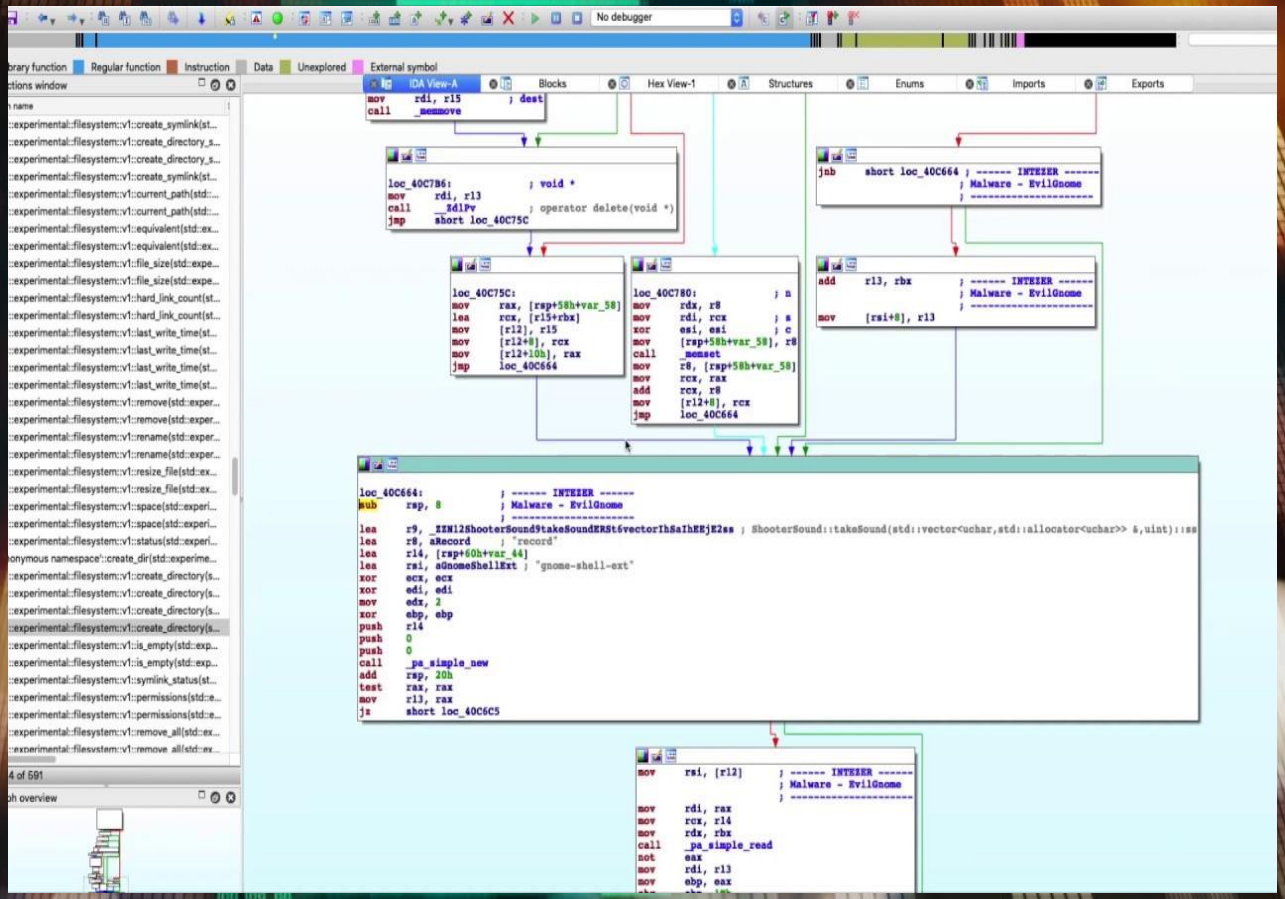
Resource Hacker



Disassembly

- به بەکارهێنانی disassemblers کان ئەتوانین کۆدی بەرنامەکان ببینین ئەمەش ئەچێتە ڕیزی reverse .
- چەندین بەرنامە هەیە بۆ پیشاندانی کۆدەکانی x86 وەك، Objdump, Python w/ libdisassemble, IDA Pro
- بەلام زۆینەی خەڵك تاوەکو ئێستاش IDA Pro بەکارئەهێنن.
- کاری disassembly ئەکرێت قورس بێت و ئازاربەخش بێت وە کاتێکی زۆریشی ئەوێ.
ئەوەی لەسەر تۆیە ئامانجەکات لە مێشك بێت و ساردنەبێتەوە.

IDA PRO


No debugger
Regular function
Instruction
Data
Unexplored
External symbol
IDA View-A
Blocks
Hex View-1
Structures
Enums
Imports
Exports
loc_40C7B6:
loc_40C75C:
loc_40C780:
loc_40C664:
_ZZN12ShooterSound9takeSoundERSt6vectorIhSaIhEEjE2ss

Dynamic Analysis

- ئەتوانیت سوود لە Static Analysis وەربگریت وە لە سەرەوە کەمێك زانیاریت پەیداکرد.
- بە هۆی Static Analysis ئەتوانیت وەلامی پرسیارەکان بەیتەوە بەلام بە گشتی سەختە.
- لێرەیا بە زۆری گرنگی بەوە ئەدەی کە ئایا مالوێر چی ئەکا وە چۆن کارئەکا.
- لە Dynamic Analysis ڕاستەوخۆ کار لەسەر بەرنامەکان ئەکرێ واتا لەوکاتەی کە کراوەن.

دروستکردنی ناوچەیەکی سەلامەت.

- لە static analysis گرنگی بە دروستکردنی ناوچەیەکی سەلامەت نە ئەدرا بۆ مالوێر ئنالسیس.
- بێگومان وەك هەمیشە پێویستت بە VMware ئەبێ ئەتوانیت چەند سیستەمێك ئامادەبکەیت بۆ ئەم کارە.
- بێگومان ئەبێ چەندین جار بەرنامەکە بکەینەوەو دایخەین بەهۆی بەکارهێنانی snapshots کارەکان ئاسانترە.

System Monitoring

- لەسەرت پێویستە کا چاودێری ئەمانە بکەیت:

Registry Activity
File Activity
Process Activity
Network Traffic

- بەرنامەکان:

SysInternals Process Monitor

Wireshark

- چەندین بەرنامەیتر کە لە دواییدا باسیان ئەکەم.

Process Monitor

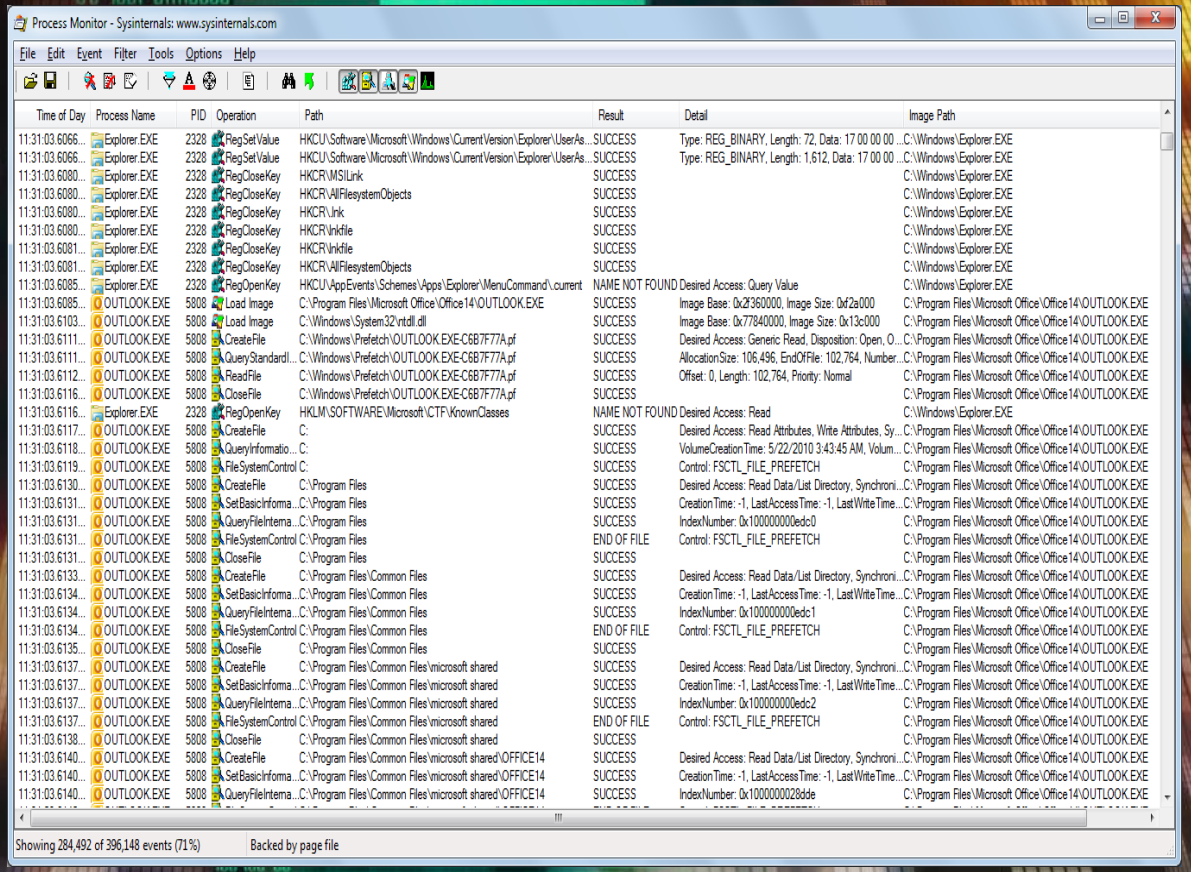
- به گشتی چاودێری یاخود ریکۆرد کردنی ئەو کارانە ئەکا کە لەنێو کۆمپیوتەرەکەتدا ئەکرێ وەک، Registry، هتد...

- هیچ کارێك بەبێ Process Monitor ناکرێ وە پێویستە بەردەوام چاودێری ئەم بەشە بکەیت.

- Filemon/Regmon:

بە گشتی ئەمانە چاودێری هەموو شتێك ئەکەن واتا ئەوەی ڕوبدات ئەمانە ریکۆردی ئەکەن.

Process Monitor



Wireshark

- بە گشتی ئەمەیان پەیوەندی بە ئینتەرنێتەوە هەیە چاودێری یاخود ئەو کارانە ریکۆرد ئەکا کە پەیوەندی بە ئینتەرنێتەکەتەوە هەیە.
- ئەمەیان هیچ پەیوەندیەکی بە Process Monitor نییە.
- ئەوەی لەسەرتۆ پێویستە بەکارهێنانی هەردوکیانە لە یەک کاتدا.

باشترین ڕێگا بۆ Dynamic Analysis

- بەکارهێنانی هەردوو بەرنامەیە لە یەک کاتدا بۆ ئەوەی بە تەواوی کۆنترۆڵی کارەکان بکەیت.

چەند بەرنامەیەکیتر

- Port Explorer

https://download.cnet.com/DiamondCS-Port-Explorer/3000-2085_4-10191769.html

- Malcode Analyst Pack

https://github.com/dzzie/MAP

- Paros

https://sourceforge.net/projects/paros/

- Fiddler

https://www.telerik.com/fiddler

- Norman Sandbox

https://www.norman.com/en-ww/homepage

چاودێریکردنی سیستەم

- بەم ڕێگایانەی کە لەسەرەوە باسم کرد ئەتوانیت وملامی زۆربەی پرسیارەکان بەیتەوە بەلام هێشتا ماوە تاوەکو وملامی هەموو پرسیارەکان بەیتەوە.
- لێرەیا پێویستمان بە چەند Debugger ئەبێت، ئەتوانیت ئەمانە بەکاربهێنیت:

Windbg (Microsoft)
Ollydbg (OlehYuschuk)
Ida Pro (Datarescue)

Armored Malware

مەبەست لێرەیا ئەم مالوێرانەیە کا پارێزراون

تایبەتمەندیەکانی

- Encryption
- Compression
- Obfuscation
- Anti-Patching:
- CRC Checking
- Anti-Tracing:
- SoftICE, ICEDumpDetection Code
- Crashes OS if they areFound in Memory
- Anti-Unpacking
- Anti-Vmware
- Polymorphic/Self-Mutating
- Restrictive Dates
- Password Protected
- Configuration Files

Packers

- تێپەراندنی دژە ڤایرۆس.
- پاراستنی لە reverse engineering.
- بە گشتی بە کارێکی پێویست دائەنرێ بۆ پرۆگرامەر ئەگەر پرۆگرامەرێك نەتوانێ بەرهەمەکەی بپارێزێت ئەوە زیانێکی زۆری پێئەگا.

Packers

- UPack by Dwing. 08.IV.2005.
- Mew by NorthFox. 22.IX.2004.
- UPX by Laszlo & Markus.03.VII.2004.
- Packman by bubba. 27.II.2005.
- EZIP by Jonathan Clark.21.VII.2001.
- PE_PaCK by ANAKiN. 12.I.1999.
- ESC by bart. 24.V.2004.
- Dropper by Gem. 13.III.2005.
- VMProtect.
- Andromeda.
- The Enigma Protector.
- CExe by Scott. 20.III.2003.
- PE Diminisher by TERAPHY.11.IX.1999.

Packers

- PECRYPT32 by random, killaand acpizer. 12.I.1999.
- PESpin by cyberbob. 09.III.2005.
- NSPack by North star Tech.05.VI.2005.
- eXPressor by CCSoftLabs.28.III.2005.
- Thinstall by Jonathan Clark.29.III.2005
- PE Bundle by Jeremy Collake.12.III.2004.
- PE Compact by DevelTek.06.IV.2005.
- AS-Pack (shareware)bySolodovnikovAlexey. 07.I.2002.
- NeoLite (shareware)byNeoWorx Inc. 04.IV.1999.
- WWPack32 by PiotrWarezak.07.VII.2000.
- ARM Protector by SMoKE.22.IX.2004.

Packing کاریگەریەکانی

- هیچ strings نامێنێ.
- ئەمانەش دیارنامێنن.

- Kernel32.dll
- LoadLibrary
- GetProcAddress
- VirtualAlloc
- VirtualFree

- شاردەنەوەی کۆدەکان یاخود تێکدانی کۆدەکان.
- گۆڕینی کێشی بەرنامەکە بۆ کێشێکی نائاسیی.
- لەگەڵ چەند بەشێکیتر.

Packing کاریگەریەکانی

Packed:

RVA	Name
0101AE3Ch	kernel32.dll

RVA	Hint	Name
0101AE00h	0000h	LoadLibraryA
0101AE04h	0000h	GetProcAddress
0101AE08h	0000h	VirtualAlloc
0101AE0Ch	0000h	VirtualFree

Unpacked:

RVA	Name
01007AACh	comdlg32.dll
01007AFAh	SHELL32.dll
01007B3Ah	WINSPOOL.DRV
01007B5Eh	COMCTL32.dll
01007C76h	msvcrt.dll
01007D08h	ADVAPI32.dll
010080ECh	KERNEL32.dll
0100825Eh	GDI32.dll
0100873Ch	USER32.dll

RVA	Hint	Name
010012C4h	000Fh	PageSetupDlgW
010012C8h	0006h	FindTextW
010012CCh	0012h	PrintDlgExW
010012D0h	0003h	ChooseFontW
010012D4h	0008h	GetFileTitleW
010012D8h	000Ah	GetOpenFileNameW
010012DCh	0015h	ReplaceTextW
010012E0h	0004h	CommDlgExtendedError
010012E4h	000Ch	GetSaveFileNameW

Packing کاریگەریەکانی

Unpacked: Entropy (st dev) 0.7653

Name	Virtual Size	Virtual Address	Size of Raw Data	Pointer to Raw Data	Characteristics	Pointing Directories
.text	00007748h	01001000h	00007800h	00000400h	60000020h	Import Table; Debug Data; Load Config...
.data	00001BA8h	01009000h	00000800h	00007C00h	C0000040h	
.rsrc	00008958h	0100B000h	00008A00h	00008400h	40000040h	Resource Table

Packed: Entropy (st dev) 1.0666

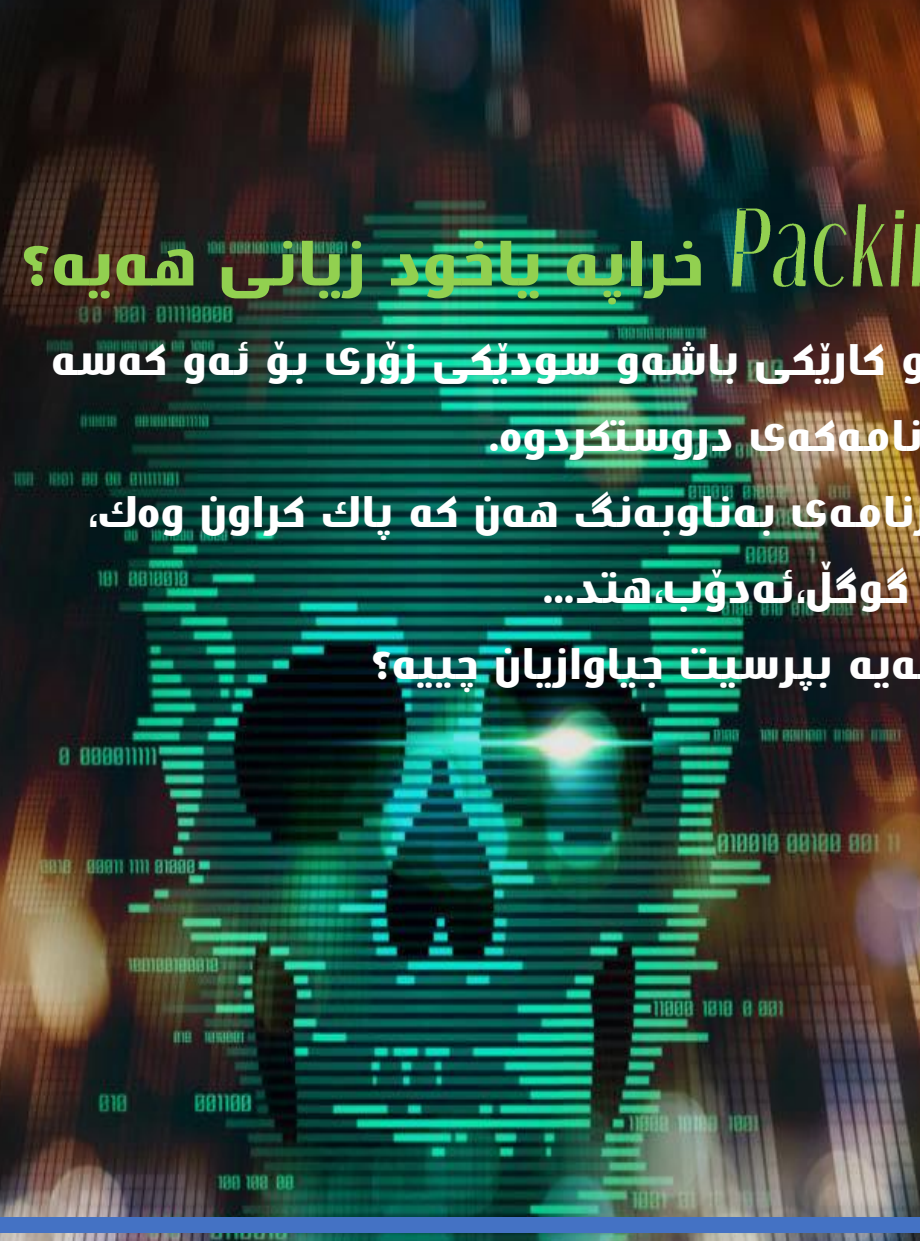
Name	Virtual Size	Virtual Address	Size of Raw Data	Pointer to Raw Data	Characteristics	Pointing Directories
.text	00013000h	01001000h	00004200h	00000400h	E0000060h	
.rsrc	00008000h	01014000h	00007C00h	00004600h	E0000020h	Import Table; Resource Table

Strings of Packed Binary

```
C:\analysis>strings sak.exe
Strings v2.1
Copyright (C) 1999-2003 Mark Russinovich
Systems Internals - www.sysinternals.com
!Windows Program
$PE
@.data
.idata
$s!
;Ot
(!B
KERNEL32.dll
LoadLibraryA
GetProcAddress
DM.D
&DS
d'D
~E-
```

باشە Packing خراپە یاخود زیانی هەیە؟

- نەخێر بەڵکو کارێکی باشەو سودێکی زۆری بۆ ئەو کەسە هەیە کە بەرنامەکەی دروستکردوە.
- چەندین بەرنامەی بەناوبەنگ هەن کە پاك کراون وەك، بەرنامەکانی گوگڵ،ئەدۆب،هتد...
- باشە لەوانەیە بپرسیت جیاوازیان چییە؟



جیاوازیان چییە؟

- زانیاری کۆبکەرەوە لەسەر Static & PE.
- هەوڵبە زانیاری دەرەکیشت هەبێت.
- لەگەڵ ناسینەوە کۆدەکان یاخود ڕێژەکان.

Unpacking

- Ollydbg>OllyScript>OllyDump
- Ollydbg>bp in Library >OllyDump
- UnFSG, upx, etc
- PEiD
- ProcDump
- OEP Finder
- Etc...

Unpackers

- Ollydbg with the Ollydumpplugin and a variety of OllyScripts.
- IDAPro with the “Universal UnpackerPlugin.
- Generic Unpacker Win32 by ChristophGabler. 31.VII.2001.Win32 Intro by VitalyEvseenko. 21.IX.1999.
- UN_PACK by Snow Panther. 21.IV.2003.
- UNPE_SHiELD by G_RoM. 1.VI.1999 de_CodeCrypt by xOANINO.10.V.2000.
- Ni2Untelock by Ni2. 31.XII.2000.
- DeYoda by C_ripper. 18.II.2001.

- UnPEProt by Lorian, 23.I.1999.
- DePE_PACK by Unknown One, 03.V.2002.
- Un_FSG by SMoKE, 12.I.2003.
- un_ASPack by dtg, 26.VIII.1999.
- StealthKiller by Snow Panther, 04.IX.2002.

بێگومان لەمانە زیاتر هەیە وە ڕێگای ئاسان بۆ هەمویان، بۆ ئەمە ئەتوانن سوود لە یوتوب و گوگڵ وەرگرن.

ئەتوانن سوود لەم خشتانە وەربگرن بۆ ئەوەی بزانن ڕێژەی ئەم 14 کۆدە چۆنە،

Opcode	Goodware	Kernel RK	User RK	Tools	Bot	Trojan	Virus	Worms
mov	25.3%	37.0%	29.0%	25.4%	34.6%	30.5%	16.1%	22.2%
push	19.5%	15.6%	16.6%	19.0%	14.1%	15.4%	22.7%	20.7%
call	8.7%	5.5%	8.9%	8.2%	11.0%	10.0%	9.1%	8.7%
pop	6.3%	2.7%	5.1%	5.9%	6.8%	7.3%	7.0%	6.2%
cmp	5.1%	6.4%	4.9%	5.3%	3.6%	3.6%	5.9%	5.0%
jz	4.3%	3.3%	3.9%	4.3%	3.3%	3.5%	4.4%	4.0%
lea	3.9%	1.8%	3.3%	3.1%	2.6%	2.7%	5.5%	4.2%
test	3.2%	1.8%	3.2%	3.7%	2.6%	3.4%	3.1%	3.0%
jmp	3.0%	4.1%	3.8%	3.4%	3.0%	3.4%	2.7%	4.5%
add	3.0%	5.8%	3.7%	3.4%	2.5%	3.0%	3.5%	3.0%
jnz	2.6%	3.7%	3.1%	3.4%	2.2%	2.6%	3.2%	3.2%
retn	2.2%	1.7%	2.3%	2.9%	3.0%	3.2%	2.0%	2.3%
xor	1.9%	1.1%	2.3%	2.1%	3.2%	2.7%	2.1%	2.3%
and	1.3%	1.5%	1.0%	1.3%	0.5%	0.6%	1.5%	1.6%

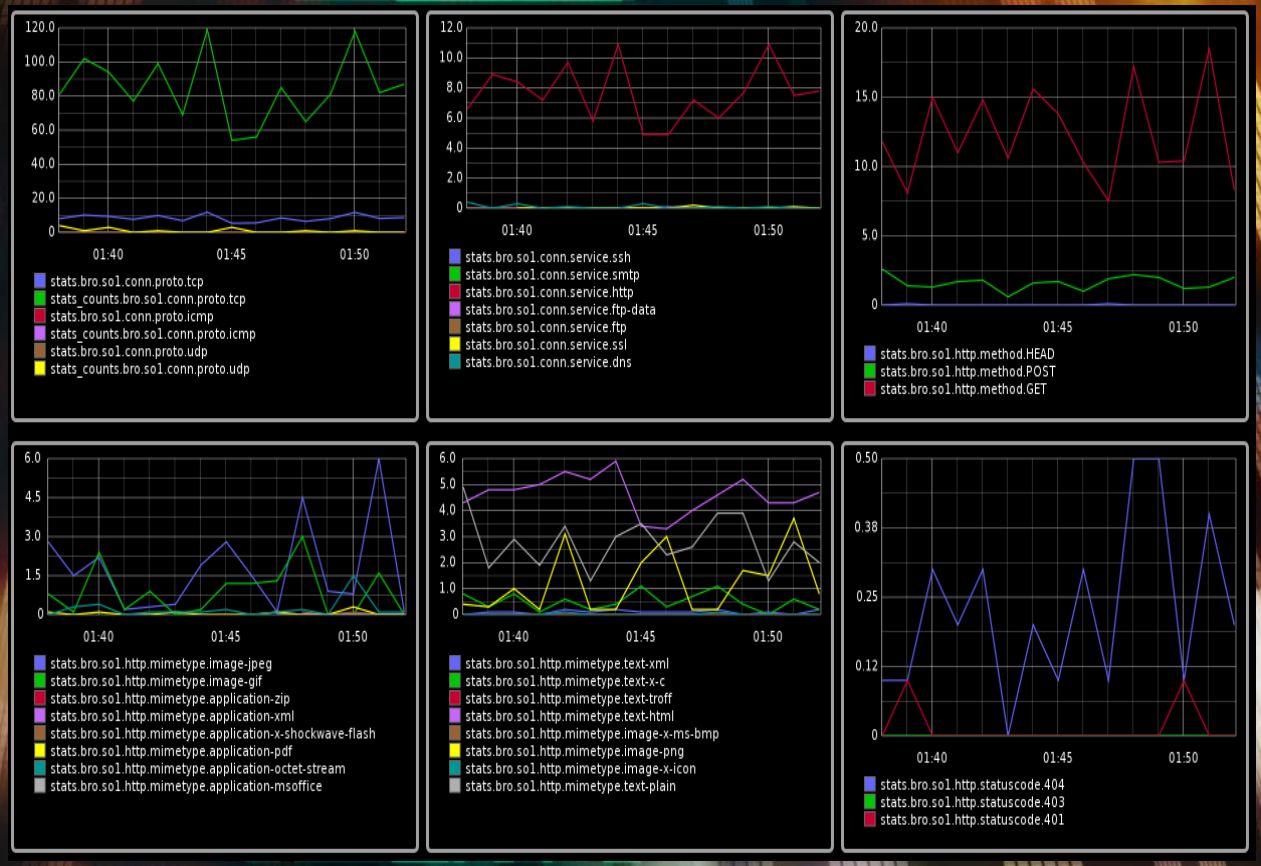
Opcode	Goodware	Kernel RK	User RK	Tools	Bot	Trojan	Virus	Worms
bt	30	0	34	47	70	83	0	118
fdivp	37	0	0	35	52	52	0	59
fild	357	0	45	0	133	115	0	438
fstcw	11	0	0	0	22	21	0	12
imul	1182	1629	1849	708	726	406	755	1126
int	25	4028	981	921	0	0	108	0
nop	216	136	101	71	7	42	647	83
pushf	116	0	11	59	0	0	54	12
rdtsc	12	0	0	0	11	0	108	0
sbb	1078	588	1330	1523	431	458	1133	782
setb	6	0	68	12	22	52	0	24
setle	20	0	0	0	0	21	0	0
shld	22	0	45	35	4	0	54	24
std	20	272	56	35	48	31	0	95

چەند بەرنامەیەك كە هی ئەم ساڵن بۆ كاری مالوێر ئنالسیس بەكاریەن

- Cuckoo Sandbox Automated Malware Analysis Tool
- Zeek Network Security Monitor
- Netcat Dynamic Malware Analysis Tool
- Yara Rules
- Netcat Dynamic Malware Analysis Tool

Cuckoo Sandbox Automated Malware Analysis Tool

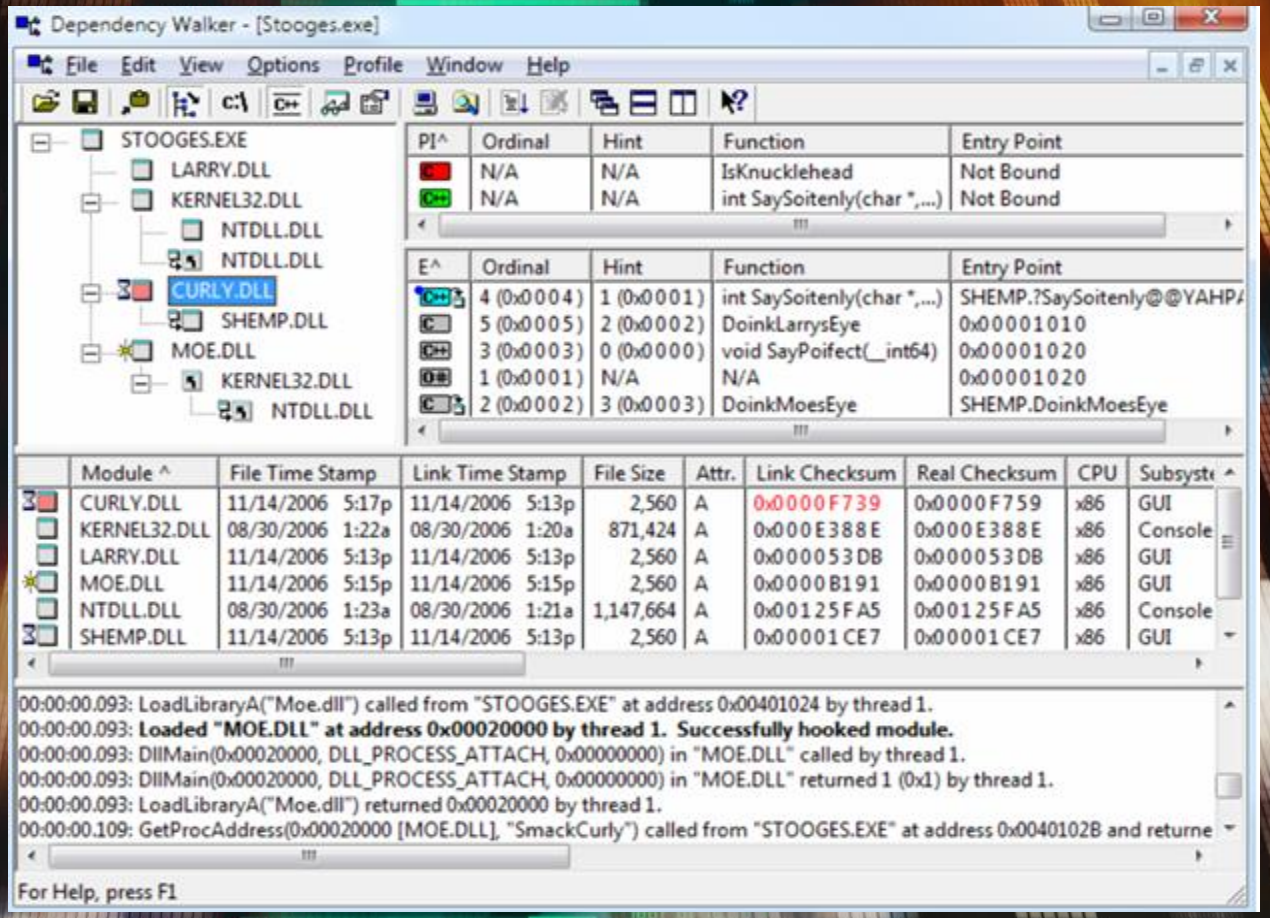
Zeek Network Security Monitor

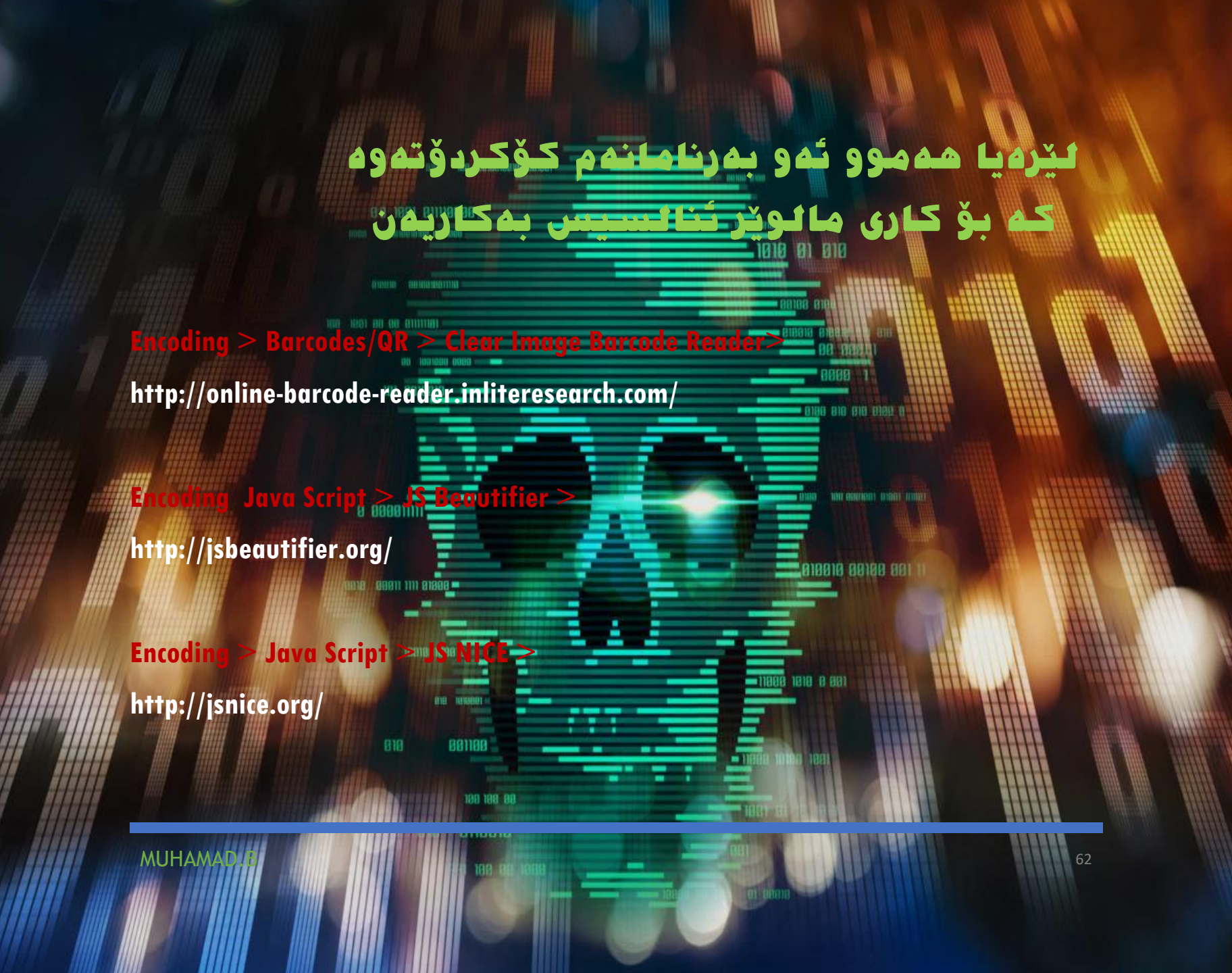


Netcat Dynamic Malware Analysis Tool

Yara Rules

Dependency Walker Malware Analysis





لێرەیا هەموو ئەو بەرنامانەم کۆکردۆتەوە کە بۆ کاری مالوێرئنالسیس بەکاریەن

Encoding > Barcodes/QR > Clear Image Barcode Reader>

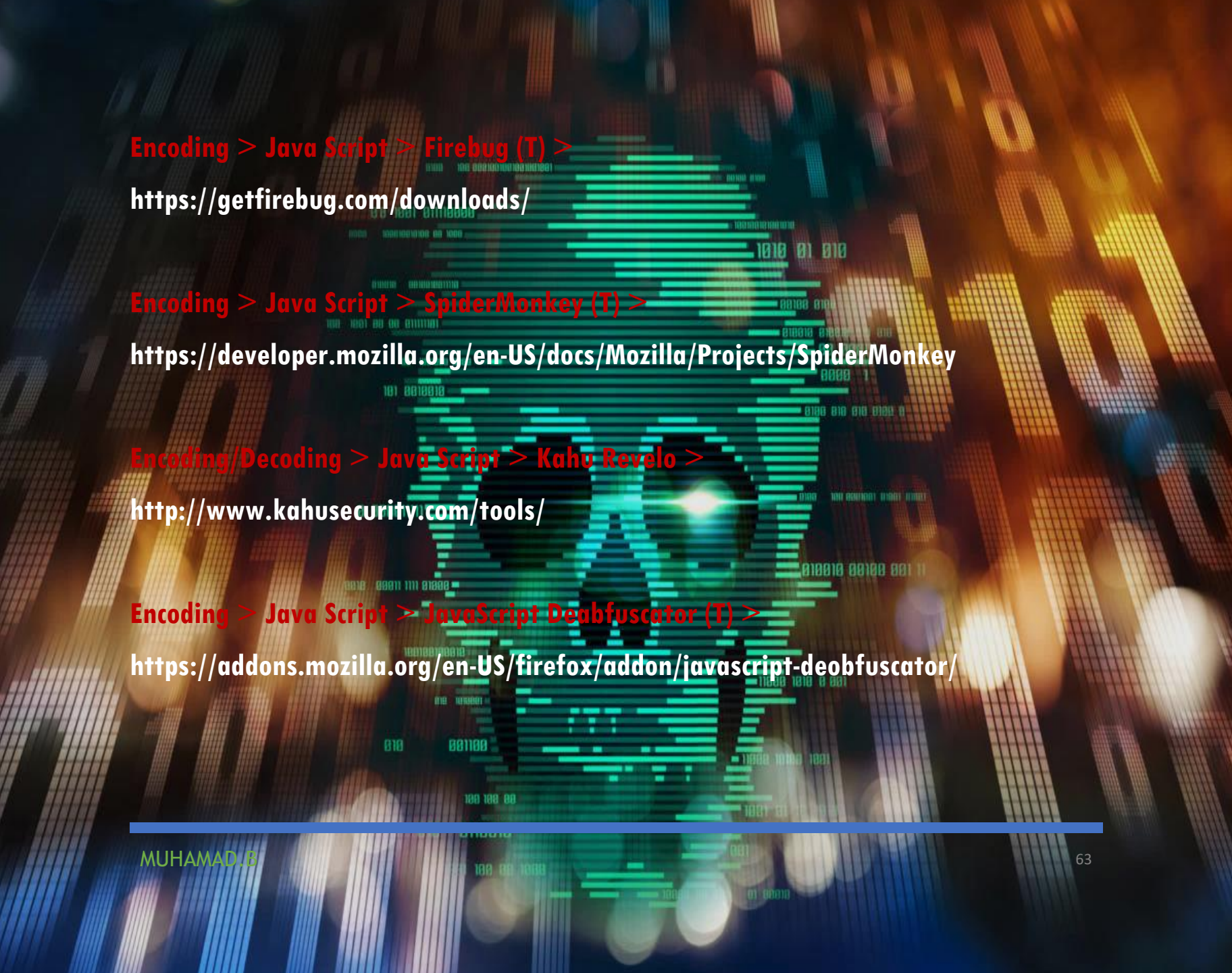
http://online-barcode-reader.inliteresearch.com/

Encoding Java Script > JS Beautifier >

http://jsbeautifier.org/

Encoding > Java Script >JS NICE>

http://jsnice.org/



Encoding > Java Script > Firebug (T) >

https://getfirebug.com/downloads/

Encoding > Java Script > SpiderMonkey (T) >

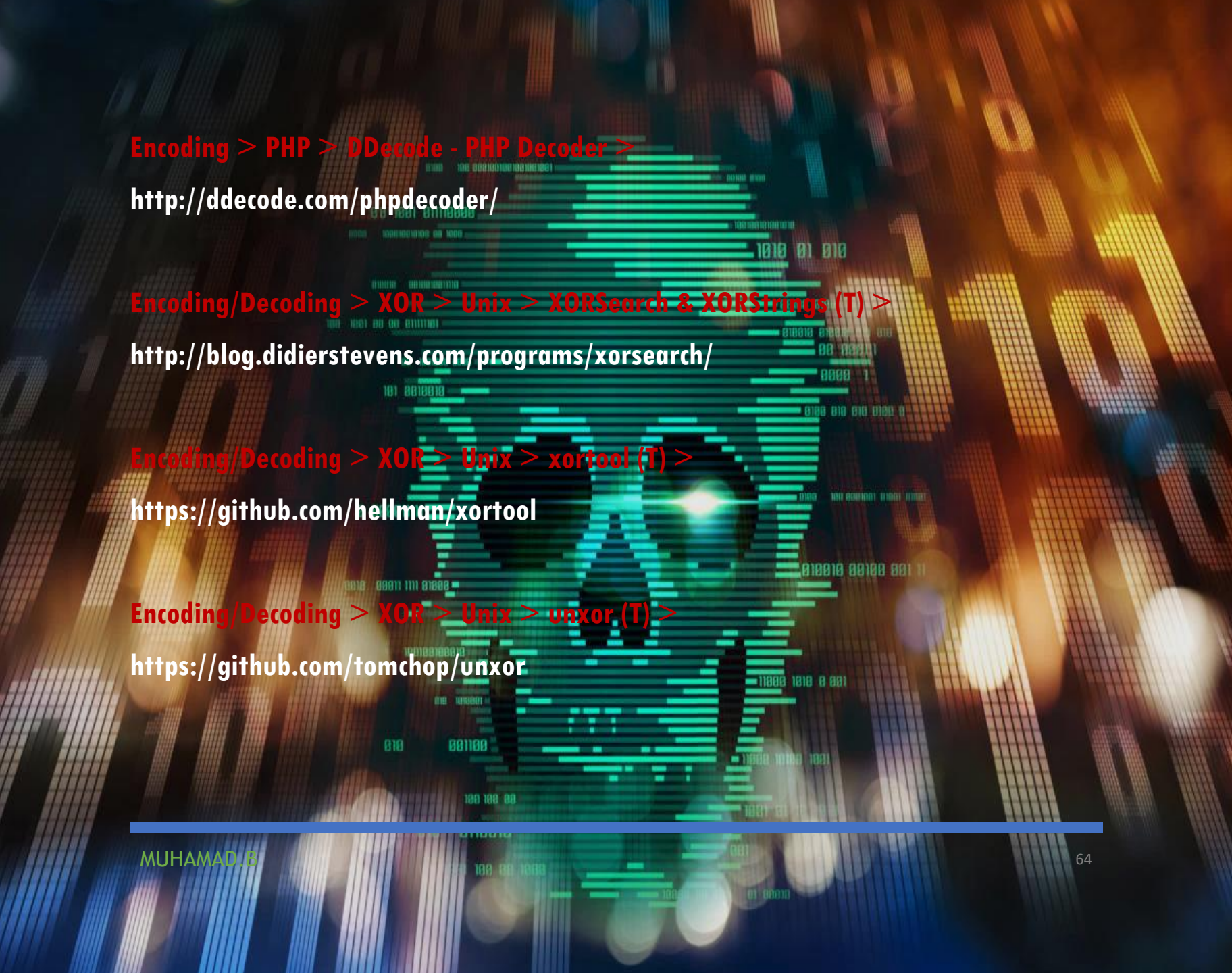
https://developer.mozilla.org/en-US/docs/Mozilla/Projects/SpiderMonkey

Encoding/Decoding > Java Script > Kahu Revelo >

http://www.kahusecurity.com/tools/

Encoding > Java Script > JavaScript Deabfuscator (T) >

https://addons.mozilla.org/en-US/firefox/addon/javascript-deobfuscator/



Encoding > PHP > DDecode - PHP Decoder >

http://ddecode.com/phpdecoder/

Encoding/Decoding > XOR > Unix > XORSearch & XORStrings (T) >

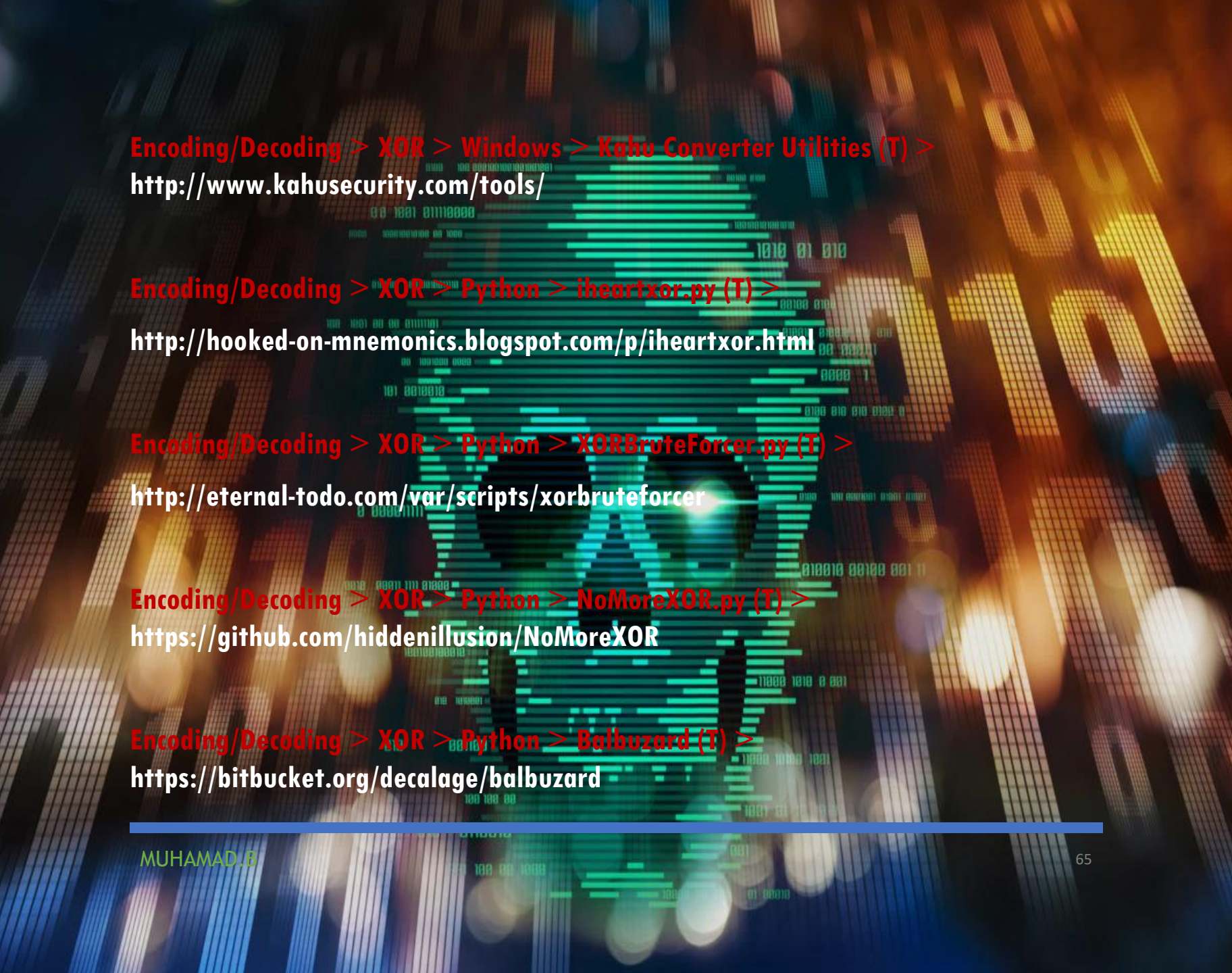
http://blog.didierstevens.com/programs/xorsearch/

Encoding/Decoding > XOR > Unix > xortool (T) >

https://github.com/hellman/xortool

Encoding/Decoding > XOR > Unix > unxor (T) >

https://github.com/tomchop/unxor



Encoding/Decoding > XOR > Windows > Kahu Converter Utilities (T) >

http://www.kahusecurity.com/tools/

Encoding/Decoding > XOR > Python > iheartxor.py (T) >

http://hooked-on-mnemonics.blogspot.com/p/iheartxor.html

Encoding/Decoding > XOR > Python > XORBruteForcer.py (T) >

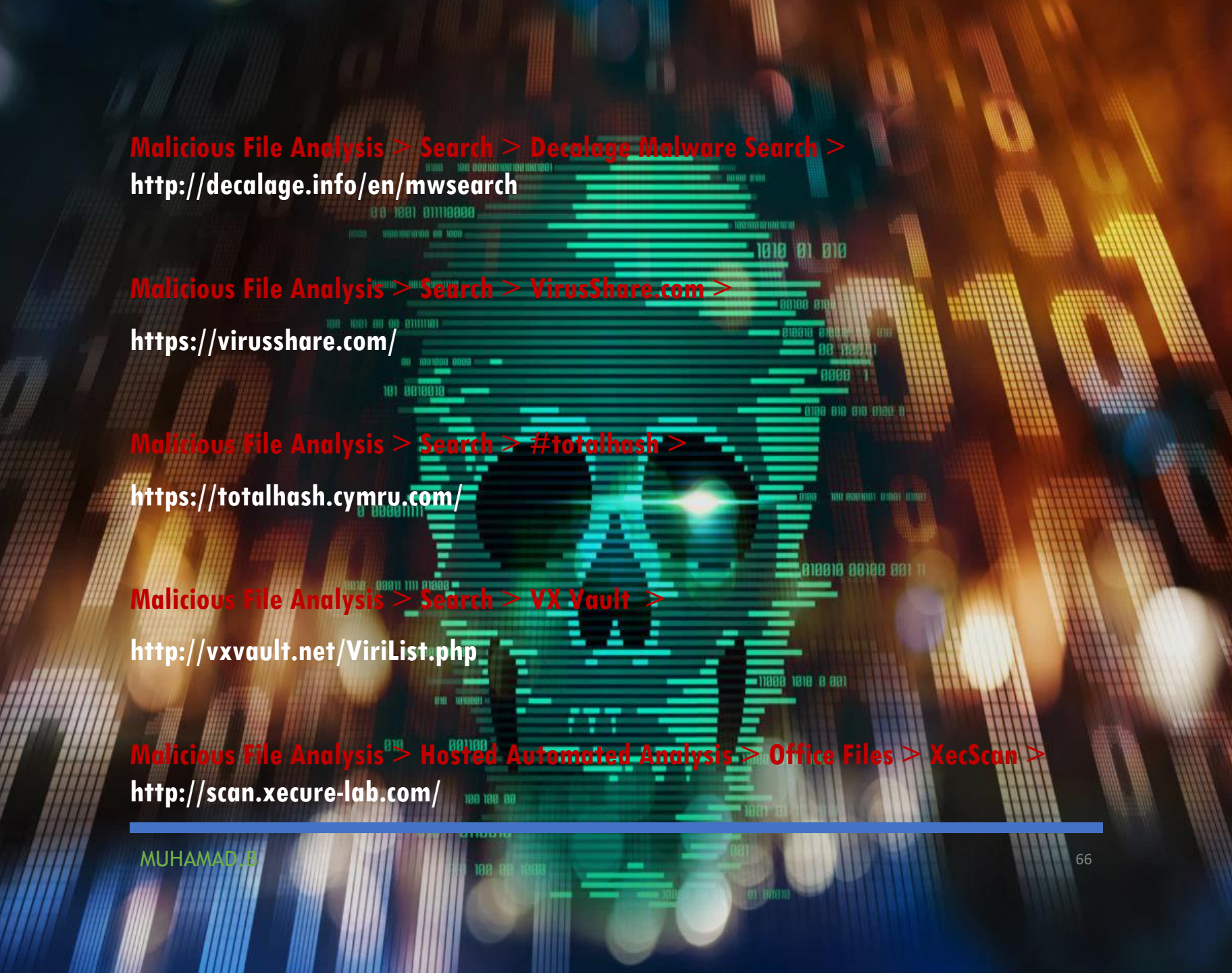
http://eternal-todo.com/var/scripts/xorbruteforcer

Encoding/Decoding > XOR > Python > NoMoreXOR.py (T) >

https://github.com/hiddenillusion/NoMoreXOR

Encoding/Decoding > XOR > Python > Balbuzard (T) >

https://bitbucket.org/decalage/balbuzard



Malicious File Analysis > Search > Decalage Malware Search >

http://decalage.info/en/mwsearch

Malicious File Analysis > Search > VirusShare.com >

https://virusshare.com/

Malicious File Analysis > Search > #totalhash >

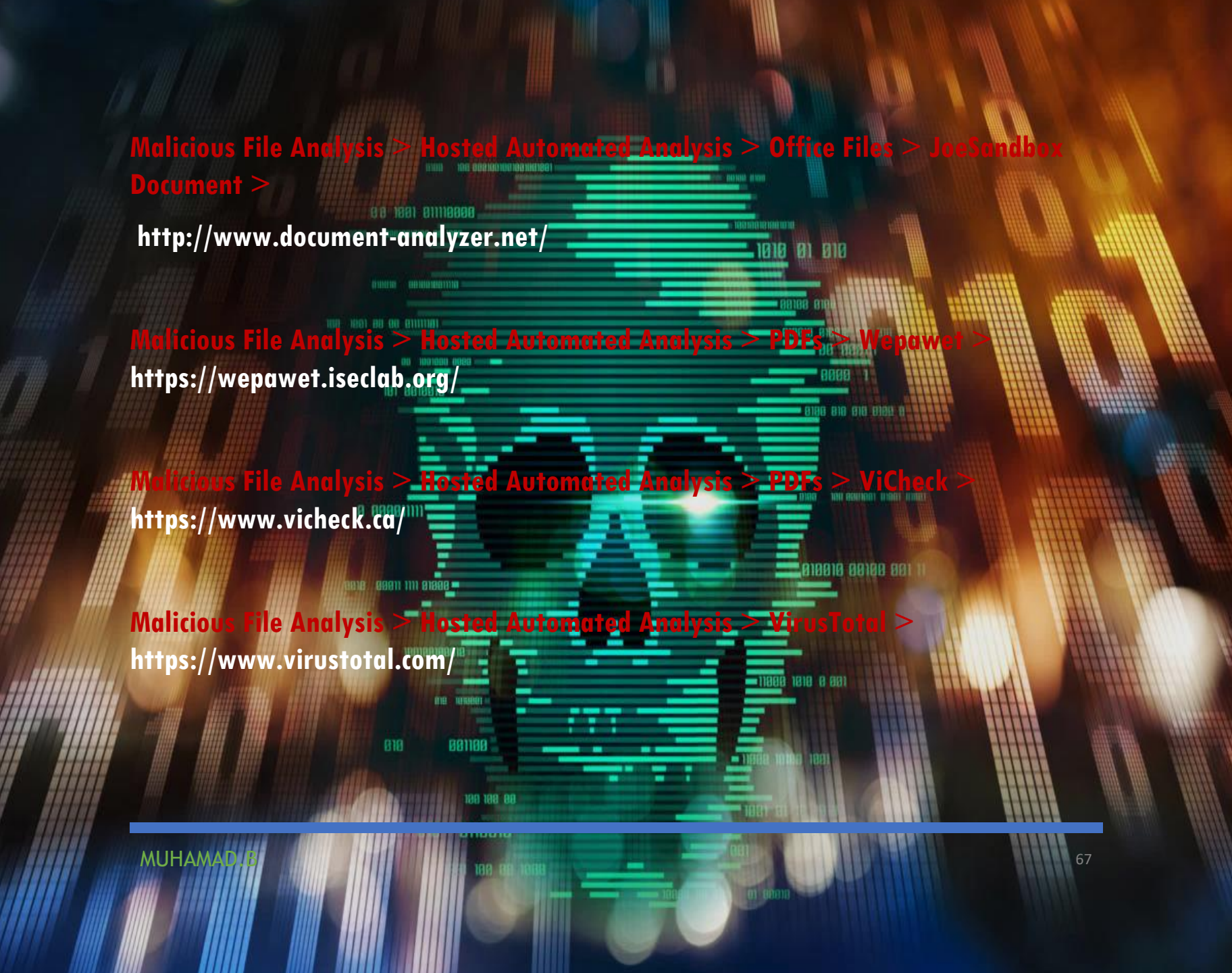
https://totalhash.cymru.com/

Malicious File Analysis > Search > VX Vault >

http://vxvault.net/ViriList.php

Malicious File Analysis > Hosted Automated Analysis > Office Files > XecScan >

http://scan.xecure-lab.com/



Malicious File Analysis > Hosted Automated Analysis > Office Files > JoeSandbox Document >

http://www.document-analyzer.net/

Malicious File Analysis > Hosted Automated Analysis > PDFs > Wepawet >

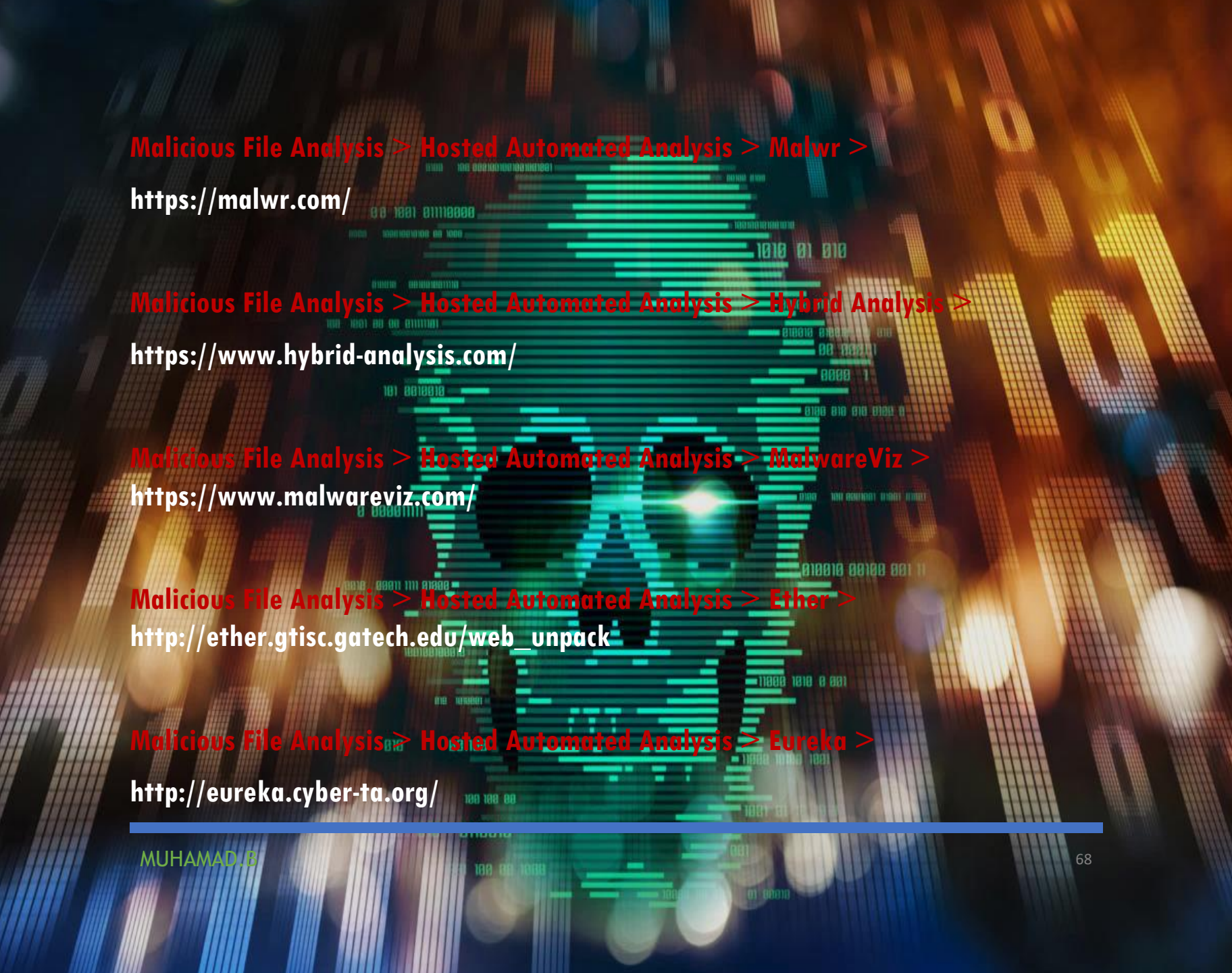
https://wepawet.iseclab.org/

Malicious File Analysis > Hosted Automated Analysis > PDFs > ViCheck >

https://www.vicheck.ca/

Malicious File Analysis > Hosted Automated Analysis > VirusTotal >

https://www.virustotal.com/



Malicious File Analysis > Hosted Automated Analysis > Malwr >

https://malwr.com/

Malicious File Analysis > Hosted Automated Analysis > Hybrid Analysis >

https://www.hybrid-analysis.com/

Malicious File Analysis > Hosted Automated Analysis > MalwareViz >

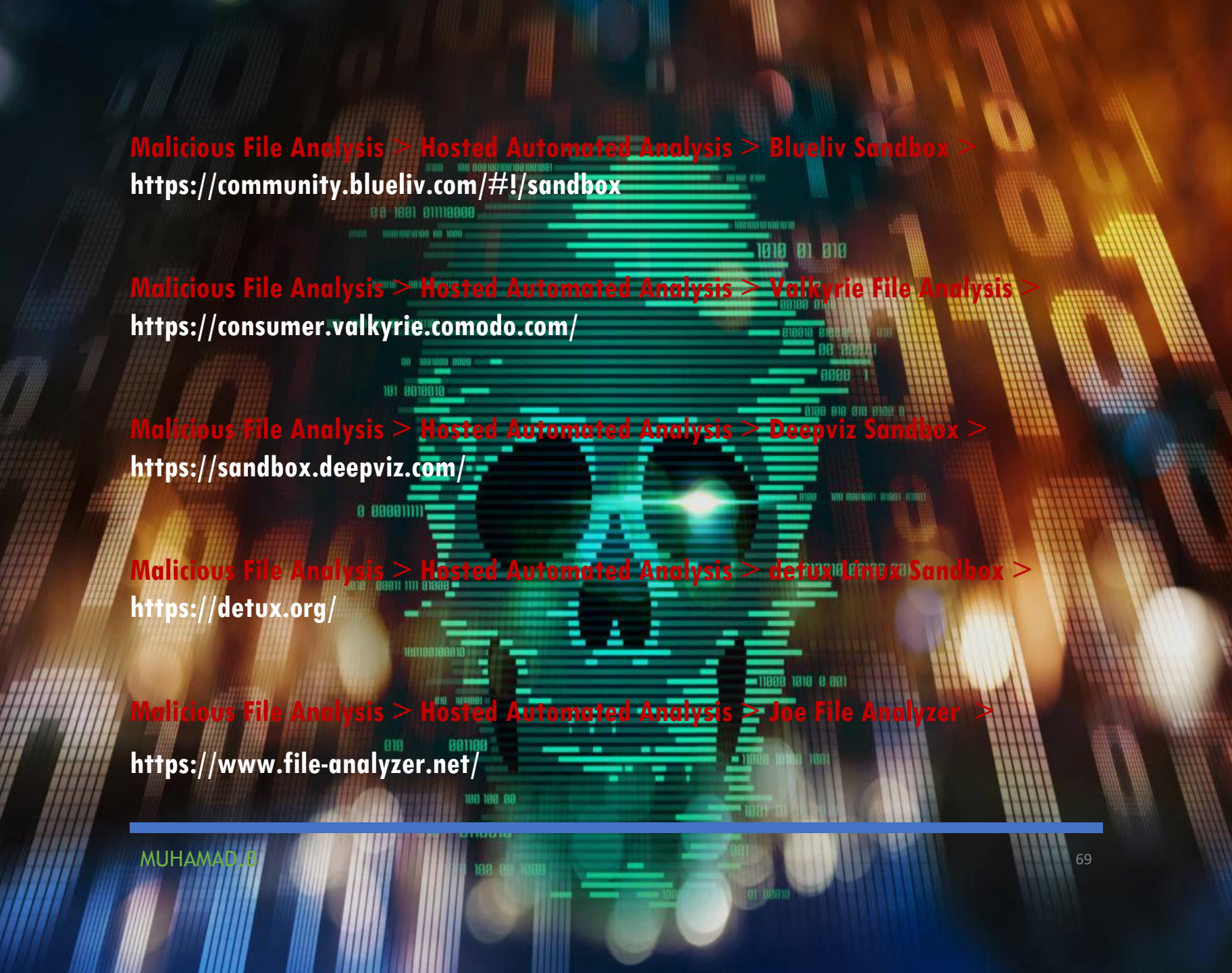
https://www.malwareviz.com/

Malicious File Analysis > Hosted Automated Analysis > Ether >

http://ether.gtisc.gatech.edu/web_unpack

Malicious File Analysis > Hosted Automated Analysis > Eureka >

http://eureka.cyber-ta.org/



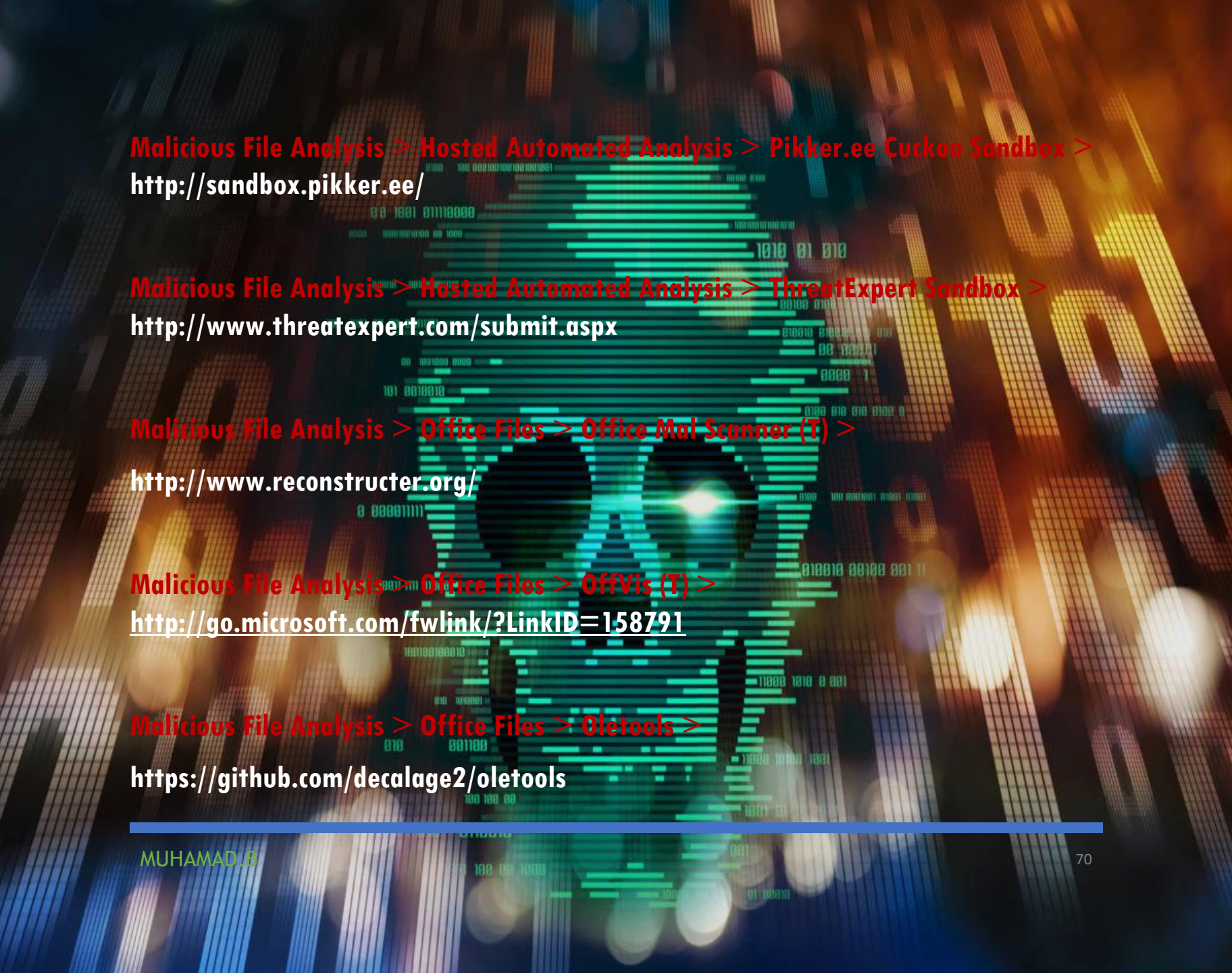
Malicious File Analysis > Hosted Automated Analysis > Blueliv Sandbox >
https://community.blueliv.com/#!/sandbox

Malicious File Analysis > Hosted Automated Analysis > Valkyrie File Analysis >
https://consumer.valkyrie.comodo.com/

Malicious File Analysis > Hosted Automated Analysis > Deepviz Sandbox >
https://sandbox.deepviz.com/

Malicious File Analysis > Hosted Automated Analysis > detux Linux Sandbox >
https://detux.org/

Malicious File Analysis > Hosted Automated Analysis > Joe File Analyzer >
https://www.file-analyzer.net/



Malicious File Analysis > Hosted Automated Analysis > Pikker.ee Cuckoo Sandbox >

http://sandbox.pikker.ee/

Malicious File Analysis > Hosted Automated Analysis > ThreatExpert Sandbox >

http://www.threatexpert.com/submit.aspx

Malicious File Analysis > Office Files > Office Mal Scanner (T) >

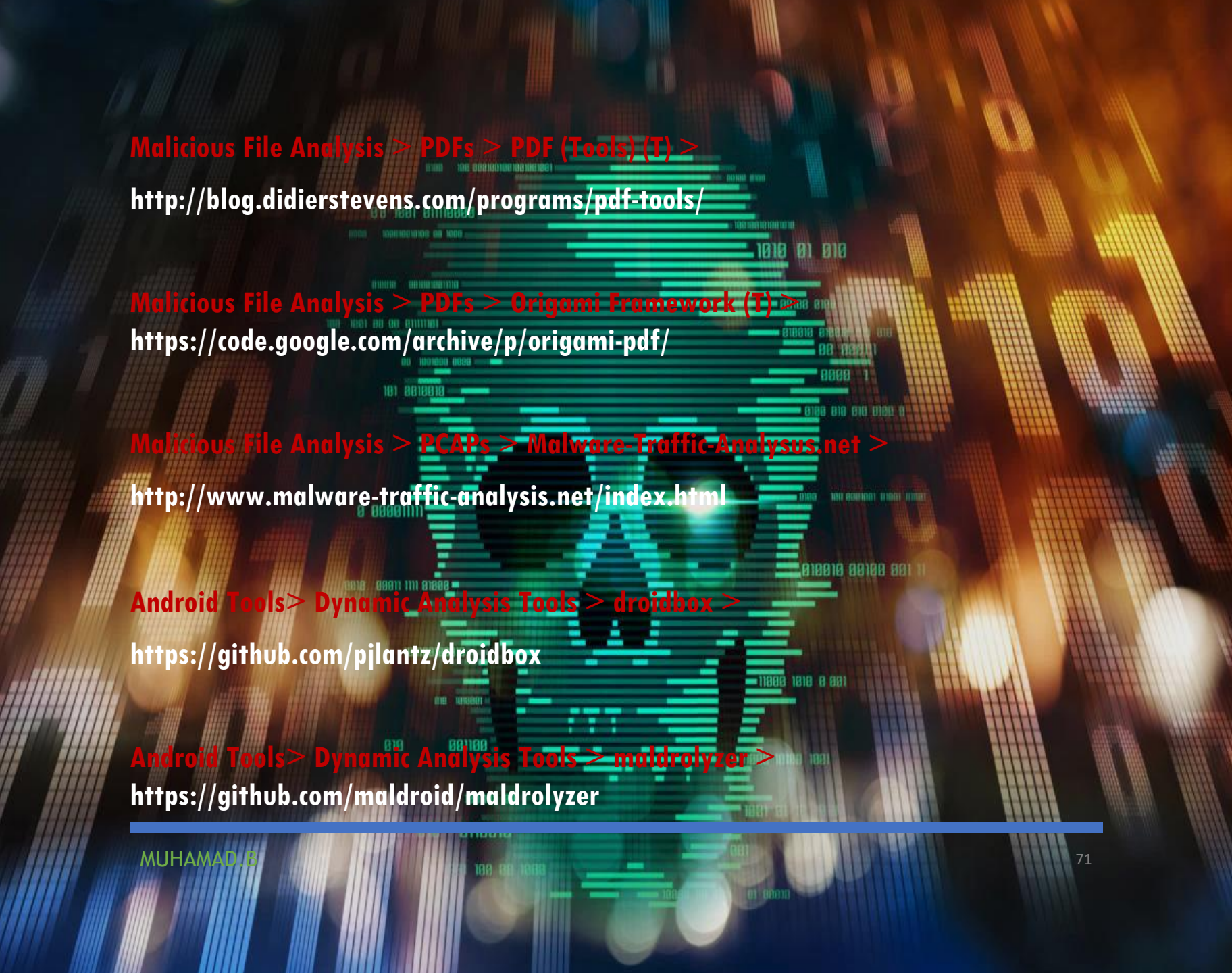
http://www.reconstructer.org/

Malicious File Analysis > Office Files > OffVis (T) >

http://go.microsoft.com/fwlink/?LinkID=158791

Malicious File Analysis > Office Files > Oletools >

https://github.com/decalage2/oletools



Malicious File Analysis > PDFs > PDF (Tools) (T) >

http://blog.didierstevens.com/programs/pdf-tools/

Malicious File Analysis > PDFs > Origami Framework (T) >

https://code.google.com/archive/p/origami-pdf/

Malicious File Analysis > PCAPs > Malware-Traffic-Analysus.net >

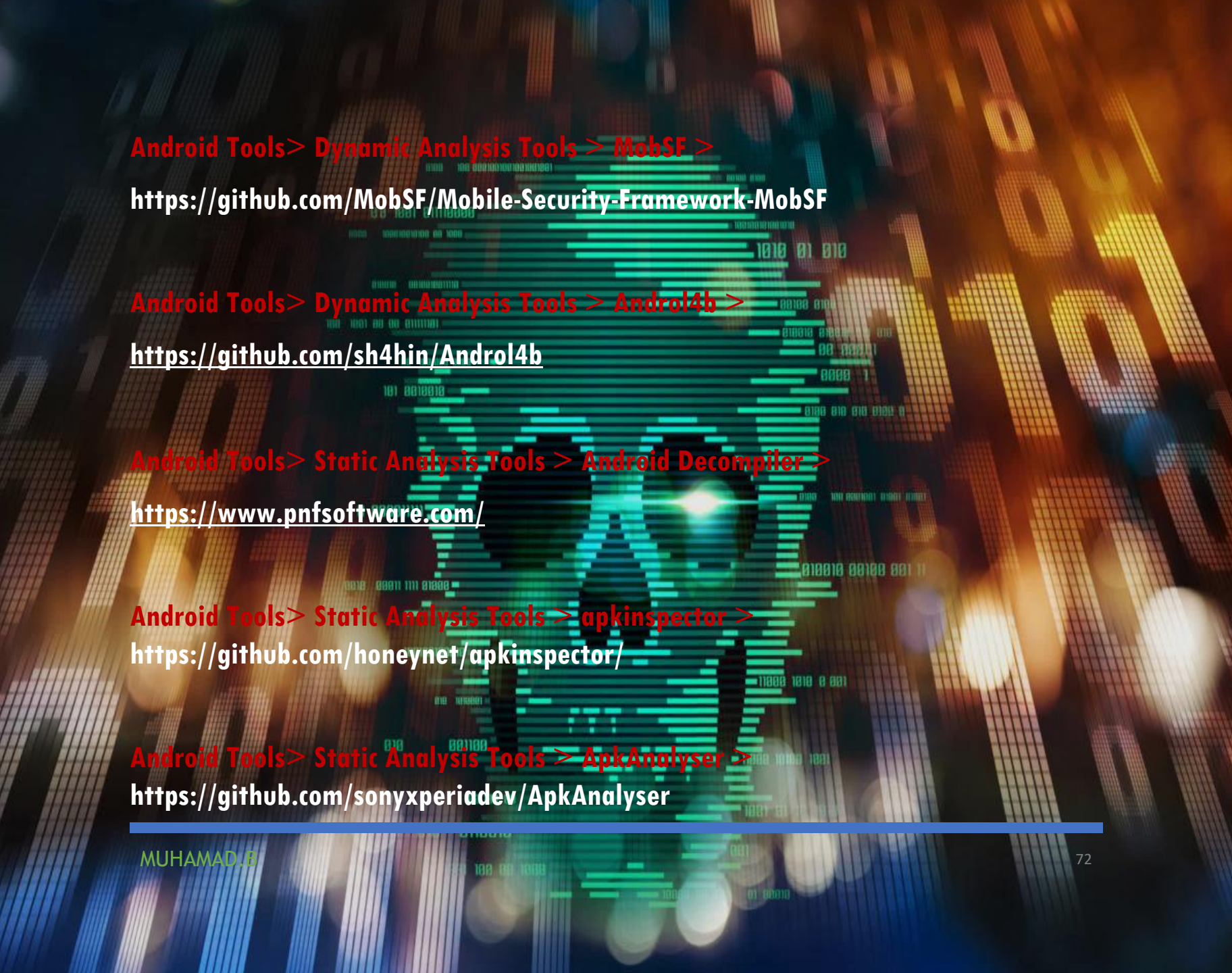
http://www.malware-traffic-analysis.net/index.html

Android Tools> Dynamic Analysis Tools > droidbox >

https://github.com/pjlantz/droidbox

Android Tools> Dynamic Analysis Tools > maldrolyzer >

https://github.com/maldroid/maldrolyzer



Android Tools> Dynamic Analysis Tools > MobSF >

https://github.com/MobSF/Mobile-Security-Framework-MobSF

Android Tools> Dynamic Analysis Tools > Androl4b >

https://github.com/sh4hin/Androl4b

Android Tools> Static Analysis Tools > Android Decompiler >

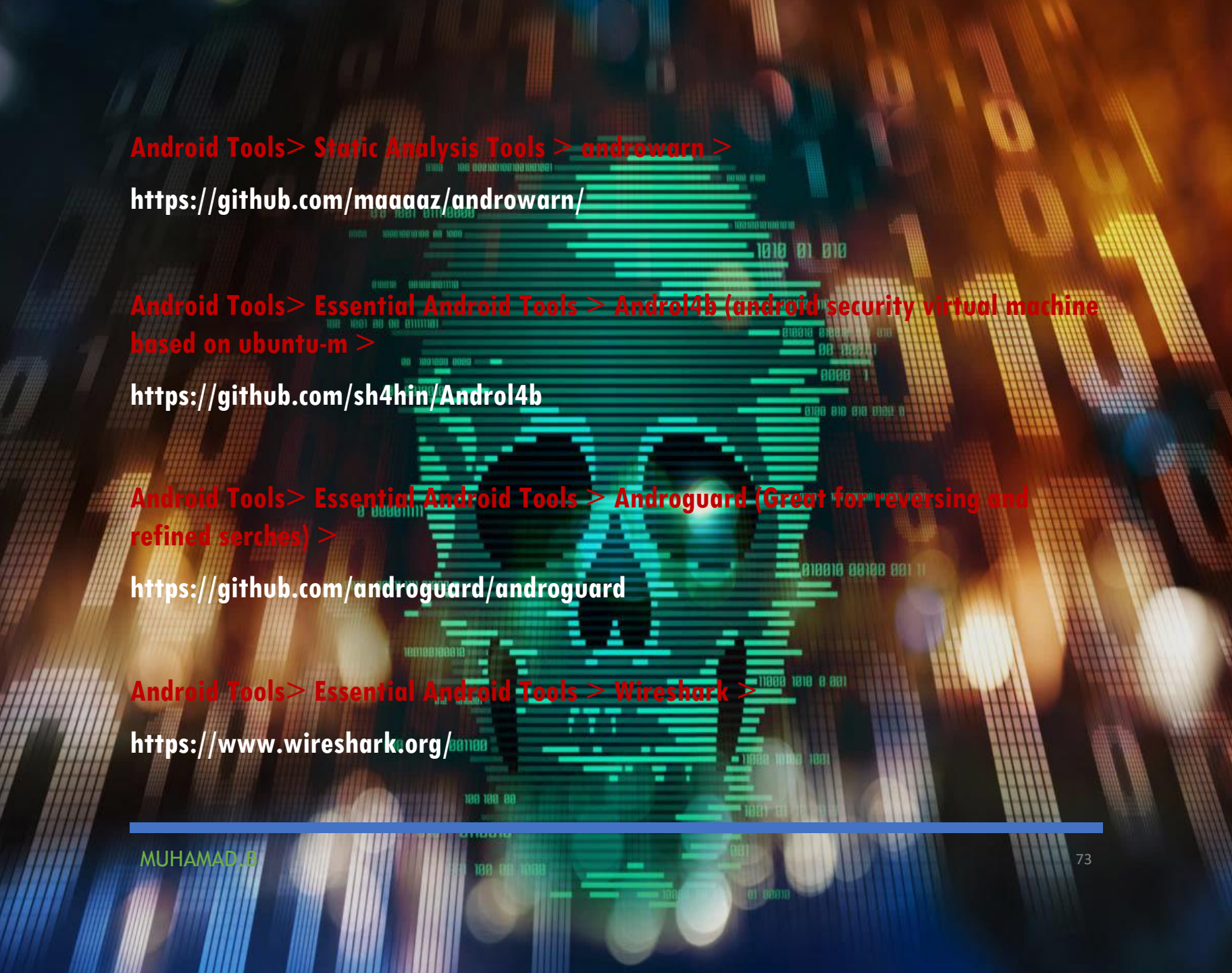
https://www.pnfsoftware.com/

Android Tools> Static Analysis Tools > apkinspector >

https://github.com/honeynet/apkinspector/

Android Tools> Static Analysis Tools > ApkAnalyser >

https://github.com/sonyxperiadev/ApkAnalyser



Android Tools> Static Analysis Tools > androwarn >

https://github.com/maaaaz/androwarn/

Android Tools> Essential Android Tools > Androl4b (android security virtual machine based on ubuntu-m >

https://github.com/sh4hin/Androl4b

Android Tools> Essential Android Tools > Androguard (Great for reversing and refined serches) >

https://github.com/androguard/androguard

Android Tools> Essential Android Tools > Wireshark >

https://www.wireshark.org/

Android Tools> Essential Android Tools > APKtool (reverse engineering Android APK format using Java r >

https://ibotpeaches.github.io/Apktool/

Android Tools> Essential Android Tools > apkinspector (Not supported anymore but still works great.) >

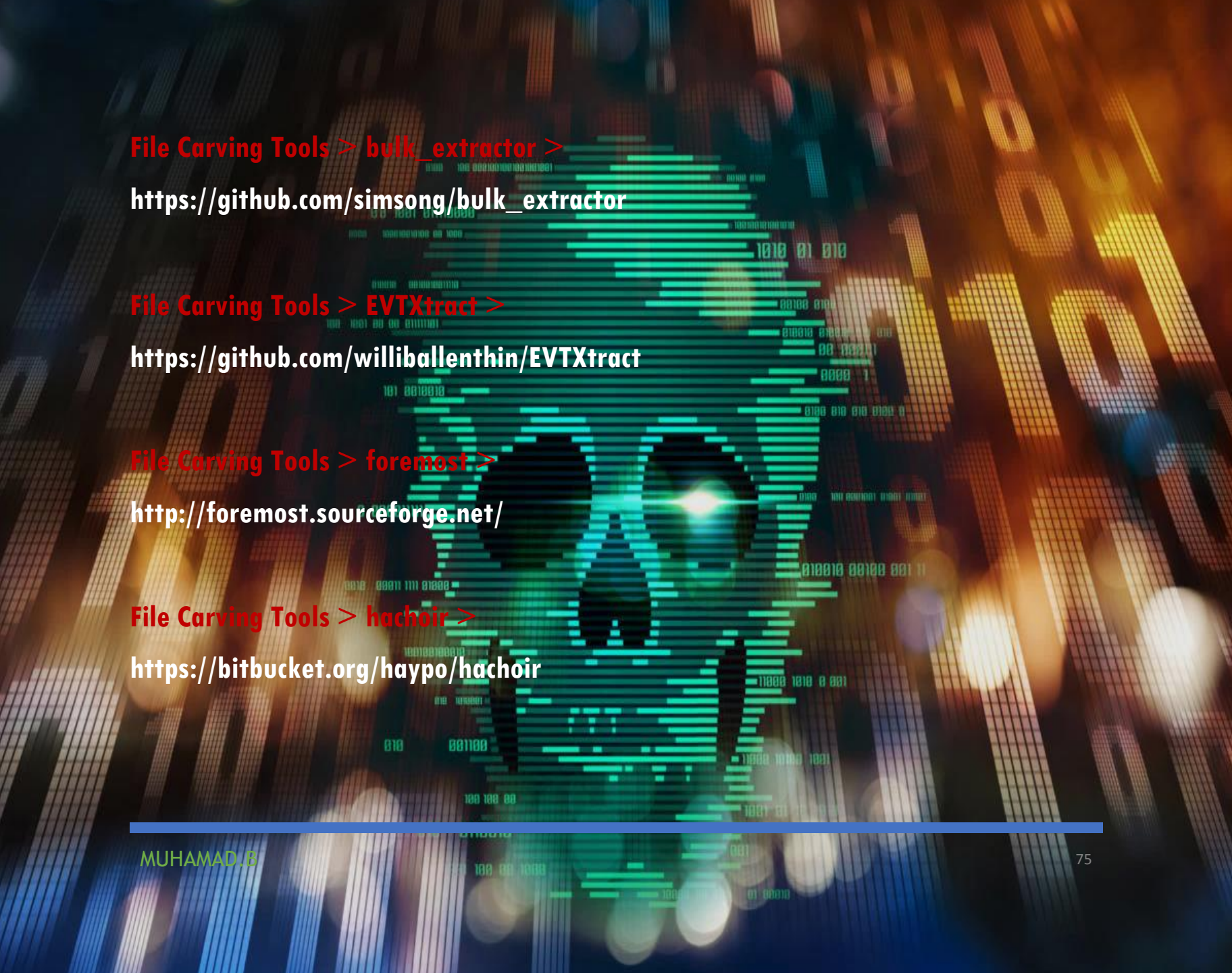
https://github.com/honeynet/apkinspector/

Android Tools> Essential Android Tools > smali (smaliis a disassembler for the dex format used by dalvik >

https://github.com/JesusFreke/smali

Android Tools> Essential Android Tools > android-x86 (Android VM's) >

http://www.android-x86.org/



File Carving Tools > bulk_extractor >

https://github.com/simsong/bulk_extractor

File Carving Tools > EVTXtract >

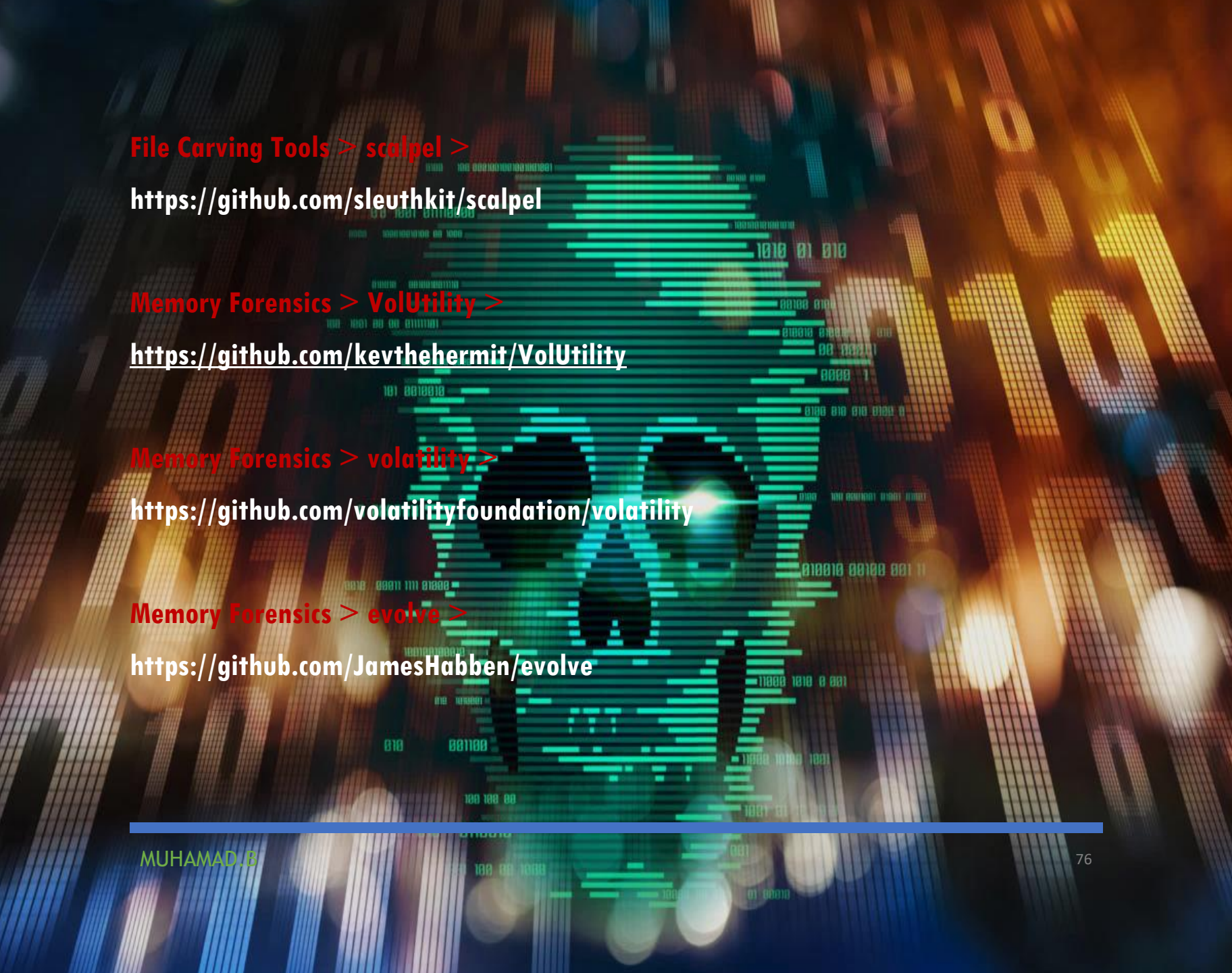
https://github.com/williballenthin/EVTXtract

File Carving Tools > foremost >

http://foremost.sourceforge.net/

File Carving Tools > hachoir >

https://bitbucket.org/haypo/hachoir



File Carving Tools > scalpel >

https://github.com/sleuthkit/scalpel

Memory Forensics > VolUtility >

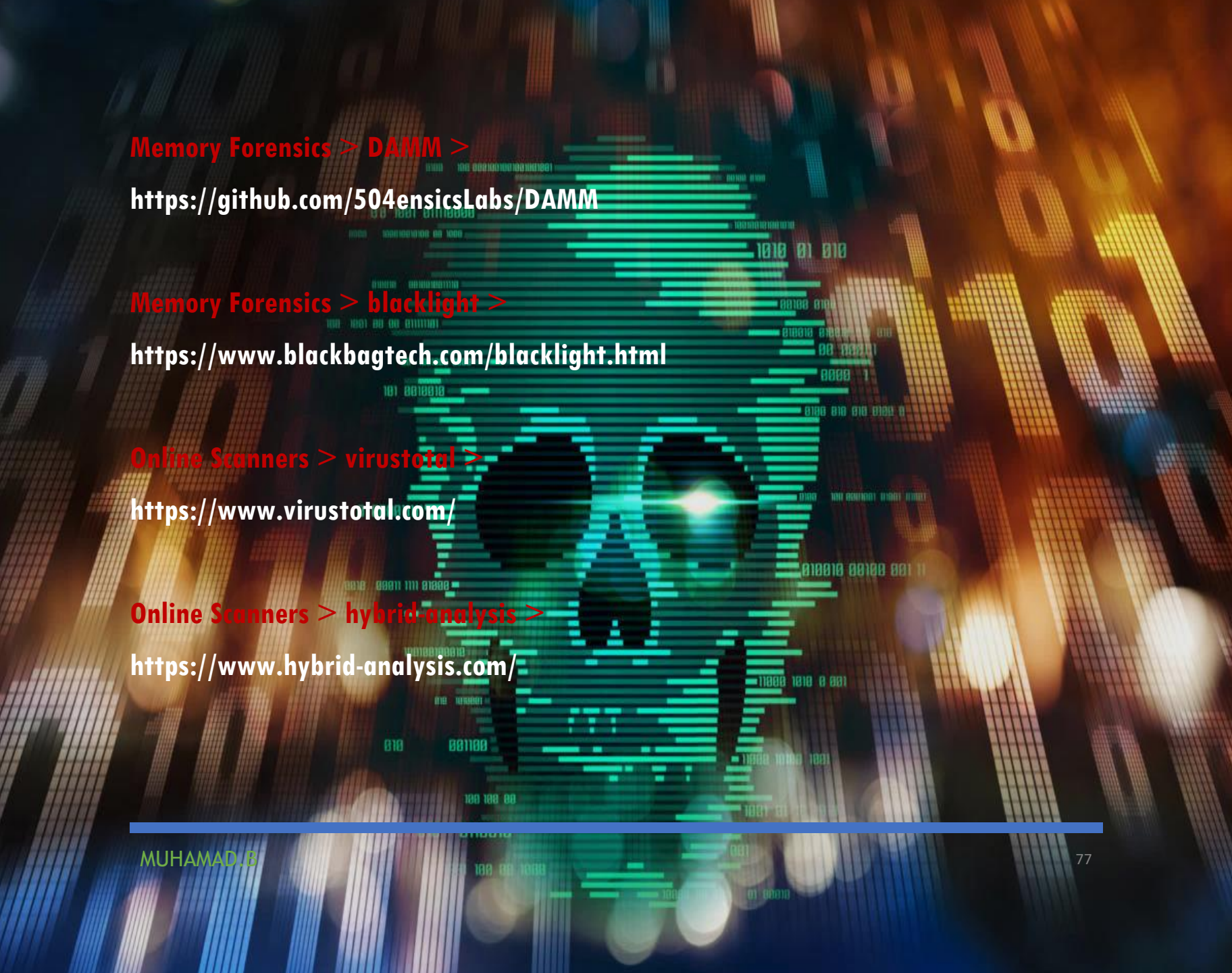
https://github.com/kevthehermit/VolUtility

Memory Forensics > volatility >

https://github.com/volatilityfoundation/volatility

Memory Forensics > evolve >

https://github.com/JamesHabben/evolve



Memory Forensics > DAMM >

https://github.com/504ensicsLabs/DAMM

Memory Forensics > blacklight >

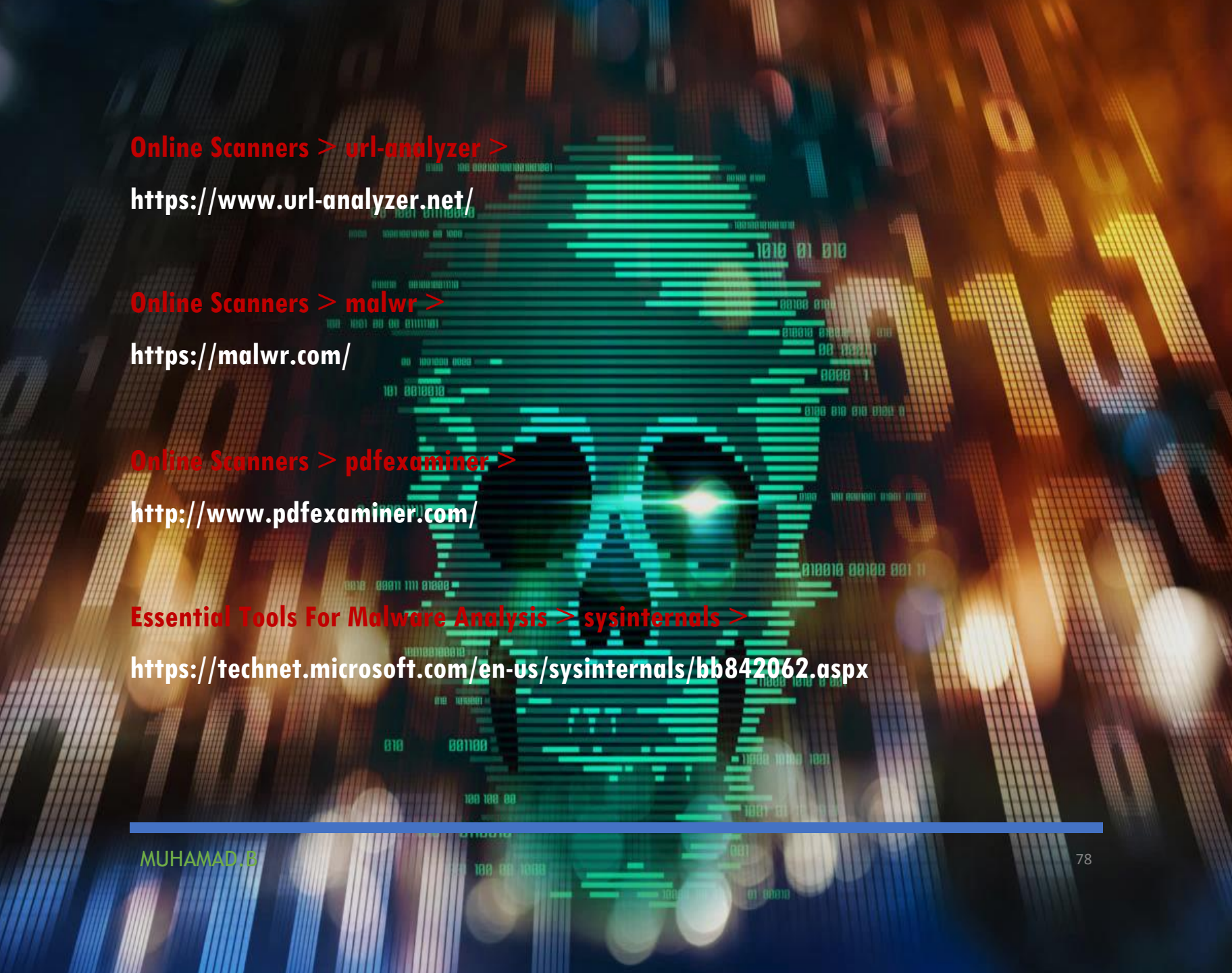
https://www.blackbagtech.com/blacklight.html

Online Scanners > virustotal >

https://www.virustotal.com/

Online Scanners > hybrid-analysis >

https://www.hybrid-analysis.com/



Online Scanners > url-analyzer >

https://www.url-analyzer.net/

Online Scanners > malwr >

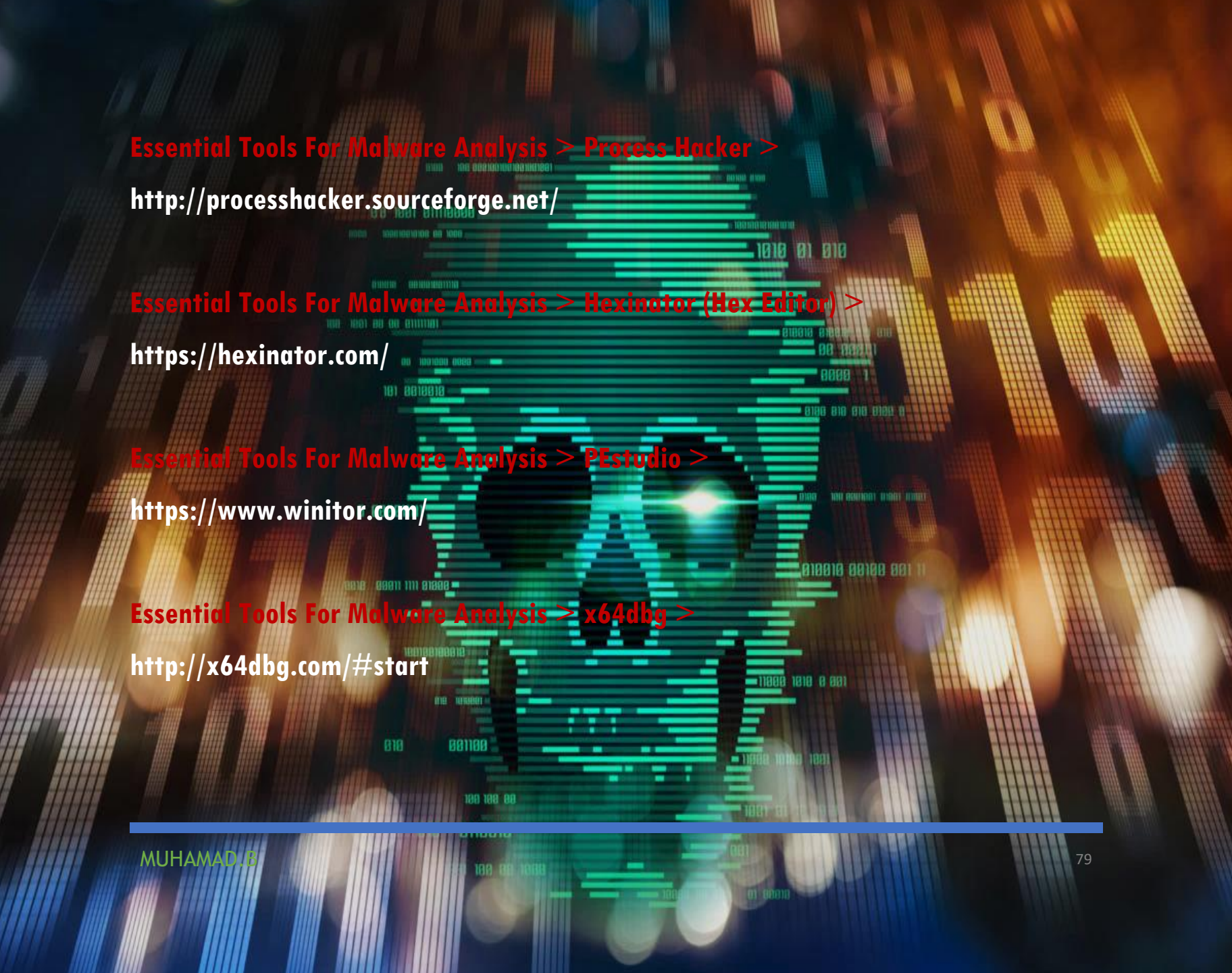
https://malwr.com/

Online Scanners > pdfexaminer >

http://www.pdfexaminer.com/

Essential Tools For Malware Analysis > sysinternals >

https://technet.microsoft.com/en-us/sysinternals/bb842062.aspx



Essential Tools For Malware Analysis > Process Hacker >

http://processhacker.sourceforge.net/

Essential Tools For Malware Analysis > Hexinator (Hex Editor) >

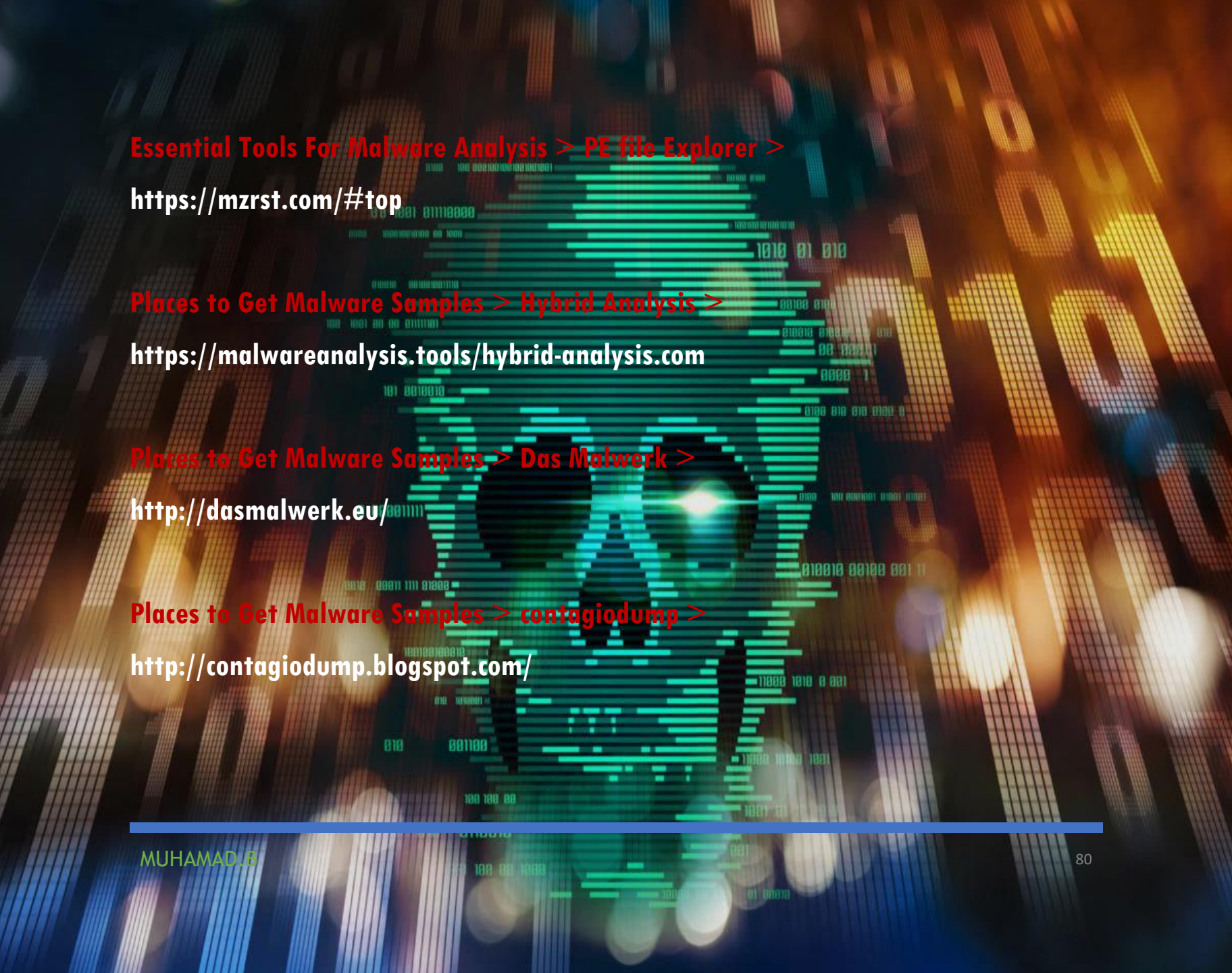
https://hexinator.com/

Essential Tools For Malware Analysis > PEstudio >

https://www.winitor.com/

Essential Tools For Malware Analysis > x64dbg >

http://x64dbg.com/#start



Essential Tools For Malware Analysis > PE file Explorer >

https://mzrst.com/#top

Places to Get Malware Samples > Hybrid Analysis >

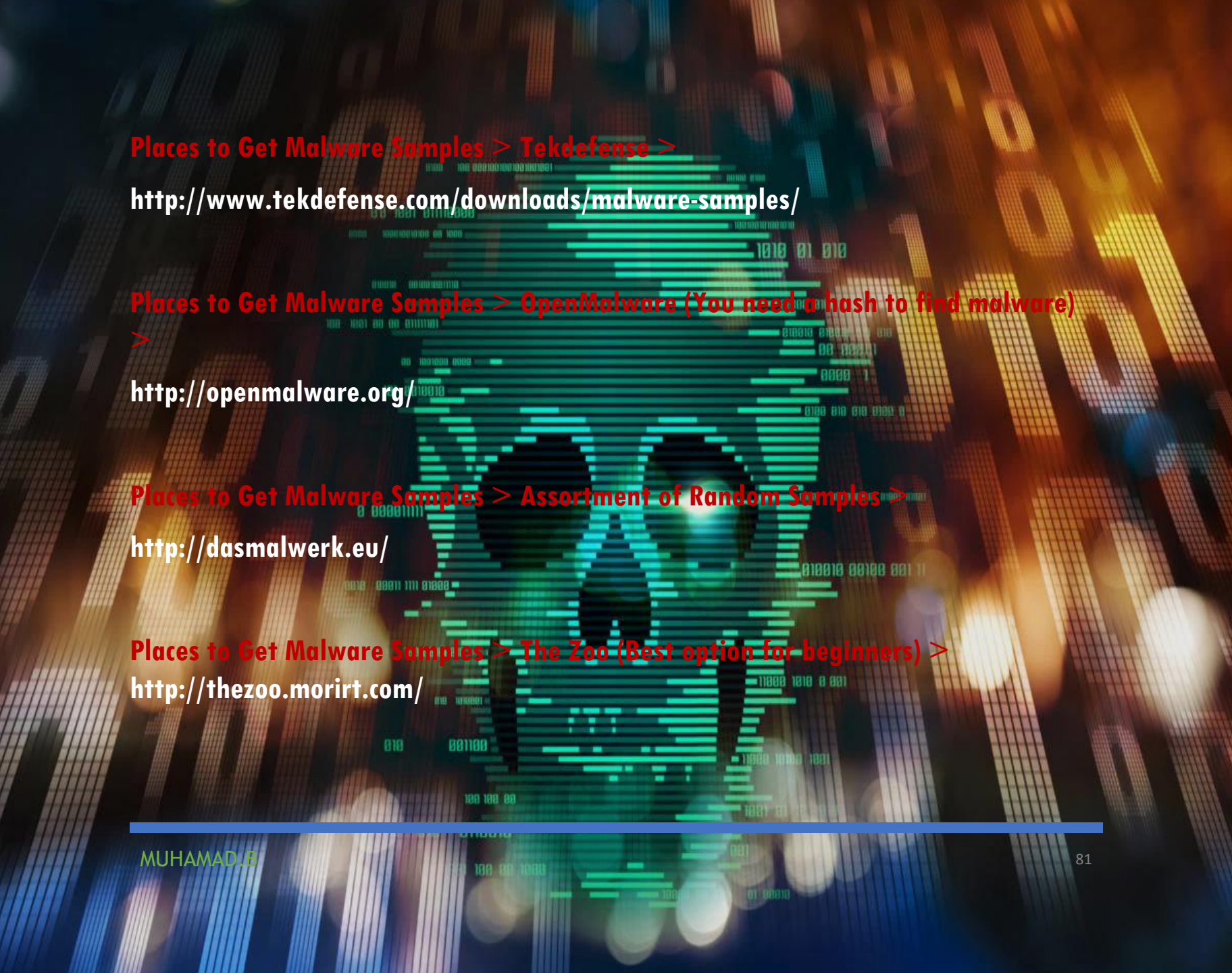
https://malwareanalysis.tools/hybrid-analysis.com

Places to Get Malware Samples > Das Malwerk >

http://dasmalwerk.eu/

Places to Get Malware Samples > contagiodump >

http://contagiodump.blogspot.com/



Places to Get Malware Samples > Tekdefense >

http://www.tekdefense.com/downloads/malware-samples/

Places to Get Malware Samples > OpenMalware (You need a hash to find malware) >

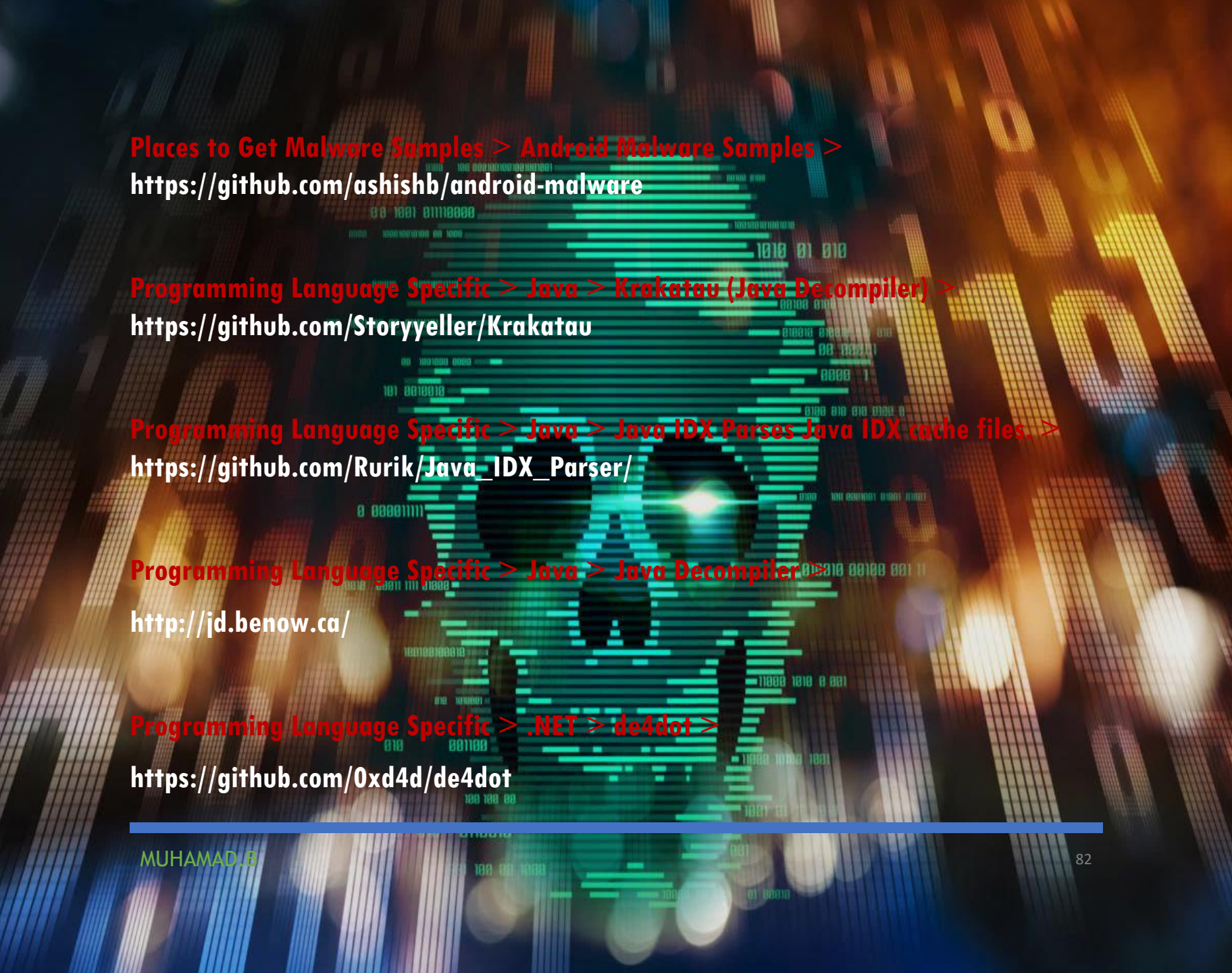
http://openmalware.org/

Places to Get Malware Samples > Assortment of Random Samples >

http://dasmalwerk.eu/

Places to Get Malware Samples > The Zoo (Best option for beginners) >

http://thezoo.morirt.com/



Places to Get Malware Samples > Android Malware Samples >

https://github.com/ashishb/android-malware

Programming Language Specific > Java > Krakatau (Java Decompiler) >

https://github.com/Storyyeller/Krakatau

Programming Language Specific > Java > Java IDX Parses Java IDX cache files. >

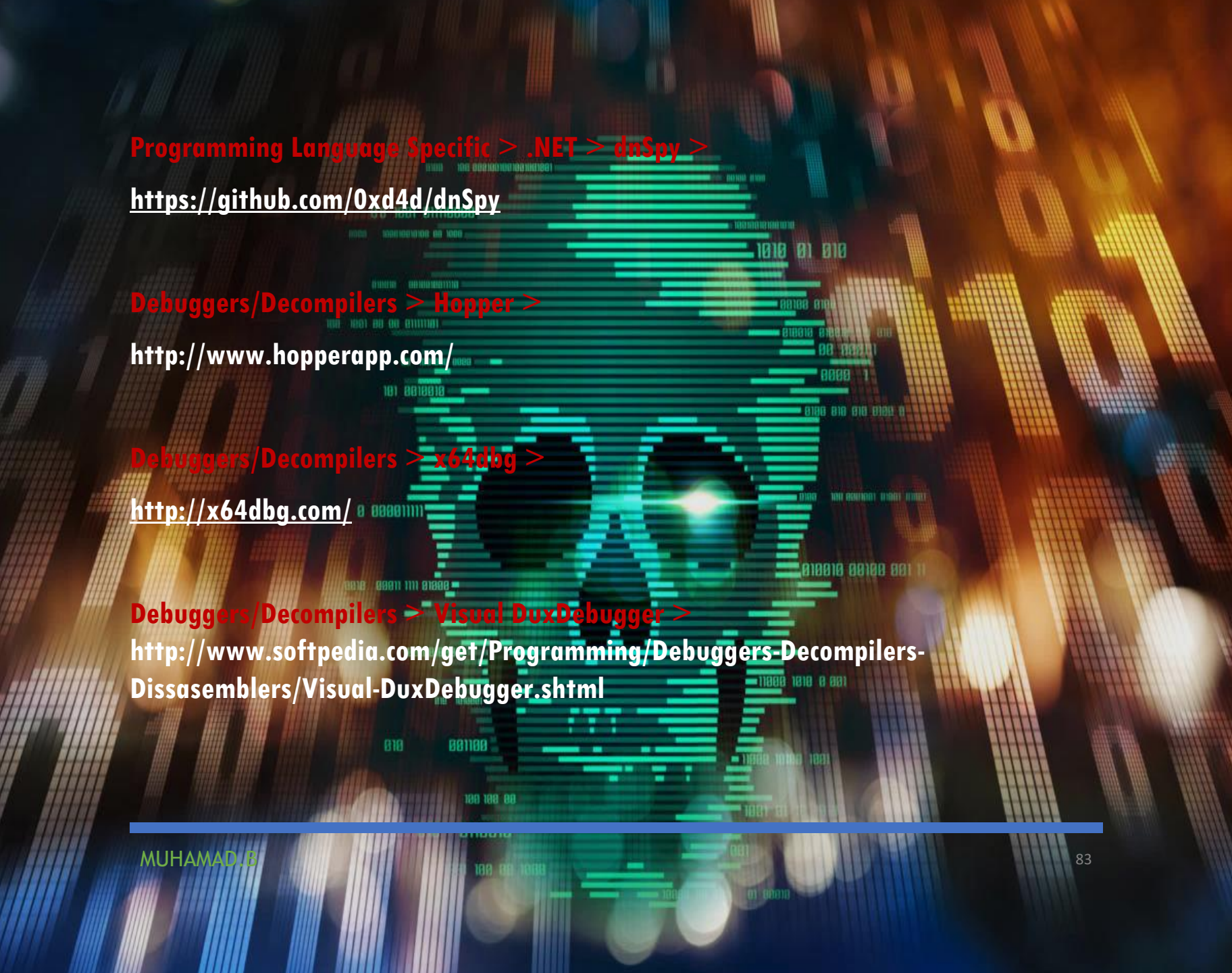
https://github.com/Rurik/Java_IDX_Parser/

Programming Language Specific > Java > Java Decompiler >

http://jd.benow.ca/

Programming Language Specific > .NET > de4dot >

https://github.com/0xd4d/de4dot



Programming Language Specific > .NET > dnSpy >

https://github.com/0xd4d/dnSpy

Debuggers/Decompilers > Hopper >

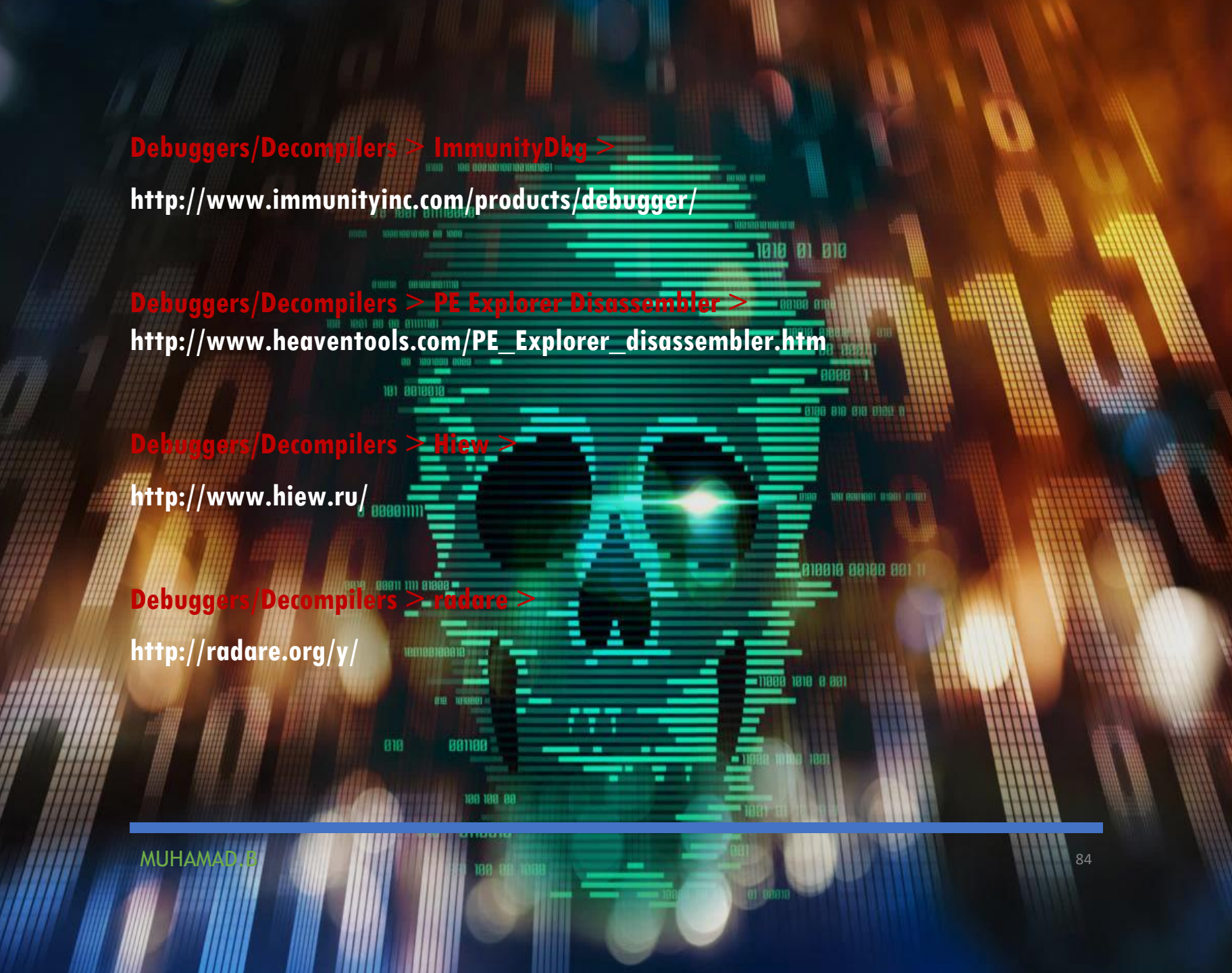
http://www.hopperapp.com/

Debuggers/Decompilers > x64dbg >

http://x64dbg.com/

Debuggers/Decompilers > Visual DuxDebugger >

http://www.softpedia.com/get/Programming/Debuggers-Decompilers-Dissasemblers/Visual-DuxDebugger.shtml



Debuggers/Decompilers > ImmunityDbg >

http://www.immunityinc.com/products/debugger/

Debuggers/Decompilers > PE Explorer Disassembler >

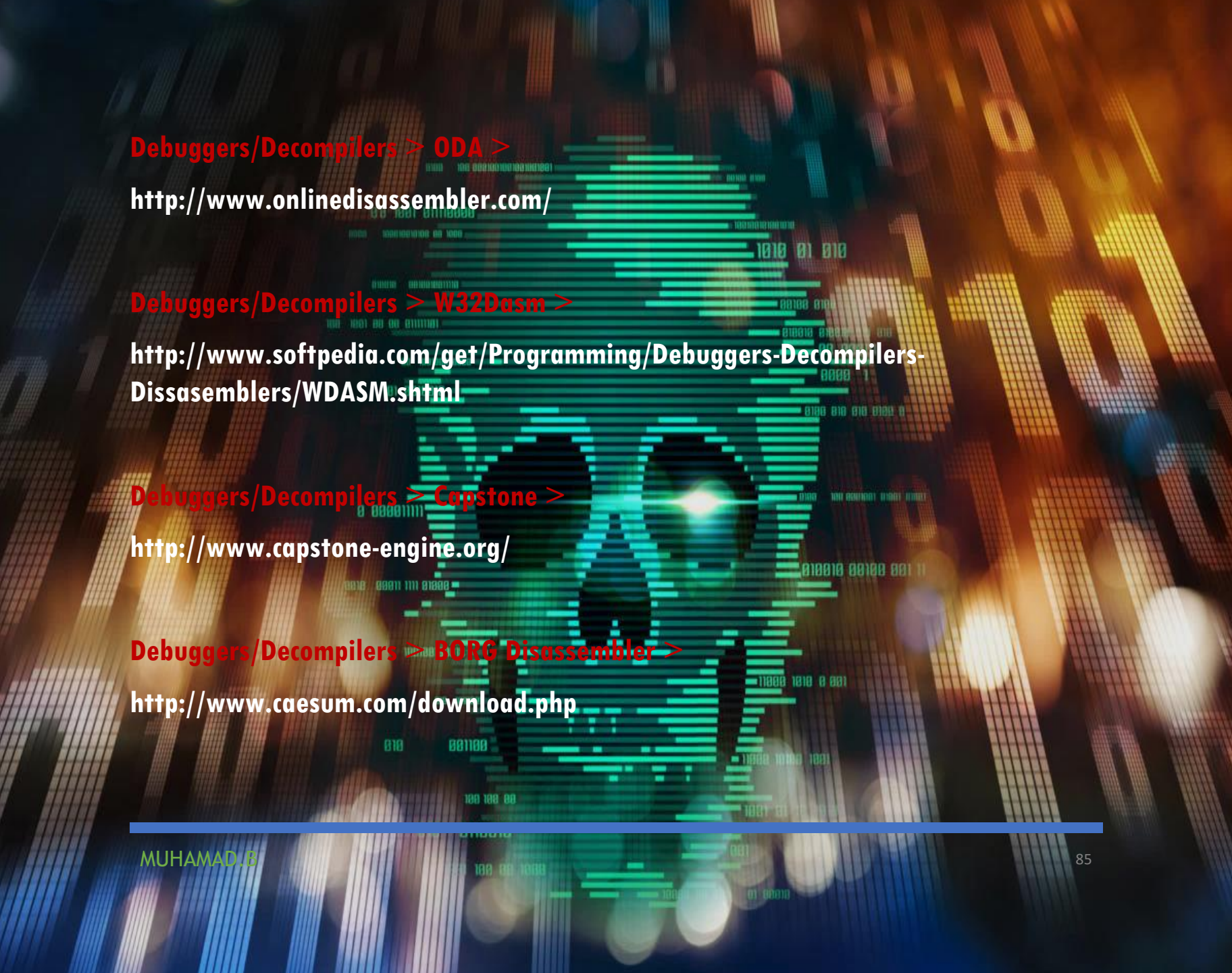
http://www.heaventools.com/PE_Explorer_disassembler.htm

Debuggers/Decompilers > Hiew >

http://www.hiew.ru/

Debuggers/Decompilers > radare >

http://radare.org/y/



Debuggers/Decompilers > ODA >

http://www.onlinedisassembler.com/

Debuggers/Decompilers > W32Dasm >

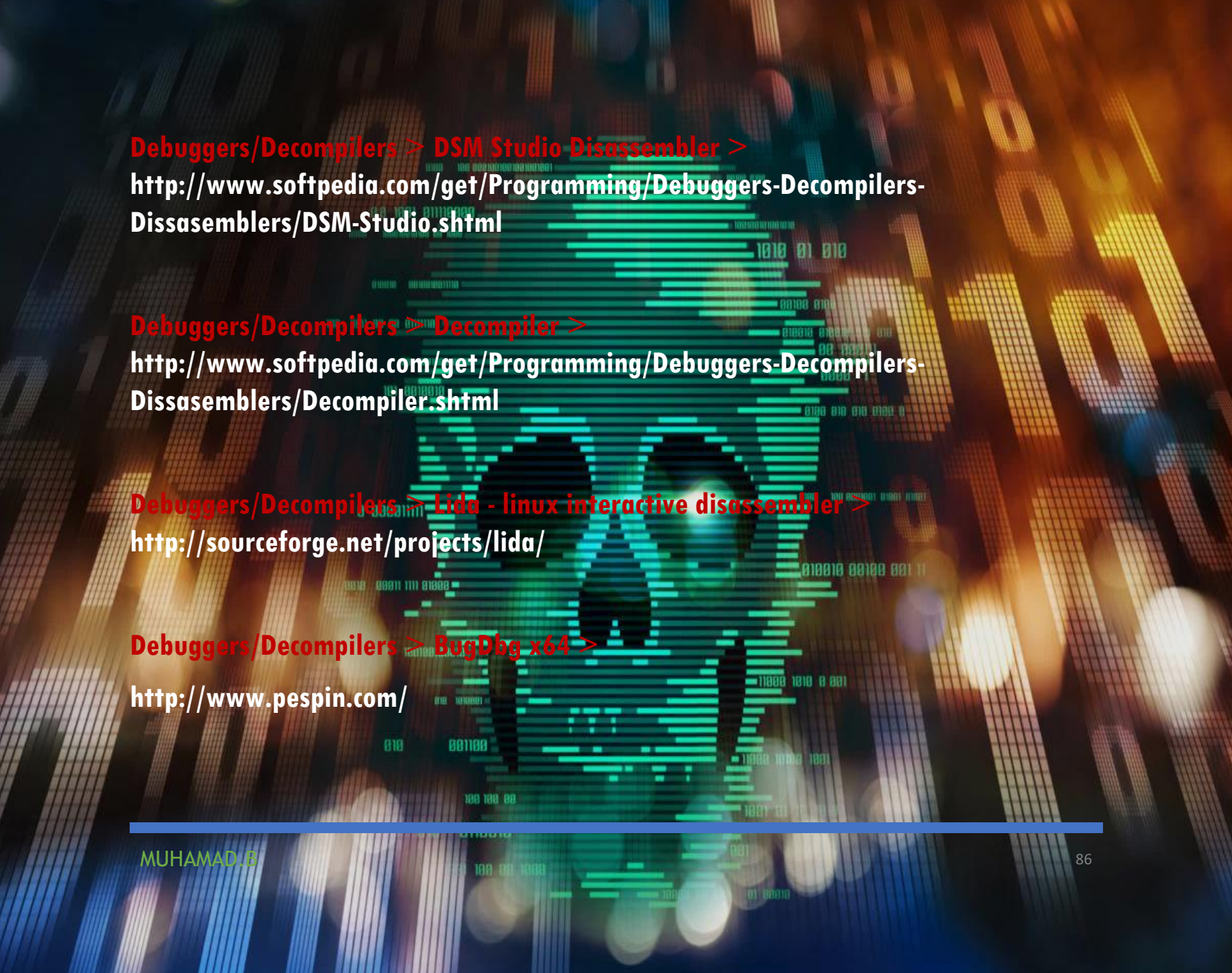
http://www.softpedia.com/get/Programming/Debuggers-Decompilers-Dissasemblers/WDASM.shtml

Debuggers/Decompilers > Capstone >

http://www.capstone-engine.org/

Debuggers/Decompilers > BORG Disassembler >

http://www.caesum.com/download.php



Debuggers/Decompilers > DSM Studio Disassembler >

http://www.softpedia.com/get/Programming/Debuggers-Decompilers-Dissasemblers/DSM-Studio.shtml

Debuggers/Decompilers > Decompiler >

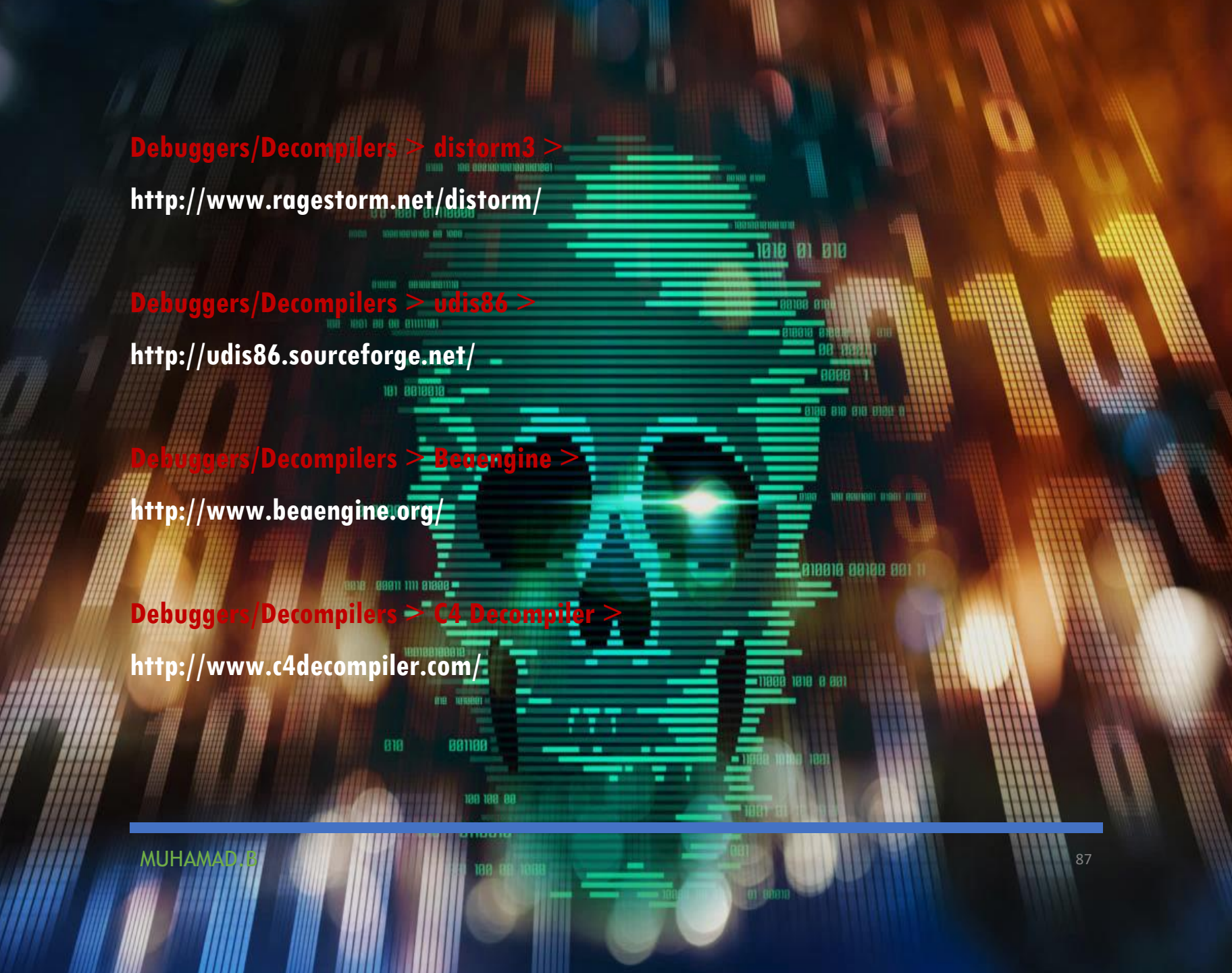
http://www.softpedia.com/get/Programming/Debuggers-Decompilers-Dissasemblers/Decompiler.shtml

Debuggers/Decompilers > Lida - linux interactive disassembler >

http://sourceforge.net/projects/lida/

Debuggers/Decompilers > BugDbg x64 >

http://www.pespin.com/



Debuggers/Decompilers > distorm3 >

http://www.ragestorm.net/distorm/

Debuggers/Decompilers > udis86 >

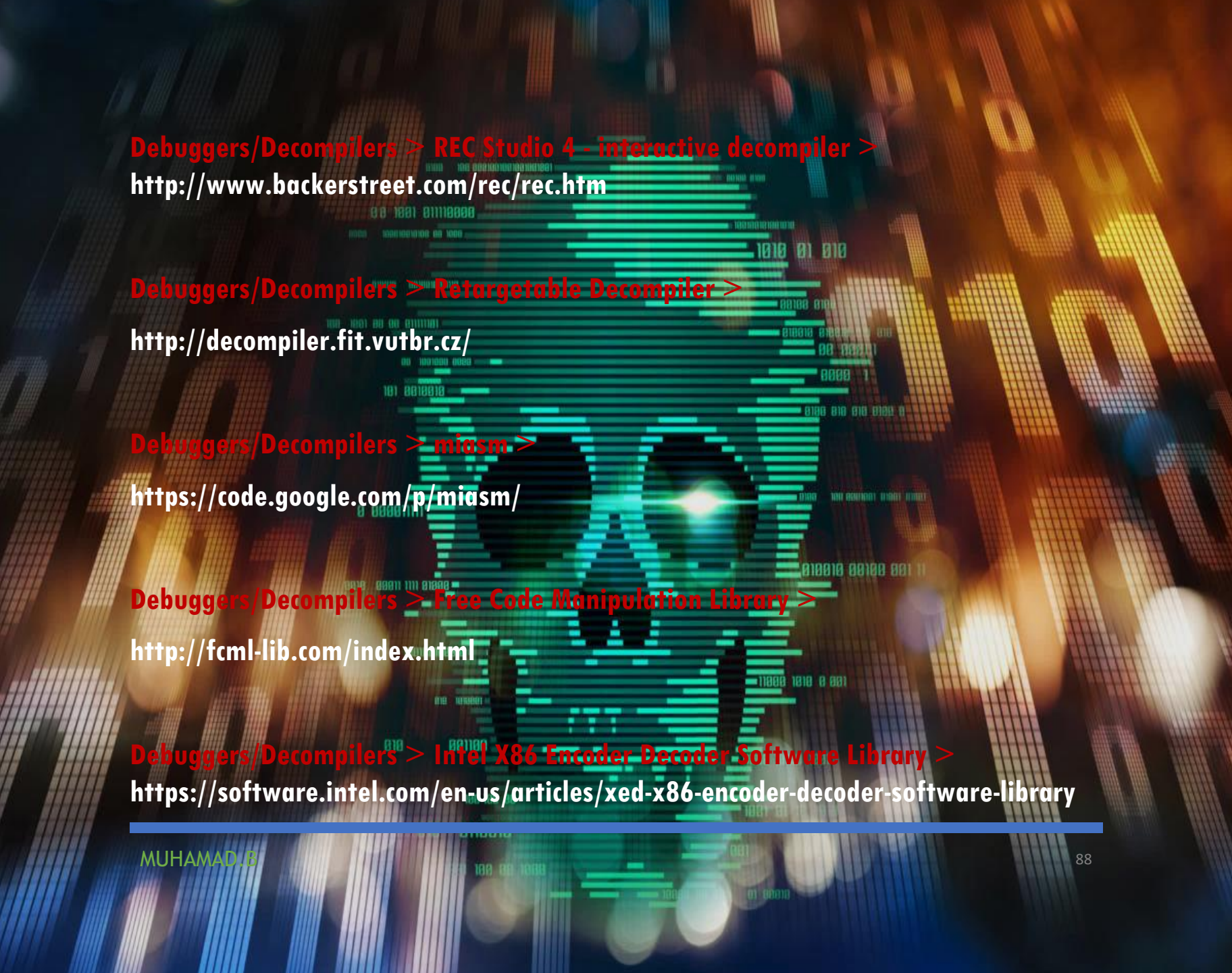
http://udis86.sourceforge.net/

Debuggers/Decompilers > Beaengine >

http://www.beaengine.org/

Debuggers/Decompilers > C4 Decompiler >

http://www.c4decompiler.com/



Debuggers/Decompilers > REC Studio 4 - interactive decompiler >

http://www.backerstreet.com/rec/rec.htm

Debuggers/Decompilers > Retargetable Decompiler >

http://decompiler.fit.vutbr.cz/

Debuggers/Decompilers > miasm >

https://code.google.com/p/miasm/

Debuggers/Decompilers > Free Code Manipulation Library >

http://fcml-lib.com/index.html

Debuggers/Decompilers > Intel X86 Encoder Decoder Software Library >

https://software.intel.com/en-us/articles/xed-x86-encoder-decoder-software-library

Debuggers/Decompilers > angr >

http://angr.io/

سەرچاوە:

https://malwareanalysis.tools/

گرنگە:

بە هیچ شێوەیەك كار لەسەر ویندۆزی سەرەكی مەكە چونكە هەر شتێك رووبا بە ئەگەری زۆرەوە فایلەكانت لەدەست ئەدەیت یاخود زیان بە سیستەمەكەت ئەگەیەنێت، بۆیە وا باشترە كار لەسەر ویندۆز وەهمی بكەیت كە ئەتوانیت سوود لەمانە وەربگریت،

VirtualBox

VMware Workstation

https://alternativeto.net/software/vmware-workstation/

ئەتوانن سوود لەم سیستەمە وەرگرن کە تایبەت بۆ کاری مالوێر ئنالسیس رێکمخستوە. زۆربەی پێداویستیەکانی مالوێر ئنالسیس تیایە هەمووی بەبێ کێشە کارئەکا،

- کێشی بە ئامادەکراوی: 30گیگابایت

واتا ئامادەکراوەو پێویستی بە ئینستاڵکردن نییە.

- کێشی سیستەمەکە: 6گیگابایت

بەبێ ئینستاڵکردن واتا ئەبێ ئینستاڵی بکەیت.

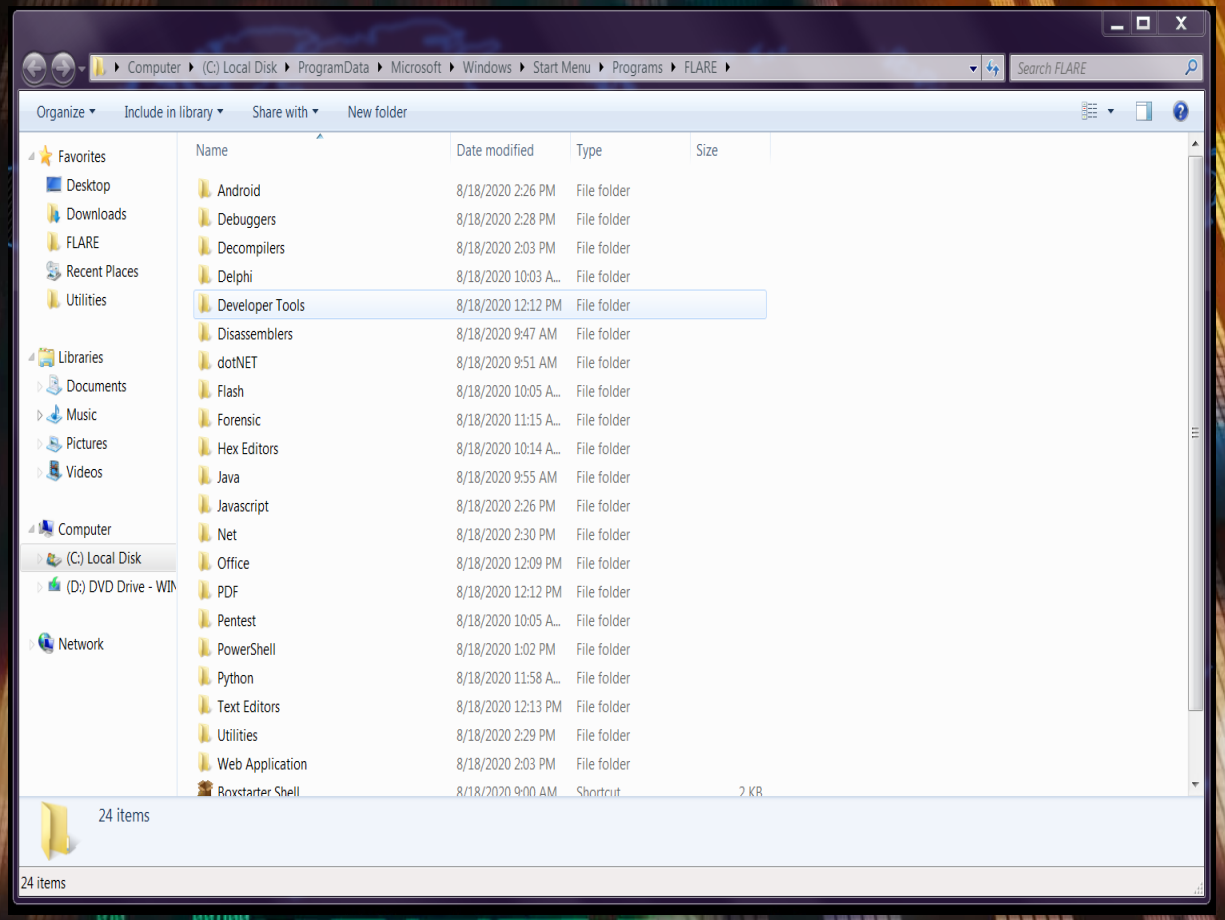
ئەتوانن لێرەوە دایگرن:

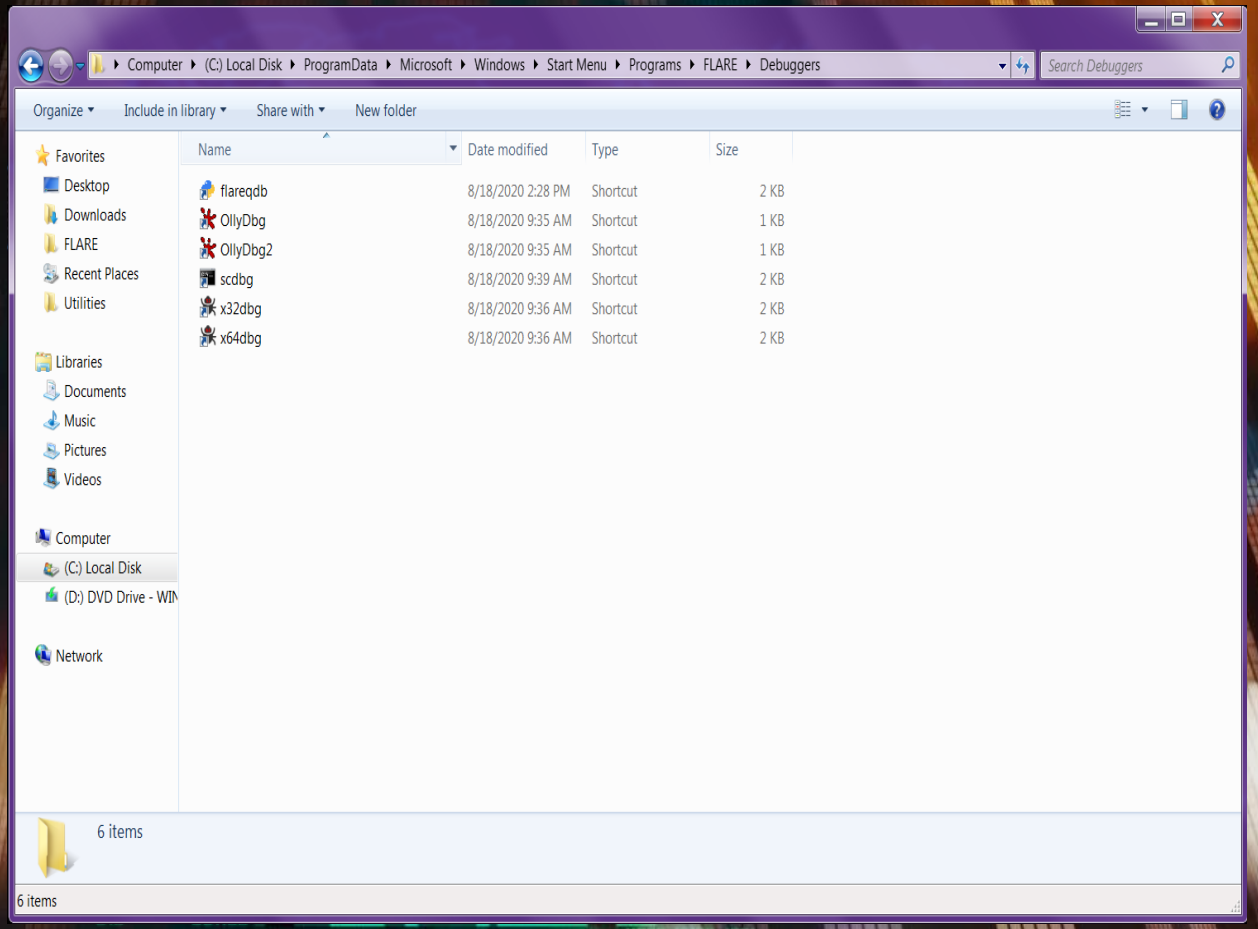
https://mega.nz/file/5gqhmbzC#AslWZiZTiQbEB-UyBi2qNo1fRDMPlxaWo4j33SOcBMo

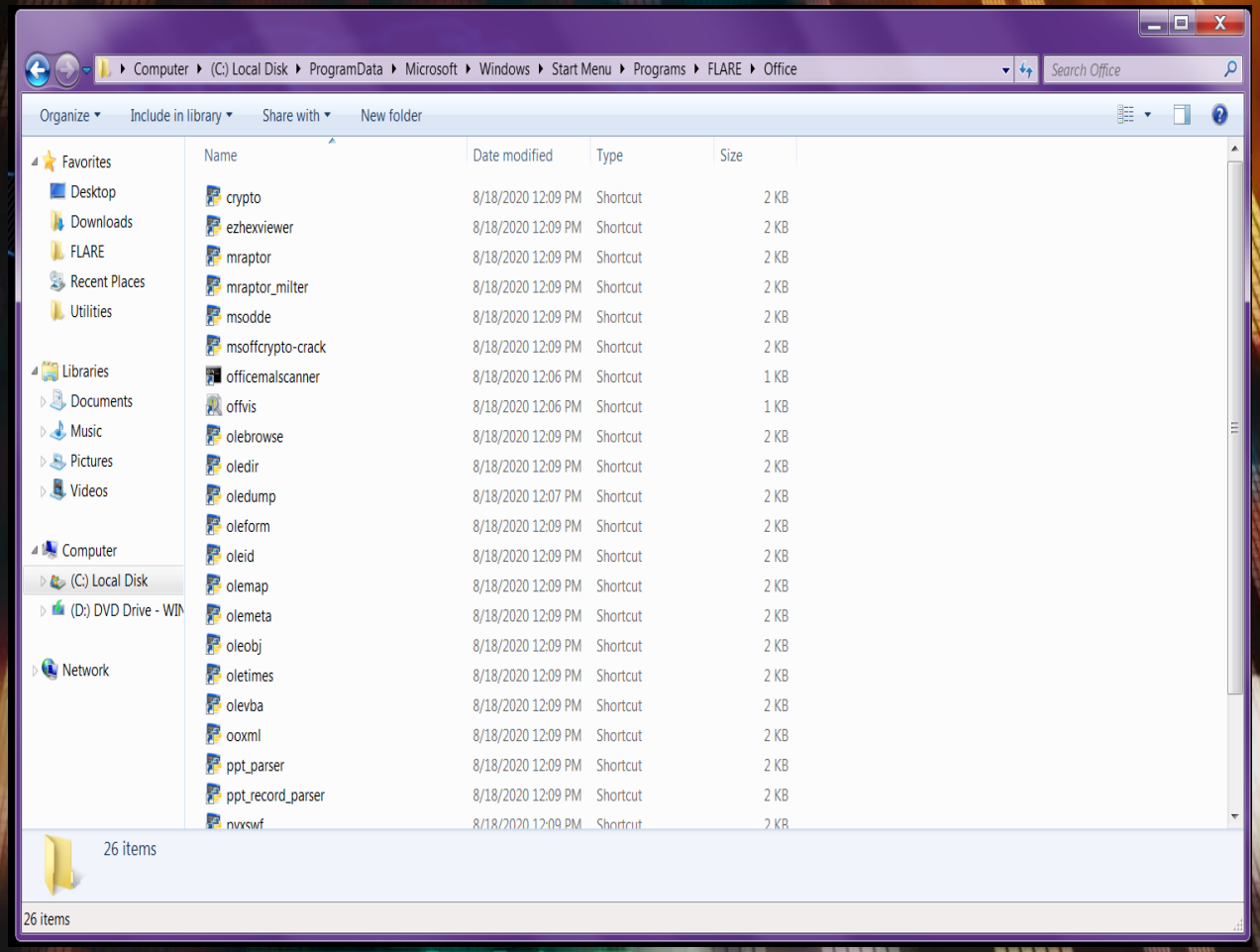
فێرکاری:

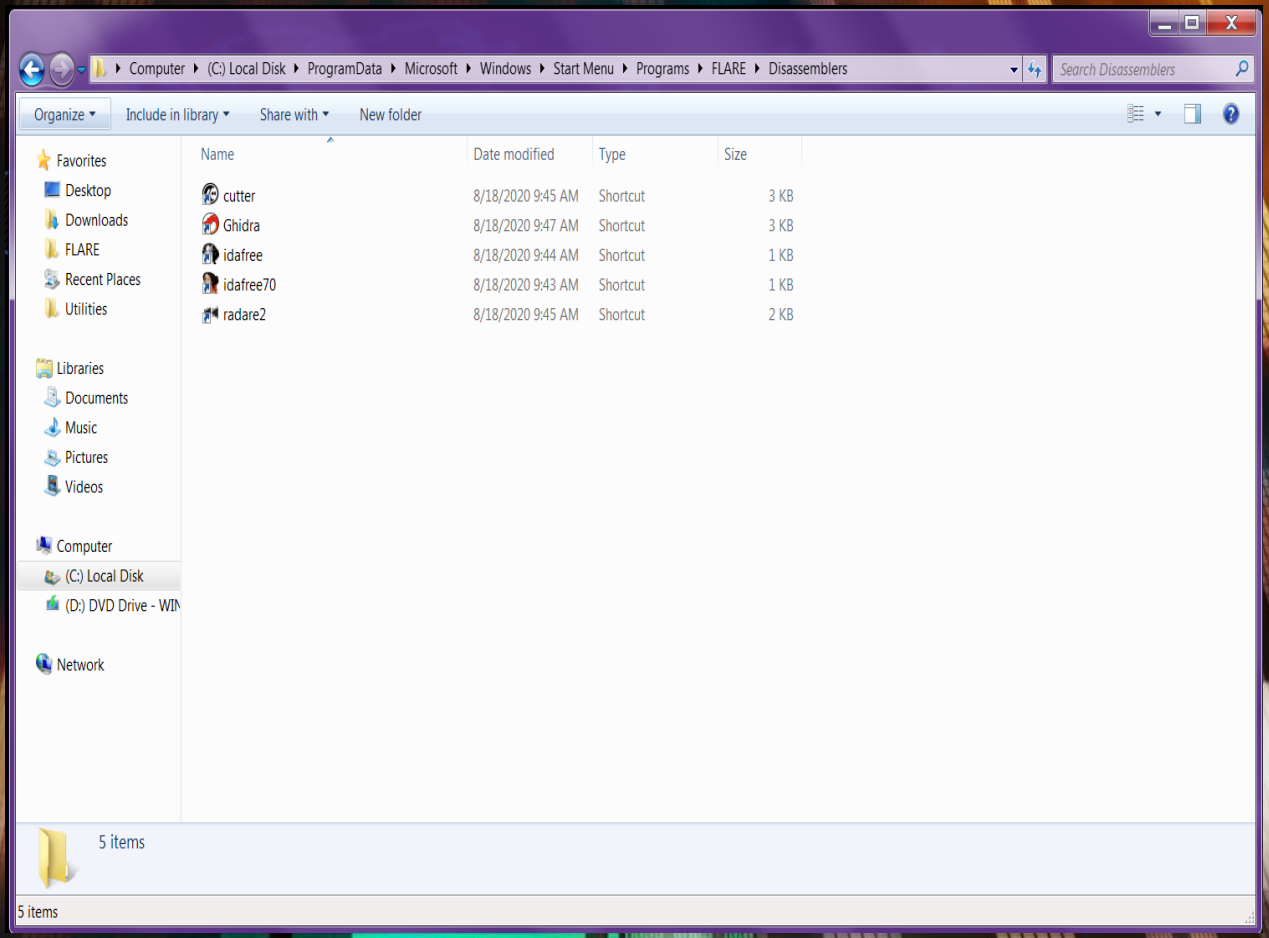
https://youtu.be/ZirxPQ62A6o

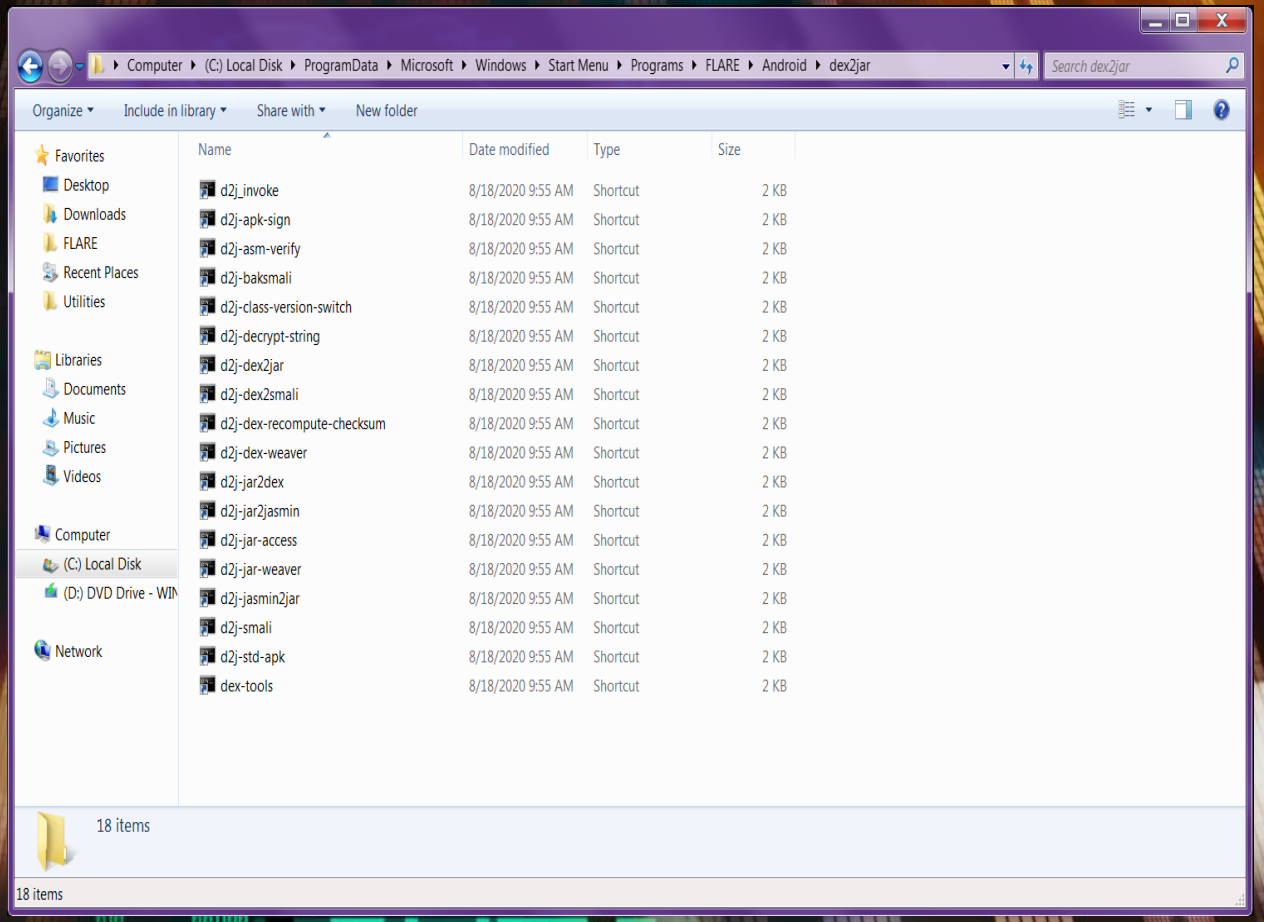
چەند وێنەیەکی سیستەمەکە


Computer ▸ (C:) Local Disk ▸ ProgramData ▸ Microsoft ▸ Windows ▸ Start Menu ▸ Programs ▸ FLARE ▸
Search FLARE
Organize
Include in library
Share with
New folder
Favorites
Desktop
Downloads
FLARE
Recent Places
Utilities
Libraries
Documents
Music
Pictures
Videos
Computer
(C:) Local Disk
(D:) DVD Drive - WIN
Network
Name
Date modified
Type
Size
Android 8/18/2020 2:26 PM File folder
Debuggers 8/18/2020 2:28 PM File folder
Decompilers 8/18/2020 2:03 PM File folder
Delphi 8/18/2020 10:03 A... File folder
Developer Tools 8/18/2020 12:12 PM File folder
Disassemblers 8/18/2020 9:47 AM File folder
dotNET 8/18/2020 9:51 AM File folder
Flash 8/18/2020 10:05 A... File folder
Forensic 8/18/2020 11:15 A... File folder
Hex Editors 8/18/2020 10:14 A... File folder
Java 8/18/2020 9:55 AM File folder
Javascript 8/18/2020 2:26 PM File folder
Net 8/18/2020 2:30 PM File folder
Office 8/18/2020 12:09 PM File folder
PDF 8/18/2020 12:12 PM File folder
Pentest 8/18/2020 10:05 A... File folder
PowerShell 8/18/2020 1:02 PM File folder
Python 8/18/2020 11:58 A... File folder
Text Editors 8/18/2020 12:13 PM File folder
Utilities 8/18/2020 2:29 PM File folder
Web Application 8/18/2020 2:03 PM File folder
Boxstarter Shell 8/18/2020 9:00 AM Shortcut 2 KB
24 items
24 items


Computer ▸ (C:) Local Disk ▸ ProgramData ▸ Microsoft ▸ Windows ▸ Start Menu ▸ Programs ▸ FLARE ▸ Debuggers
Search Debuggers
Organize
Include in library
Share with
New folder
Favorites
Desktop
Downloads
FLARE
Recent Places
Utilities
Libraries
Documents
Music
Pictures
Videos
Computer
(C:) Local Disk
(D:) DVD Drive - WIN
Network
Name
Date modified
Type
Size
flareqdb 8/18/2020 2:28 PM Shortcut 2 KB
OllyDbg 8/18/2020 9:35 AM Shortcut 1 KB
OllyDbg2 8/18/2020 9:35 AM Shortcut 1 KB
scdbg 8/18/2020 9:39 AM Shortcut 2 KB
x32dbg 8/18/2020 9:36 AM Shortcut 2 KB
x64dbg 8/18/2020 9:36 AM Shortcut 2 KB
6 items
6 items

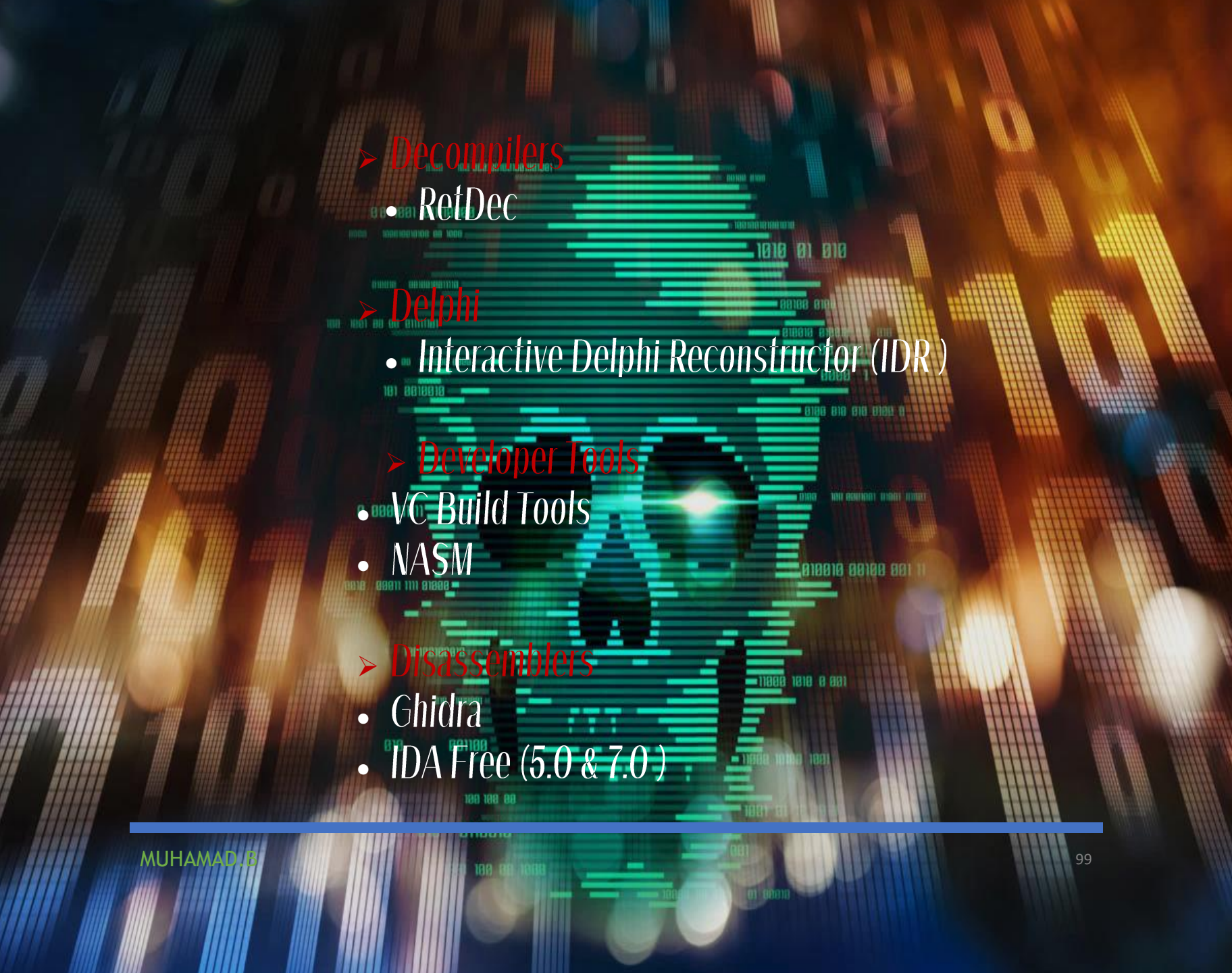

Computer ▸ (C:) Local Disk ▸ ProgramData ▸ Microsoft ▸ Windows ▸ Start Menu ▸ Programs ▸ FLARE ▸ Office
Search Office
Organize
Include in library
Share with
New folder
Favorites
Desktop
Downloads
FLARE
Recent Places
Utilities
Libraries
Documents
Music
Pictures
Videos
Computer
(C:) Local Disk
(D:) DVD Drive - WIN
Network
Name
Date modified
Type
Size
crypto 8/18/2020 12:09 PM Shortcut 2 KB
ezhexviewer 8/18/2020 12:09 PM Shortcut 2 KB
mraptor 8/18/2020 12:09 PM Shortcut 2 KB
mraptor_milter 8/18/2020 12:09 PM Shortcut 2 KB
msodde 8/18/2020 12:09 PM Shortcut 2 KB
msoffcrypto-crack 8/18/2020 12:09 PM Shortcut 2 KB
officemalscanner 8/18/2020 12:06 PM Shortcut 1 KB
offvis 8/18/2020 12:06 PM Shortcut 1 KB
olebrowse 8/18/2020 12:09 PM Shortcut 2 KB
oledir 8/18/2020 12:09 PM Shortcut 2 KB
oledump 8/18/2020 12:07 PM Shortcut 2 KB
oleform 8/18/2020 12:09 PM Shortcut 2 KB
oleid 8/18/2020 12:09 PM Shortcut 2 KB
olemap 8/18/2020 12:09 PM Shortcut 2 KB
olemeta 8/18/2020 12:09 PM Shortcut 2 KB
oleobj 8/18/2020 12:09 PM Shortcut 2 KB
oletimes 8/18/2020 12:09 PM Shortcut 2 KB
olevba 8/18/2020 12:09 PM Shortcut 2 KB
ooxml 8/18/2020 12:09 PM Shortcut 2 KB
ppt_parser 8/18/2020 12:09 PM Shortcut 2 KB
ppt_record_parser 8/18/2020 12:09 PM Shortcut 2 KB
pyxswf 8/18/2020 12:09 PM Shortcut 2 KB
26 items
26 items


Computer ▸ (C:) Local Disk ▸ ProgramData ▸ Microsoft ▸ Windows ▸ Start Menu ▸ Programs ▸ FLARE ▸ Disassemblers
Search Disassemblers
Organize
Include in library
Share with
New folder
Favorites
Desktop
Downloads
FLARE
Recent Places
Utilities
Libraries
Documents
Music
Pictures
Videos
Computer
(C:) Local Disk
(D:) DVD Drive - WIN
Network
Name
Date modified
Type
Size
cutter 8/18/2020 9:45 AM Shortcut 3 KB
Ghidra 8/18/2020 9:47 AM Shortcut 3 KB
idafree 8/18/2020 9:44 AM Shortcut 1 KB
idafree70 8/18/2020 9:43 AM Shortcut 1 KB
radare2 8/18/2020 9:45 AM Shortcut 2 KB
5 items
5 items

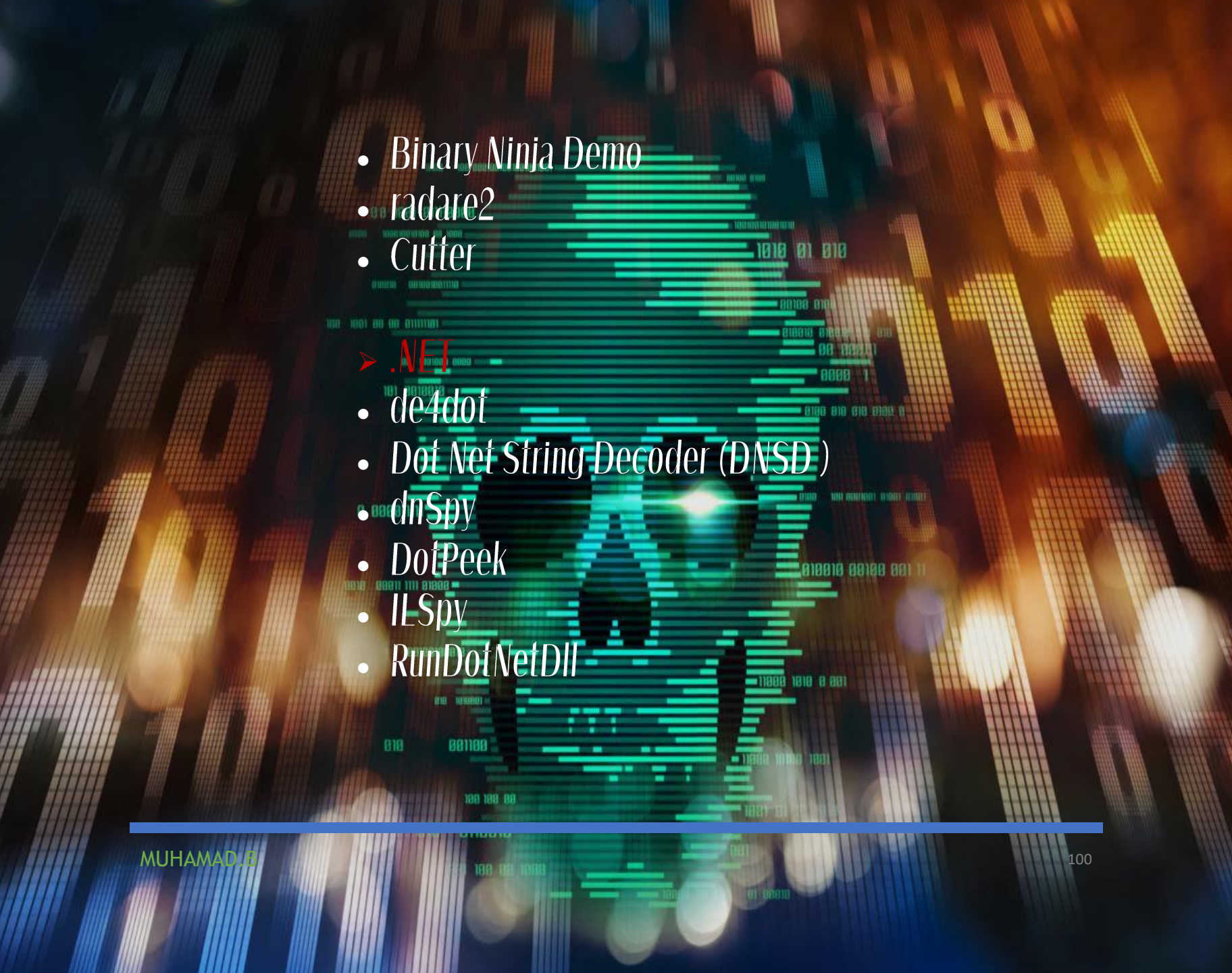

Computer ▸ (C:) Local Disk ▸ ProgramData ▸ Microsoft ▸ Windows ▸ Start Menu ▸ Programs ▸ FLARE ▸ Android ▸ dex2jar
Search dex2jar
Organize
Include in library
Share with
New folder
Favorites
Desktop
Downloads
FLARE
Recent Places
Utilities
Libraries
Documents
Music
Pictures
Videos
Computer
(C:) Local Disk
(D:) DVD Drive - WIN
Network
Name
Date modified
Type
Size
d2j_invoke 8/18/2020 9:55 AM Shortcut 2 KB
d2j-apk-sign 8/18/2020 9:55 AM Shortcut 2 KB
d2j-asm-verify 8/18/2020 9:55 AM Shortcut 2 KB
d2j-baksmali 8/18/2020 9:55 AM Shortcut 2 KB
d2j-class-version-switch 8/18/2020 9:55 AM Shortcut 2 KB
d2j-decrypt-string 8/18/2020 9:55 AM Shortcut 2 KB
d2j-dex2jar 8/18/2020 9:55 AM Shortcut 2 KB
d2j-dex2smali 8/18/2020 9:55 AM Shortcut 2 KB
d2j-dex-recompute-checksum 8/18/2020 9:55 AM Shortcut 2 KB
d2j-dex-weaver 8/18/2020 9:55 AM Shortcut 2 KB
d2j-jar2dex 8/18/2020 9:55 AM Shortcut 2 KB
d2j-jar2jasmin 8/18/2020 9:55 AM Shortcut 2 KB
d2j-jar-access 8/18/2020 9:55 AM Shortcut 2 KB
d2j-jar-weaver 8/18/2020 9:55 AM Shortcut 2 KB
d2j-jasmin2jar 8/18/2020 9:55 AM Shortcut 2 KB
d2j-smali 8/18/2020 9:55 AM Shortcut 2 KB
d2j-std-apk 8/18/2020 9:55 AM Shortcut 2 KB
dex-tools 8/18/2020 9:55 AM Shortcut 2 KB
18 items
18 items

لیستی ئەو بەرنامانەی کە لەسەر سیستەمەکە دانراون

- Android
  - dex2jar
  - apktool
- Debuggers
  - flare-qdb
  - scdbg
  - OllyDbg + OllyDump + OllyDumpEx
  - OllyDbg2 + OllyDumpEx
  - x64dbg
  - WinDbg + OllyDumpex + pykd



- **Decompilers**
  - RetDec
- **Delphi**
  - Interactive Delphi Reconstructor (IDR)
- **Developer Tools**
  - VC Build Tools
  - NASM
- **Disassemblers**
  - Ghidra
  - IDA Free (5.0 & 7.0)



- Binary Ninja Demo
- radare2
- Cutter
- .NET
- de4dot
- Dot Net String Decoder (DNSD)
- dnSpy
- DotPeek
- ILSpy
- RunDotNetDll

- AutoIt
  - AutoItExtractor
- Flash
  - FFDec
- Forensic
  - Volatility
  - Autopsy
- Hex Editors
  - FileInsight
  - HxD

- 010 Editor

- Java
  - JD-GUI
  - Bytecode-Viewer
  - Java-Deobfuscator
- JavaScript
  - malware-jail
- Networking
  - FakeNet-NG
  - ncat

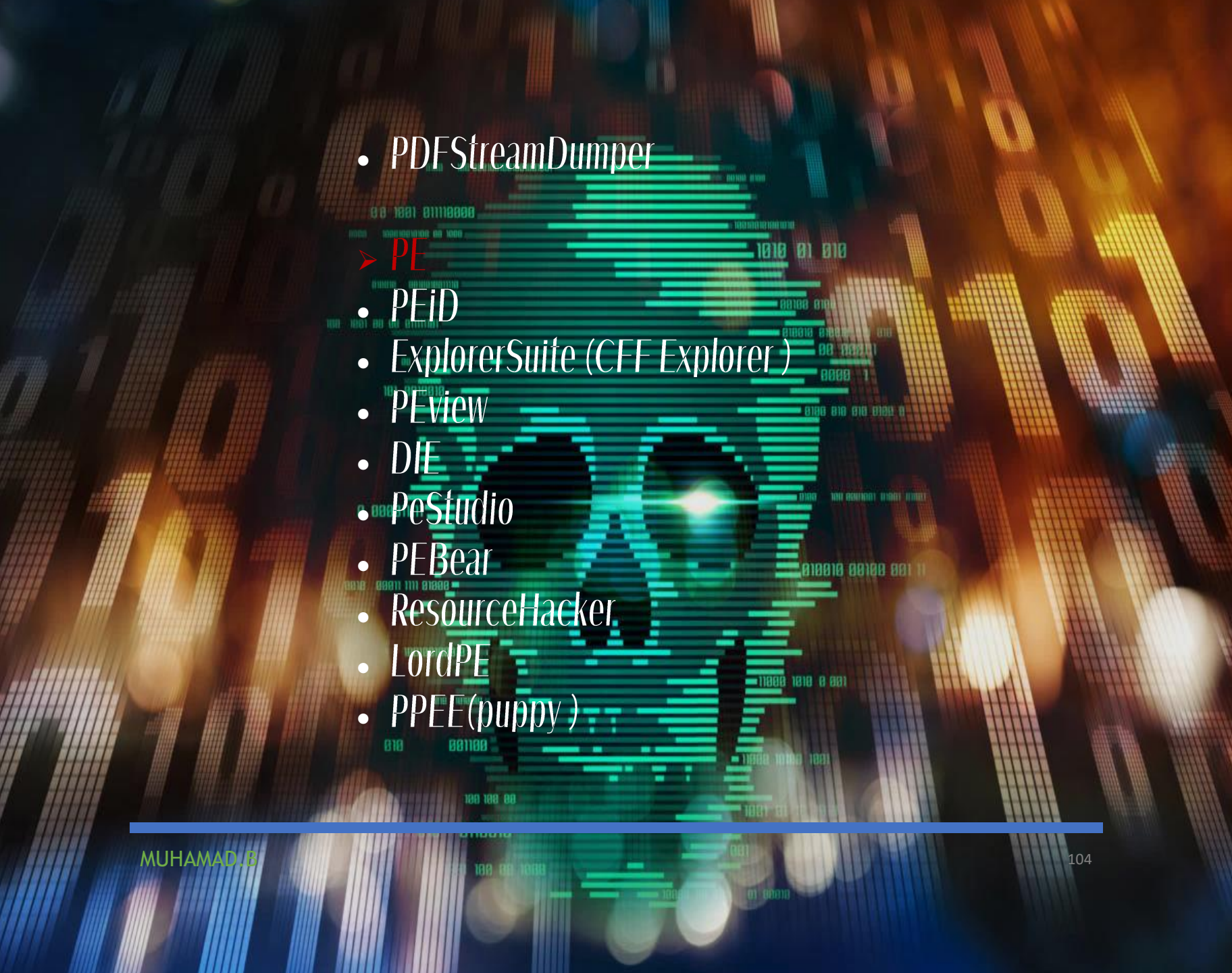
- nmap
- Wireshark

➢ Office

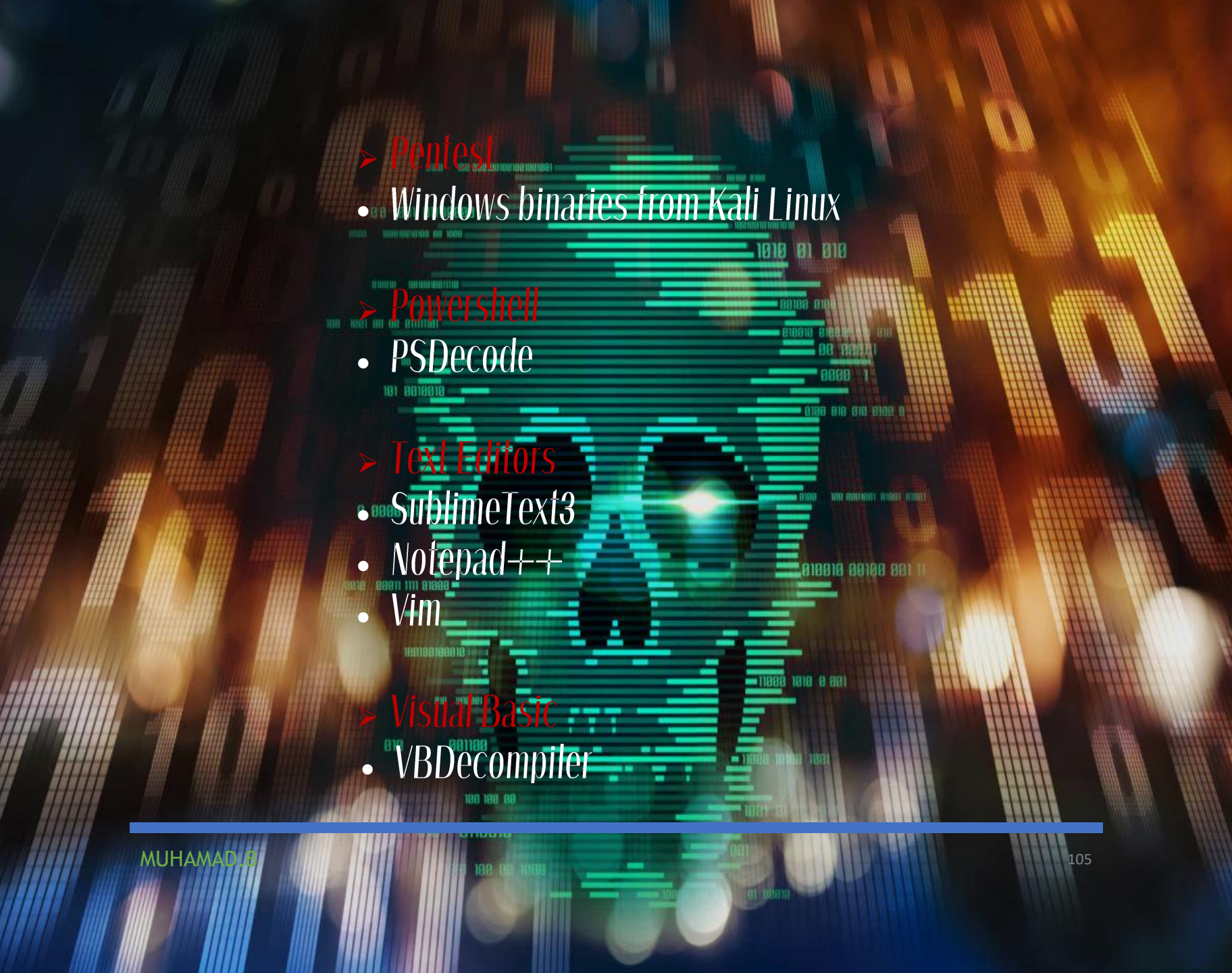
- Offvis
- OfficeMalScanner
- oledump.py
- rtfdump.py
- msoffcrypto-crack.py

➢ PDF

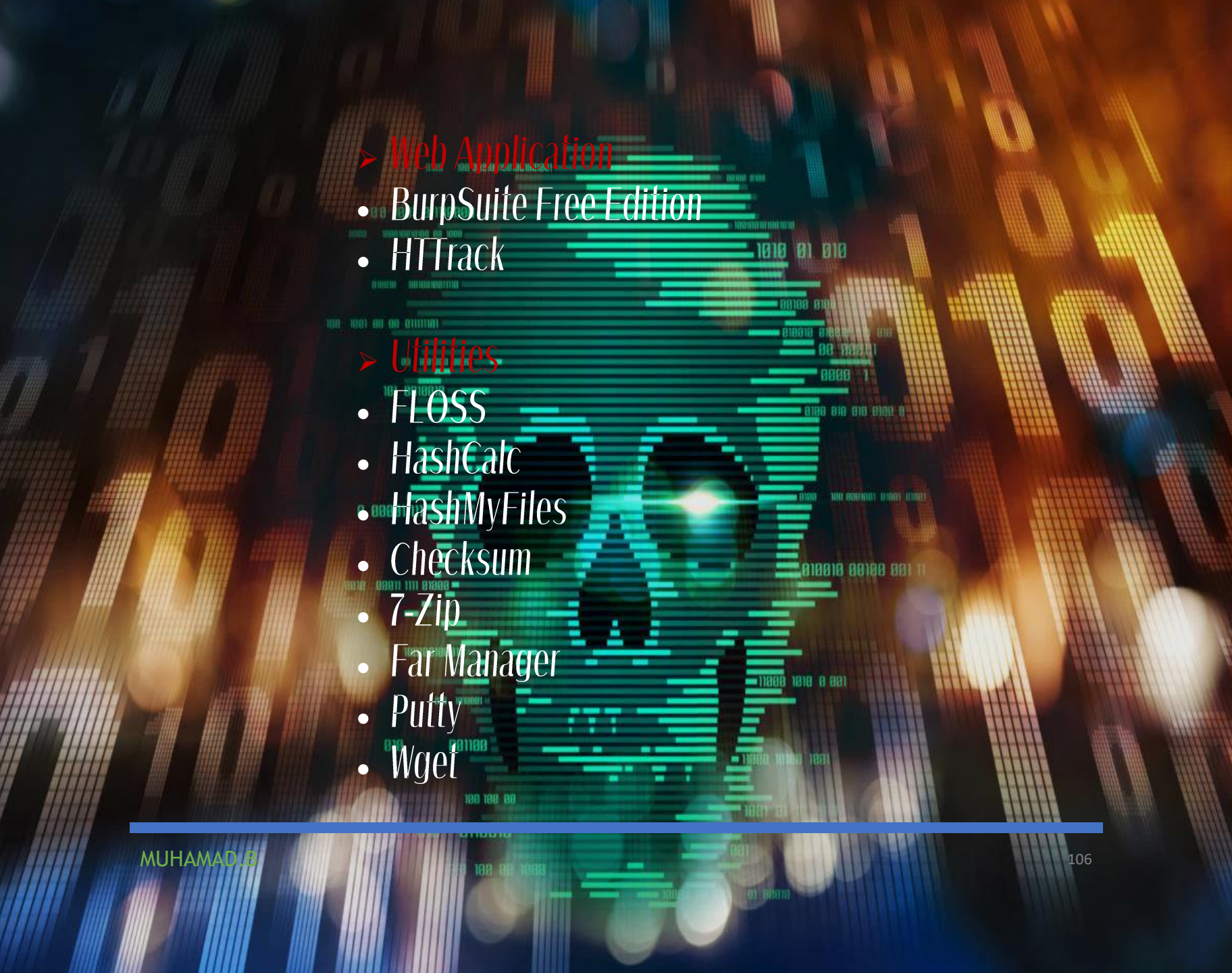
- PDFiD
- PDFParser



- PDFStreamDumper
- PE
- PEiD
- ExplorerSuite (CFF Explorer)
- PEview
- DIE
- PeStudio
- PEBear
- ResourceHacker
- LordPE
- PPEE(puppy)

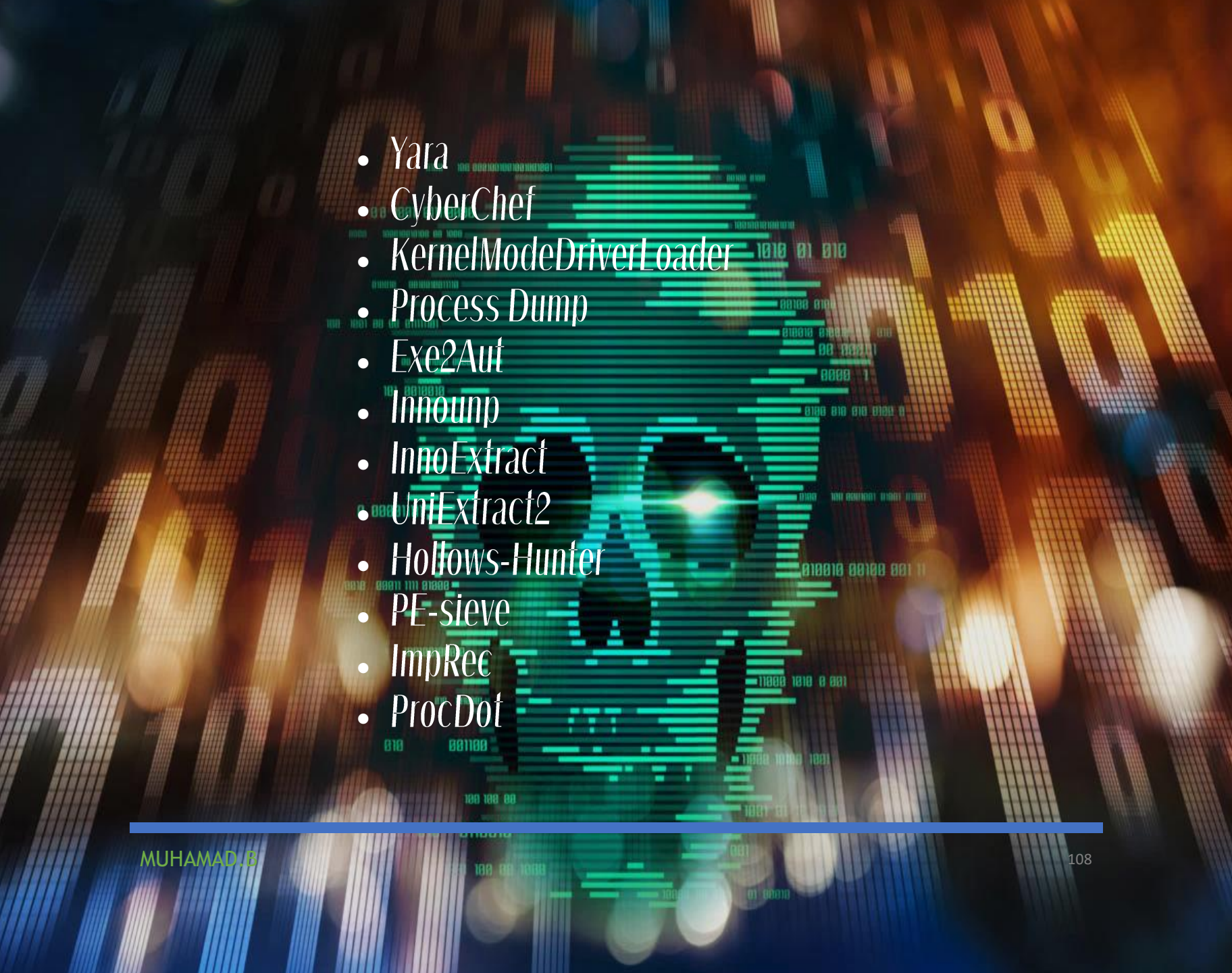


- Pentest
  - Windows binaries from Kali Linux
- Powershell
  - PSDecode
- Text Editors
  - SublimeText3
  - Notepad++
  - Vim
- Visual Basic
  - VBDecompiler

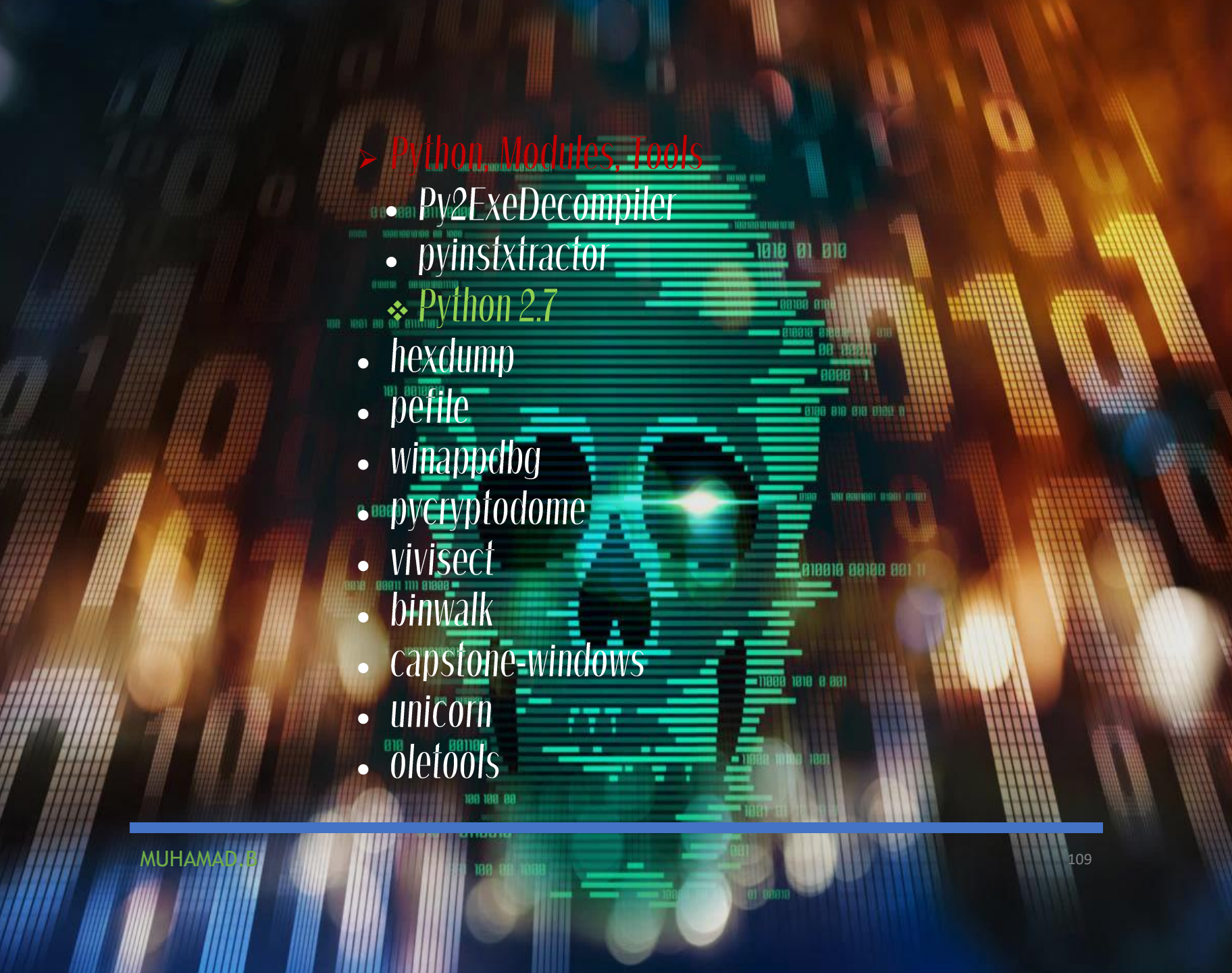


- Web Application
  - BurpSuite Free Edition
  - HTTrack
- Utilities
  - FLOSS
  - HashCalc
  - HashMyFiles
  - Checksum
  - 7-Zip
  - Far Manager
  - Putty
  - Wget

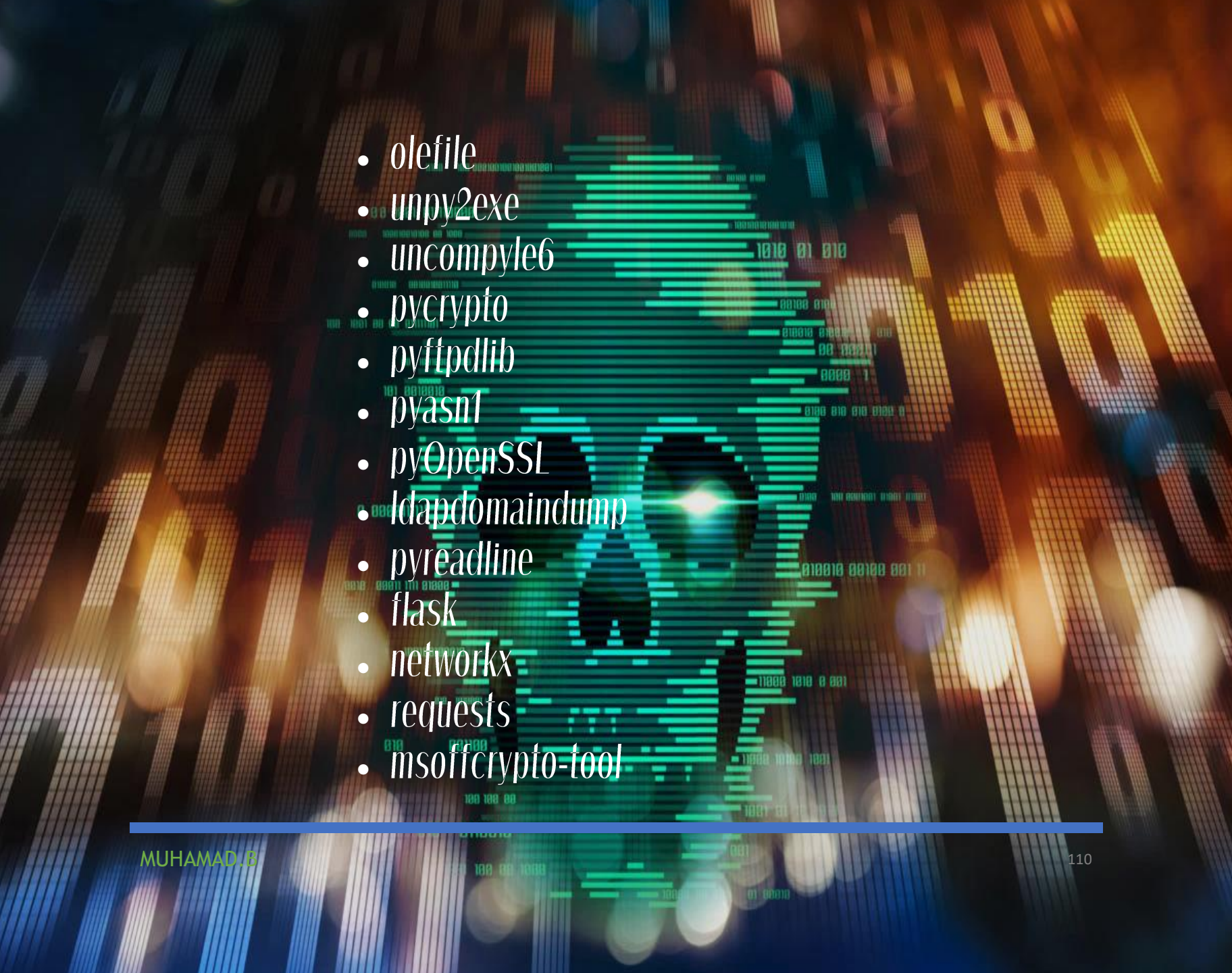
- RawCap
- UPX
- RegShot
- Process Hacker
- Sysinternals Suite
- API Monitor
- SpyStudio
- Shellcode Launcher
- Cygwin
- Unxutils
- Malcode Analyst Pack (MAP)
- XORSearch
- XORStrings



- Yara
- CyberChef
- KernelModeDriverLoader
- Process Dump
- Exe2Aut
- Innounp
- InnoExtract
- UniExtract2
- Hollows-Hunter
- PE-sieve
- ImpRec
- ProcDot



- Python Modules, Tools
  - Py2ExeDecompiler
  - pyinstxtractor
    - Python 2.7
- hexdump
- pefile
- winappdbg
- pycryptodome
- vivisect
- binwalk
- capstone-windows
- unicorn
- oletools



- olefile
- unpy2exe
- uncompyle6
- pycrypto
- pyftpdlib
- pyasn1
- pyOpenSSL
- ldapdomaindump
- pyreadline
- flask
- networkx
- requests
- msoffcrypto-tool

- yara-python
- mkyara
  - Python 3.7
- binwalk
- unpy2exe
- uncompyle6
- StringSifter
- hexdump
- pycryptodome
- oletools
- olefile
- msoffcrypto-tool
- pyftpdlib

- pyasn1
- pyOpenSSL
- acefile
- requests
- yara-python
- mkyara

➢ Other

- VC Redistributable Modules (2005, 2008, 2010, 2012, 2013, 2015, 2017)
- .NET Framework versions 4.8
- Practical Malware Analysis Labs
- Google Chrome & Cmder

- لەگەڵ چەندین بەرنامەیتر کە وەك فایلێك دامناوە ئەتوانن سودیان لێببینن.

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
Autoruns.zip	2,674,525	2,668,080	WinRAR ZIP archive	8/15/2020 10:0...	28885739
BytecodeViewer.2.9.8.zip	2,344,916	2,321,142	WinRAR ZIP archive	8/15/2020 10:0...	77CCB5A4
Bytecode-Viewer-2.9.22.jar	28,351,228	25,326,899	WinRAR archive	8/15/2020 10:0...	BE90517F
dnSpy-netcore-win64.zip	85,149,416	84,088,642	WinRAR ZIP archive	8/15/2020 10:0...	03DD9BA0
exeinfope.zip	2,069,093	2,069,093	WinRAR ZIP archive	8/15/2020 11:1...	04B8C067
flare-vm-master.zip	42,102	40,251	WinRAR ZIP archive	8/17/2020 11:4...	69D87D4D
ghidra_9.1.2_PUBLIC_202002...	302,233,568	284,179,233	WinRAR ZIP archive	8/15/2020 9:57 ...	916C11E2
odbg110.zip	1,333,471	1,333,471	WinRAR ZIP archive	8/15/2020 11:2...	B3B6856A
PEiD-0.95-20081103.zip	398,311	397,596	WinRAR ZIP archive	8/15/2020 11:1...	D06DD9E...
pestudio.zip	938,695	938,695	WinRAR ZIP archive	8/18/2020 12:2...	E2F144E9
PEview.zip	31,521	31,521	WinRAR ZIP archive	8/15/2020 11:0...	96CA23A4
PracticalMalwareAnalysis-La...	1,921,158	1,921,158	WinRAR ZIP archive	8/15/2020 9:49 ...	809C09EF
ProcessMonitor.zip	1,567,005	1,567,005	WinRAR ZIP archive	8/15/2020 10:0...	68223954
sitespy-511nulled.rar	52,046,727	50,594,300	WinRAR archive	8/15/2020 9:53 ...	99B8412D
snapshot_2020-08-07_14-32....	32,125,214	31,789,052	WinRAR ZIP archive	8/15/2020 9:49 ...	F203EDE3
Win7AndW2K8R2-KB319156...	68,076,477	68,076,477	WinRAR ZIP archive	8/18/2020 6:41 ...	E643FBD2
autopsy-4.15.0-64bit.msi	866,508,288	817,956,523	Windows Installer P...	8/23/2020 6:03 ...	176D7EF7
ExplorerSuite.exe	3,613,174	3,531,741	Application	8/18/2020 12:2...	C773E1BC
filealyz-2.0.5.57.exe	4,333,832	4,312,503	Application	8/15/2020 11:0...	5566BB4C
idafree70_windows.exe	60,955,032	57,387,018	Application	8/15/2020 10:1...	A8D4BC0C
ImmunityDebugger_1_85_set...	22,749,412	22,688,216	Application	8/15/2020 10:0...	5EA6BAB1
JavaSetup8u261.exe	2,083,464	706,727	Application	8/15/2020 10:5...	2FE9041E
jdk-14.0.2_windows-x64_bin....	169,989,784	168,341,442	Application	8/15/2020 10:5...	517428BB
NM34_x64.exe	6,837,560	6,791,743	Application	8/15/2020 10:4...	4713AD7A
npp.7.8.9.Installer.exe	3,774,904	3,687,709	Application	8/15/2020 11:1...	7B344424
processhacker-2.39-setup.exe	2,267,848	2,224,463	Application	8/15/2020 10:0...	D91BEB8F
python-3.8.5-amd64.exe	27,864,320	27,589,708	Application	8/15/2020 10:5...	50423392
reshacker_setup.exe	2,961,328	2,913,595	Application	8/15/2020 11:1...	331C9A11
Wireshark-win64-3.2.6.exe	60,127,072	59,981,857	Application	8/15/2020 10:1...	4FA007E1

ئەتوانن لێرەوە بینەری کۆرسی مالوێر ئنالسیس بن،

https://niuji-my.sharepoint.com/:f:/g/personal/lonewolf0_5th_live/EsvmakgDPk1EqxSeei9RPEoBviSESMMTYI8pN1xXK2mBVq2e=pnPvmP

Flare-On FireEye 2018 CTF - Malware Analy...	5 minutes ago	lonewolf0	259 MB	Shared
How To Setup A Sandbox Environment For ...	7 minutes ago	lonewolf0	64.1 MB	Shared
Malware Analysis Bootcamp - Analyzing Th...	7 minutes ago	lonewolf0	74.2 MB	Shared
Malware Analysis Bootcamp - Creating YAR...	7 minutes ago	lonewolf0	63.4 MB	Shared
Malware Analysis Bootcamp - Examining Th...	3 minutes ago	lonewolf0	38.5 MB	Shared
Malware Analysis Bootcamp - Extracting Str...	6 minutes ago	lonewolf0	22.0 MB	Shared
Malware Analysis Bootcamp - Generating ...	6 minutes ago	lonewolf0	20.8 MB	Shared
Malware Analysis Bootcamp - Introduction ...	6 minutes ago	lonewolf0	38.7 MB	Shared
Malware Analysis Bootcamp - Introduction ...	5 minutes ago	lonewolf0	10.3 MB	Shared
Malware Analysis Bootcamp - Introduction ...	5 minutes ago	lonewolf0	6.50 MB	Shared
Malware Analysis Bootcamp - Malware Clas...	5 minutes ago	lonewolf0	30.8 MB	Shared
Malware Analysis Bootcamp - Packers & Un...	About a minute ago	lonewolf0	30.4 MB	Shared
Malware Analysis Bootcamp - Setting Up O...	3 minutes ago	lonewolf0	62.4 MB	Shared
Malware Analysis Bootcamp - Understandin...	3 minutes ago	lonewolf0	17.2 MB	Shared
Malware Analysis With Ghidra - Stuxnet An...	About a minute ago	lonewolf0	104 MB	Shared

ئەتوانن سوود لەم راپۆرتە ببینن،

راپۆرتێك دەربارەی: ڕێگاکانی هاك و خۆپاراستن

https://www.home4t.com/2019/12/blog-post.html

کۆتایی.

بەهیوای سوود