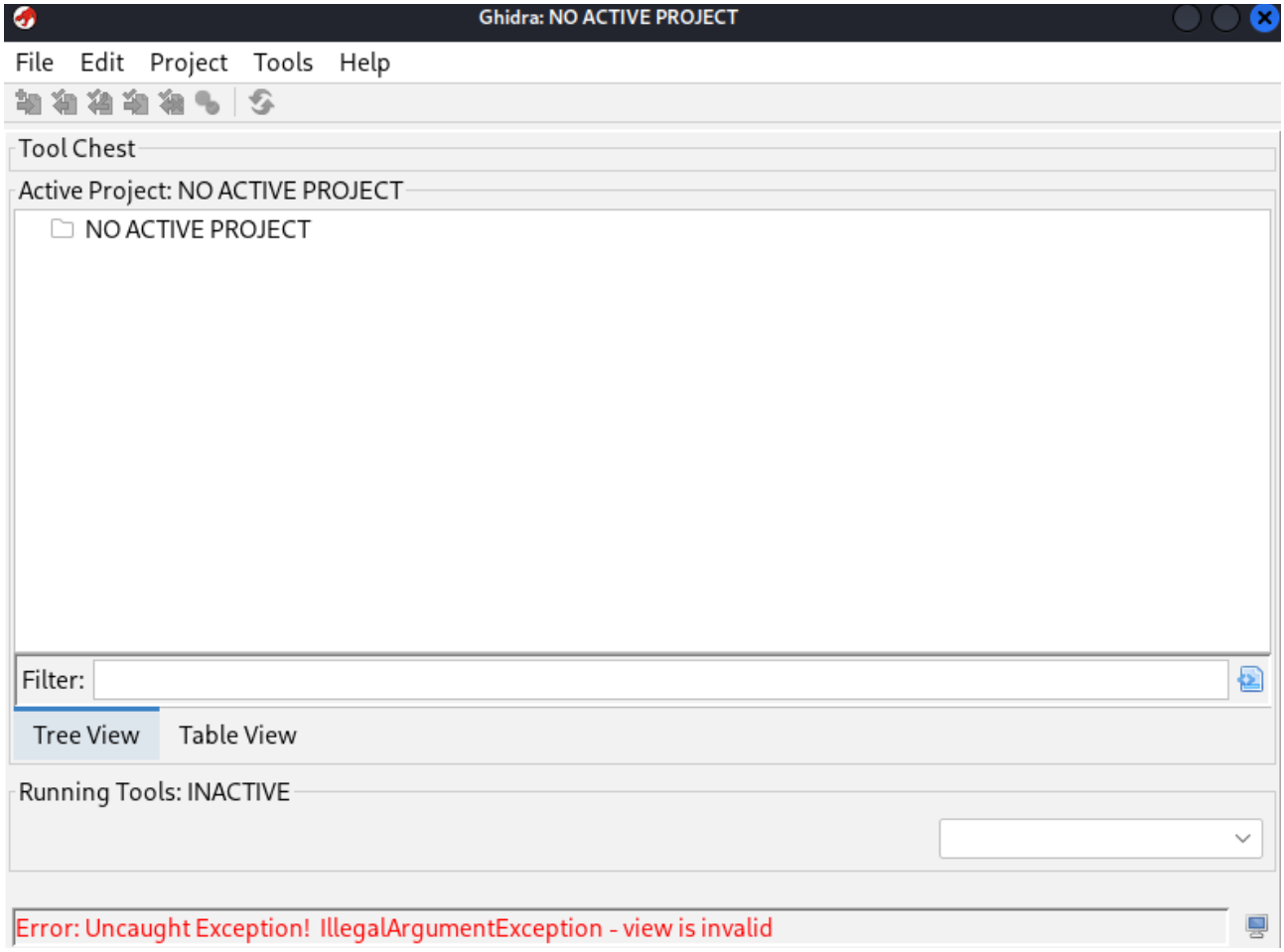
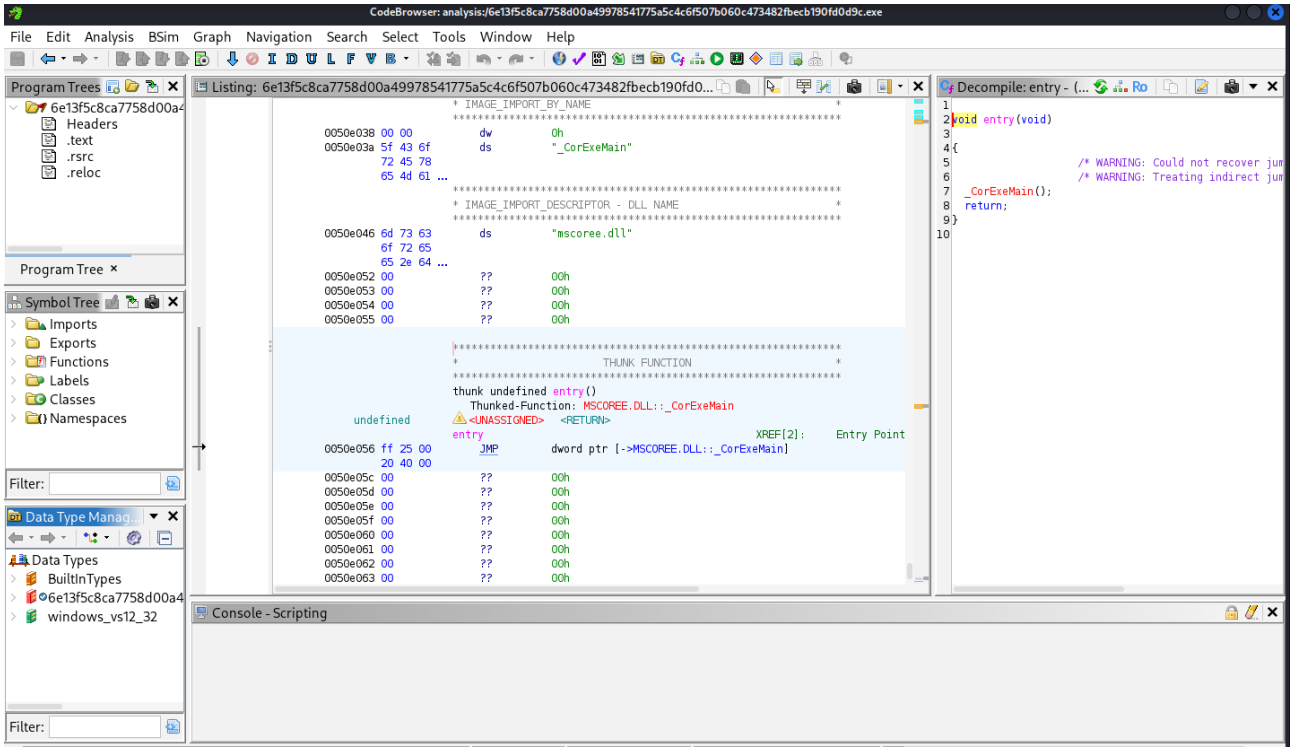
OUTPUT:

Ghidra:



Malware Analysis:



Main part of malware:

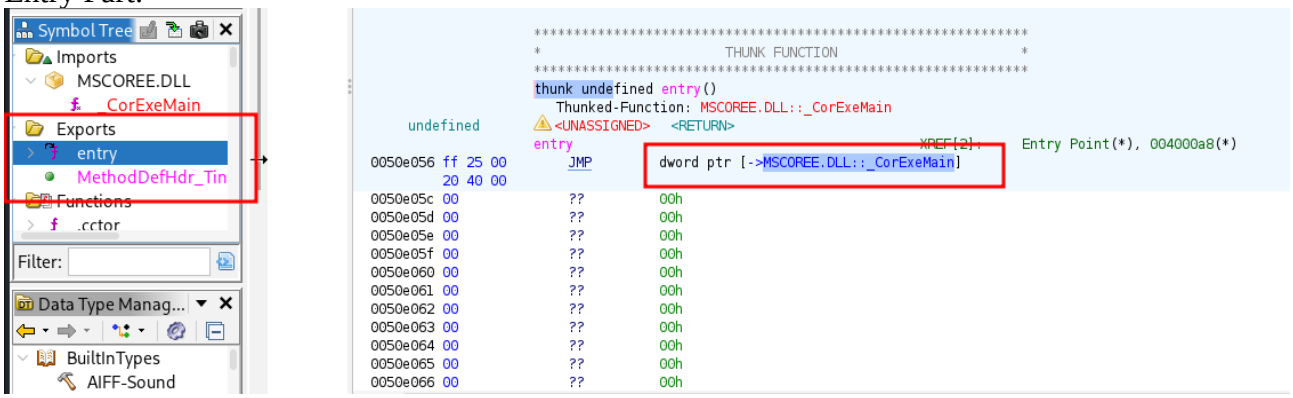
```
Decompile: entry - (6e13f5c8ca7758d00a49978541775a5c4c6f507b060c473482fbecb190f...
1
2 void entry(void)
3
4 {
5                     /* WARNING: Could not recover jumptable at 0x0050e056. Too many branches */
6                     /* WARNING: Treating indirect jump as call */
7   _CorExeMain();
8   return;
9 }
10
```

```
.....
                    //
                    // .text
                    // ram:00402000-ram:0050e1ff
                    //

                    *************************************************************
                    *                POINTER to EXTERNAL FUNCTION               *
                    *************************************************************
                    undefined _CorExeMain()
      undefined     <UNASSIGNED>   <RETURN>
                    0  _CorExeMain  <<not bound>>
                    PTR__CorExeMain_00402000                XREF[4]:     004000ac(*), 00400158(*),
                                                                         00400184(*), entry:0050e056
 00402000 38 e0 10 00     addr        MSCOREE.DLL::_CorExeMain
 00402004 00              ??          00h
 00402005 00              ??          00h
 00402006 00              ??          00h                                  ? -> 00480000
 00402007 00              ??          00h

                    IMAGE_COR20_HEADER_00402008             XREF[1]:     00400168(*)
 00402008 48 00 00        IMAGE_CO...                                      Size of the structure
          00 02 00
          05 00 48 ...
 00402050 13 30 02        MethodDe...                                      L.S. Bits 0:3 Size of hdr in byt...
          00 43 00
          00 00 00 ...
```

Trigger Part:

```
                    *************************************************************
                    *                          FUNCTION                         *
                    *************************************************************
                    undefined4 __fastcall button_main_Click(undefined4 sende...
     undefined4       EAX:4          <RETURN>
     undefined4       ECX:4          sender
     uint *           EDX:4          e
                    .NET CLR Managed Code
                    button_main_Click
 00404b14 00 02 7b        db[306]
          2b 00 00
          04 6f 83 ...
    00404b14 [0]              0h,  2h, 7Bh, 2Bh,
```

Entry Part:


Symbol Tree
Imports
MSCOREE.DLL
_CorExeMain
Exports
entry
MethodDefHdr_Tin
Functions
.cctor
Filter:
Data Type Manag...
BuiltInTypes
AIFF-Sound
thunk undefined entry()
Thunked-Function: MSCOREE.DLL::_CorExeMain
undefined
<UNASSIGNED> <RETURN>
entry
XREF[2]: Entry Point(*), 004000a8(*)
0050e056 ff 25 00 20 40 00 JMP dword ptr [->MSCOREE.DLL::_CorExeMain]
0050e05c 00 ?? 00h
0050e05d 00 ?? 00h
0050e05e 00 ?? 00h
0050e05f 00 ?? 00h
0050e060 00 ?? 00h
0050e061 00 ?? 00h
0050e062 00 ?? 00h
0050e063 00 ?? 00h
0050e064 00 ?? 00h
0050e065 00 ?? 00h
0050e066 00 ?? 00h