

Reply to Mr. Gotaimbara,

Response To: All the bloggers at Mr. Kalinga's Blog and Anonymous bloggers

What is the Core programming language of xAurora Web Browser?

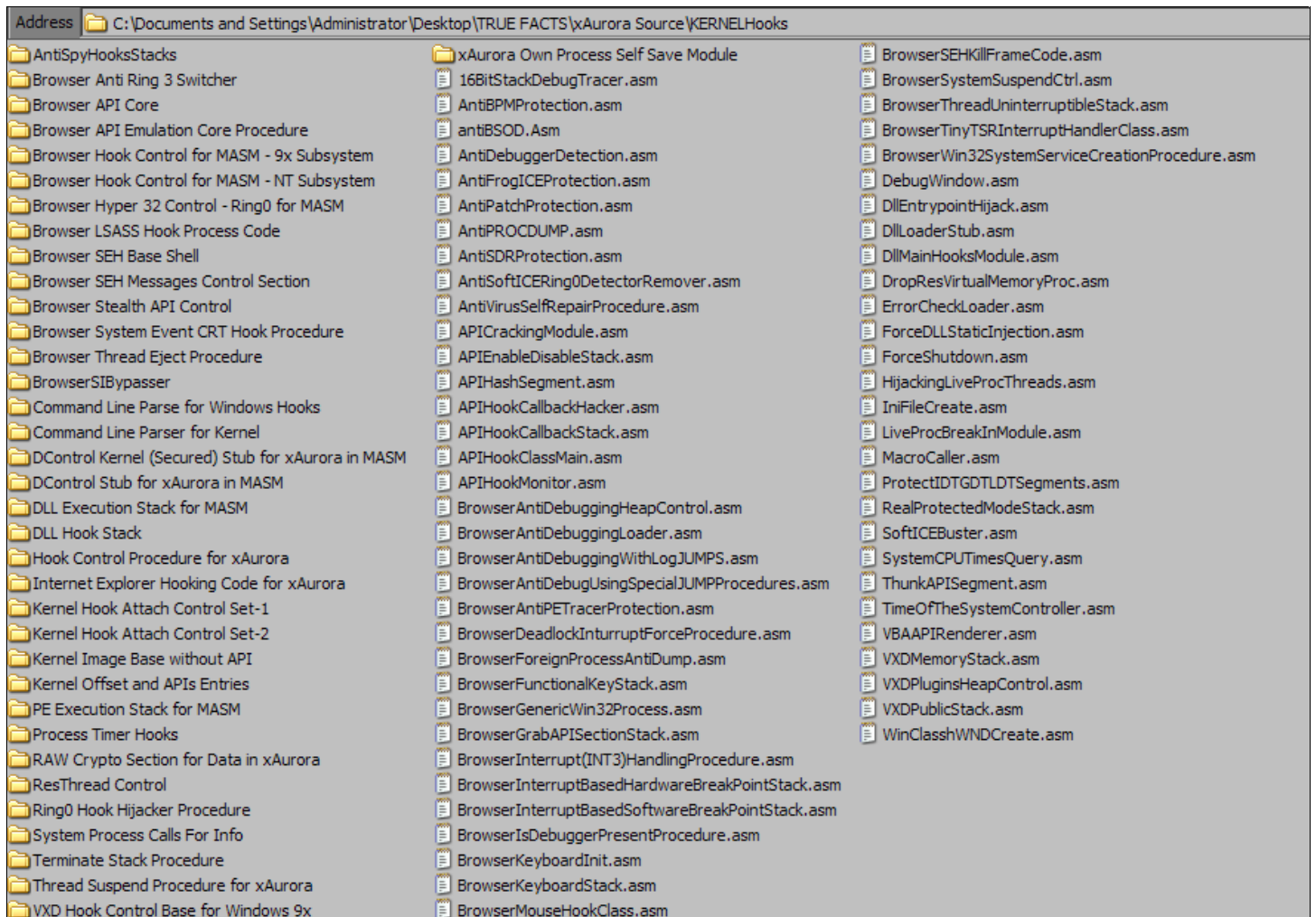
&

Is xAurora 100% coded in Win32-Microsoft Macro Assembler v8.20?

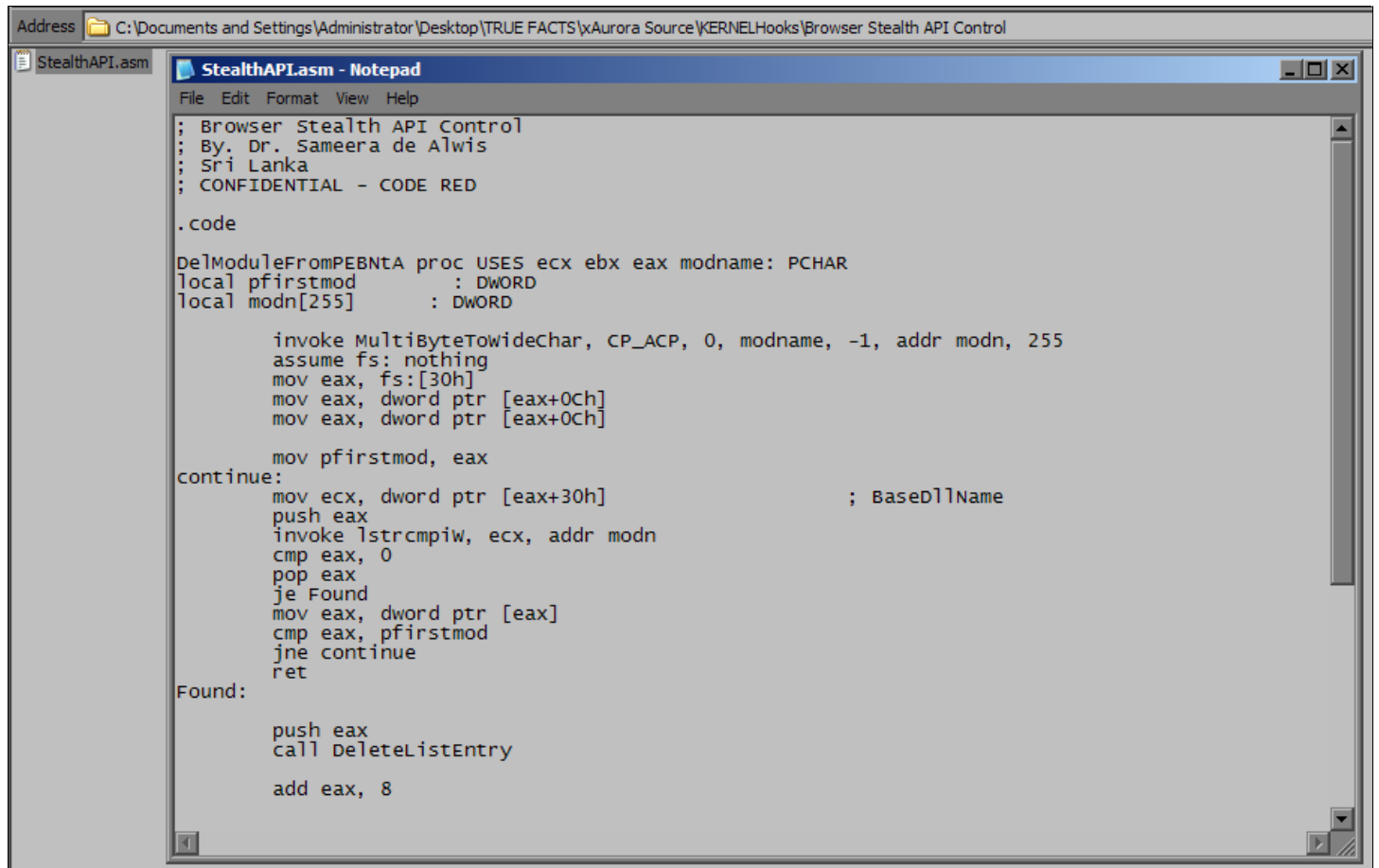
## xAurora Developers Pod Revealed - Visual Approach - PART 2

STRICTLY COFIDENTIAL SOURCE CODE (CATEGORY: **CODE RED**)

### 1. Kernel Hooking Segment Core Root



## 2. Browser Stealth API Control Stack



```
Address C:\Documents and Settings\Administrator\Desktop\TRUE FACTS\Aurora Source\KERNELHooks\Browser Stealth API Control
StealthAPI.asm
StealthAPI.asm - Notepad
File Edit Format View Help
; Browser Stealth API Control
; By: Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

.code

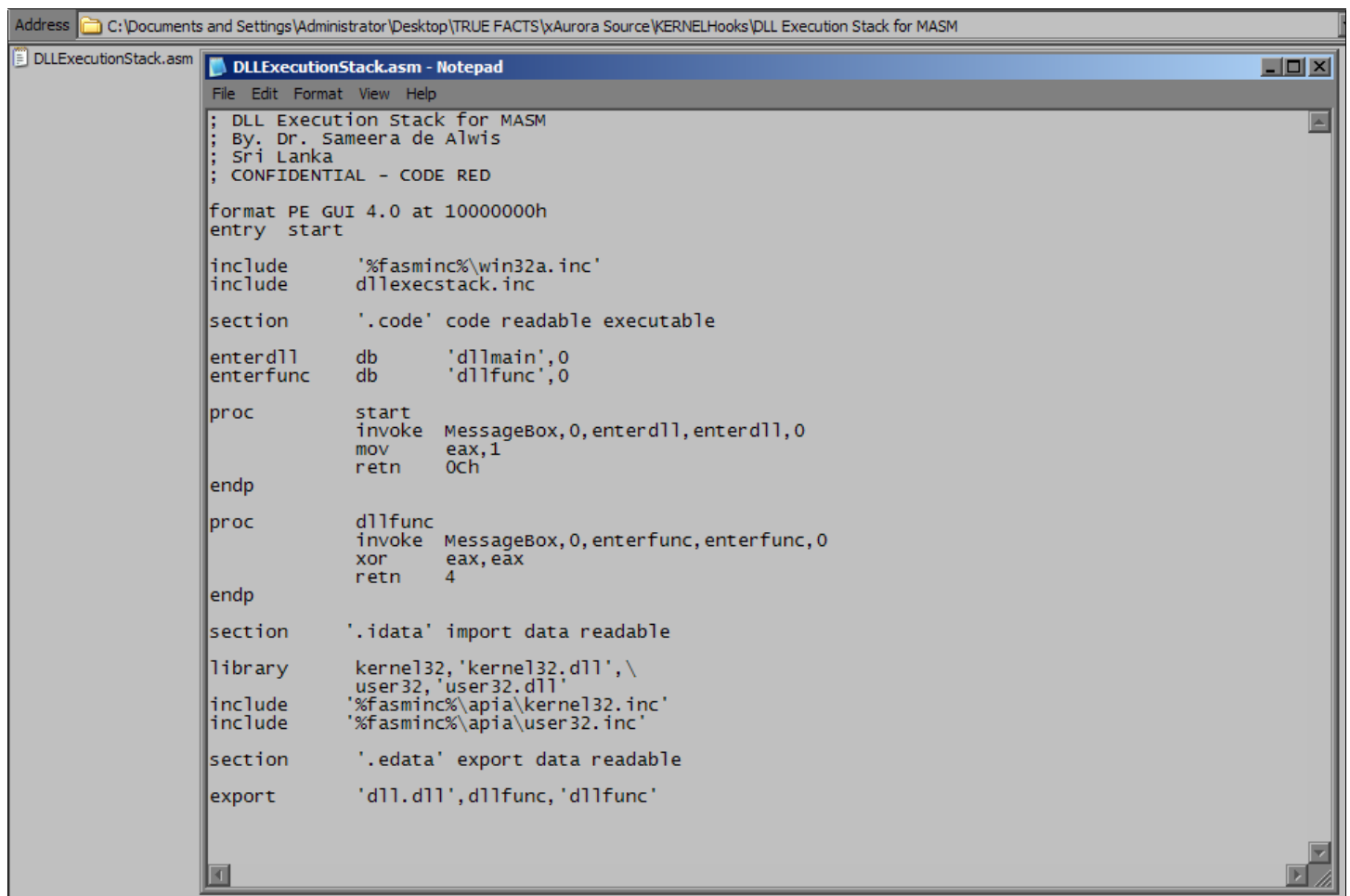
DelModuleFromPEBNTA proc USES ecx ebx eax modname: PCHAR
local pfirstmod : DWORD
local modn[255] : DWORD

    invoke MultiByteToWideChar, CP_ACP, 0, modname, -1, addr modn, 255
    assume fs: nothing
    mov eax, fs:[30h]
    mov eax, dword ptr [eax+0Ch]
    mov eax, dword ptr [eax+0Ch]

    mov pfirstmod, eax
continue:
    mov ecx, dword ptr [eax+30h] ; BasedllName
    push eax
    invoke lstrcmpiw, ecx, addr modn
    cmp eax, 0
    pop eax
    je Found
    mov eax, dword ptr [eax]
    cmp eax, pfirstmod
    jne continue
    ret
Found:
    push eax
    call DeleteListEntry

    add eax, 8
```

### 3. DLL Execution Stack



```
Address C:\Documents and Settings\Administrator\Desktop\TRUE FACTS\Aurora Source\KERNELHooks\DLL Execution Stack for MASM
DLLExecutionStack.asm
DLLExecutionStack.asm - Notepad
File Edit Format View Help
; DLL Execution Stack for MASM
; By. Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

format PE GUI 4.0 at 10000000h
entry start

include '%fasminc%\win32a.inc'
include dllexecstack.inc

section '.code' code readable executable

enterd11 db 'dllmain',0
enterfunc db 'dllfunc',0

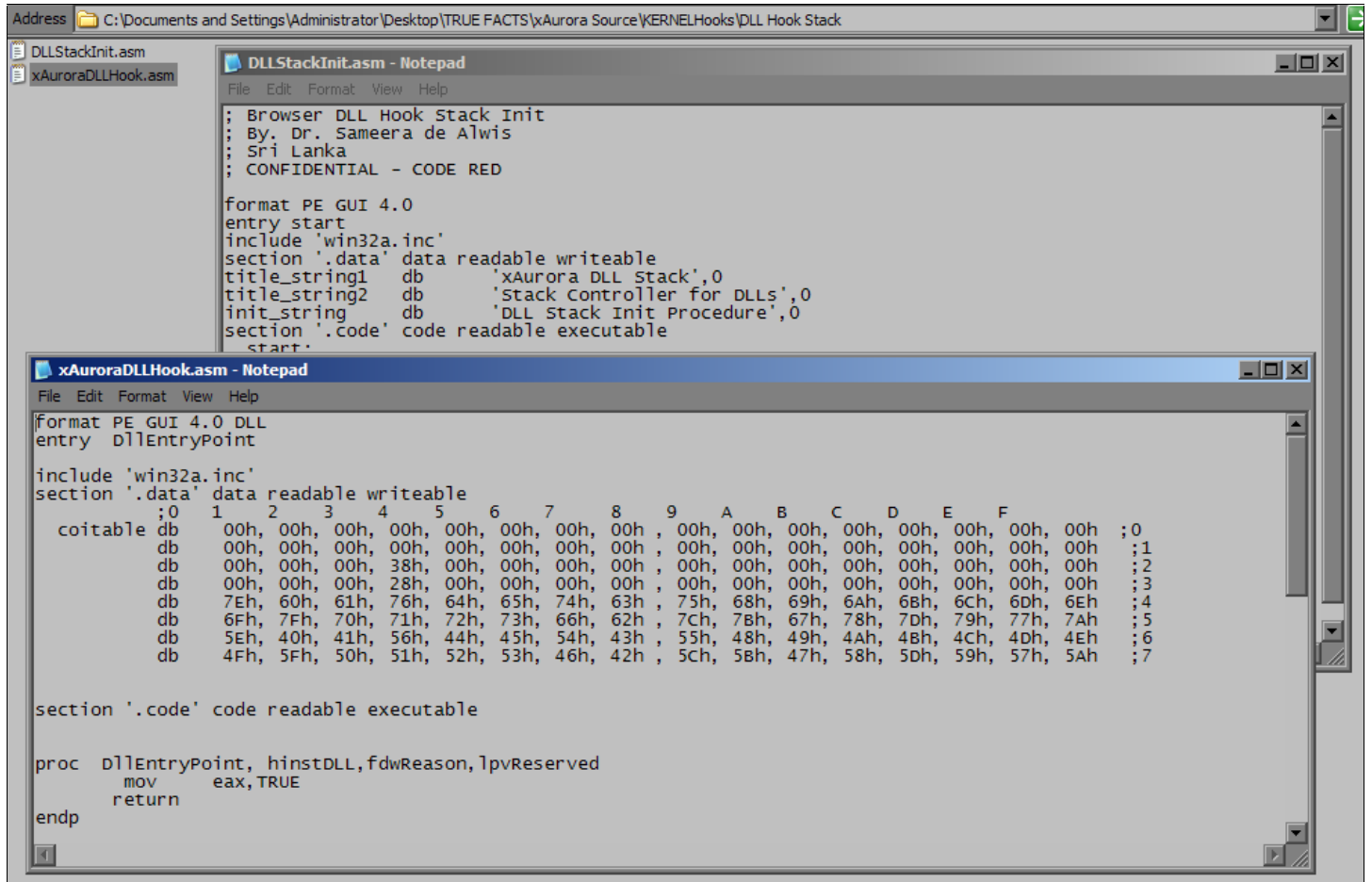
proc start
invoke MessageBox,0,enterd11,enterd11,0
mov eax,1
retn 0ch
endp

proc dllfunc
invoke MessageBox,0,enterfunc,enterfunc,0
xor eax,eax
retn 4
endp

section '.idata' import data readable
library kernel32,'kernel32.dll',\
user32,'user32.dll'
include '%fasminc%\apia\kernel32.inc'
include '%fasminc%\apia\user32.inc'

section '.edata' export data readable
export 'dll.dll',dllfunc,'dllfunc'
```

## 4. DLL Hook Stack



The image shows two Notepad windows. The top window, titled 'DLLStackInit.asm - Notepad', contains the following assembly code:

```
; Browser DLL Hook Stack Init
; By. Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

format PE GUI 4.0
entry start
include 'win32a.inc'
section '.data' data readable writeable
title_string1 db 'xAurora DLL Stack',0
title_string2 db 'Stack Controller for DLLs',0
init_string db 'DLL Stack Init Procedure',0
section '.code' code readable executable
start:
```

The bottom window, titled 'xAuroraDLLHook.asm - Notepad', contains the following assembly code:

```
format PE GUI 4.0 DLL
entry DllEntryPoint

include 'win32a.inc'
section '.data' data readable writeable
;0 1 2 3 4 5 6 7 8 9 A B C D E F
coitable db 00h, 00h, 00h, 00h, 00h, 00h, 00h, 00h, 00h, 00h, 00h, 00h, 00h, 00h, 00h, 00h ;0
db 00h, 00h, 00h, 00h, 00h, 00h, 00h, 00h, 00h, 00h, 00h, 00h, 00h, 00h, 00h, 00h ;1
db 00h, 00h, 00h, 38h, 00h, 00h, 00h, 00h, 00h, 00h, 00h, 00h, 00h, 00h, 00h, 00h ;2
db 00h, 00h, 00h, 28h, 00h, 00h, 00h, 00h, 00h, 00h, 00h, 00h, 00h, 00h, 00h, 00h ;3
db 7Eh, 60h, 61h, 76h, 64h, 65h, 74h, 63h, 75h, 68h, 69h, 6Ah, 68h, 6Ch, 6Dh, 6Eh ;4
db 6Fh, 7Fh, 70h, 71h, 72h, 73h, 66h, 62h, 7Ch, 7Bh, 67h, 78h, 7Dh, 79h, 77h, 7Ah ;5
db 5Eh, 40h, 41h, 56h, 44h, 45h, 54h, 43h, 55h, 48h, 49h, 4Ah, 4Bh, 4Ch, 4Dh, 4Eh ;6
db 4Fh, 5Fh, 50h, 51h, 52h, 53h, 46h, 42h, 5Ch, 5Bh, 47h, 58h, 5Dh, 59h, 57h, 5Ah ;7

section '.code' code readable executable

proc DllEntryPoint, hinstDLL, fdwReason, lpvReserved
mov eax, TRUE
return
endp
```

## 5. Internet Explorer Hooking Code

```
Address C:\Documents and Settings\Administrator\Desktop\TRUE FACTS\xAurora Source\KERNELHooks\Internet Explorer Hooking Code for xAurora
iehookformasm.asm

iehookformasm.asm - Notepad
File Edit Format View Help
; Internet Explorer Hooking Code for xAurora
; By: Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

.386
.model flat,stdcall
.option casemap:none
assume fs:nothing
code segment
null equ ebx

include c:\masm32\include\windows.inc
include c:\masm32\include\masm32.inc
include c:\masm32\include\kernel32.inc
include c:\masm32\include\wininet.inc
include c:\masm32\include\wsock32.inc
include c:\masm32\include\advapi32.inc
include c:\masm32\include\user32.inc

includelib c:\masm32\lib\masm32.lib
includelib c:\masm32\lib\kernel32.lib
includelib c:\masm32\lib\wininet.lib
includelib c:\masm32\lib\wsock32.lib
includelib c:\masm32\lib\advapi32.lib
includelib c:\masm32\lib\user32.lib

include hook.inc

pushsz macro sz:req
call $ + @sizeStr(sz) + 04h
db sz,0
endm
```

```
Address C:\Documents and Settings\Administrator\Desktop\TRUE FACTS\xAurora Source\KERNELHooks\Internet Explorer Hooking Code for xAurora
iehookformasm.asm

iehookformasm.asm - Notepad
File Edit Format View Help
invoke Process32First,\
hSnapshot,\
addr pe32
; _____ Call IE _____
_____Process32Next:

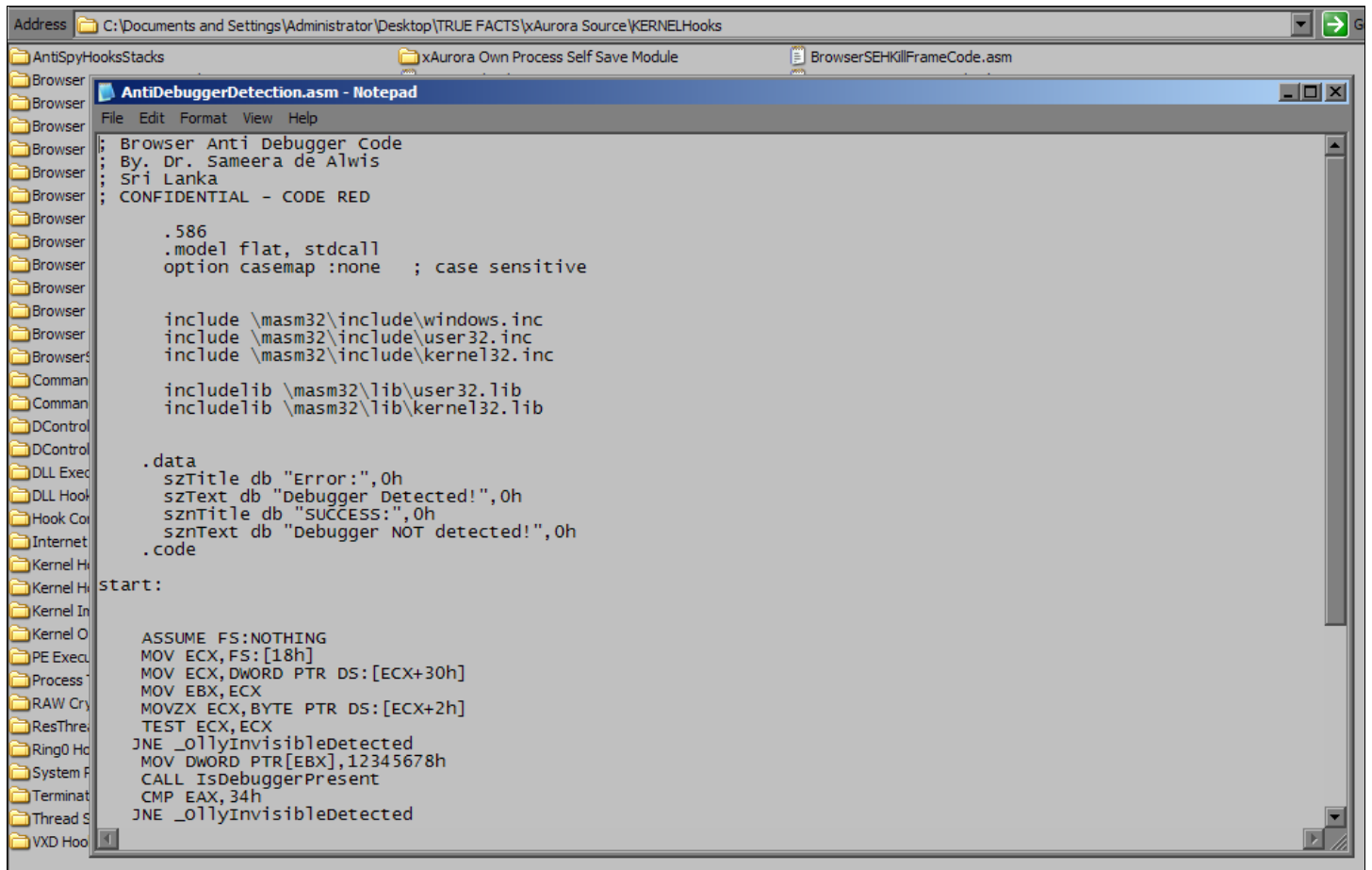
pushsz 'iexplore.exe'
lea eax,pe32.szExeFile
push eax
call lstrcmpi
test eax,eax
jnz _____DontHook

invoke OpenProcess,\
PROCESS_ALL_ACCESS,\
null,\
pe32.th32ProcessID
mov hProcess,eax

invoke CheckAPIHook,\
hProcess,\
CreateFilew

.if eax != 0
invoke APIHook,\
hProcess,\
CreateFilew,\
offset CreateFilewHook,\
CreateFilewHookSize
.endif
invoke CheckAPIHook,\
```

## 6. Anti Debugger Code – Basic



The image shows a Notepad window titled "AntiDebuggerDetection.asm - Notepad" with the following assembly code:

```
Address C:\Documents and Settings\Administrator\Desktop\TRUE FACTS\xAurora Source\KERNELHooks
xAurora Own Process Self Save Module
BrowserSEKillFrameCode.asm

; Browser Anti Debugger Code
; By. Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

.586
.model flat, stdcall
option casemap :none ; case sensitive

include \masm32\include\windows.inc
include \masm32\include\user32.inc
include \masm32\include\kernel32.inc

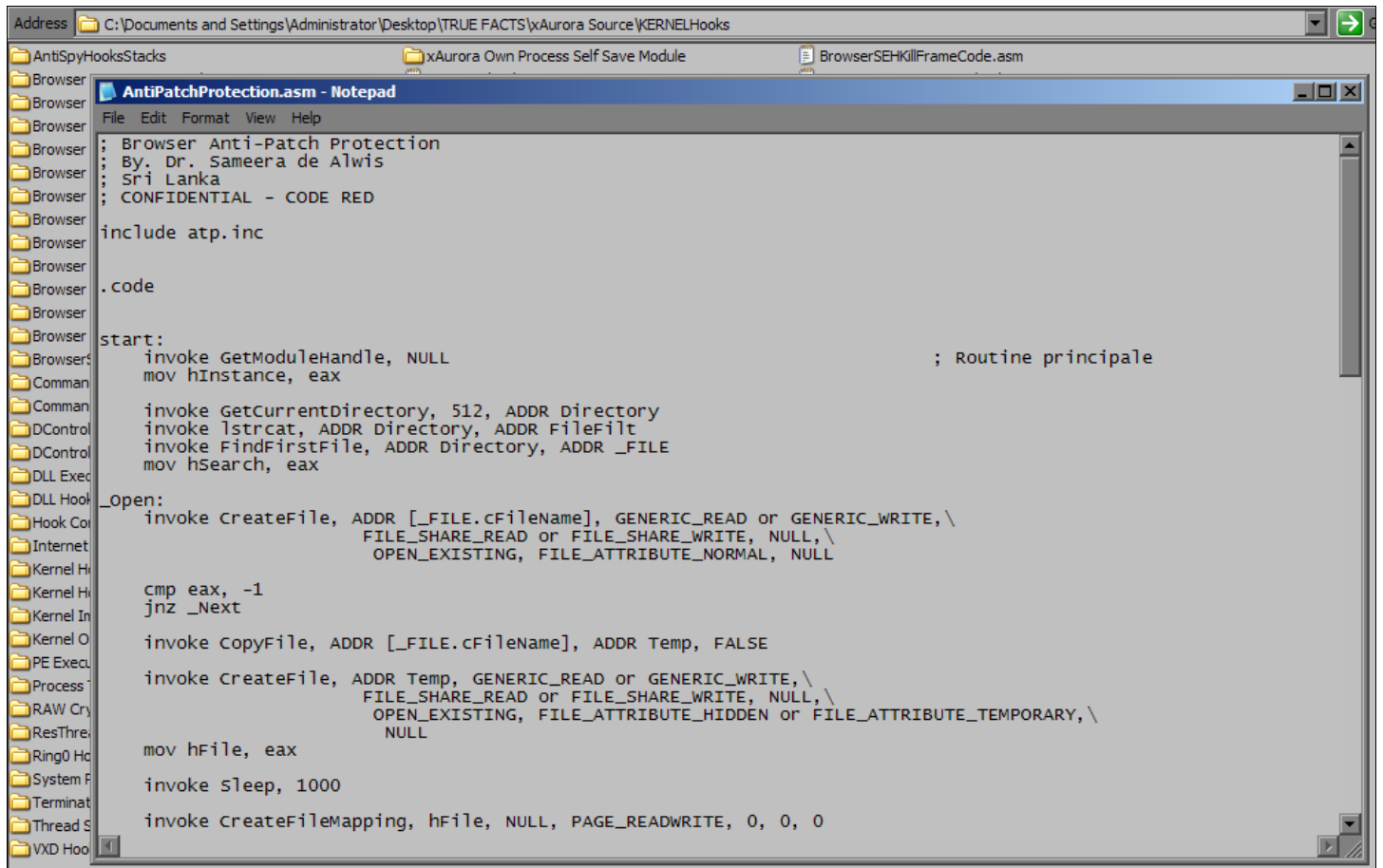
includelib \masm32\lib\user32.lib
includelib \masm32\lib\kernel32.lib

.data
szTitle db "Error:",0h
szText db "Debugger Detected!",0h
sznTitle db "SUCCESS:",0h
sznText db "Debugger NOT detected!",0h
.code

start:

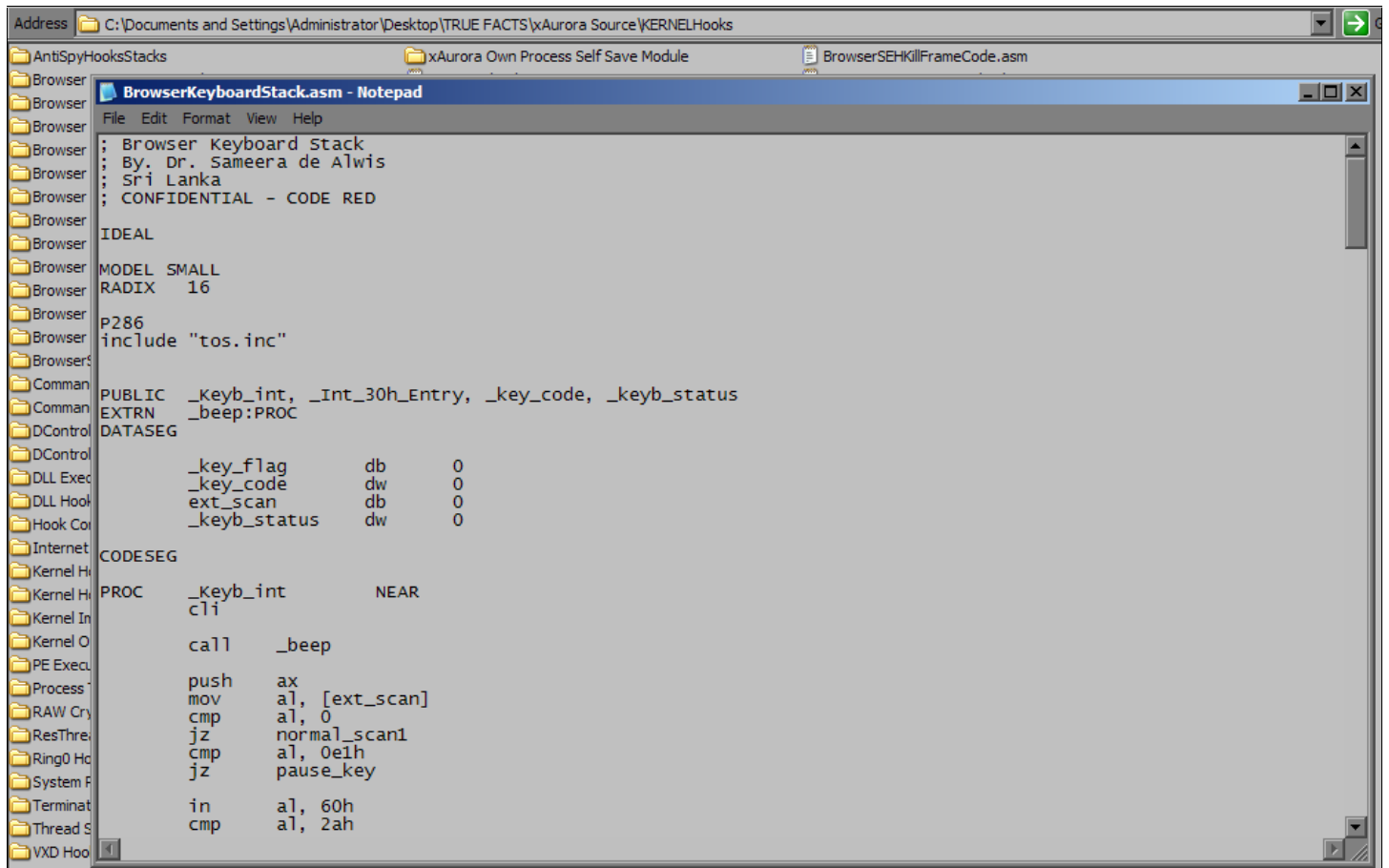
ASSUME FS:NOTHING
MOV ECX,FS:[18h]
MOV ECX,DWORD PTR DS:[ECX+30h]
MOV EBX,ECX
MOVZX ECX,BYTE PTR DS:[ECX+2h]
TEST ECX,ECX
JNE _0llyInvisibleDetected
MOV DWORD PTR [EBX],12345678h
CALL IsDebuggerPresent
CMP EAX,34h
JNE _0llyInvisibleDetected
```

## 7. Browser Anti-Patch Protection



```
Address C:\Documents and Settings\Administrator\Desktop\TRUE FACTS\xAurora Source\KERNELHooks
AntiSpyHooksStacks xAurora Own Process Self Save Module BrowserSEHKillFrameCode.asm
AntiPatchProtection.asm - Notepad
File Edit Format View Help
; Browser Anti-Patch Protection
; By. Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED
include atp.inc
.code
start:
    invoke GetModuleHandle, NULL ; Routine principale
    mov hInstance, eax
    invoke GetCurrentDirectory, 512, ADDR Directory
    invoke lstrcat, ADDR Directory, ADDR FileFilt
    invoke FindFirstFile, ADDR Directory, ADDR _FILE
    mov hSearch, eax
_Open:
    invoke CreateFile, ADDR [_FILE.cfileName], GENERIC_READ or GENERIC_WRITE, \
        FILE_SHARE_READ or FILE_SHARE_WRITE, NULL, \
        OPEN_EXISTING, FILE_ATTRIBUTE_NORMAL, NULL
    cmp eax, -1
    jnz _Next
    invoke CopyFile, ADDR [_FILE.cfileName], ADDR Temp, FALSE
    invoke CreateFile, ADDR Temp, GENERIC_READ or GENERIC_WRITE, \
        FILE_SHARE_READ or FILE_SHARE_WRITE, NULL, \
        OPEN_EXISTING, FILE_ATTRIBUTE_HIDDEN or FILE_ATTRIBUTE_TEMPORARY, \
        NULL
    mov hFile, eax
    invoke Sleep, 1000
    invoke CreateFileMapping, hFile, NULL, PAGE_READWRITE, 0, 0, 0
```

## 8. Browser Keyboard Stack



```
Address C:\Documents and Settings\Administrator\Desktop\TRUE FACTS\xAurora Source\KERNELHooks
xAurora Own Process Self Save Module
BrowserSEHKillFrameCode.asm

BrowserKeyboardStack.asm - Notepad
File Edit Format View Help

; Browser Keyboard Stack
; By. Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

IDEAL

MODEL SMALL
RADIX 16

P286
include "tos.inc"

PUBLIC _keyb_int, _Int_30h_Entry, _key_code, _keyb_status
EXTRN _beep:PROC

DATASEG

    _key_flag      db    0
    _key_code      dw    0
    ext_scan       db    0
    _keyb_status   dw    0

CODESEG

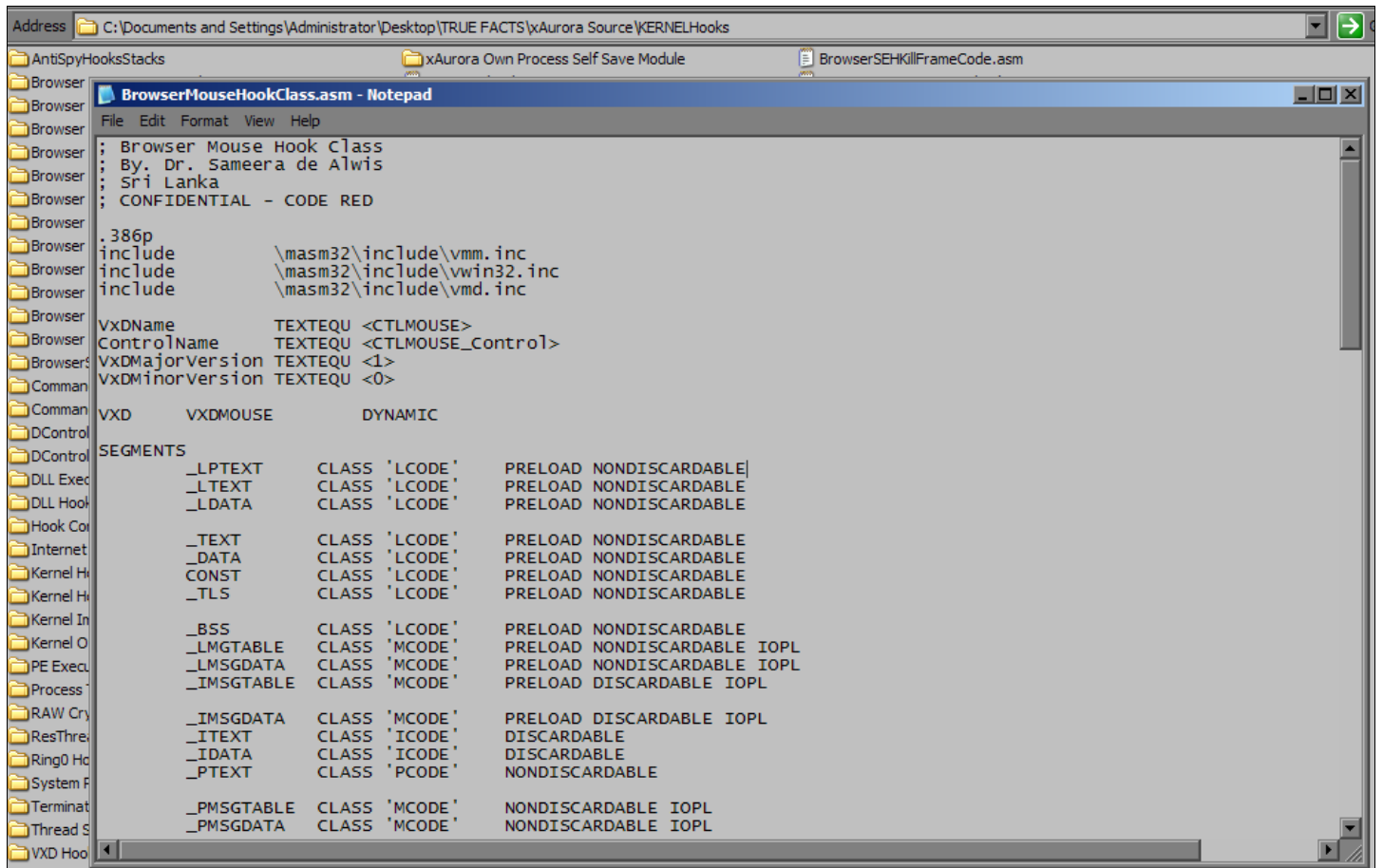
PROC    _keyb_int      NEAR
cli

    call    _beep

    push   ax
    mov    al, [ext_scan]
    cmp    al, 0
    jz     normal_scan1
    cmp    al, 0e1h
    jz     pause_key

    in     al, 60h
    cmp    al, 2ah
```

## 9. Browser Mouse Hook Class



```
Address C:\Documents and Settings\Administrator\Desktop\TRUE FACTS\xAurora Source\KERNELHooks
xAurora Own Process Self Save Module
BrowserSEHKillFrameCode.asm

BrowserMouseHookClass.asm - Notepad
File Edit Format View Help

; Browser Mouse Hook Class
; By: Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

.386p
include \masm32\include\mmm.inc
include \masm32\include\win32.inc
include \masm32\include\vmx.inc

VxDName TEXT EQU <CTLMOUSE>
ControlName TEXT EQU <CTLMOUSE_Control>
VxDMajorVersion TEXT EQU <1>
VxDMinorVersion TEXT EQU <0>

VXD VXDMOUSE DYNAMIC

SEGMENTS
  _LPTEXT CLASS 'LCODE' PRELOAD NONDISCARDABLE
  _LTEXT CLASS 'LCODE' PRELOAD NONDISCARDABLE
  _LDATA CLASS 'LCODE' PRELOAD NONDISCARDABLE

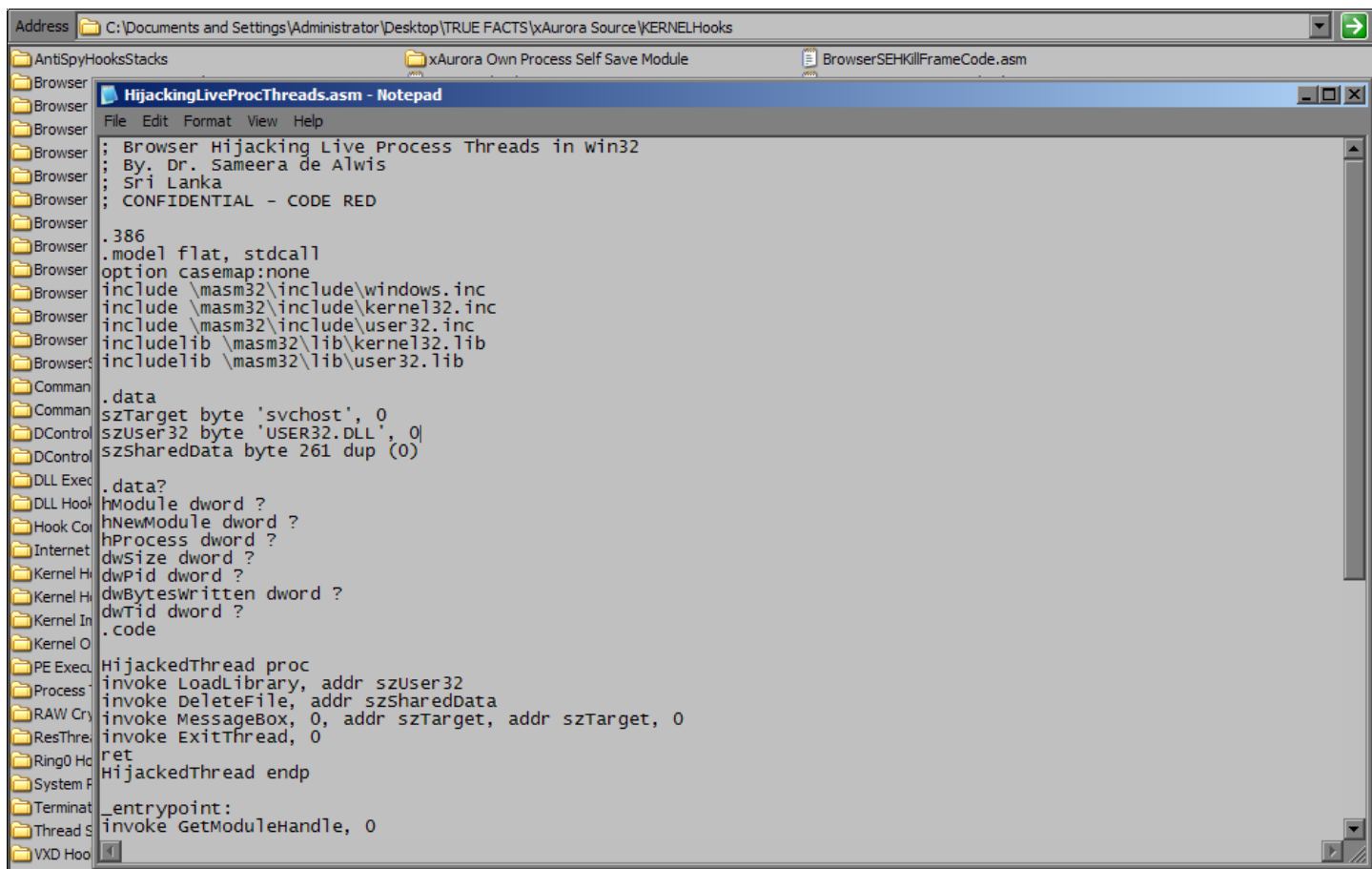
  _TEXT CLASS 'LCODE' PRELOAD NONDISCARDABLE
  _DATA CLASS 'LCODE' PRELOAD NONDISCARDABLE
  CONST CLASS 'LCODE' PRELOAD NONDISCARDABLE
  _TLS CLASS 'LCODE' PRELOAD NONDISCARDABLE

  _BSS CLASS 'LCODE' PRELOAD NONDISCARDABLE
  _LMGTABLE CLASS 'MCODE' PRELOAD NONDISCARDABLE IOPL
  _LMSGDATA CLASS 'MCODE' PRELOAD NONDISCARDABLE IOPL
  _IMSGTABLE CLASS 'MCODE' PRELOAD DISCARDABLE IOPL

  _IMSGDATA CLASS 'MCODE' PRELOAD DISCARDABLE IOPL
  _ITEXT CLASS 'ICODE' DISCARDABLE
  _IDATA CLASS 'ICODE' DISCARDABLE
  _PTEXT CLASS 'PCODE' NONDISCARDABLE

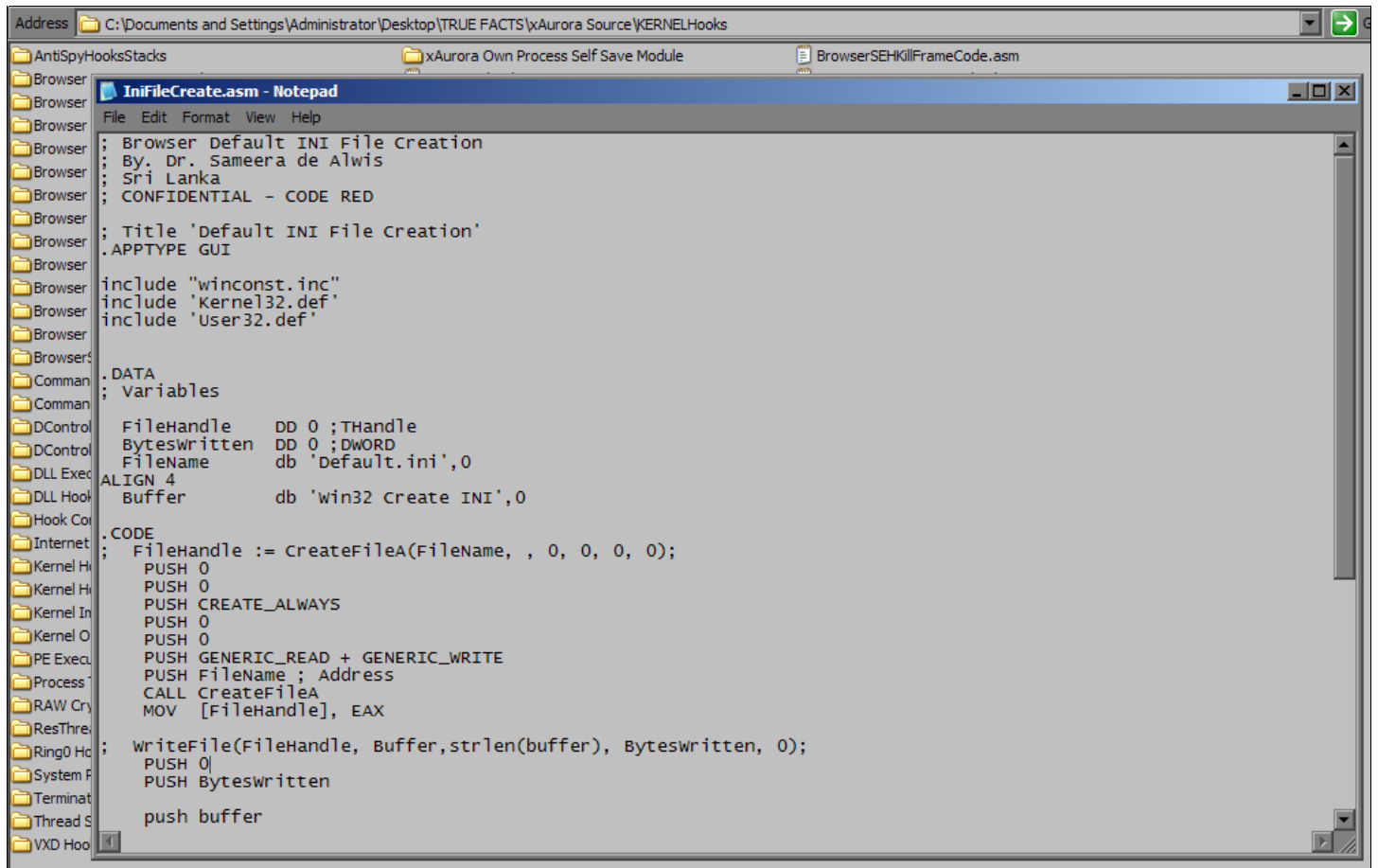
  _PMSGTABLE CLASS 'MCODE' NONDISCARDABLE IOPL
  _PMSGDATA CLASS 'MCODE' NONDISCARDABLE IOPL
```

## 10. Browser Hijacking Live Process Threads



```
Address C:\Documents and Settings\Administrator\Desktop\TRUE FACTS\xAurora Source\KERNELHooks
AntiSpyHooksStacks xAurora Own Process Self Save Module BrowserSEHKillFrameCode.asm
HijackingLiveProcThreads.asm - Notepad
File Edit Format View Help
; Browser Hijacking Live Process Threads in win32
; By. Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED
.386
.model flat, stdcall
.option casemap:none
include \masm32\include\windows.inc
include \masm32\include\kernel32.inc
include \masm32\include\user32.inc
includelib \masm32\lib\kernel32.lib
includelib \masm32\lib\user32.lib
.data
szTarget byte 'svchost', 0
szUser32 byte 'USER32.DLL', 0
szSharedData byte 261 dup (0)
.data?
hModule dword ?
hNewModule dword ?
hProcess dword ?
dwSize dword ?
dwPid dword ?
dwBytesWritten dword ?
dwTid dword ?
.code
HijackedThread proc
invoke LoadLibrary, addr szUser32
invoke DeleteFile, addr szSharedData
invoke MessageBox, 0, addr szTarget, addr szTarget, 0
invoke ExitThread, 0
ret
HijackedThread endp
_entrypoint:
invoke GetModuleHandle, 0
```

## 11. Browser Default INI File Creation



```
Address C:\Documents and Settings\Administrator\Desktop\TRUE FACTS\xAurora Source\KERNELHooks
xAurora Own Process Self Save Module
BrowserSEHKillFrameCode.asm

IniFileCreate.asm - Notepad
File Edit Format View Help

; Browser Default INI File Creation
; By. Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

; Title 'Default INI File Creation'
.APPTYPE GUI

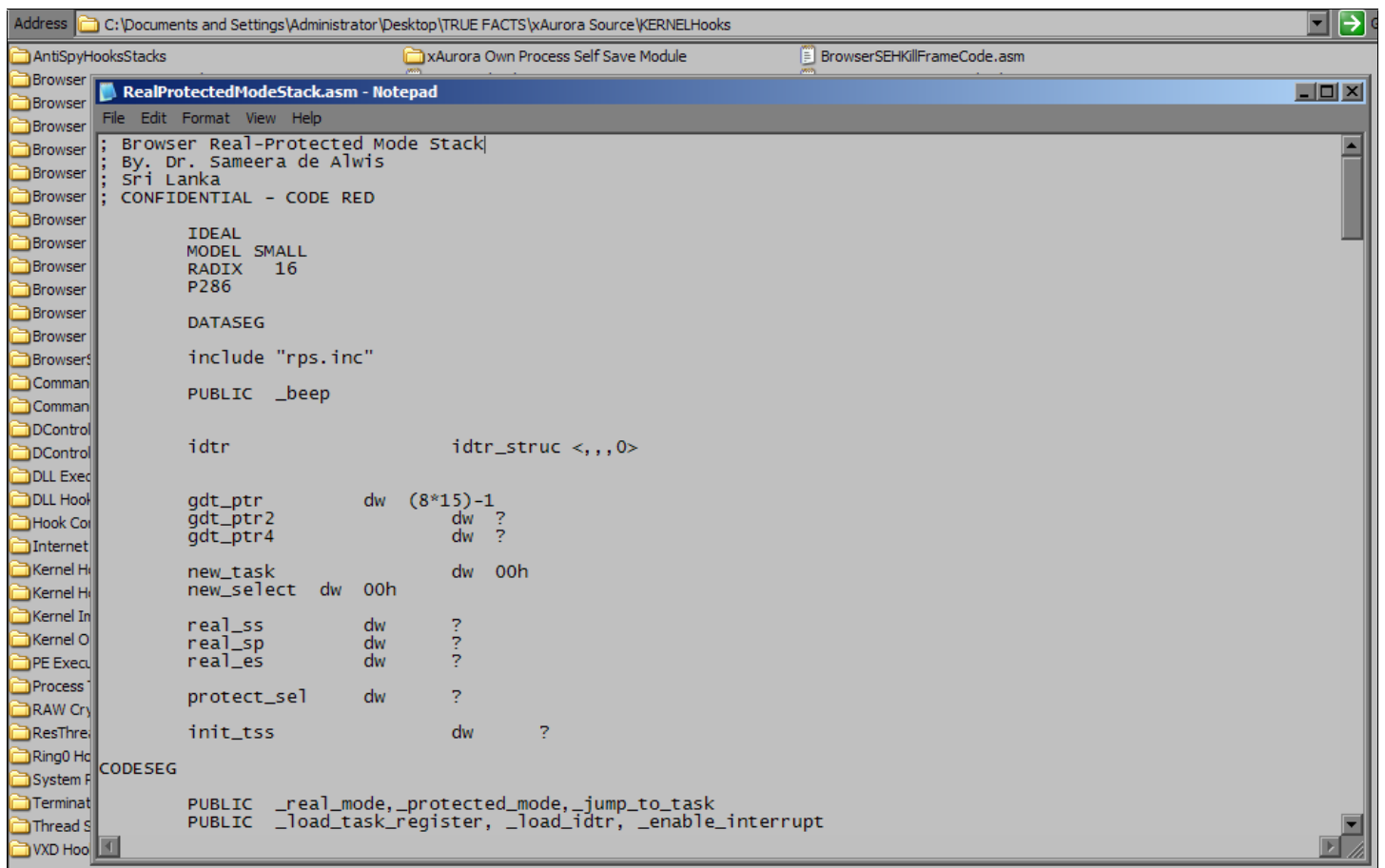
include "winconst.inc"
include 'kernel32.def'
include 'user32.def'

.DATA
; Variables
FileHandle DD 0 ;THandle
BytesWritten DD 0 ;DWORD
FileName db 'default.ini',0
ALIGN 4
Buffer db 'win32 Create INI',0

.CODE
; FileHandle := CreateFileA(FileName, , 0, 0, 0, 0);
PUSH 0
PUSH 0
PUSH CREATE_ALWAYS
PUSH 0
PUSH 0
PUSH 0
PUSH GENERIC_READ + GENERIC_WRITE
PUSH FileName ; Address
CALL CreateFileA
MOV [FileHandle], EAX

; writeFile(FileHandle, Buffer,strlen(buffer), BytesWritten, 0);
PUSH 0
PUSH BytesWritten
push buffer
```

## 12. Browser Real-Protected Mode Stack



```
Address C:\Documents and Settings\Administrator\Desktop\TRUE FACTS\xAurora Source\KERNELHooks
xAurora Own Process Self Save Module
BrowserSEHKillFrameCode.asm

RealProtectedModeStack.asm - Notepad
File Edit Format View Help
; Browser Real-Protected Mode Stack
; By: Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

        IDEAL
        MODEL SMALL
        RADIX 16
        P286

        DATASEG

        include "rps.inc"

        PUBLIC _beep

        idtr                idtr_struct <,,0>

        gdt_ptr             dw (8*15)-1
        gdt_ptr2            dw ?
        gdt_ptr4            dw ?

        new_task            dw 00h
        new_select          dw 00h

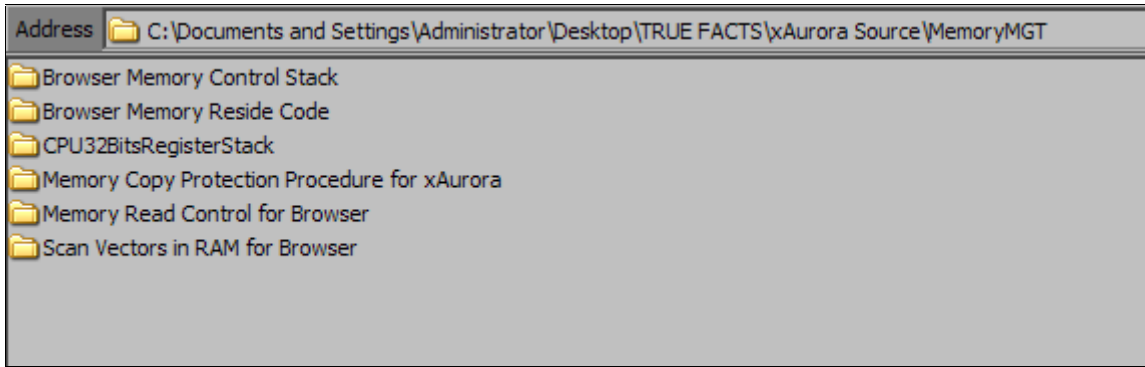
        real_ss             dw ?
        real_sp             dw ?
        real_es             dw ?

        protect_sel        dw ?

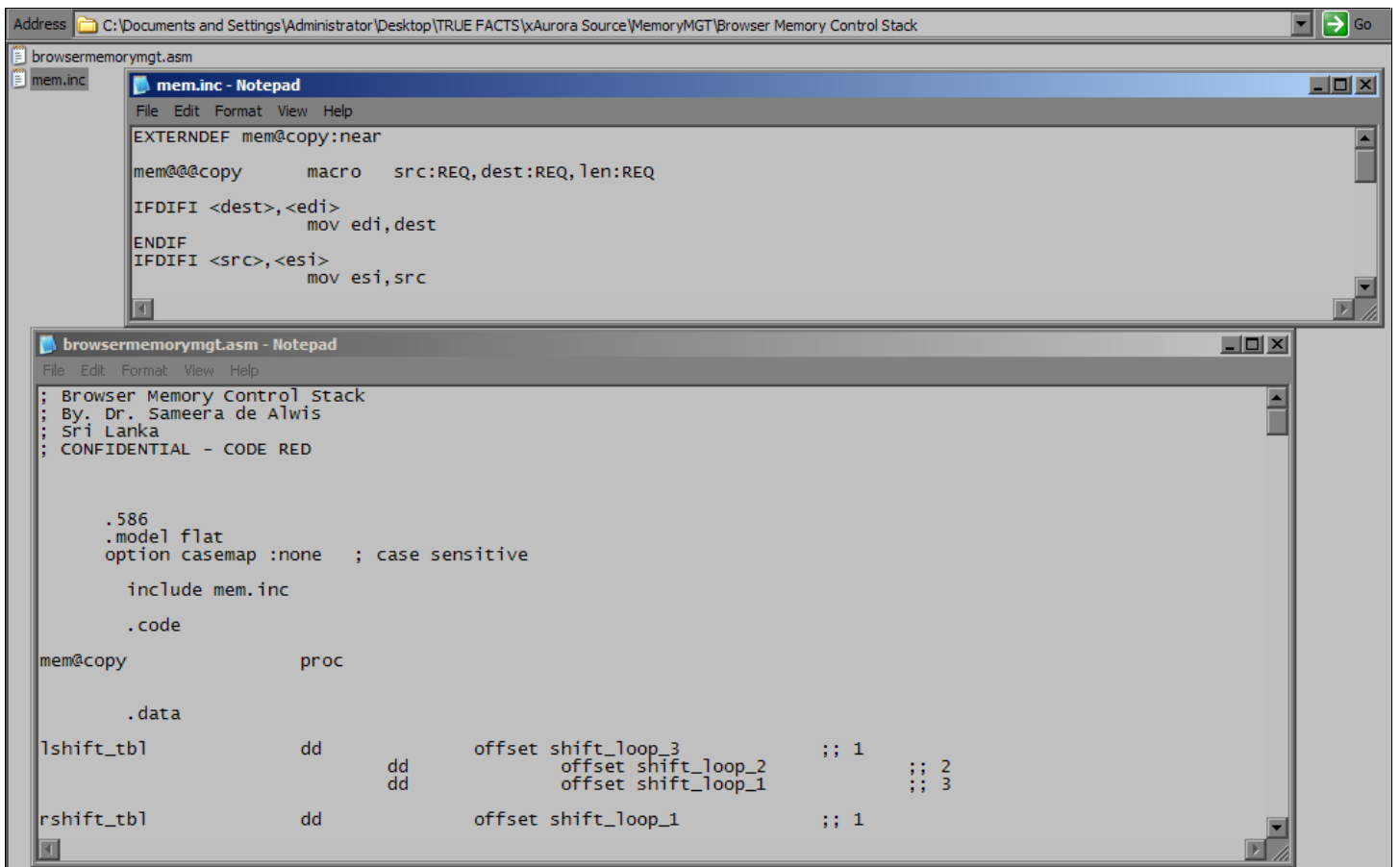
        init_tss            dw ?

CODESEG
        PUBLIC _real_mode,_protected_mode,_jump_to_task
        PUBLIC _load_task_register,_load_idtr,_enable_interrupt
```

## \* Memory Management Stack



### 13. Browser Memory Control Stack



## 14. Memory Copy Protection Procedure

```
Address C:\Documents and Settings\Administrator\Desktop\TRUE FACTS\xAurora Source\MemoryMGT\Memory Copy Protection Procedure for xAurora
MemCopyMainSecurity.asm

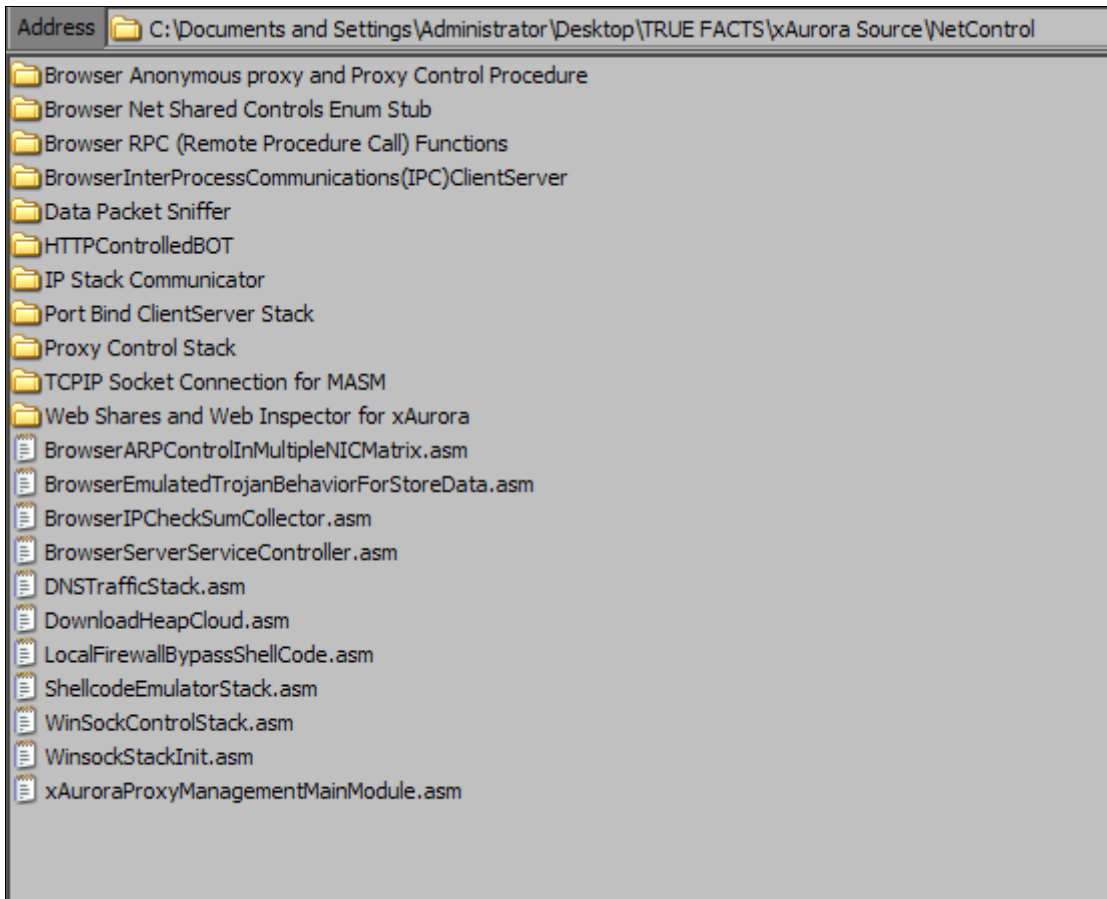
MemCopyMainSecurity.asm - Notepad
File Edit Format View Help

; Memory Copy Protection Procedure for xAurora
; By. Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

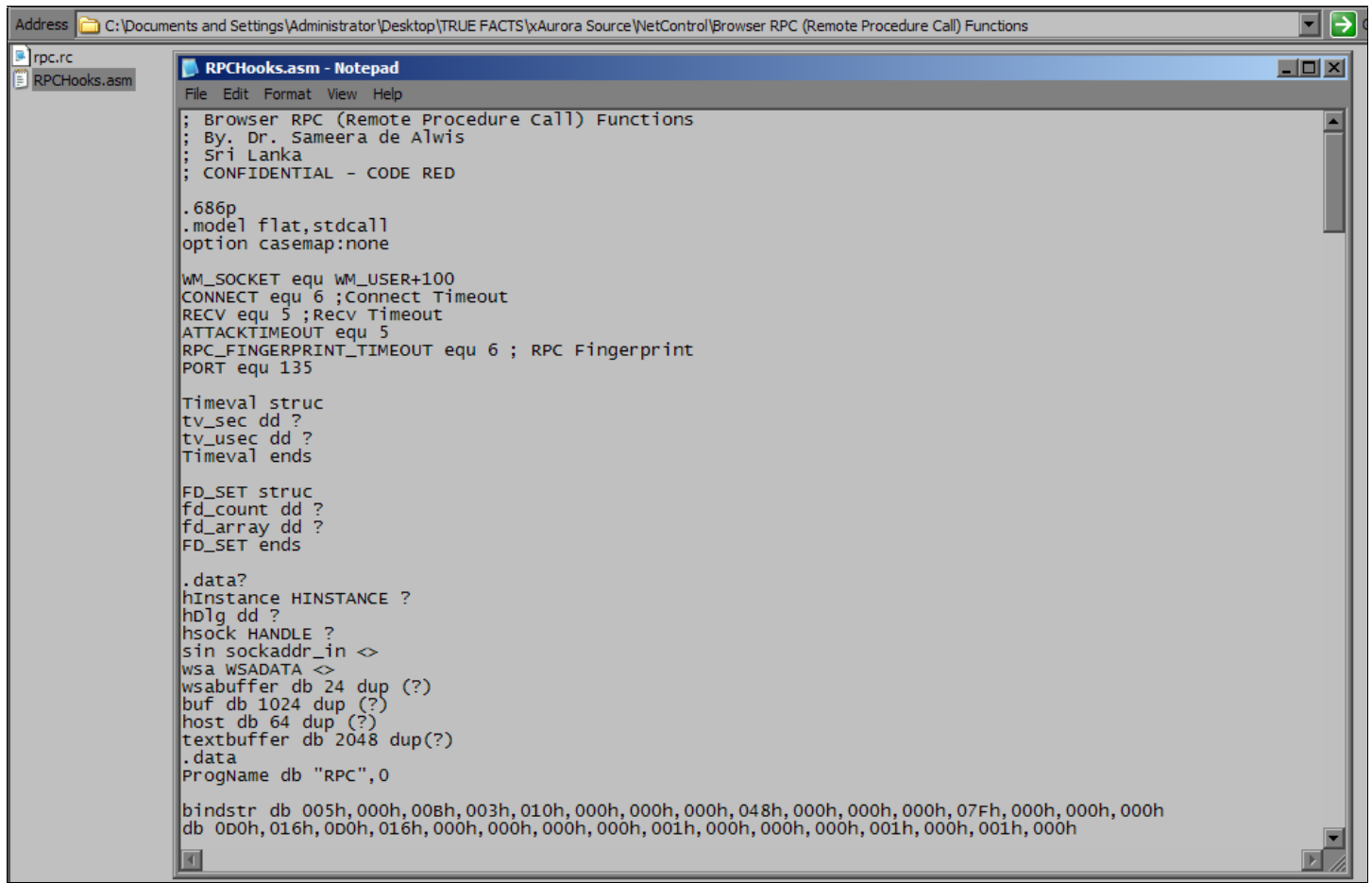
include 'PE.inc'
usedll user32
;;-----

align 16
copy_mmxopt:
CACHELINE equ 20h ;; for Celerons etc
CACHESIZE equ 20000h ;; 128Kb for celeron/duron
mov esi, src ;; source array
mov edi, dst ;; destination array
mov ecx, [EBP+4] ;; number of bytes
lea esi, [ESI+ECX]
lea edi, [EDI+ECX]
neg ecx
.l: add ecx, CACHESIZE ;; move up to end of cached block
mov eax, CACHESIZE / (CACHELINE*2) ;; note: prefetch loop is unrolled 2X
;; prefetch data
@@: test ebx, [ESI+ECX-CACHELINE] ;; access one address in this cache line...
test ebx, [ESI+ECX-CACHELINE*2] ;; ... and one in the previous line
sub ecx, CACHELINE*2
dec eax
jnz @b
;; copy block from the cache
@@: mov eax, CACHESIZE / 64
movq mm0, qword [esi+ecx]
movq mm1, qword [esi+ecx+8]
movq mm2, qword [esi+ecx+16]
movq mm3, qword [esi+ecx+24]
movq mm4, qword [esi+ecx+32]
movq mm5, qword [esi+ecx+40]
movq mm6, qword [esi+ecx+48]
movq mm7, qword [esi+ecx+56]
```

\* Network/Internet Control Stack



## 15. Browser RPC (Remote Procedure Call) Functions



```
Address C:\Documents and Settings\Administrator\Desktop\TRUE FACTS\Aurora Source\NetControl\Browser RPC (Remote Procedure Call) Functions

rpc.rc
RPCHooks.asm

RPCHooks.asm - Notepad
File Edit Format View Help

; Browser RPC (Remote Procedure Call) Functions
; By. Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

.686p
.model flat,stdcall
.option casemap:none

WM_SOCKET equ WM_USER+100
CONNECT equ 6 ;Connect Timeout
RECV equ 5 ;Recv Timeout
ATTACKTIMEOUT equ 5
RPC_FINGERPRINT_TIMEOUT equ 6 ; RPC Fingerprint
PORT equ 135

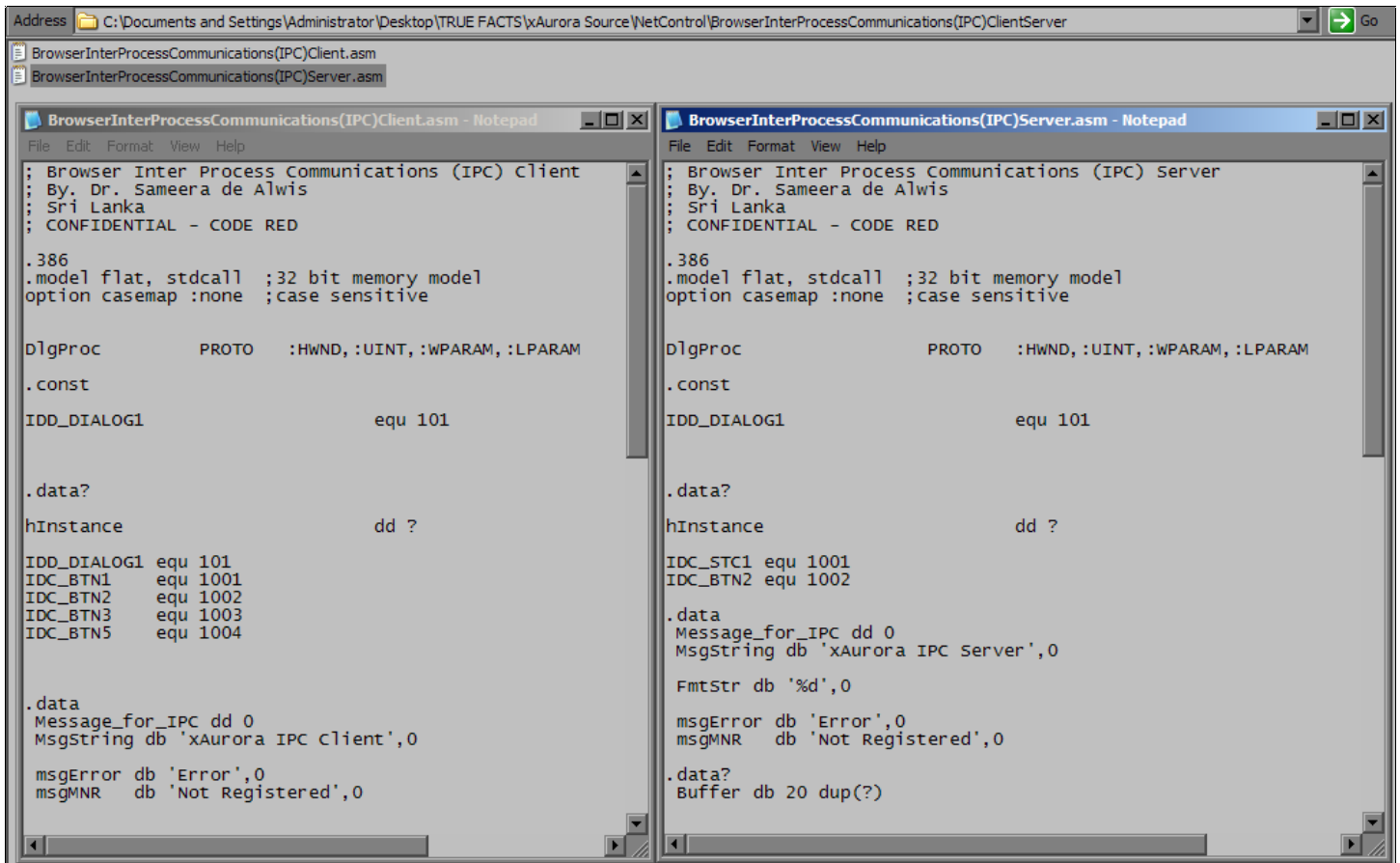
Timeval struc
tv_sec dd ?
tv_usec dd ?
Timeval ends

FD_SET struc
fd_count dd ?
fd_array dd ?
FD_SET ends

.data?
hInstance HINSTANCE ?
hDlg dd ?
hsock HANDLE ?
sin sockaddr_in <>
wsa WSADATA <>
wsabuffer db 24 dup (?)
buf db 1024 dup (?)
host db 64 dup (?)
textbuffer db 2048 dup(?)
.data
ProgName db "RPC",0

bindstr db 005h,000h,008h,003h,010h,000h,000h,000h,048h,000h,000h,000h,07Fh,000h,000h,000h
db 0d0h,016h,0d0h,016h,000h,000h,000h,000h,001h,000h,000h,000h,001h,000h,001h,000h
```

## 16. Browser Inter Process Communications (IPC) Client-Server



The image shows two Notepad windows side-by-side, displaying assembly code for a Browser Inter Process Communications (IPC) Client-Server application. The address bar at the top indicates the file path: C:\Documents and Settings\Administrator\Desktop\TRUE FACTS\xAurora Source\NetControl\BrowserInterProcessCommunications(IPC)ClientServer. The left window is titled "BrowserInterProcessCommunications(IPC)Client.asm - Notepad" and the right window is titled "BrowserInterProcessCommunications(IPC)Server.asm - Notepad". Both windows show assembly code with comments and data definitions.

```
BrowserInterProcessCommunications(IPC)Client.asm - Notepad
; Browser Inter Process Communications (IPC) Client
; By. Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

.386
.model flat, stdcall ;32 bit memory model
.option casemap :none ;case sensitive

DlgProc          PROTO :HWND, :UINT, :WPARAM, :LPARAM

.const
IDD_DIALOG1      equ 101

.data?
hInstance        dd ?

IDD_DIALOG1 equ 101
IDC_BTN1      equ 1001
IDC_BTN2      equ 1002
IDC_BTN3      equ 1003
IDC_BTN5      equ 1004

.data
Message_for_IPC dd 0
MsgString db 'xAurora IPC Client',0

msgError db 'Error',0
msgMNR   db 'Not Registered',0

BrowserInterProcessCommunications(IPC)Server.asm - Notepad
; Browser Inter Process Communications (IPC) Server
; By. Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

.386
.model flat, stdcall ;32 bit memory model
.option casemap :none ;case sensitive

DlgProc          PROTO :HWND, :UINT, :WPARAM, :LPARAM

.const
IDD_DIALOG1      equ 101

.data?
hInstance        dd ?

IDC_STC1 equ 1001
IDC_BTN2 equ 1002

.data
Message_for_IPC dd 0
MsgString db 'xAurora IPC Server',0

FmtStr db '%d',0

msgError db 'Error',0
msgMNR   db 'Not Registered',0

.data?
Buffer db 20 dup(?)
```

## 17. Data Packet Sniffer

```
Address C:\Documents and Settings\Administrator\Desktop\TRUE FACTS\Aurora Source\NetControl\Data Packet Sniffer Go
dialog1.res
sniffer.asm

sniffer.asm - Notepad
File Edit Format View Help
; Data Packet Sniffer
; By. Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

.586
.model flat,stdcall
.option casemap:none

wsadata struct
wVersion dw ?
wHighVersion dw ?
szDescription db 257 dup(0)
szSystemStatus db 257 dup(0)
iMaxSockets dw ?
iMaxUdpDg dw ?
lpVendorInfo db ?
wsadata ends

IP_HEADER          STRUCT
Version_and_HdrLen db ? ;+0
ServiceType        db ? ;+1
TotalLen           dw ? ;+2
ID                 dw ? ;+4
Flags_and_Fragoff  dw ? ;+6
TimeToLive         db ? ;+8
Protocol           db ? ;+9
HdrChecksum        dw ? ;+A
SrcAddr            dd ? ;+C
DstAddr            dd ? ;+E
IP_HEADER          ENDS

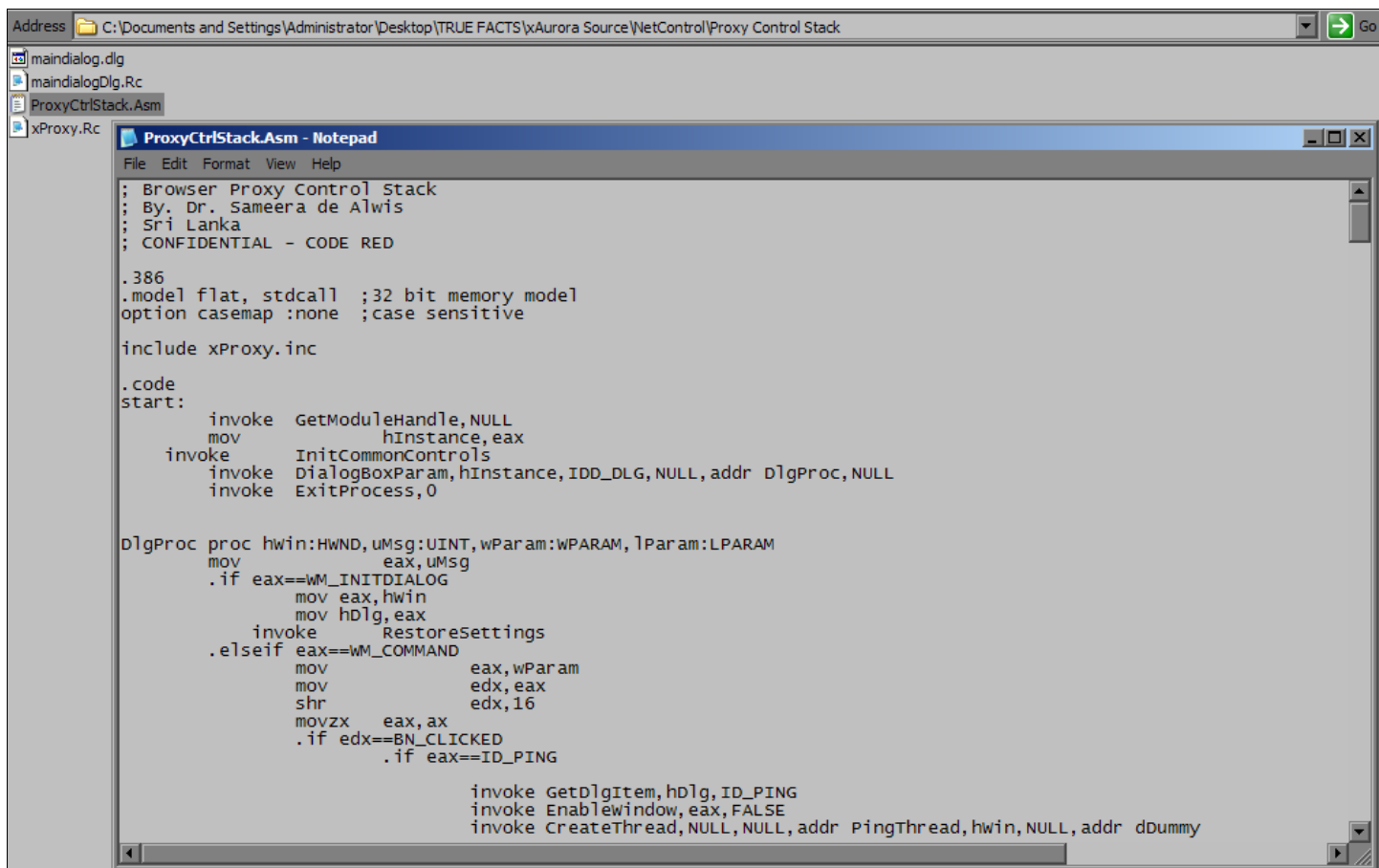
WSockThread proto :DWORD
WSockGetInterfase proto :DWORD, :DWORD, :DWORD

sniffer.asm - Notepad
File Edit Format View Help
WSockThread proto :DWORD
WSockGetInterfase proto :DWORD, :DWORD, :DWORD
ZeroFill proto :DWORD, :DWORD
DecodeIpHeader proto :DWORD
DlgProc proto :DWORD, :DWORD, :DWORD, :DWORD
.data
Dest db "Destination IP adress",0
Source db "Source IP adress",0
SocketError db "Socket Error!",0
CreateSocket db "Can't create socket!",0
InitSocket db "Can't initialize winSocket!",0
Interface db "Can't get interface!",0
NoInterface db "Interface wasn't found!",0
File db "pcapfile.dat",0
string db "Packet Flow Sniff", 5 dup(30h),0
Active db "Incomming Flow",0
Passive db "Outgoing Flow",0
RecPack dd 0
TermThread db 1
ThreadId dd 0
.data?
DATA db 523 dup(?)
pcap_buffer db 0FFFFh dup(?)
hInstance HINSTANCE ?
handle dd ?
IPDest db 17 dup(?)
IPSource db 17 dup(?)
ThreadId dd ?
hFile dd ?
wb dw ?
TEMP dd ?
note NOTIFYICONDATA <>

WM_SHELLNOTIFY equ WM_USER+5

.code
```

## 18. Browser Proxy Control Stack



The image shows a Notepad window titled "ProxyCtrlStack.As" with the following assembly code:

```
File Edit Format View Help
; Browser Proxy Control Stack
; By. Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

.386
.model flat, stdcall ;32 bit memory model
option casemap :none ;case sensitive

include xProxy.inc

.code
start:
    invoke GetModuleHandle, NULL
    mov     hInstance, eax
    invoke InitCommonControls
    invoke DialogBoxParam, hInstance, IDD_DLG, NULL, addr DlgProc, NULL
    invoke ExitProcess, 0

DlgProc proc hwin:HWND, uMsg:UINT, wParam:WPARAM, lParam:LPARAM
    mov     eax, uMsg
    .if eax==WM_INITDIALOG
        mov     eax, hwin
        mov     hDlg, eax
        invoke RestoreSettings
    .elseif eax==WM_COMMAND
        mov     eax, wParam
        mov     edx, eax
        shr     edx, 16
        movzx  eax, ax
        .if edx==BN_CLICKED
            .if eax==ID_PING

                invoke GetDlgItem, hDlg, ID_PING
                invoke EnableWindow, eax, FALSE
                invoke CreateThread, NULL, NULL, addr PingThread, hwin, NULL, addr dDummy
```

## 19. TCP/IP Socket Connections

```
Address C:\Documents and Settings\Administrator\Desktop\TRUE FACTS\xAurora Source\NetControl\TCPIP Socket Connection for MASM Go
connect.res
main.dlg
mainDlg.rc
tcpipconnect.asm
tcpipconnect.rc
xaurora.ico

; TCP/IP socket connection for MASM
; By. Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

.486
.model flat, stdcall
option casemap:none

DlgProc          PROTO :HWND, :UINT, :WPARAM, :LPARAM
Connect          PROTO :DWORD

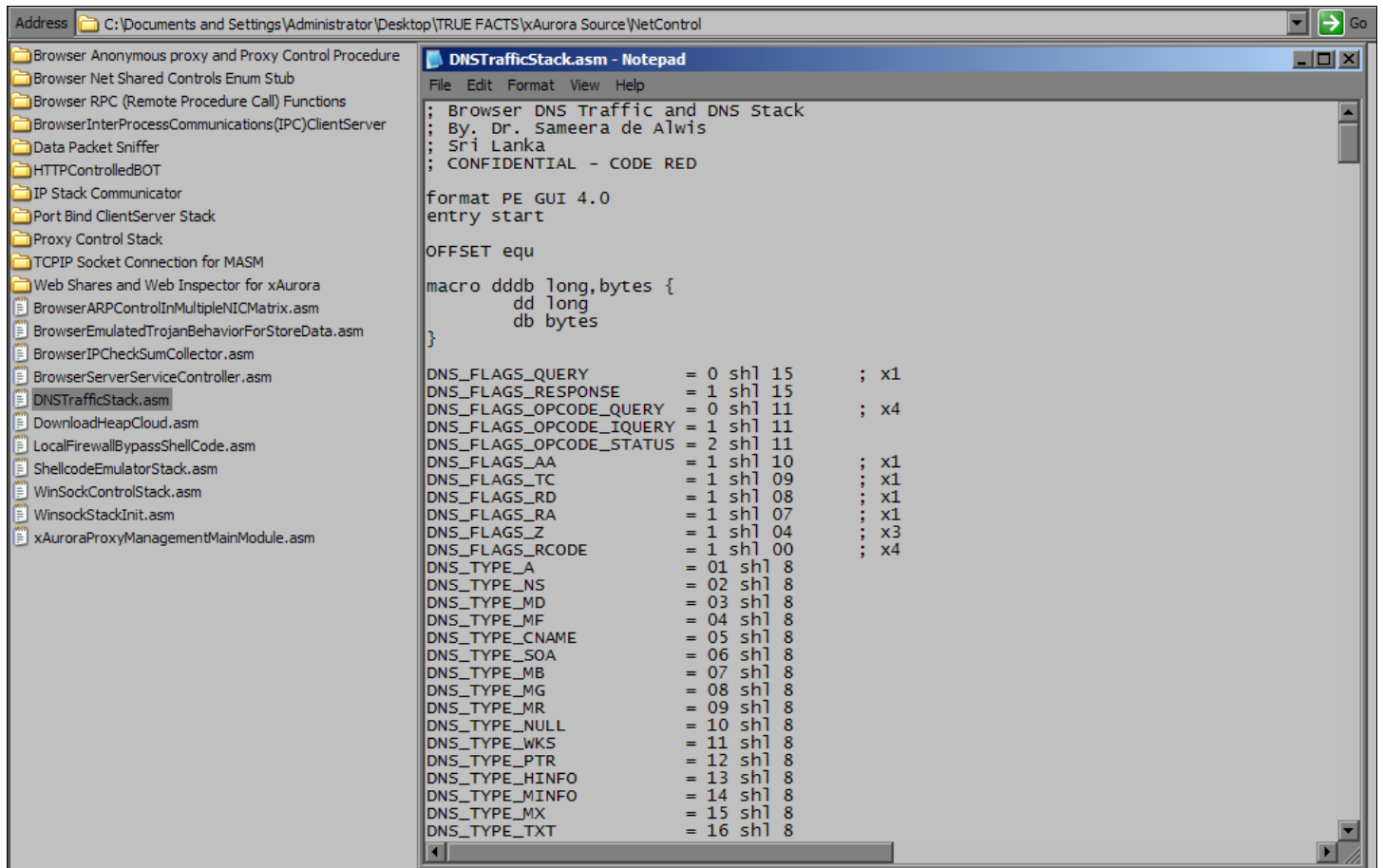
.const
IDD_DLG1          equ 1000
BUFFER_SIZE      equ 300

.data
server db "127.0.0.1",0
connecting db "TCP/IP Connection.. to",0
end_connect db "End of Connection.",0
ok db "Ok!",0
error db "Error",0
tempBuffer db BUFFER_SIZE dup(0)
;-----ssocket-----
Port dd 80
wsadata WSADATA <>
sin sockaddr_in <>
socketerror db "Could not create a socket",0
socerrdes db "Invalid Socket",0
gethosterr db "Could not resolve hostname",0
socERR1 db "Could not connect to host",0

.data?
hInstance          dd ?
hList              dd ?
hEdit              dd ?
hsock              dd ?

LOWORD MACRO bigword
    mov eax, bigword
    and eax, 0FFFFh
```

## 20. Browser DNS Traffic and DNS Stack



```
Address C:\Documents and Settings\Administrator\Desktop\TRUE FACTS\xAurora Source\NetControl
Browser Anonymous proxy and Proxy Control Procedure
Browser Net Shared Controls Enum Stub
Browser RPC (Remote Procedure Call) Functions
BrowserInterProcessCommunications(IPC)ClientServer
Data Packet Sniffer
HTTPControlledBOT
IP Stack Communicator
Port Bind ClientServer Stack
Proxy Control Stack
TCP/IP Socket Connection for MASM
Web Shares and Web Inspector for xAurora
BrowserARPControlInMultipleNICMatrix.asm
BrowserEmulatedTrojanBehaviorForStoreData.asm
BrowserIPChecksumCollector.asm
BrowserServerServiceController.asm
DNSTrafficStack.asm
DownloadHeapCloud.asm
LocalFirewallBypassShellCode.asm
ShellcodeEmulatorStack.asm
WinSockControlStack.asm
WinsockStackInit.asm
xAuroraProxyManagementMainModule.asm

DNSTrafficStack.asm - Notepad
File Edit Format View Help
; Browser DNS Traffic and DNS Stack
; By: Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

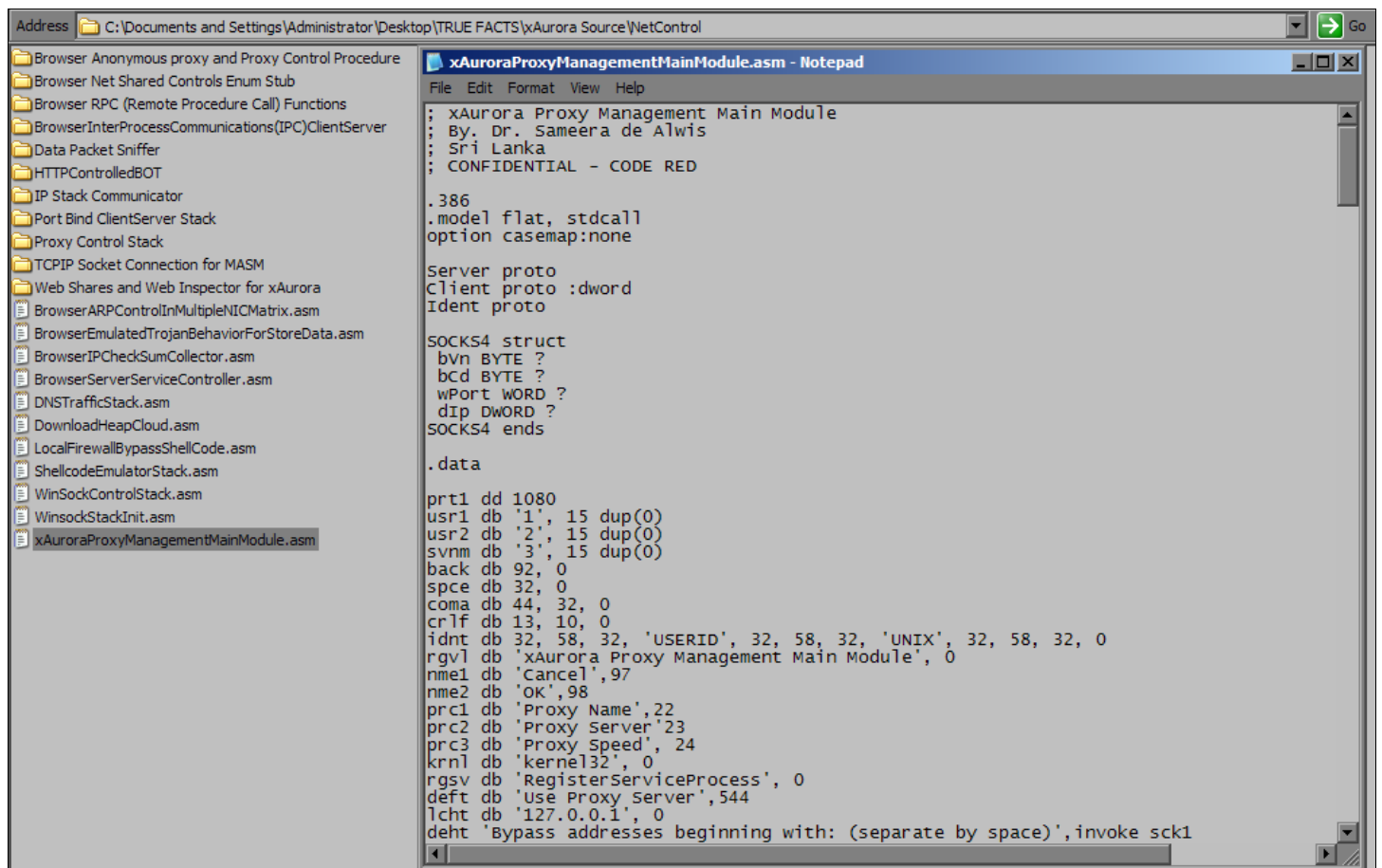
format PE GUI 4.0
entry start

OFFSET equ

macro dddb long,bytes {
    dd long
    db bytes
}

DNS_FLAGS_QUERY      = 0 shl 15      ; x1
DNS_FLAGS_RESPONSE   = 1 shl 15      ; x1
DNS_FLAGS_OPCODE_QUERY = 0 shl 11      ; x4
DNS_FLAGS_OPCODE_IQUERY = 1 shl 11
DNS_FLAGS_OPCODE_STATUS = 2 shl 11
DNS_FLAGS_AA         = 1 shl 10      ; x1
DNS_FLAGS_TC         = 1 shl 09      ; x1
DNS_FLAGS_RD         = 1 shl 08      ; x1
DNS_FLAGS_RA         = 1 shl 07      ; x1
DNS_FLAGS_Z          = 1 shl 04      ; x3
DNS_FLAGS_RCODE      = 1 shl 00      ; x4
DNS_TYPE_A           = 01 shl 8
DNS_TYPE_NS          = 02 shl 8
DNS_TYPE_MD          = 03 shl 8
DNS_TYPE_MF          = 04 shl 8
DNS_TYPE_CNAME       = 05 shl 8
DNS_TYPE_SOA         = 06 shl 8
DNS_TYPE_MB          = 07 shl 8
DNS_TYPE_MG          = 08 shl 8
DNS_TYPE_MR          = 09 shl 8
DNS_TYPE_NULL        = 10 shl 8
DNS_TYPE_WKS         = 11 shl 8
DNS_TYPE_PTR         = 12 shl 8
DNS_TYPE_HINFO       = 13 shl 8
DNS_TYPE_MINFO       = 14 shl 8
DNS_TYPE_MX          = 15 shl 8
DNS_TYPE_TXT         = 16 shl 8
```

## 21. xAurora Proxy Management Main Module



```
Address C:\Documents and Settings\Administrator\Desktop\TRUE FACTS\xAurora Source\NetControl
xAuroraProxyManagementMainModule.asm - Notepad
File Edit Format View Help
; xAurora Proxy Management Main Module
; By: Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

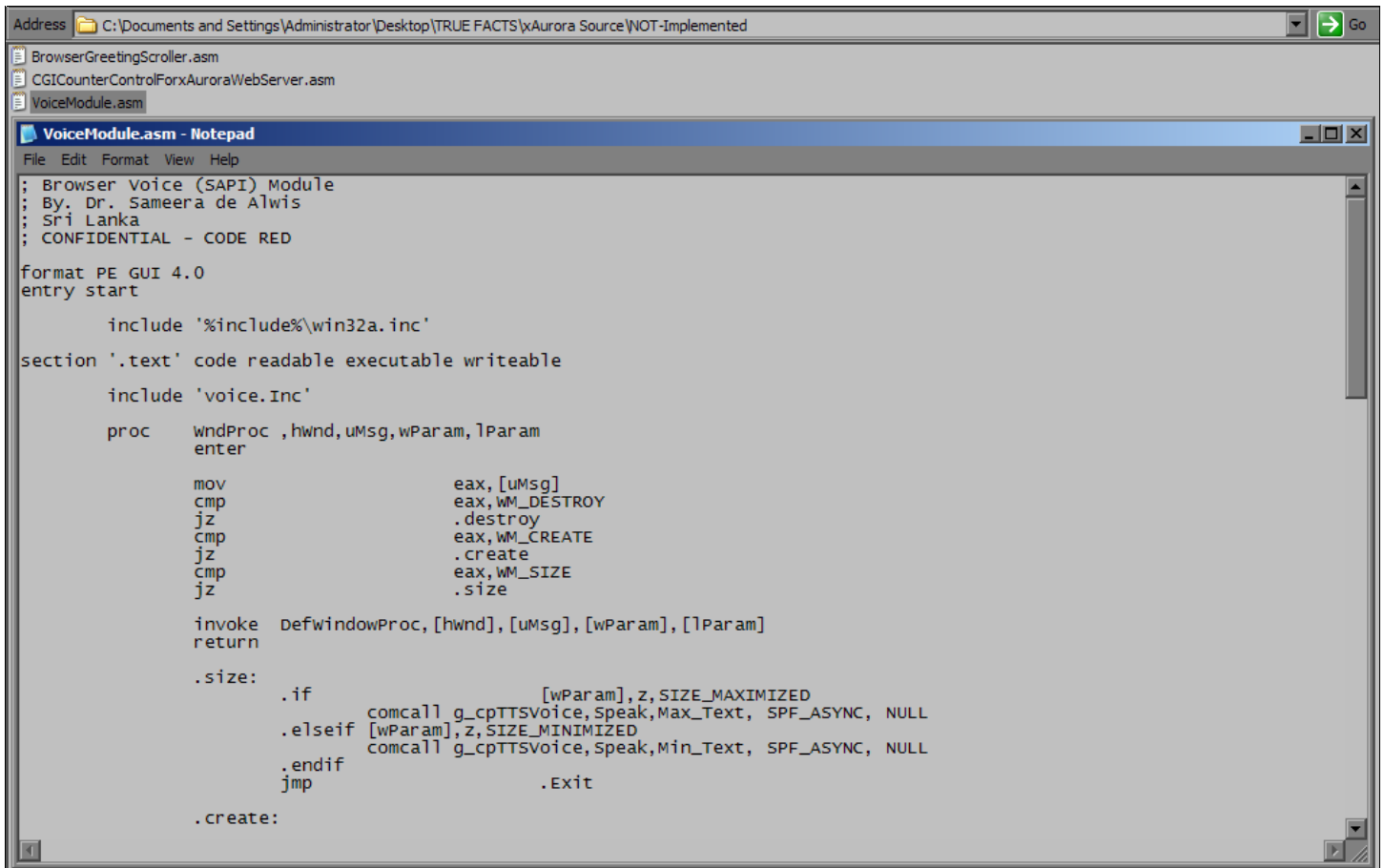
.386
.model flat, stdcall
option casemap:none

server proto
Client proto :dword
Ident proto

SOCKS4 struct
    bvn BYTE ?
    bcd BYTE ?
    wPort WORD ?
    dIp DWORD ?
SOCKS4 ends

.data
prt1 dd 1080
usr1 db '1', 15 dup(0)
usr2 db '2', 15 dup(0)
svnm db '3', 15 dup(0)
back db 92, 0
spce db 32, 0
coma db 44, 32, 0
crlf db 13, 10, 0
idnt db 32, 58, 32, 'USERID', 32, 58, 32, 'UNIX', 32, 58, 32, 0
rgvl db 'xAurora Proxy Management Main Module', 0
nme1 db 'Cancel', 97
nme2 db 'OK', 98
prc1 db 'Proxy Name', 22
prc2 db 'Proxy Server', 23
prc3 db 'Proxy Speed', 24
krnl db 'kernel32', 0
rgsv db 'RegisterServiceProcess', 0
deft db 'Use Proxy Server', 544
lcht db '127.0.0.1', 0
deht db 'Bypass addresses beginning with: (separate by space)', invoke sck1
```

## 22. Browser Voice (SAPI) Module - NOT IMPLEMENTED



```
Address C:\Documents and Settings\Administrator\Desktop\TRUE FACTS\xAurora Source\NOT-Implemented Go
BrowserGreetingScroller.asm
CGICounterControlForxAuroraWebServer.asm
VoiceModule.asm
VoiceModule.asm - Notepad
File Edit Format View Help
; Browser voice (SAPI) Module
; By. Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

format PE GUI 4.0
entry start

    include '%include%\win32a.inc'
section '.text' code readable executable writeable
    include 'voice.Inc'

    proc    wndProc ,hwnd,uMsg,wParam,lParam
    enter

        mov     eax,[uMsg]
        cmp     eax,WM_DESTROY
        jz      .destroy
        cmp     eax,WM_CREATE
        jz      .create
        cmp     eax,WM_SIZE
        jz      .size

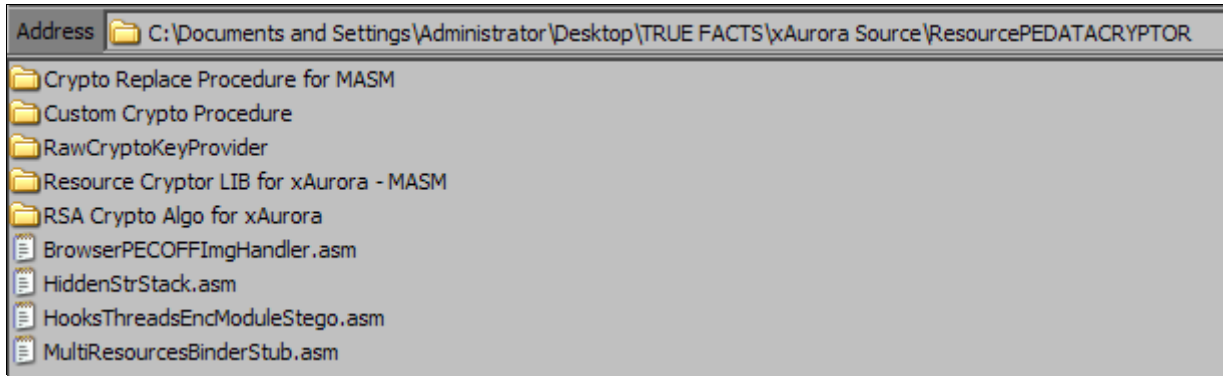
        invoke DefWindowProc,[hwnd],[uMsg],[wParam],[lParam]
        return

    .size:
        .if [wParam],z,SIZE_MAXIMIZED
        comcall g_cpTTSvoice,Speak,Max_Text,SPF_ASYNC,NULL
        .elseif [wParam],z,SIZE_MINIMIZED
        comcall g_cpTTSvoice,Speak,Min_Text,SPF_ASYNC,NULL
        .endif
        jmp     .Exit

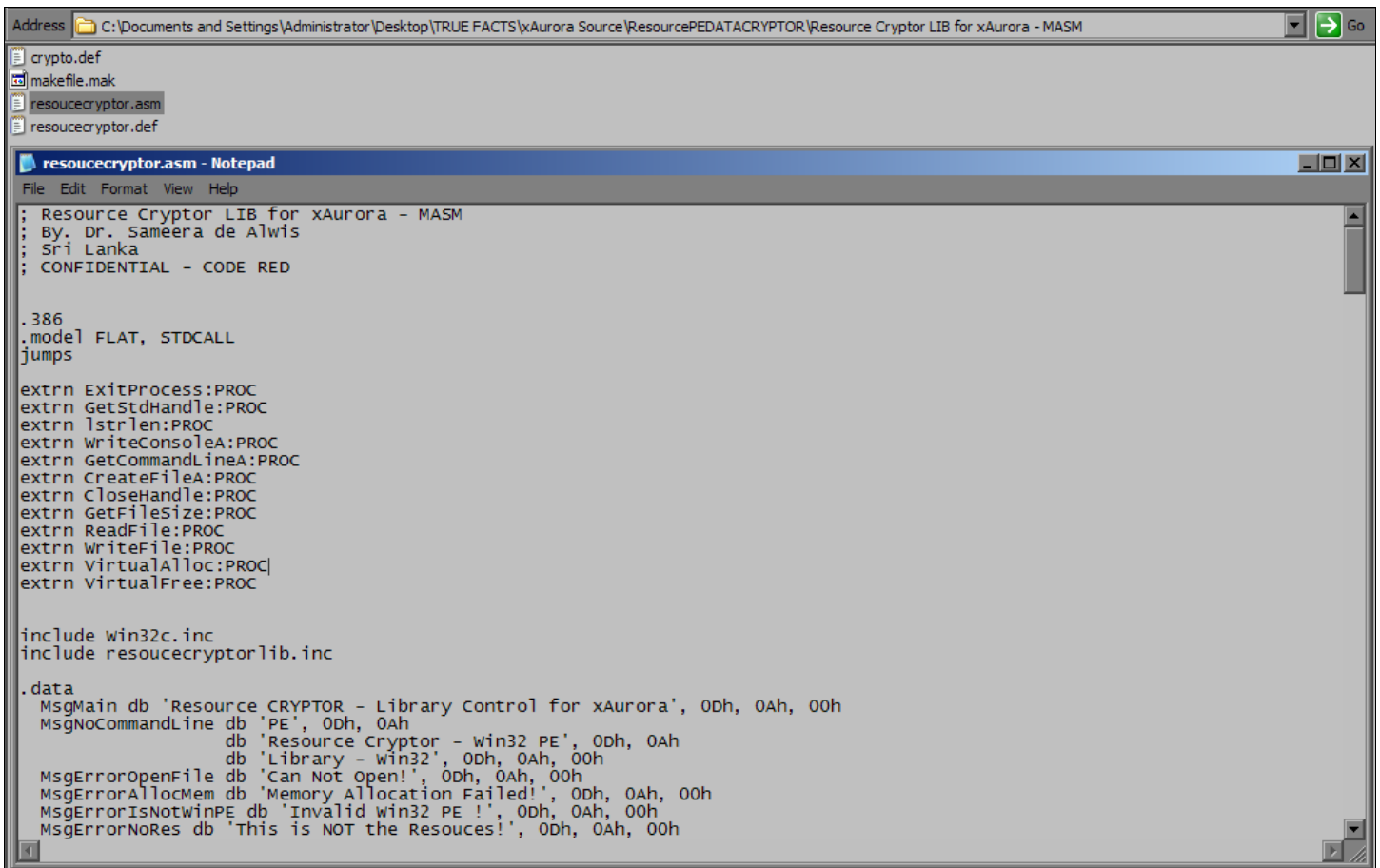
    .create:

```

## \* PE Data Encryption Segment



## 23. Resource Cryptor LIB for xAurora



## 24. Browser Multi Resources Binder

```
Address C:\Documents and Settings\Administrator\Desktop\TRUE FACTS\xAurora Source\ResourcePEDATACRYPTOR

Crypto Replace Procedure for MASM
Custom Crypto Procedure
RawCryptoKeyProvider
Resource Cryptor LIB for xAurora - MASM
RSA Crypto Algo for xAurora
BrowserPECOFFImgHandler.asm
HiddenStrStack.asm
HooksThreadsEndModuleStego.asm
MultiResourcesBinderStub.asm

MultiResourcesBinderStub.asm - Notepad
File Edit Format View Help

; Browser Multi Resources Binder for MASM
; By. Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

.386
.model flat, stdcall
option casemap:none

include \masm32\include\windows.inc
include \masm32\include\kernel32.inc
includelib \masm32\lib\kernel32.lib

ExtractFile proto :dword

.data

;set this to the size in bytes of the stub
fBegin dword 0

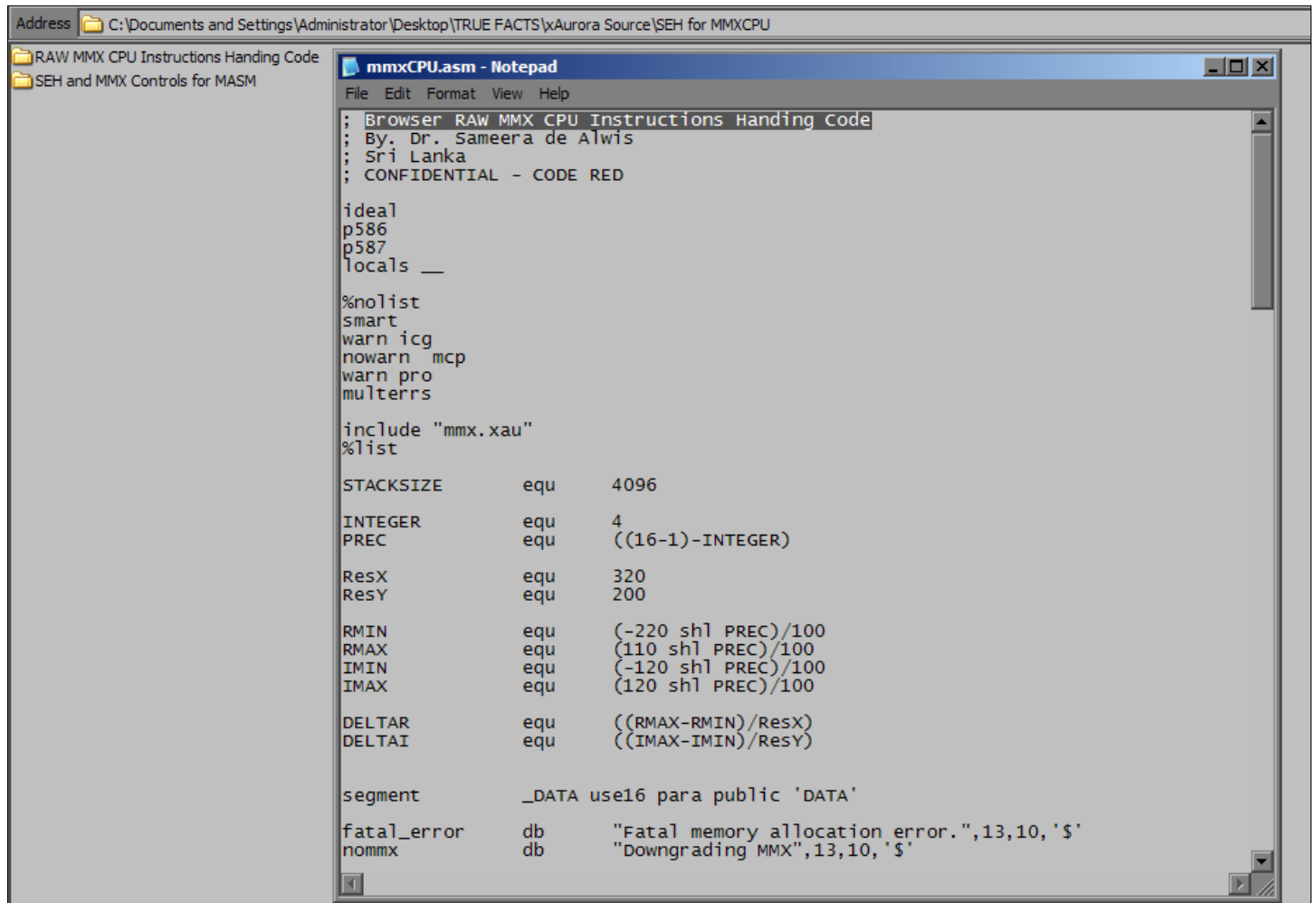
;set these to the size in bytes of each of
;the files to bind, then simply append the
;data to the end of the exe using writeFile

fLen01 dword 0
fLen02 dword 0
fLen03 dword 0
fLen04 dword 0
fLen05 dword 0
fLen06 dword 0
fLen07 dword 0
fLen08 dword 0
fLen09 dword 0
fLen10 dword 0

szExe byte 'exe', 0
szFileMask byte '~A', 0

.data?
hMainFile dword ?
```

## 25. Browser RAW MMX CPU Instructions Handing Code



The image shows a Notepad window titled 'mmxCPU.asm - Notepad' with the following assembly code:

```
; Browser RAW MMX CPU Instructions Handing Code
; By: Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

ideal
p586
p587
locals __

%no1ist
smart
warn icg
nowarn mcp
warn pro
multerrs

include "mmx.xau"
%1ist

STACKSIZE      equ      4096

INTEGER        equ      4
PREC           equ      ((16-1)-INTEGER)

ResX           equ      320
ResY           equ      200

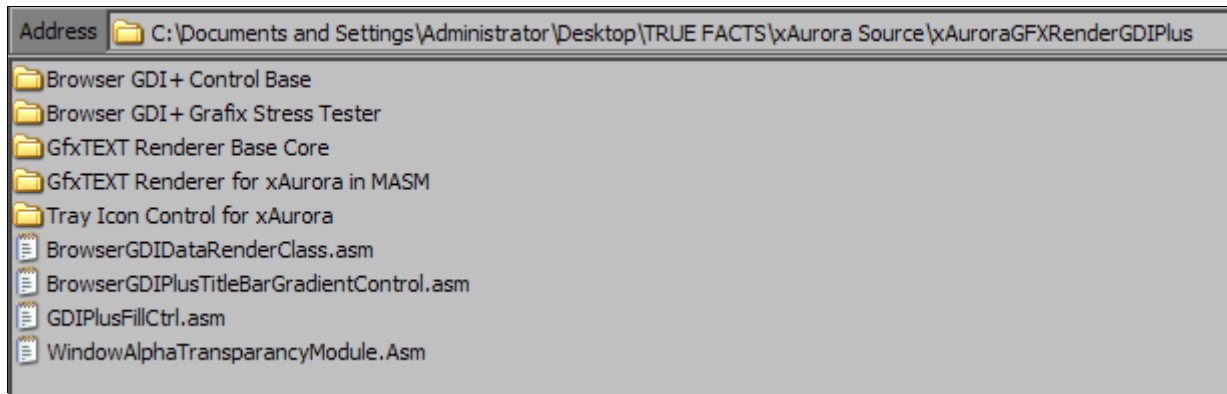
RMIN           equ      (-220 shl PREC)/100
RMAX           equ      (110 shl PREC)/100
IMIN           equ      (-120 shl PREC)/100
IMAX           equ      (120 shl PREC)/100

DELTAR         equ      ((RMAX-RMIN)/ResX)
DELTAI         equ      ((IMAX-IMIN)/ResY)

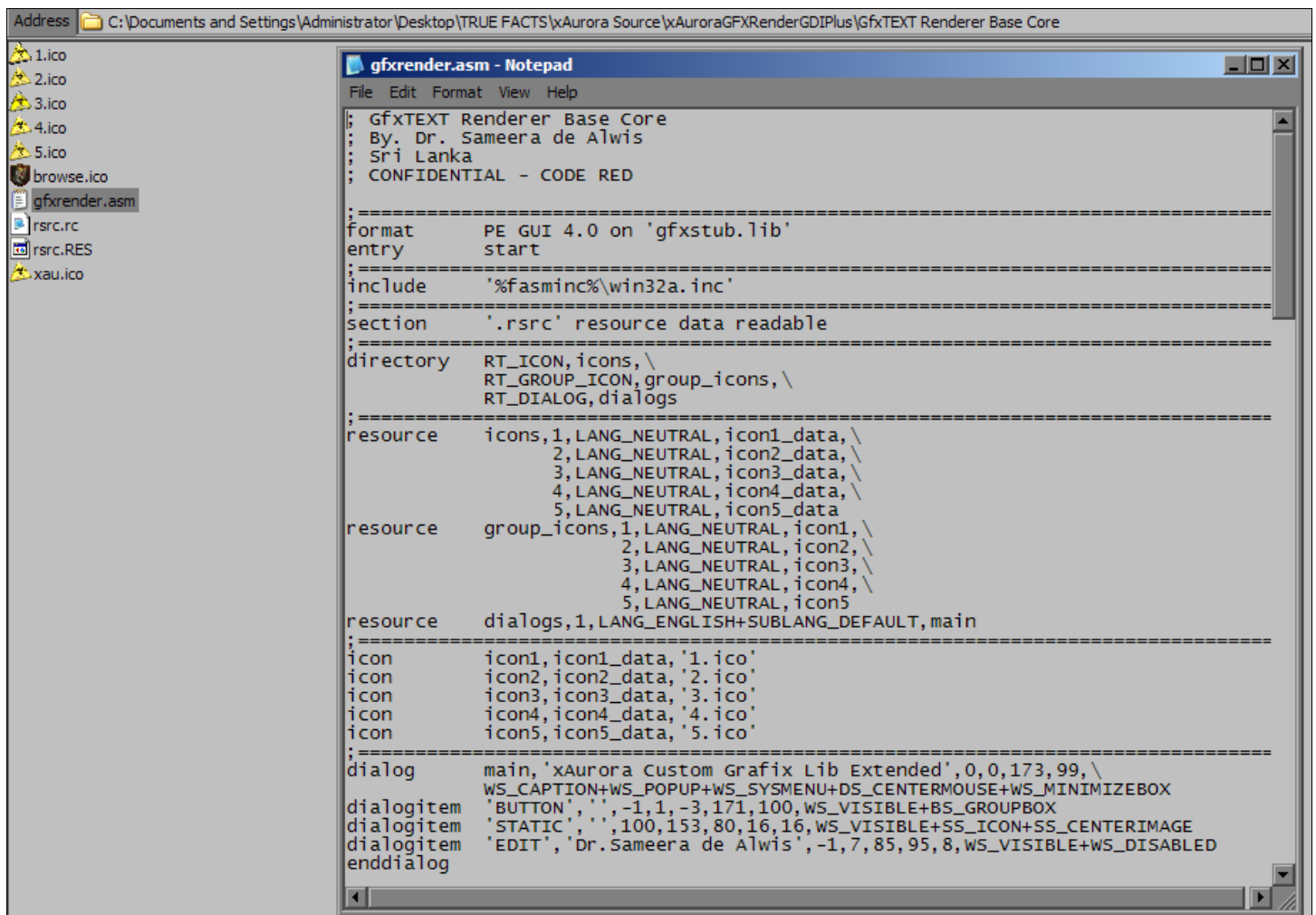
segment        _DATA use16 para public 'DATA'

fatal_error    db        "Fatal memory allocation error.",13,10,'$'
nommx          db        "Downgrading MMX",13,10,'$'
```

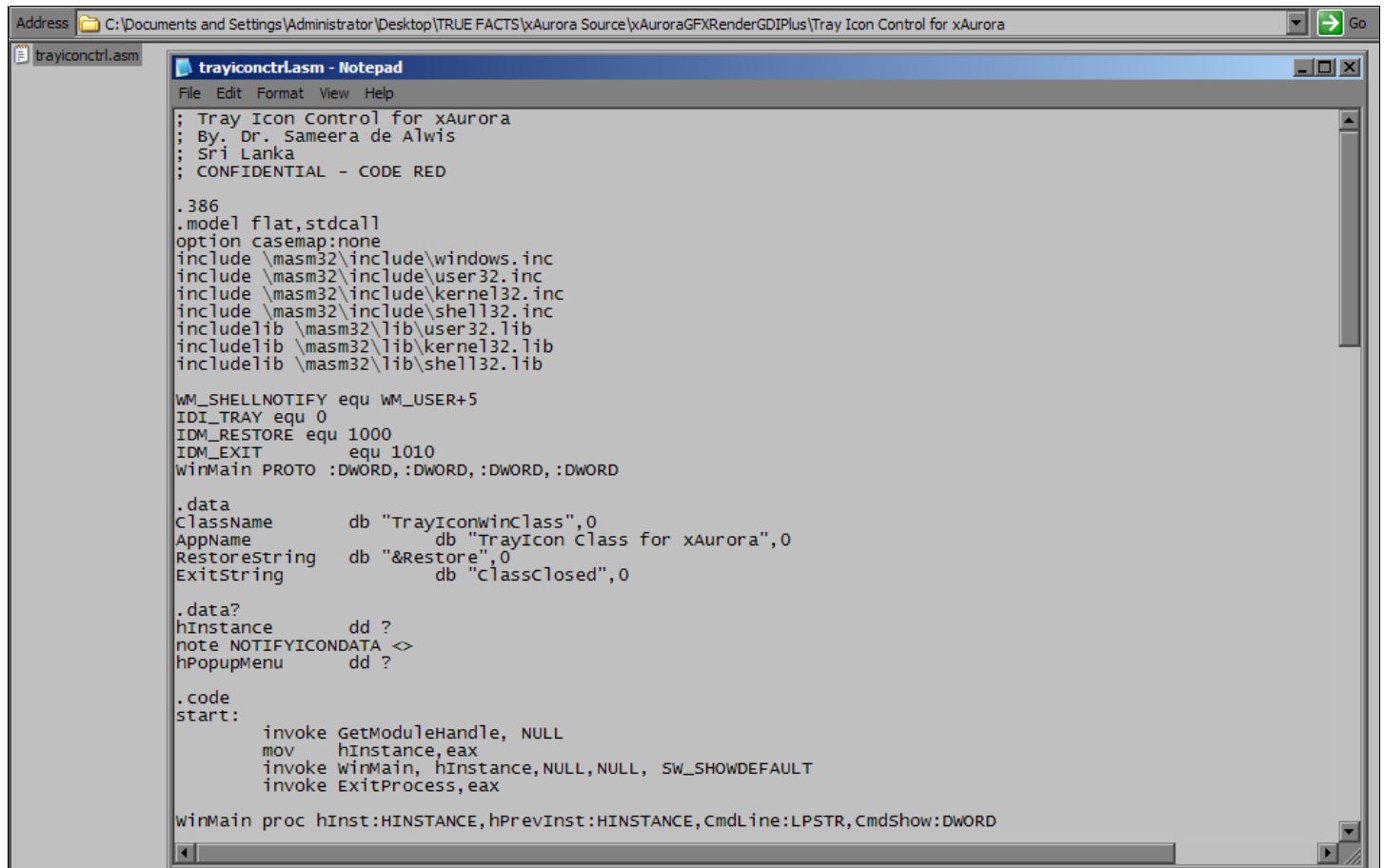
## \* xAurora GFX/TEXT Render GDI Plus



## 26. GfxTEXT Renderer Base Core



## 27. Tray Icon Control for xAurora



```
Address C:\Documents and Settings\Administrator\Desktop\TRUE FACTS\xAurora Source\xAuroraGFXRenderGDIPlus\Tray Icon Control for xAurora
trayiconctrl.asm
trayiconctrl.asm - Notepad
File Edit Format View Help
; Tray Icon Control for xAurora
; By: Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

.386
.model flat,stdcall
option casemap:none
include \masm32\include\windows.inc
include \masm32\include\user32.inc
include \masm32\include\kernel32.inc
include \masm32\include\shell32.inc
include lib \masm32\lib\user32.lib
include lib \masm32\lib\kernel32.lib
include lib \masm32\lib\shell32.lib

WM_SHELLNOTIFY equ WM_USER+5
IDI_TRAY equ 0
IDM_RESTORE equ 1000
IDM_EXIT equ 1010
winMain proto :DWORD,:DWORD,:DWORD,:DWORD

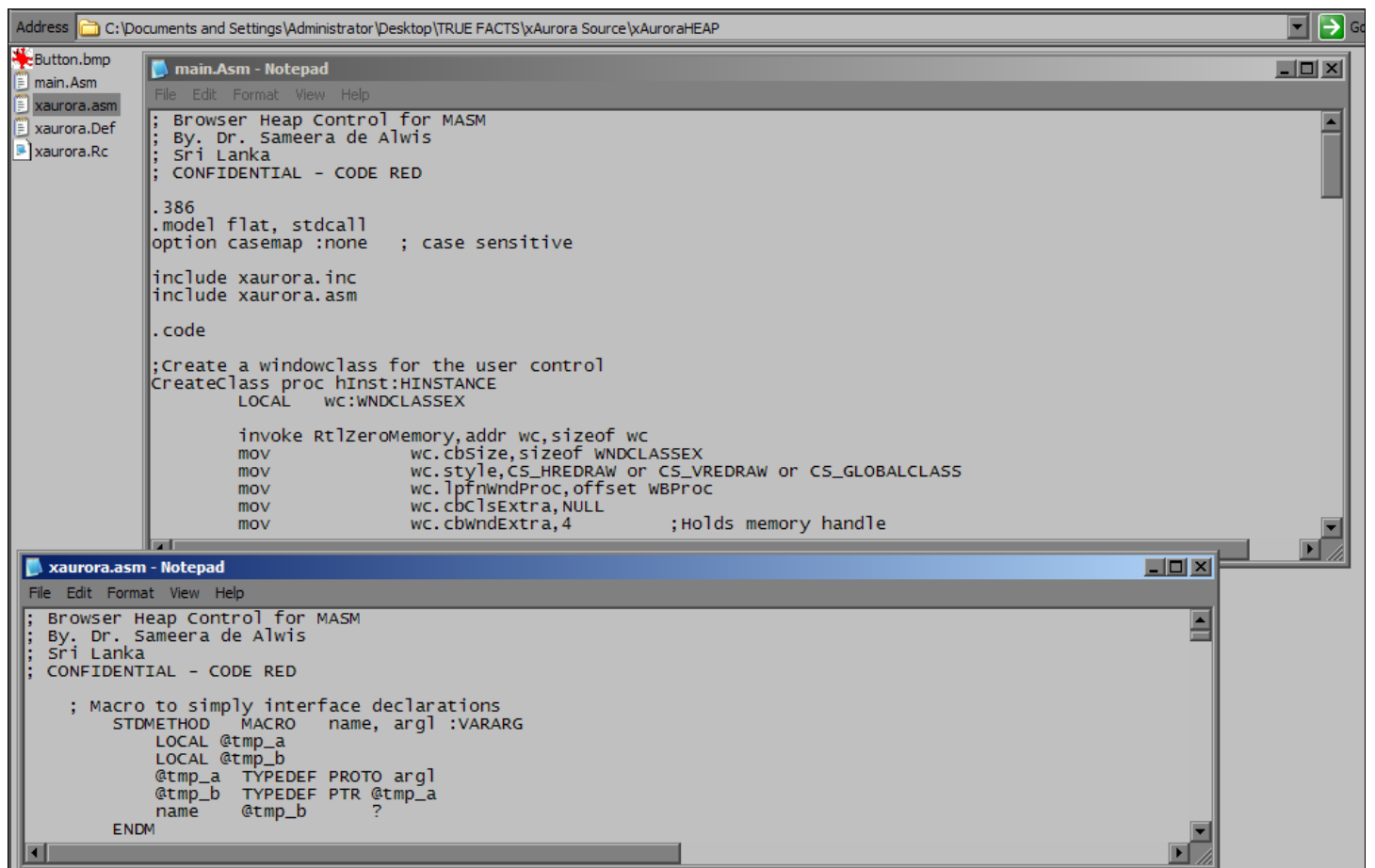
.data
ClassName db "TrayIconwinClass",0
AppName db "TrayIcon Class for xAurora",0
RestoreString db "&Restore",0
ExitString db "ClassClosed",0

.data?
hInstance dd ?
note NOTIFYICONDATA <
hPopupMenu dd ?

.code
start:
    invoke GetModuleHandle, NULL
    mov hInstance, eax
    invoke winMain, hInstance, NULL, NULL, SW_SHOWDEFAULT
    invoke ExitProcess, eax

winMain proc hInst:HINSTANCE, hPrevInst:HINSTANCE, CmdLine:LPSTR, CmdShow:DWORD
```

## 28. Browser Heap Control



The image shows two Notepad windows displaying assembly code. The top window, titled 'main.asm - Notepad', shows the main program structure. The bottom window, titled 'xaurora.asm - Notepad', shows a macro definition for interface declarations.

```
main.asm - Notepad
; Browser Heap Control for MASM
; By. Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

.386
.model flat, stdcall
option casemap :none ; case sensitive

include xaurora.inc
include xaurora.asm

.code

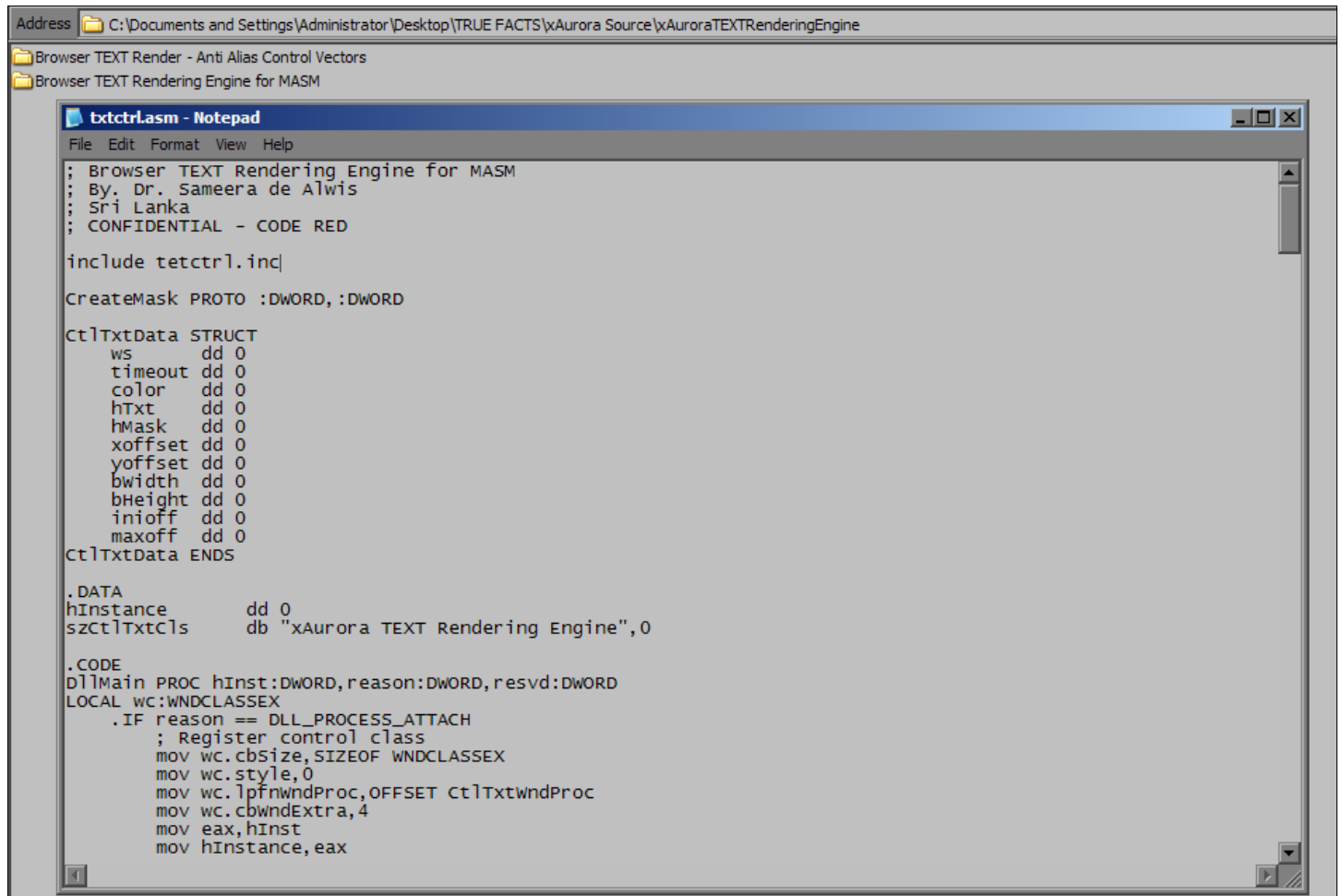
;Create a windowclass for the user control
CreateClass proc hInst:HINSTANCE
    LOCAL wc:WNDCLASSEX

    invoke RtlZeroMemory,addr wc,sizeof wc
    mov     wc.cbSize,sizeof WNDCLASSEX
    mov     wc.style,CS_HREDRAW or CS_VREDRAW or CS_GLOBALCLASS
    mov     wc.lpfnWndProc,offset WBProc
    mov     wc.cbClsExtra,NULL
    mov     wc.cbWndExtra,4 ;Holds memory handle
CreateClass endp

xaurora.asm - Notepad
; Browser Heap Control for MASM
; By. Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

; Macro to simply interface declarations
STDMETHOD MACRO name, arg1 :VARARG
    LOCAL @tmp_a
    LOCAL @tmp_b
    @tmp_a TYPEDEF PROTO arg1
    @tmp_b TYPEDEF PTR @tmp_a
    name @tmp_b ?
ENDM
```

## 29. Browser TEXT Rendering Engine



```
Address C:\Documents and Settings\Administrator\Desktop\TRUE FACTS\xAurora Source\xAuroraTEXTRenderingEngine
Browser TEXT Render - Anti Alias Control Vectors
Browser TEXT Rendering Engine for MASM

bxtctrlasm - Notepad
File Edit Format View Help
; Browser TEXT Rendering Engine for MASM
; By. Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

include tetctrl.inc

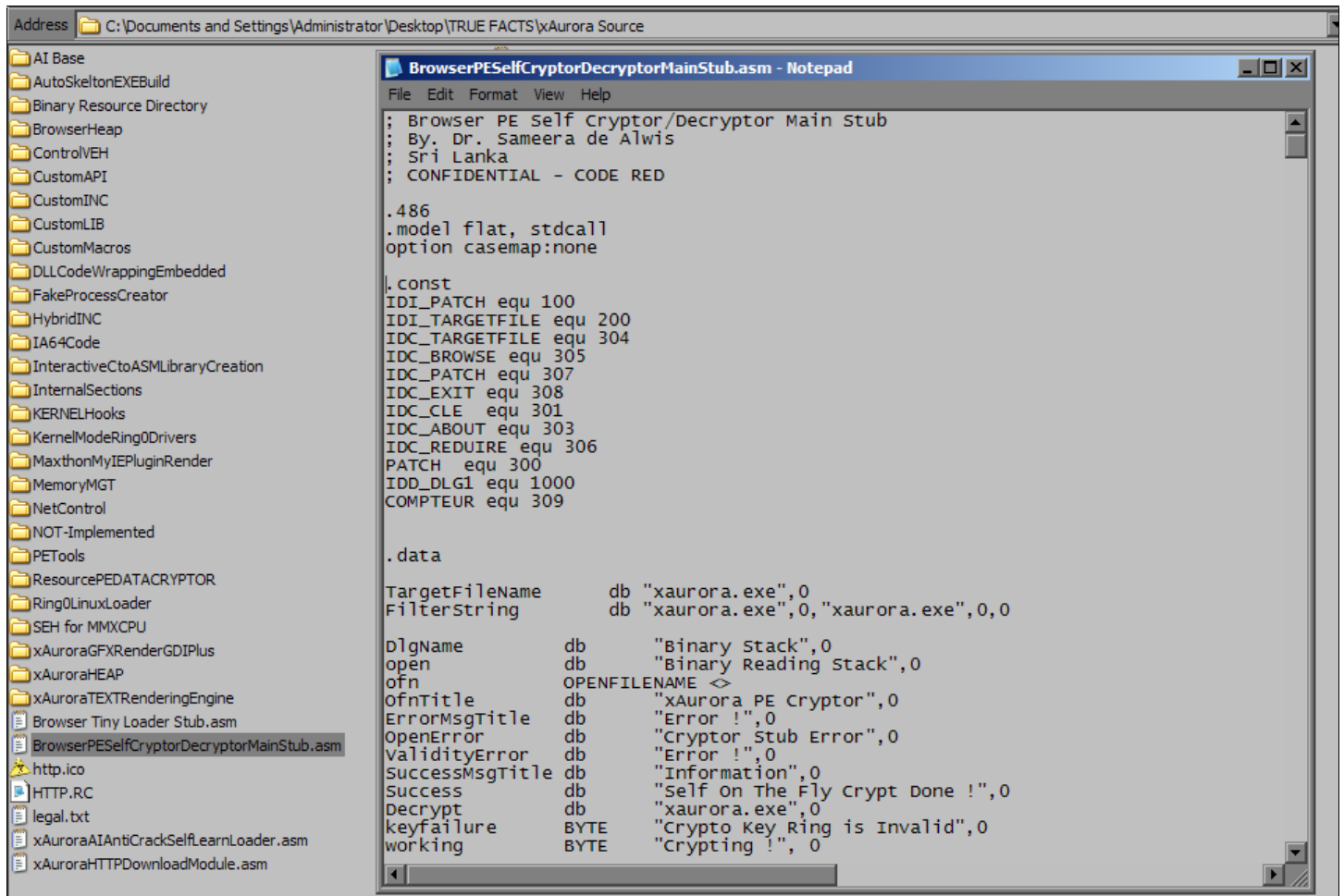
CreateMask PROTO :DWORD, :DWORD

Ct\TxtData STRUCT
    ws      dd 0
    timeout dd 0
    color   dd 0
    hTxt    dd 0
    hMask   dd 0
    xoffset dd 0
    yoffset dd 0
    bwidth  dd 0
    bHeight dd 0
    inioff  dd 0
    maxoff  dd 0
Ct\TxtData ENDS

.DATA
hInstance      dd 0
szCt\TxtCls    db "xAurora TEXT Rendering Engine", 0

.CODE
DllMain PROC hInst:DWORD, reason:DWORD, resvd:DWORD
LOCAL wc:WNDCLASSEX
    .IF reason == DLL_PROCESS_ATTACH
        ; Register control class
        mov wc.cbSize, SIZEOF WNDCLASSEX
        mov wc.style, 0
        mov wc.lpfnWndProc, OFFSET Ct\TxtWndProc
        mov wc.cbWndExtra, 4
        mov eax, hInst
        mov hInstance, eax
    .ENDIF
DllMain ENDP
```

## 30. Browser PE Self Cryptor/Decryptor Main Stub



```
Address C:\Documents and Settings\Administrator\Desktop\TRUE FACTS\xAurora Source

AI Base
AutoSkeltonEXEBuild
Binary Resource Directory
BrowserHeap
ControlVEH
CustomAPI
CustomINC
CustomLIB
CustomMacros
DLLCodeWrappingEmbedded
FakeProcessCreator
HybridINC
IA64Code
InteractiveCtoASMLibraryCreation
InternalSections
KERNELHooks
KernelModeRing0Drivers
MaxthonMyIEPluginRender
MemoryMGT
NetControl
NOT-Implemented
PETools
ResourcePEDATACRYPTOR
Ring0LinuxLoader
SEH for MMXCPU
xAuroraGFXRenderGDIPlus
xAuroraHEAP
xAuroraTEXTREnderingEngine
Browser Tiny Loader Stub.asm
BrowserPESelfCryptorDecryptorMainStub.asm
http.ico
HTTP.RC
legal.txt
xAuroraAIAntiCrackSelfLearnLoader.asm
xAuroraHTTPDownloadModule.asm

BrowserPESelfCryptorDecryptorMainStub.asm - Notepad
File Edit Format View Help
: Browser PE Self Cryptor/Decryptor Main Stub
: By. Dr. Sameera de Alwis
: Sri Lanka
: CONFIDENTIAL - CODE RED

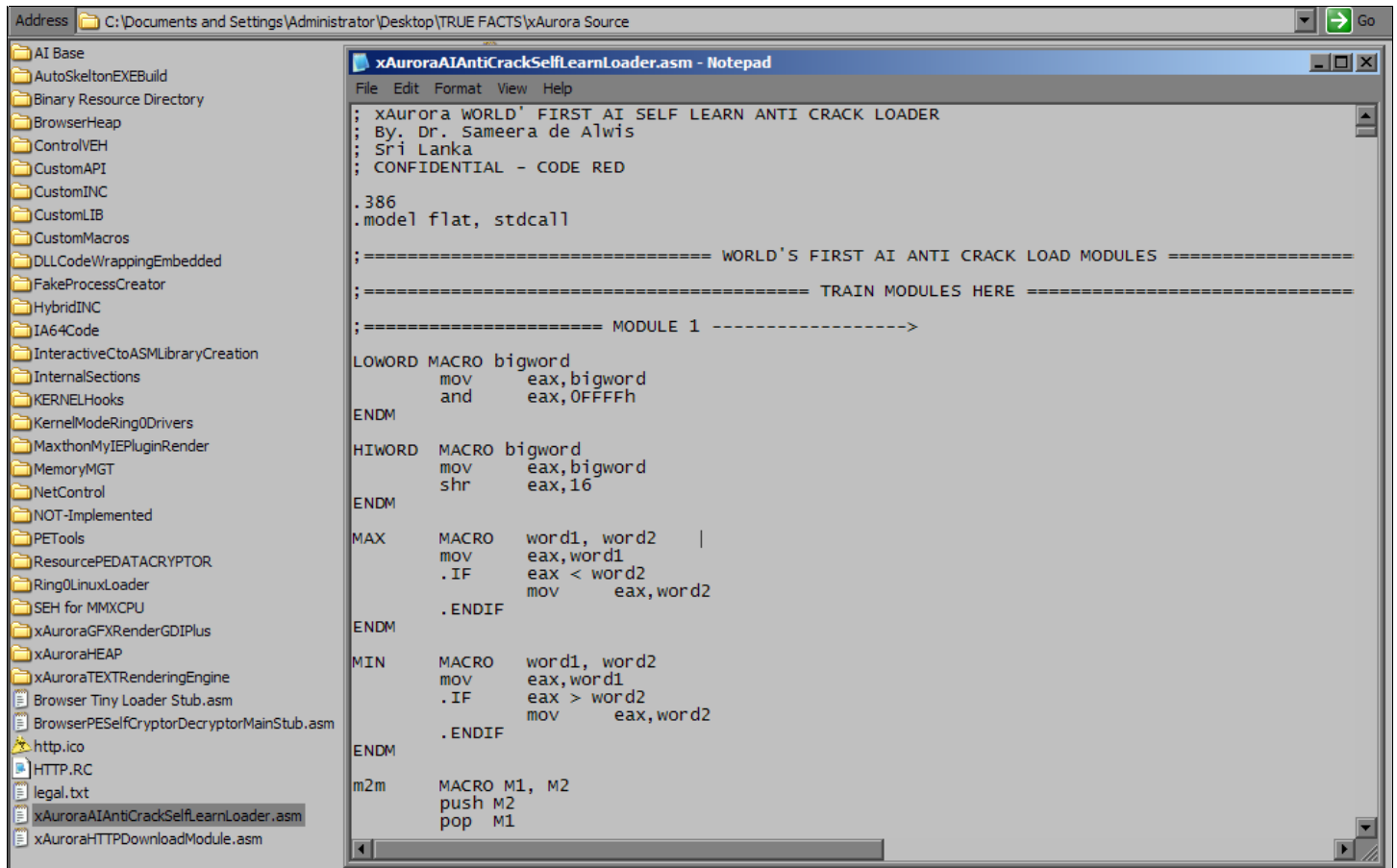
.486
.model flat, stdcall
option casemap:none

|.const
IDI_PATCH equ 100
IDI_TARGETFILE equ 200
IDC_TARGETFILE equ 304
IDC_BROWSE equ 305
IDC_PATCH equ 307
IDC_EXIT equ 308
IDC_CLE equ 301
IDC_ABOUT equ 303
IDC_REQUIRE equ 306
PATCH equ 300
IDD_DLGI equ 1000
COMPTEUR equ 309

.data
TargetFileName db "xaurora.exe",0
FilterString db "xaurora.exe",0,"xaurora.exe",0,0

DlgName db "Binary Stack",0
open db "Binary Reading Stack",0
ofn OPENFILENAME <
ofnTitle db "xAurora PE Cryptor",0
ErrorMsgTitle db "Error !",0
OpenError db "Cryptor Stub Error",0
ValidityError db "Error !",0
SuccessMsgTitle db "Information",0
Success db "Self on The Fly Crypt Done !",0
Decrypt db "xaurora.exe",0
keyfailure BYTE "Crypto Key Ring is Invalid",0
working BYTE "Crypting !", 0
```

## 31. xAurora WORLD' FIRST AI SELF LEARN ANTI CRACK LOADER



```
Address C:\Documents and Settings\Administrator\Desktop\TRUE FACTS\xAurora Source
xAuroraAIAntiCrackSelfLearnLoader.asm - Notepad
File Edit Format View Help
; xAurora WORLD' FIRST AI SELF LEARN ANTI CRACK LOADER
; By. Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

.386
.model flat, stdcall

;===== WORLD'S FIRST AI ANTI CRACK LOAD MODULES =====
;===== TRAIN MODULES HERE =====
;===== MODULE 1 ----->

LOWORD MACRO bigword
        mov     eax, bigword
        and     eax, 0FFFFh
ENDM

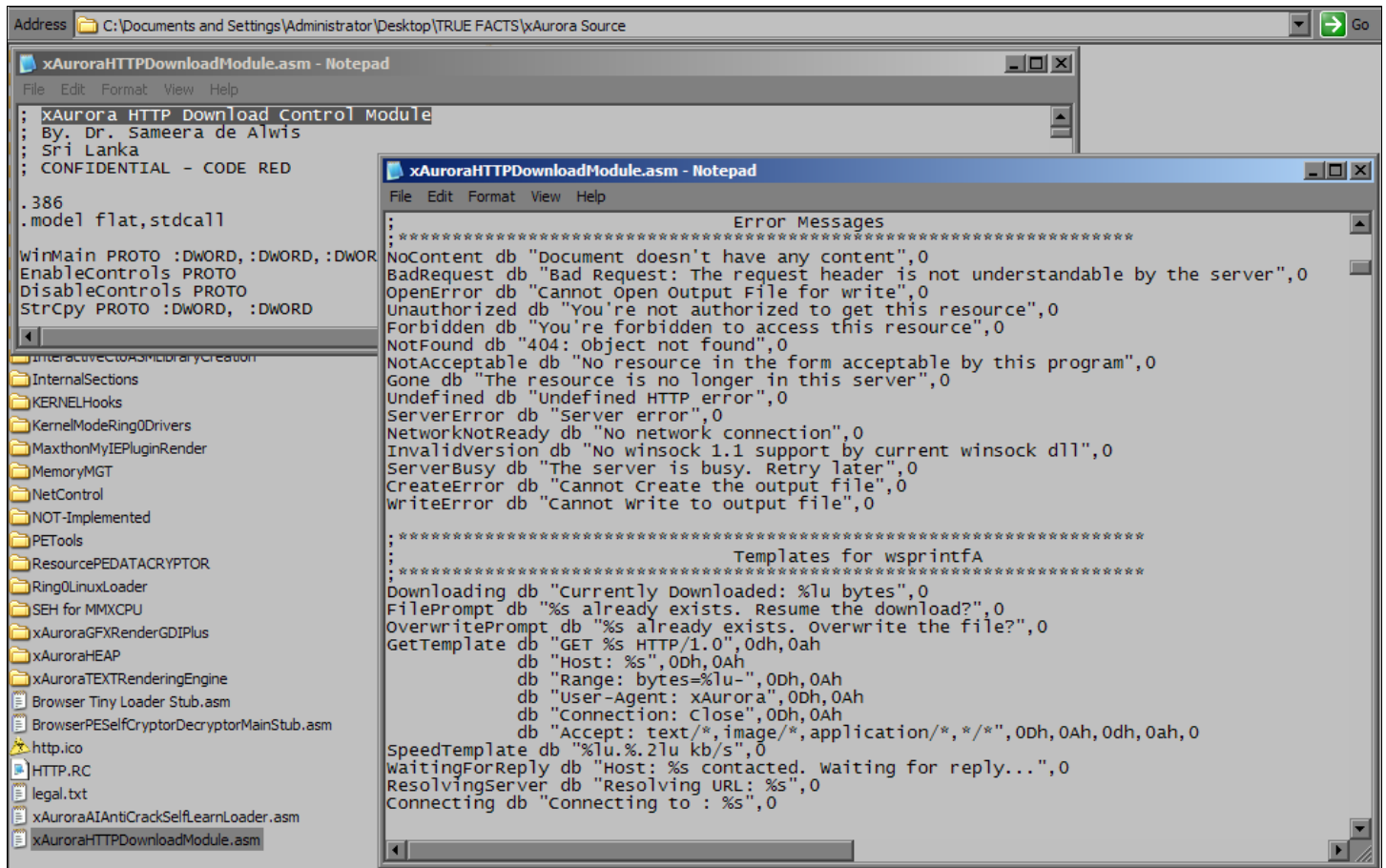
HIWORD MACRO bigword
        mov     eax, bigword
        shr     eax, 16
ENDM

MAX MACRO word1, word2
        mov     eax, word1
        .IF     eax < word2
            mov     eax, word2
        .ENDIF
ENDM

MIN MACRO word1, word2
        mov     eax, word1
        .IF     eax > word2
            mov     eax, word2
        .ENDIF
ENDM

m2m MACRO M1, M2
        push M2
        pop M1
```

## 32. xAurora HTTP Download Control Module



```
Address C:\Documents and Settings\Administrator\Desktop\TRUE FACTS\xAurora Source
Go

xAuroraHTTPDownloadModule.asm - Notepad
File Edit Format View Help
; XAurora HTTP Download Control Module
; By: Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

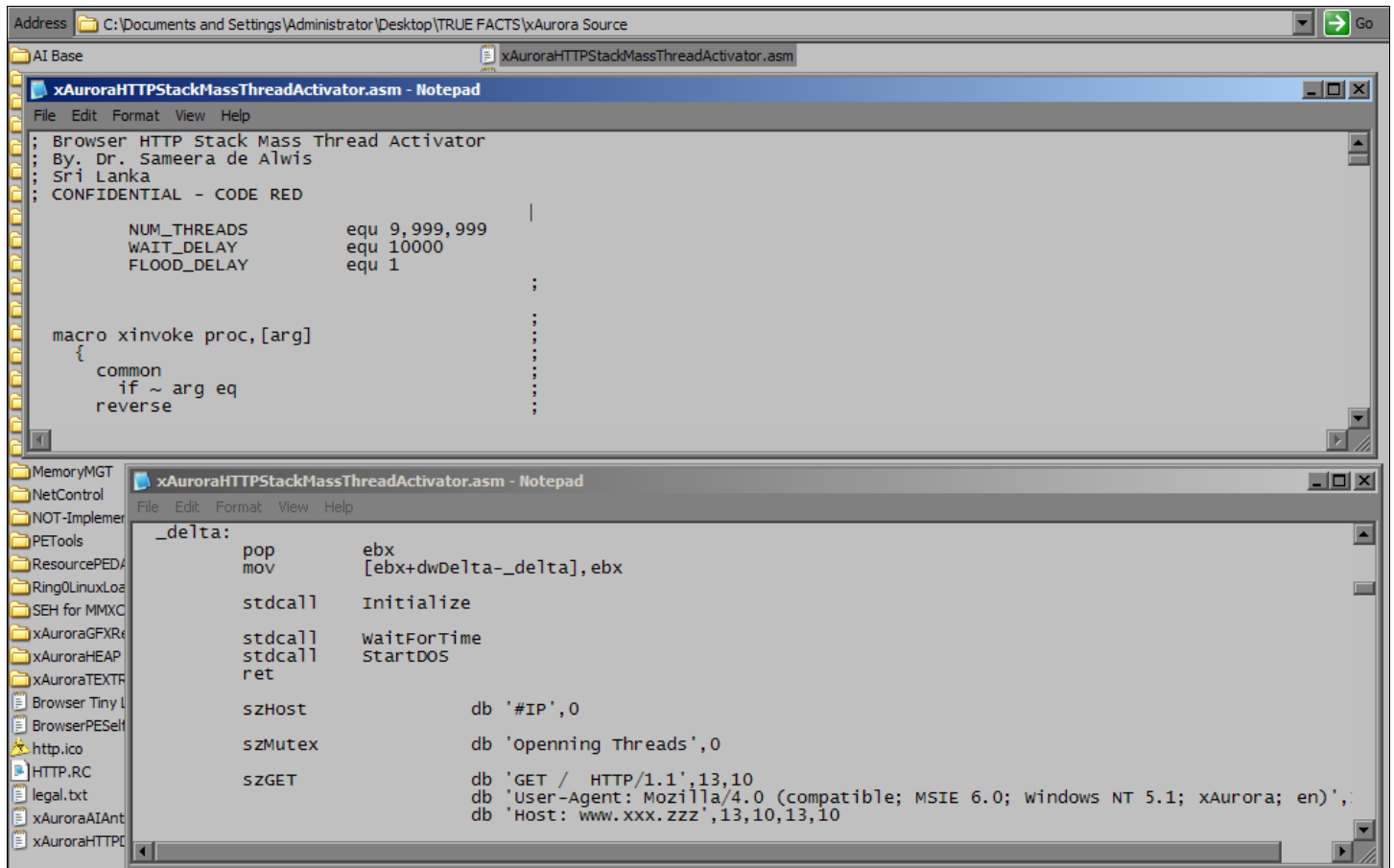
.386
.model flat,stdcall

winMain PROTO :DWORD, :DWORD, :DWORD
EnableControls PROTO
DisableControls PROTO
StrCpy PROTO :DWORD, :DWORD

InteractiveToAMMLibraryCreation
InternalSections
KERNELHooks
KernelModeRing0Drivers
MaxthonMyIEPluginRender
MemoryMGT
NetControl
NOT-Implemented
PETools
ResourcePEDATACRYPTOR
Ring0LinuxLoader
SEH for MMXCPU
xAuroraGFXRenderGDIPlus
xAuroraHEAP
xAuroraTEXTRenderingEngine
Browser Tiny Loader Stub.asm
BrowserPESelfCryptorDecryptorMainStub.asm
http.ico
HTTP.RC
legal.txt
xAuroraAIAntiCrackSelfLearnLoader.asm
xAuroraHTTPDownloadModule.asm

xAuroraHTTPDownloadModule.asm - Notepad
File Edit Format View Help
; ***** Error Messages *****
;
; NoContent db "Document doesn't have any content",0
; BadRequest db "Bad Request: The request header is not understandable by the server",0
; OpenError db "Cannot Open Output File for write",0
; Unauthorized db "You're not authorized to get this resource",0
; Forbidden db "You're forbidden to access this resource",0
; NotFound db "404: Object not found",0
; NotAcceptable db "No resource in the form acceptable by this program",0
; Gone db "The resource is no longer in this server",0
; Undefined db "undefined HTTP error",0
; ServerError db "server error",0
; NetworkNotReady db "No network connection",0
; InvalidVersion db "No winsock 1.1 support by current winsock dll",0
; ServerBusy db "The server is busy. Retry later",0
; CreateError db "Cannot Create the output file",0
; WriteError db "Cannot write to output file",0
;
; ***** Templates for sprintfA *****
;
; Downloading db "Currently Downloaded: %lu bytes",0
; FilePrompt db "%s already exists. Resume the download?",0
; OverwritePrompt db "%s already exists. Overwrite the file?",0
; GetTemplate db "GET %s HTTP/1.0",0dh,0ah
;             db "Host: %s",0dh,0ah
;             db "Range: bytes=%lu-",0dh,0ah
;             db "User-Agent: xAurora",0dh,0ah
;             db "Connection: Close",0dh,0ah
;             db "Accept: text/*,image/*,application/*,*/*",0dh,0ah,0dh,0ah,0
; SpeedTemplate db "%lu.%2lu kb/s",0
; WaitForReply db "Host: %s contacted. waiting for reply...",0
; ResolvingServer db "Resolving URL: %s",0
; Connecting db "Connecting to : %s",0
```

### 33. Browser HTTP Stack Mass Thread Activator



## 34. Browser HTTP Stack Verification/Filter Module

```
Address C:\Documents and Settings\Administrator\Desktop\TRUE FACTS\xAurora Source
AI Base xAuroraHTTPStackMassThreadActivator.asm
AutoSkeletonEXEBuild xAuroraHTTPStackVerificationFilterModule.asm
xAuroraHTTPStackVerificationFilterModule.asm - Notepad
File Edit Format View Help
: Browser HTTP Stack Verification/Filter Module
: By. Dr. Sameera de Alwis
: Sri Lanka
: CONFIDENTIAL - CODE RED

.386
.model flat, stdcall
option casemap:none
title HTTP Stack Check

szText MACRO Name, Text:VARARG
LOCAL lbl
    jmp     lbl
    Name   db     Text, 0
lbl:
ENDM
m2m MACRO M1, M2

ErrorHandler PROTO C :DWORD, :DWORD, :DWORD, :DWORD
ExceptionFilter PROTO :DWORD
.const
    szMsgAbout      db     "HTTP Stack Check", 13, 10
                    db     "401 HTTP Stack Check Scan", 13, 10
    dwMsgAboutLen   equ    $ - szMsgAbout
    szStatuswork    db     "Processing...", 13, 10
    szStatusDone    db     "Succeed", 13, 10
    szErrorThread   db     13, 10, "Error at %08xh", 13, 10, "Registers:", 13, 10, "eax = %08xh ebx = %08xh
ecx = %08xh", 13, 10, "edx = %08xh esp = %08xh ebp = %08xh", 13, 10, "esi = %08xh edi = %08xh", 13, 10, 13, 10,
"Recovering...", 13, 10, 0
    szErrorFinal    db     13, 10, "Error at %08xh", 13, 10, "Quitting...", 13, 10, 0

    szRequest       db     "GET / HTTP/1.0", 13, 10, "Accept: /*/*", 13, 10, "connection: close", 13, 10,
13, 10

.data
.data?
```

## 35. Browser Kernel Process Control Base

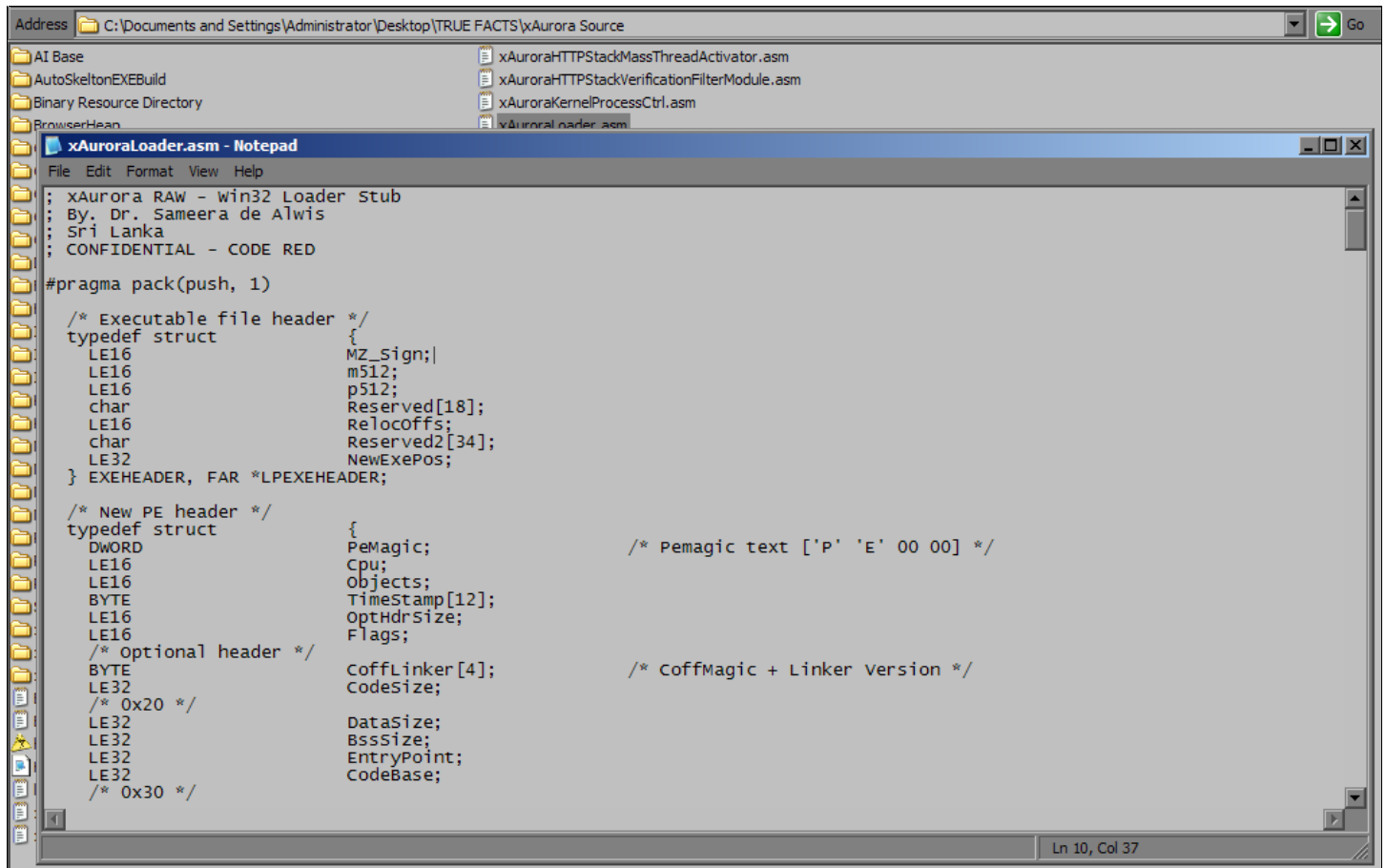
```
Address C:\Documents and Settings\Administrator\Desktop\TRUE FACTS\xAurora Source
xAuroraHTTPStackMassThreadActivator.asm
xAuroraHTTPStackVerificationFilterModule.asm
xAuroraKernelProcessCtrl.asm
xAuroraKernelProcessCtrl.asm
xAuroraKernelProcessCtrl.asm

xAuroraKernelProcessCtrl.asm - Notepad
File Edit Format View Help
; Browser Kernel Process Control Base
; By. Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

KPROCESS STRUCT ; sizeof = 06Ch
  Header          DISPATCHER_HEADER <> ; 000h DO_TYPE_PROCESS (0x1B)
  ProfileListHead LIST_ENTRY <> ; 010h
  DirectoryTableBase DWORD ? ; 018h
  PageTableBase    DWORD ? ; 01Ch
  LdtDescriptor    KGDTENTRY <> ; 020h
  Int21Descriptor  KIDTENTRY <> ; 028h
  IopmOffset      WORD ? ; 030h
  Iopl             BYTE ? ; 032h
  VdmFlag         BOOLEAN ? ; 033h
  ActiveProcessors DWORD ? ; 034h
  KernelTime      DWORD ? ; 038h ticks
  UserTime        DWORD ? ; 03Ch ticks
  ReadyListHead  LIST_ENTRY <> ; 040h
  SwapListEntry  LIST_ENTRY <> ; 048h
  ThreadListHead LIST_ENTRY <> ; 050h KTHREAD.ThreadListEntry
  ProcessLock    PVOID ? ; 058h
  Affinity       KAFFINITY ? ; 05Ch
  StackCount     WORD ? ; 060h
  BasePriority    BYTE ? ; 062h
  ThreadQuantum  BYTE ? ; 063h
  AutoAlignment  BOOLEAN ? ; 064h
  State          BYTE ? ; 065h
  ThreadSeed     BYTE ? ; 066h
  DisableBoost   BOOLEAN ? ; 067h
  PowerState     BYTE ? ; 068h
  DisableQuantum BOOLEAN ? ; 069h
  Spare          BYTE 2 dup(?) ; 06Ah
KPROCESS ENDS
PKPROCESS typedef PTR KPROCESS

Ln 10, Col 34
```

## 36. xAurora RAW – Win32 Loader Stub



```
Address C:\Documents and Settings\Administrator\Desktop\TRUE FACTS\xAurora Source
AI Base
AutoSkeltonEXEBuild
Binary Resource Directory
BrowserHeap
xAuroraHTTPStackMassThreadActivator.asm
xAuroraHTTPStackVerificationFilterModule.asm
xAuroraKernelProcessCtrl.asm
xAuroraLoader.asm

xAuroraLoader.asm - Notepad
File Edit Format View Help
; xAurora RAW - win32 Loader Stub
; By, Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

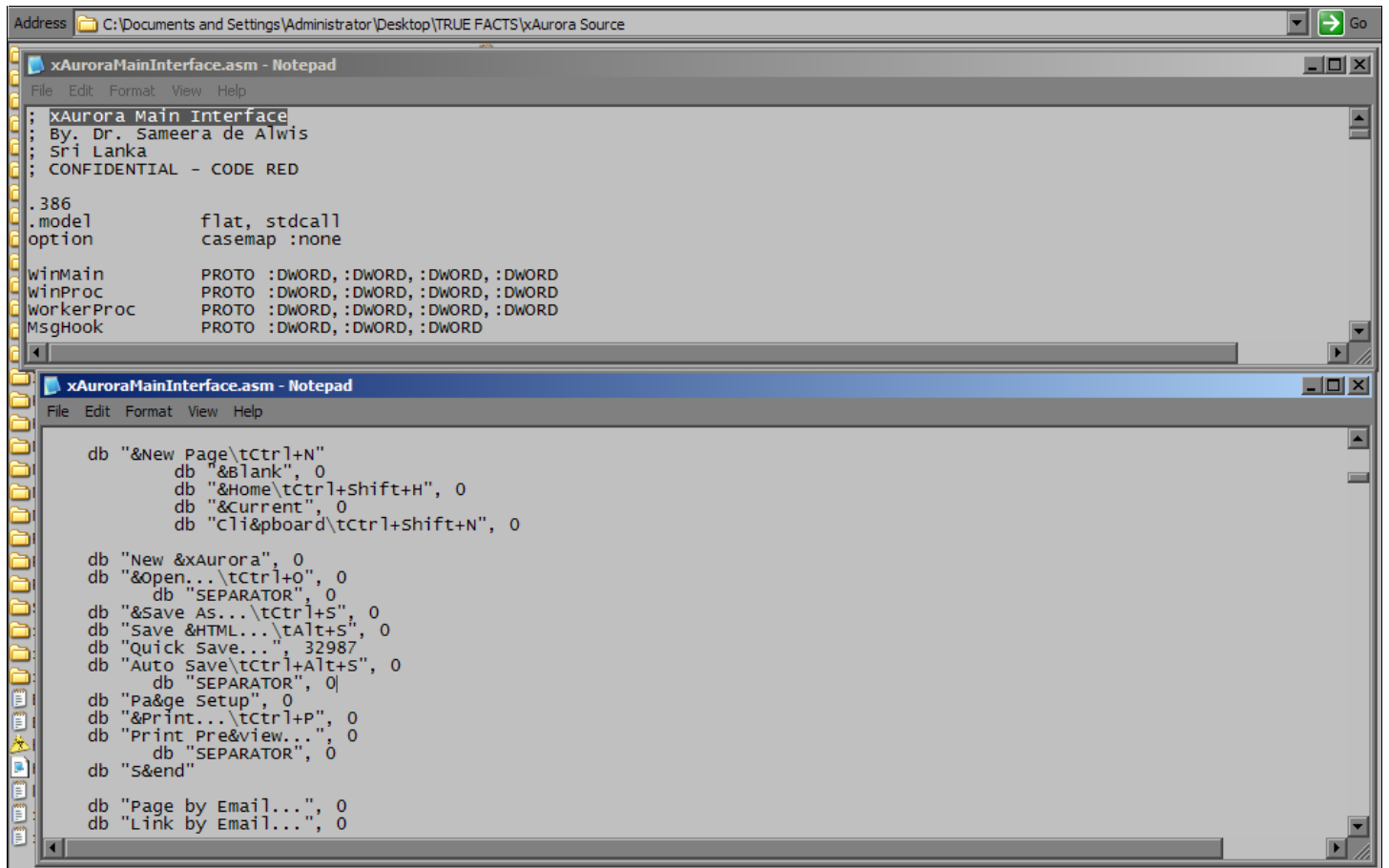
#pragma pack(push, 1)

/* Executable file header */
typedef struct
{
    LE16 MZ_sign;|
    LE16 m512;
    LE16 p512;
    char Reserved[18];
    LE16 RelocOffs;
    char Reserved2[34];
    LE32 NewExePos;
} EXEHEADER, FAR *LPEXEHEADER;

/* New PE header */
typedef struct
{
    DWORD PeMagic; /* Pemagic text ['P' 'E' 00 00] */
    LE16 Cpu;
    LE16 Objects;
    BYTE Timestamp[12];
    LE16 optHdrSize;
    LE16 Flags;
    /* optional header */
    BYTE CoffLinker[4]; /* CoffMagic + Linker version */
    LE32 CodeSize;
    /* 0x20 */
    LE32 DataSize;
    LE32 BssSize;
    LE32 EntryPoint;
    LE32 CodeBase;
    /* 0x30 */
} PEHEADER, FAR *LPEHEADER;
```

Ln 10, Col 37

## 37. xAurora Main Interface



```
Address C:\Documents and Settings\Administrator\Desktop\TRUE FACTS\xAurora Source
Go

xAuroraMainInterface.asm - Notepad
File Edit Format View Help
: xAurora Main Interface
: By. Dr. Sameera de Alwis
: Sri Lanka
: CONFIDENTIAL - CODE RED

.386
.model flat, stdcall
.option casemap :none

winMain PROTO :DWORD, :DWORD, :DWORD, :DWORD
winProc PROTO :DWORD, :DWORD, :DWORD, :DWORD
workerProc PROTO :DWORD, :DWORD, :DWORD, :DWORD
MsgHook PROTO :DWORD, :DWORD, :DWORD

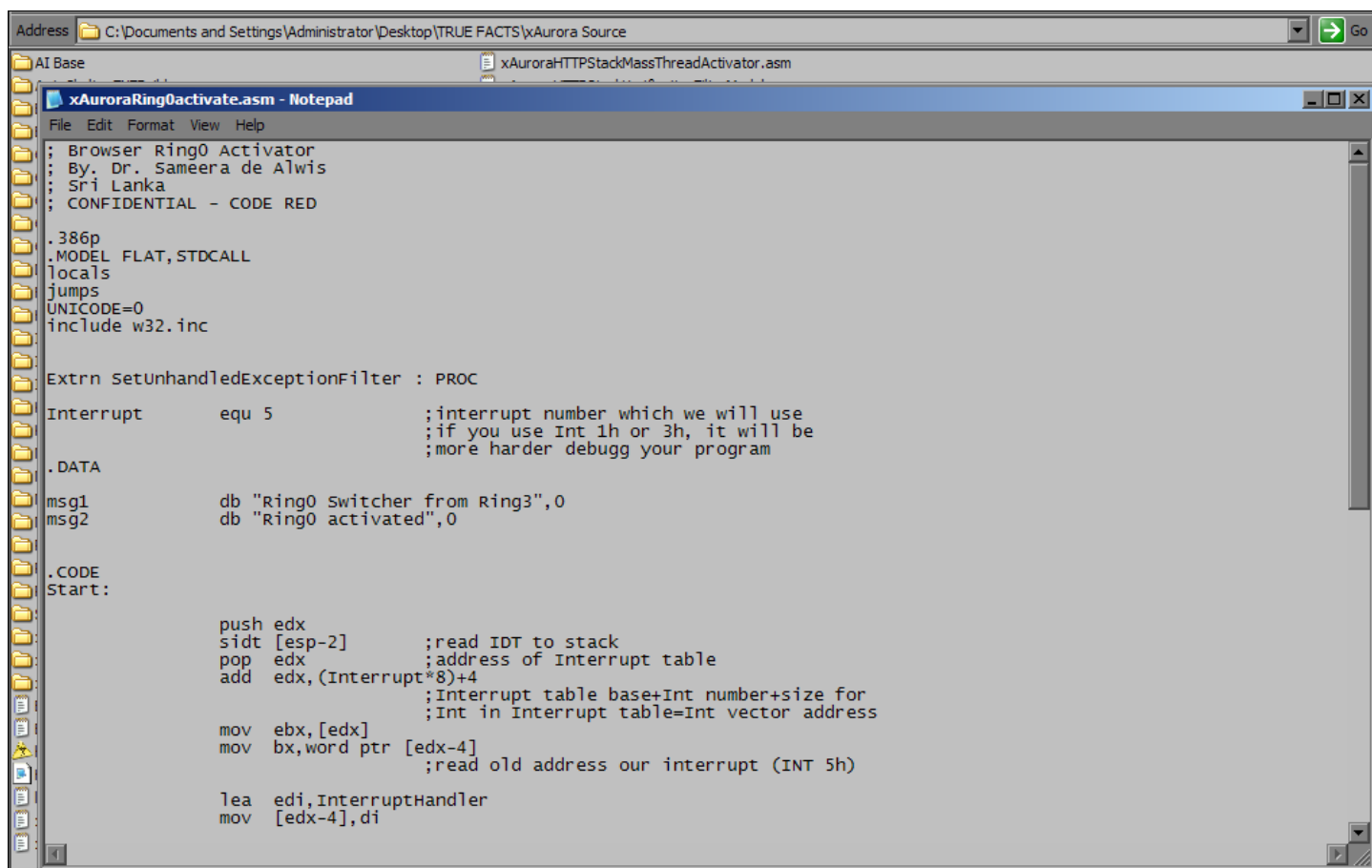
xAuroraMainInterface.asm - Notepad
File Edit Format View Help

db "&New Page\tCtrl+N"
db "&Blank", 0
db "&Home\tCtrl+Shift+H", 0
db "&Current", 0
db "Clipboard\tCtrl+Shift+N", 0

db "New &xAurora", 0
db "&Open...\tCtrl+O", 0
db "SEPARATOR", 0
db "&Save As...\tCtrl+S", 0
db "Save &HTML...\tAlt+S", 0
db "Quick Save...", 32987
db "Auto Save\tCtrl+Alt+S", 0
db "SEPARATOR", 0
db "Pa&ge Setup", 0
db "&Print...\tCtrl+P", 0
db "Print Pre&view...", 0
db "SEPARATOR", 0
db "s&end"

db "Page by Email...", 0
db "Link by Email...", 0
```

## 38. Browser Ring0 Activator



```
Address C:\Documents and Settings\Administrator\Desktop\TRUE FACTS\xAurora Source
xAuroraHTTPStackMassThreadActivator.asm
xAuroraRing0Activate.asm - Notepad
File Edit Format View Help
; Browser Ring0 Activator
; By. Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

.386p
.MODEL FLAT, STDCALL
.locals
jumps
UNICODE=0
include w32.inc

Extrn setUnhandledExceptionFilter : PROC

Interrupt      equ 5          ;interrupt number which we will use
                ;if you use Int 1h or 3h, it will be
                ;more harder debugg your program

.DATA

msg1           db "Ring0 Switcher from Ring3",0
msg2           db "Ring0 activated",0

.CODE
Start:

    push edx
    sidt [esp-2]          ;read IDT to stack
    pop  edx             ;address of Interrupt table
    add  edx,(Interrupt*8)+4
                        ;Interrupt table base+Int number+size for
                        ;Int in Interrupt table=Int vector address

    mov  ebx,[edx]
    mov  bx,word ptr [edx-4]
                        ;read old address our interrupt (INT 5h)

    lea  edi,InterruptHandler
    mov  [edx-4],di
```

### 39. xAurora (SDDK) Self Driver Development Kit Loader

```
Address C:\Documents and Settings\Administrator\Desktop\TRUE FACTS\xAurora Source
xAuroraSDDKSelfDriverDevelopmentKitLoader.asm - Notepad
File Edit Format View Help
; xAurora (SDDK) Self Driver Development Kit Loader
; By. Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

ABOUT_BUTTON equ 102
RUN_BUTTON equ 101

.386
.model flat,stdcall

dlg_call PROTO

.data
    dlg db "DDK_MAIN",0

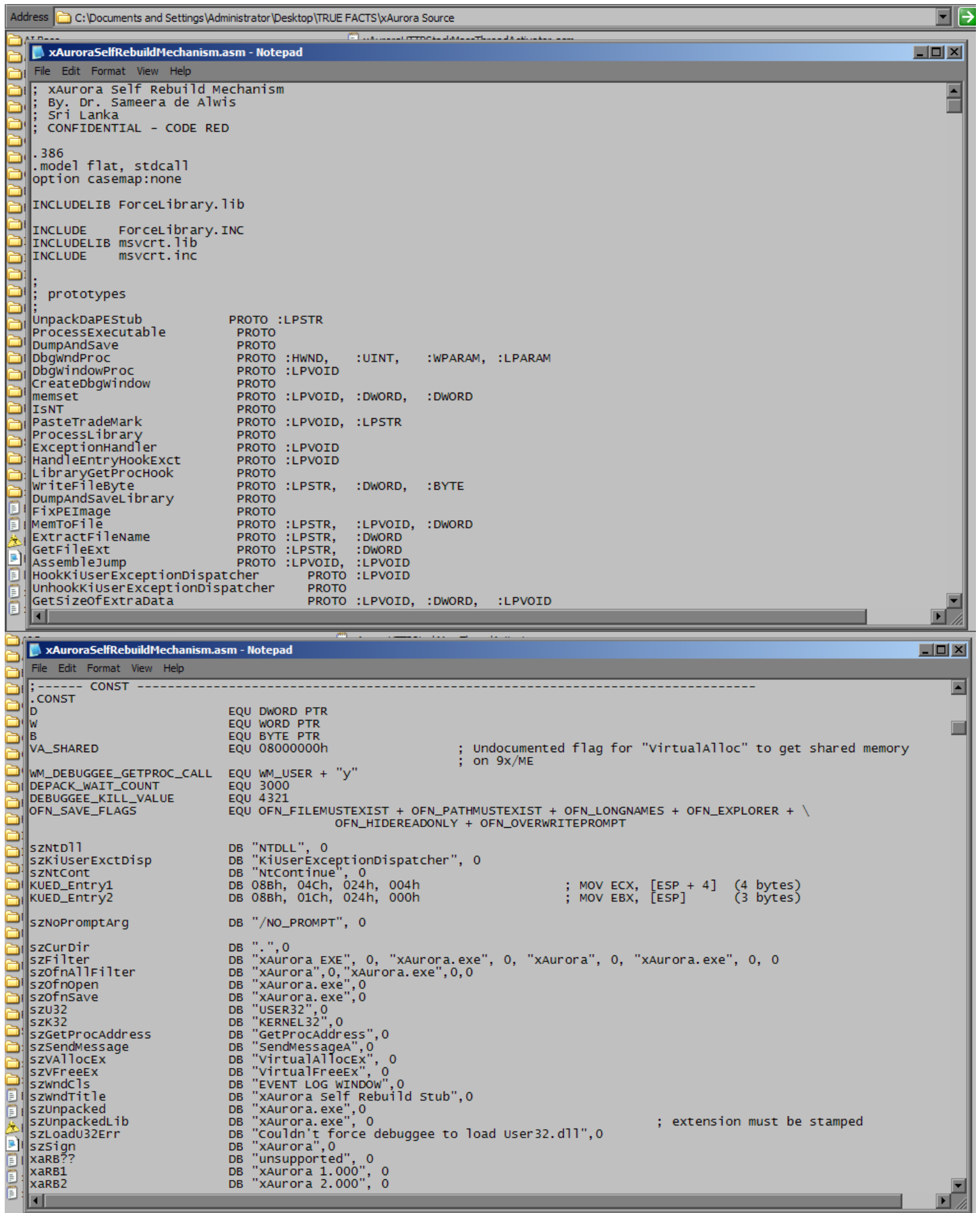
    about_message db "xAurora (SDDK) Self Driver Development Kit",13,10
    about_title db "Build OK",0

    error_title db "Error Loading Driver",0

    gets_number db 2 dup(0)

I
    T equ 06666665h
    dd 0
    A dd 0
    B dd 0
    Cr dd 0
    p db 0
    R1 db 0
H
    R equ 0110b
    db 0
    kkk db 0
    Cn db 0
```

## 40. xAurora Self Rebuild Mechanism



```
Address C:\Documents and Settings\Administrator\Desktop\TRUE FACTS\xAurora Source
xAuroraSelfRebuildMechanism.asm - Notepad
File Edit Format View Help
; xAurora Self Rebuild Mechanism
; By. Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

.386
.model flat, stdcall
option casemap:none

INCLUDELIB ForceLibrary.lib

INCLUDE ForceLibrary.INC
INCLUDELIB msvcrt.lib
INCLUDE msvcrt.inc

;
; prototypes
;
UnpackDaPEStub          PROTO :LPSTR
ProcessExecutable      PROTO
DumpAndSave            PROTO
DbgWndProc             PROTO :HWND, :UINT, :WPARAM, :LPARAM
DbgWindowProc          PROTO :LPVOID
CreateDbgWindow        PROTO
memset                 PROTO :LPVOID, :DWORD, :DWORD
IsNT                   PROTO
PasteTradeMark         PROTO :LPVOID, :LPSTR
ProcessLibrary         PROTO
ExceptionHandler       PROTO :LPVOID
HandleEntryHookExct    PROTO :LPVOID
LibraryGetProcAddress  PROTO
WriteFileByte          PROTO :LPSTR, :DWORD, :BYTE
DumpAndSaveLibrary     PROTO
FixPEImage             PROTO
MemToFile              PROTO :LPSTR, :LPVOID, :DWORD
ExtractFileName        PROTO :LPSTR, :DWORD
GetFileExt             PROTO :LPSTR, :DWORD
AssembleJump           PROTO :LPVOID, :LPVOID
HookKiUserExceptionDispatcher PROTO :LPVOID
UnhookKiUserExceptionDispatcher PROTO
GetSizeOfExtraData     PROTO :LPVOID, :DWORD, :LPVOID

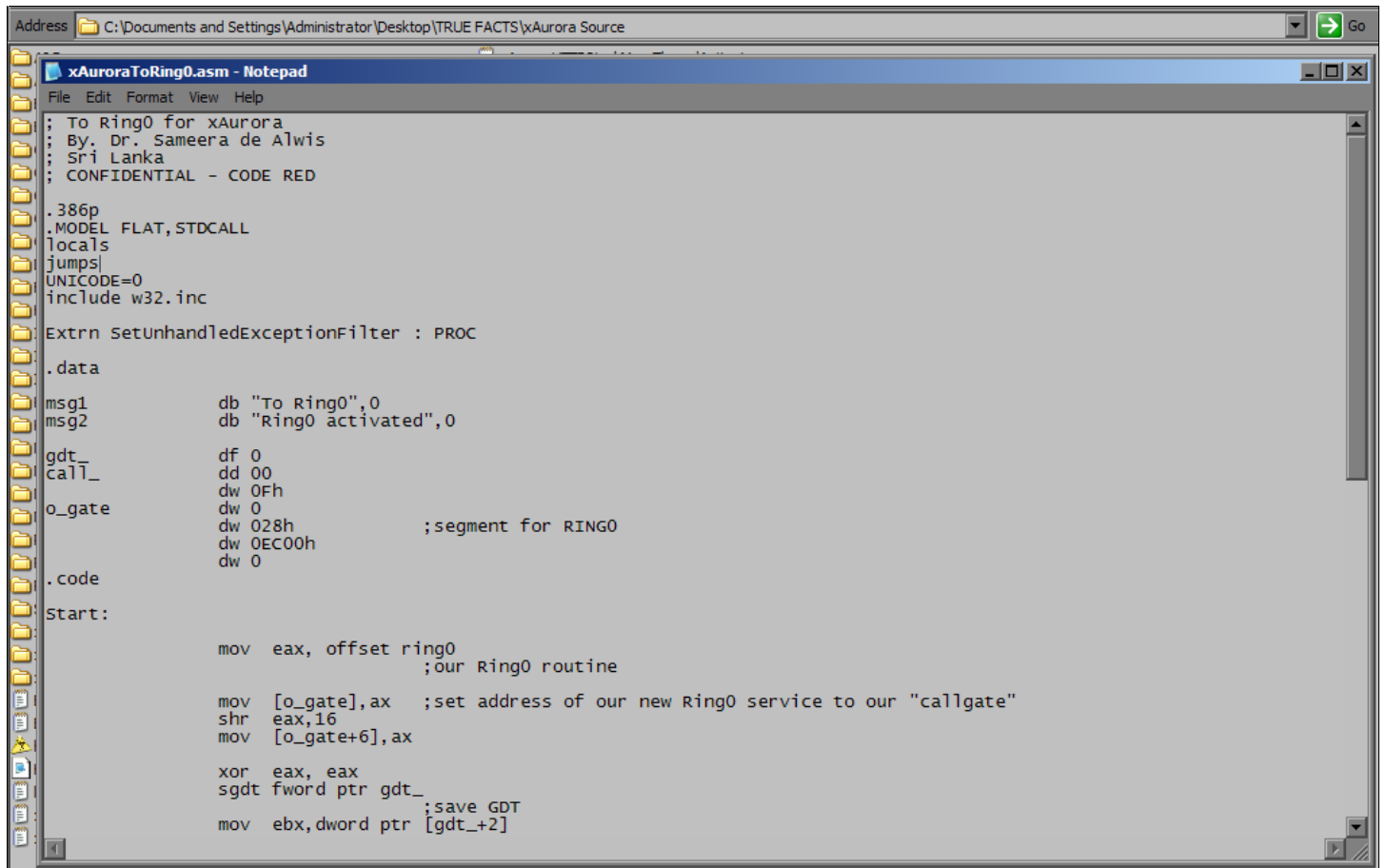
xAuroraSelfRebuildMechanism.asm - Notepad
File Edit Format View Help
;----- CONST -----
.CONST
D          EQU DWORD PTR
W          EQU WORD PTR
B          EQU BYTE PTR
VA_SHARED EQU 08000000h ; Undocumented flag for "VirtualAlloc" to get shared memory
; on 9x/ME
WM_DEBUGGEE_GETPROC_CALL EQU WM_USER + "y"
DEPACK_WAIT_COUNT EQU 3000
DEBUGGEE_KILL_VALUE EQU 4321
OFN_SAVE_FLAGS EQU OFN_FILEMUSTEXIST + OFN_PATHMUSTEXIST + OFN_LONGNAMES + OFN_EXPLORER + \
OFN_HIDEREADONLY + OFN_OVERWRITEPROMPT

szNtdll DB "NTDLL", 0
szKiUserExctDisp DB "KiUserExceptionDispatcher", 0
szNtCont DB "NtContinue", 0
KUED_Entry1 DB 08Bh, 04Ch, 024h, 004h ; MOV ECX, [ESP + 4] (4 bytes)
KUED_Entry2 DB 08Bh, 01Ch, 024h, 000h ; MOV EBX, [ESP] (3 bytes)

szNoPromptArg DB "/NO_PROMPT", 0

szCurDir DB ".", 0
szFilter DB "xAurora EXE", 0, "xAurora.exe", 0, "xAurora", 0, "xAurora.exe", 0, 0
szofnAllFilter DB "xAurora", 0, "xAurora.exe", 0, 0
szofnOpen DB "xAurora.exe", 0
szofnSave DB "xAurora.exe", 0
szU32 DB "USER32", 0
szK32 DB "KERNEL32", 0
szGetProcAddress DB "GetProcAddress", 0
szSendMessage DB "SendMessageA", 0
szVirtualAllocEx DB "VirtualAllocEx", 0
szVirtualFreeEx DB "VirtualFreeEx", 0
szWndCls DB "EVENT LOG WINDOW", 0
szWndTitle DB "xAurora Self Rebuild stub", 0
szUnpacked DB "xAurora.exe", 0
szUnpackedLib DB "xAurora.exe", 0 ; extension must be stamped
szLoadU32Err DB "Couldn't force debuggee to load user32.dll", 0
szSign DB "xAurora", 0
xAxB?? DB "unsupported", 0
xAxB1 DB "xAurora 1.000", 0
xAxB2 DB "xAurora 2.000", 0
```

## 41. To Ring0 for xAurora



The image shows a Notepad window titled "xAuroraToRing0.asm - Notepad" with the following assembly code:

```
Address C:\Documents and Settings\Administrator\Desktop\TRUE FACTS\xAurora Source
xAuroraToRing0.asm - Notepad
File Edit Format View Help
; To Ring0 for xAurora
; By, Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

.386p
.MODEL FLAT, STDCALL
.locals
.jumps|
.UNICODE=0
.include w32.inc

Extrn SetUnhandledExceptionFilter : PROC

.data
msg1      db "To Ring0",0
msg2      db "Ring0 activated",0

gdt_      df 0
call_     dd 00
          dw 0Fh
o_gate    dw 0
          dw 028h      ;segment for RING0
          dw 0EC00h
          dw 0

.code
Start:

mov  eax, offset ring0
          ;our Ring0 routine

mov  [o_gate],ax  ;set address of our new Ring0 service to our "callgate"
shr  eax,16
mov  [o_gate+6],ax

xor  eax, eax
sgdt fword ptr gdt_
          ;save GDT
mov  ebx,dword ptr [gdt_+2]
```



## END NOTE

xAurora Web Browser was entirely written in 100% Pure Win32 Macro Assembler. Therefore, xAurora is a very handy, Intelligent and very hardy web browser. Entire KMD(s) coded also in Win32 ASM to show the strength. This is the 1<sup>st</sup> and only web browser in the world of this kind.

## SPECIAL NOTE

For any reason I am NOT going to release the xAurora Web Browser Confidential Source Code to any authority/party. And even I DO NOT sell this. This browser is dedicated to MY MOTHER'S POOR LOST SOUL. This is going to be a FREEWARE forever and Closed Source. This is deemed official and final.

## CONCLUSION

Kalinga's blog members do not have any clue to identify the coding language and they did not spend a minute for that. But truth remains always. xAurora is a proud innovation from motherland Sri Lanka and entirely coded in Win32 Assembly Language. This guideline document will help you to understand the coded language of xAurora Web Browser.

I know my own code better than all of you. Because, I am the founder of xAurora's concepts and I am the programmer of the xAurora Web Browser. No one can admit the wrong conclusion without proving it in the real world and to the community. Because, xAurora is a COPYRIGHTED, TRADEMARKED and PATENTED SOFTWARE.

xAurora is a great Sri Lankan product that entirely coded in Win32 Assembly Language. Hope you may be able to understand it. In future I will show you many stories behind the xAurora case. Hope Mr. Gotaimbara will help me to sort out the matters soon. Thank you very much for the great support and your support in the future is greatly appreciated.

End of xAurora Developers Pod Revealed – Visual Approach – PART 1 & 2.

Hope you all enjoyed lot....!!!

Kind Regards

Dr. Sameera de Alwis

Founder – Team xAurora 2009