

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?

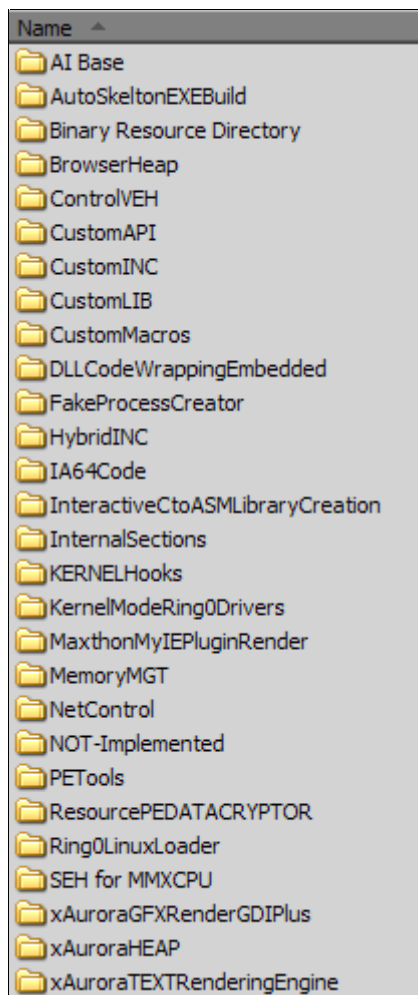
&

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

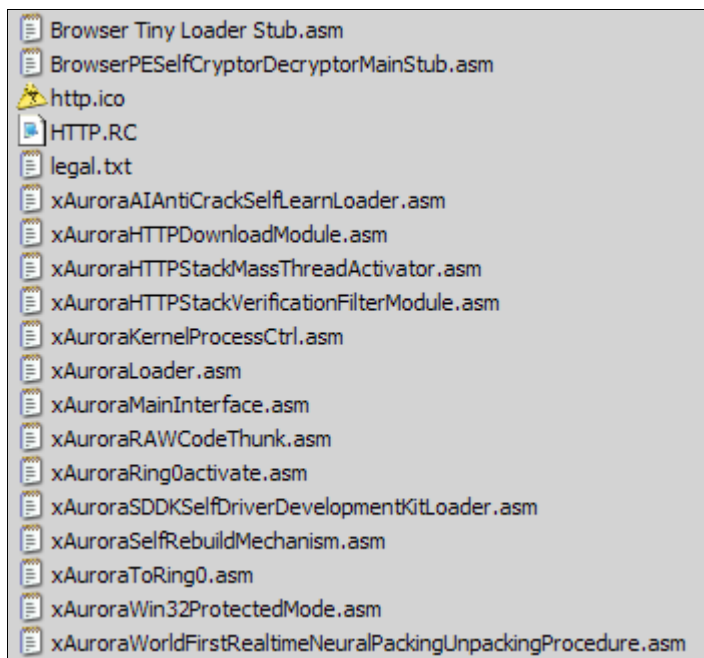
## xAurora Developers Pod Revealed - Visual Approach - PART 1

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

### 1. Main Base & Directory Structure of the Main Root

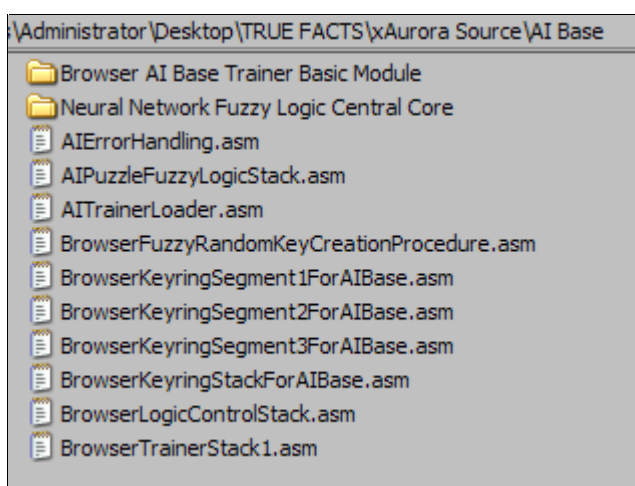


Root Folder Structure

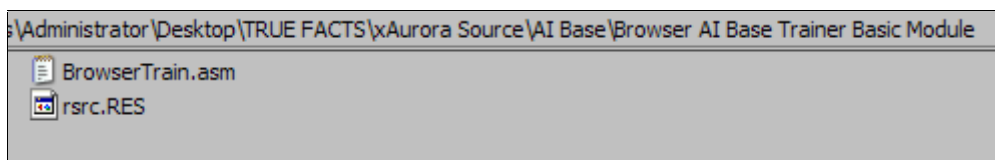


## Root Files

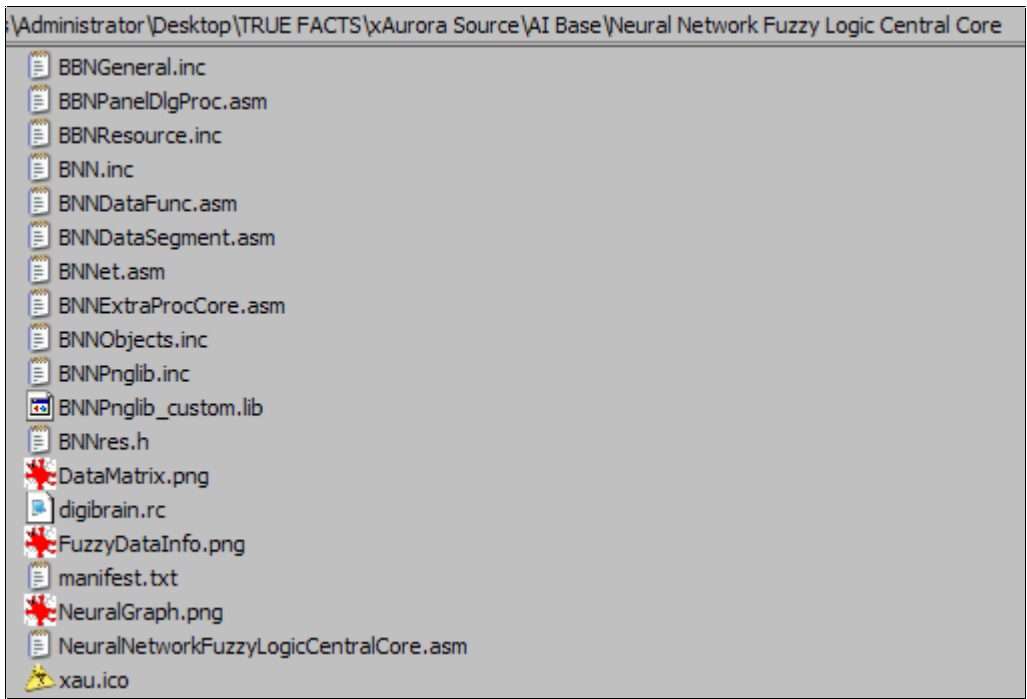
## 2. AI Base & Neural Network (Fuzzy Algorithm Based AI Engine)



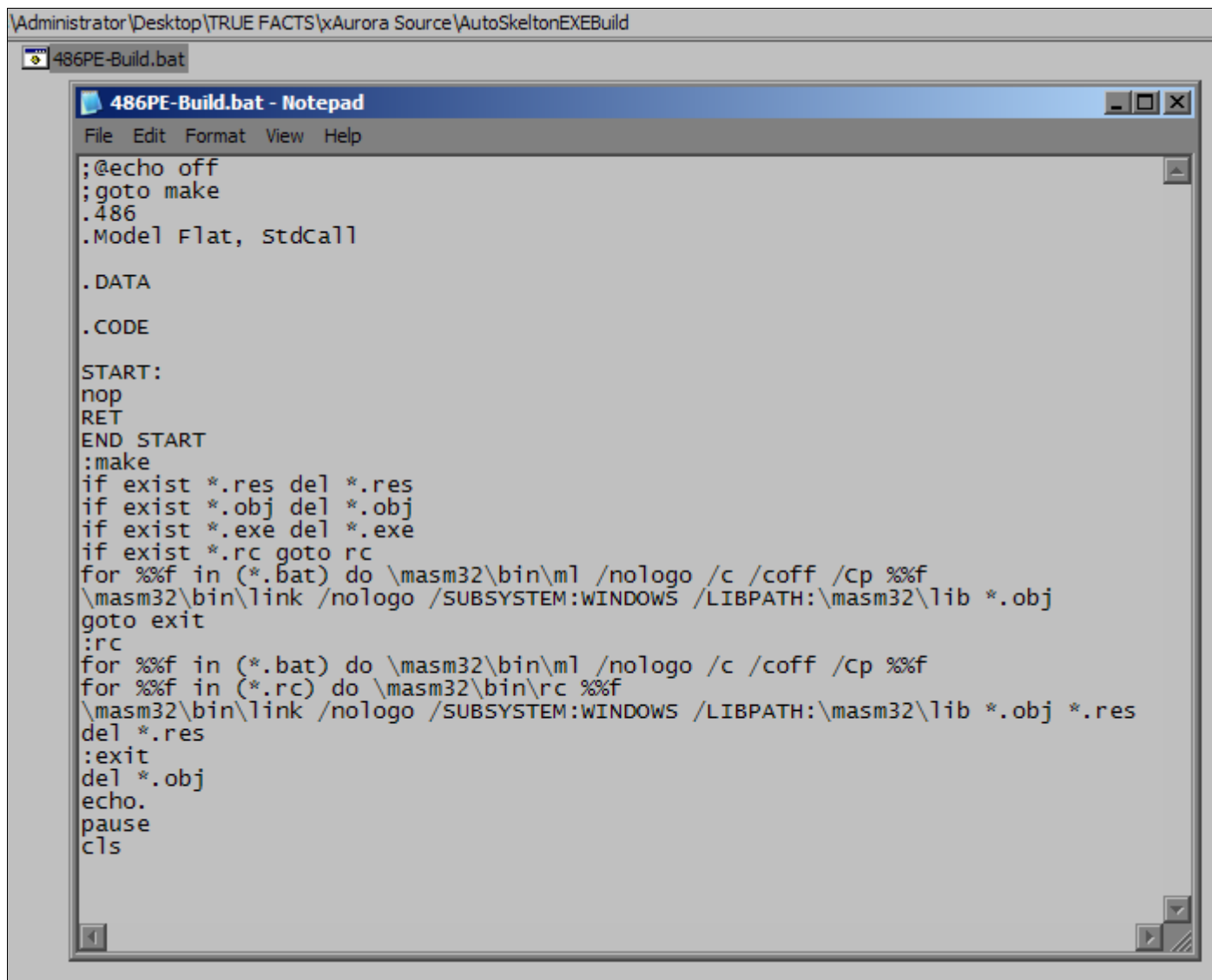
### \* Browser AI Base Trainer



\* Neural Network based on FUZZY LOGIC – Central Core Code Library



### 3. Browser Skelton EXE Builder BAT Script



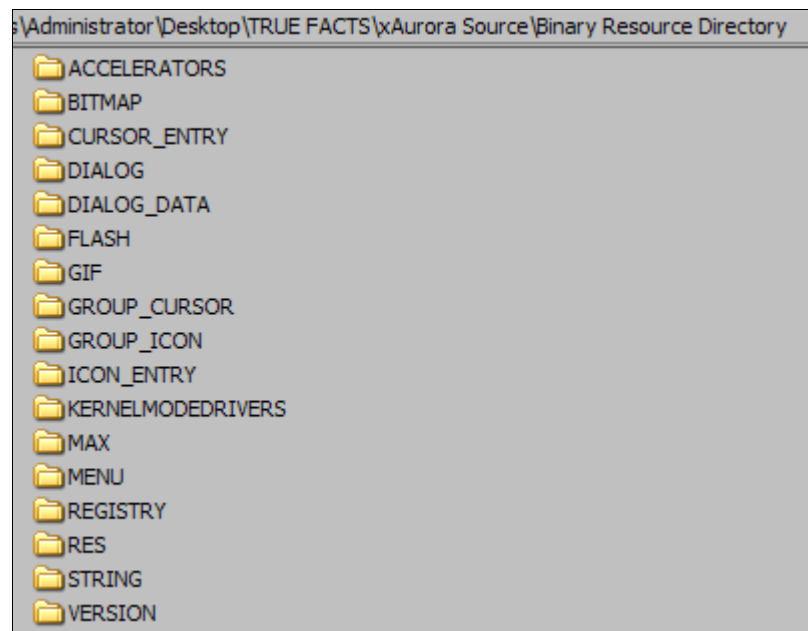
```
Administrator\Desktop\TRUE FACTS\Aurora Source\AutoSkeltonEXEBuild
486PE-Build.bat
486PE-Build.bat - Notepad
File Edit Format View Help
;@echo off
;goto make
.486
.Model Flat, stdcall

.DATA

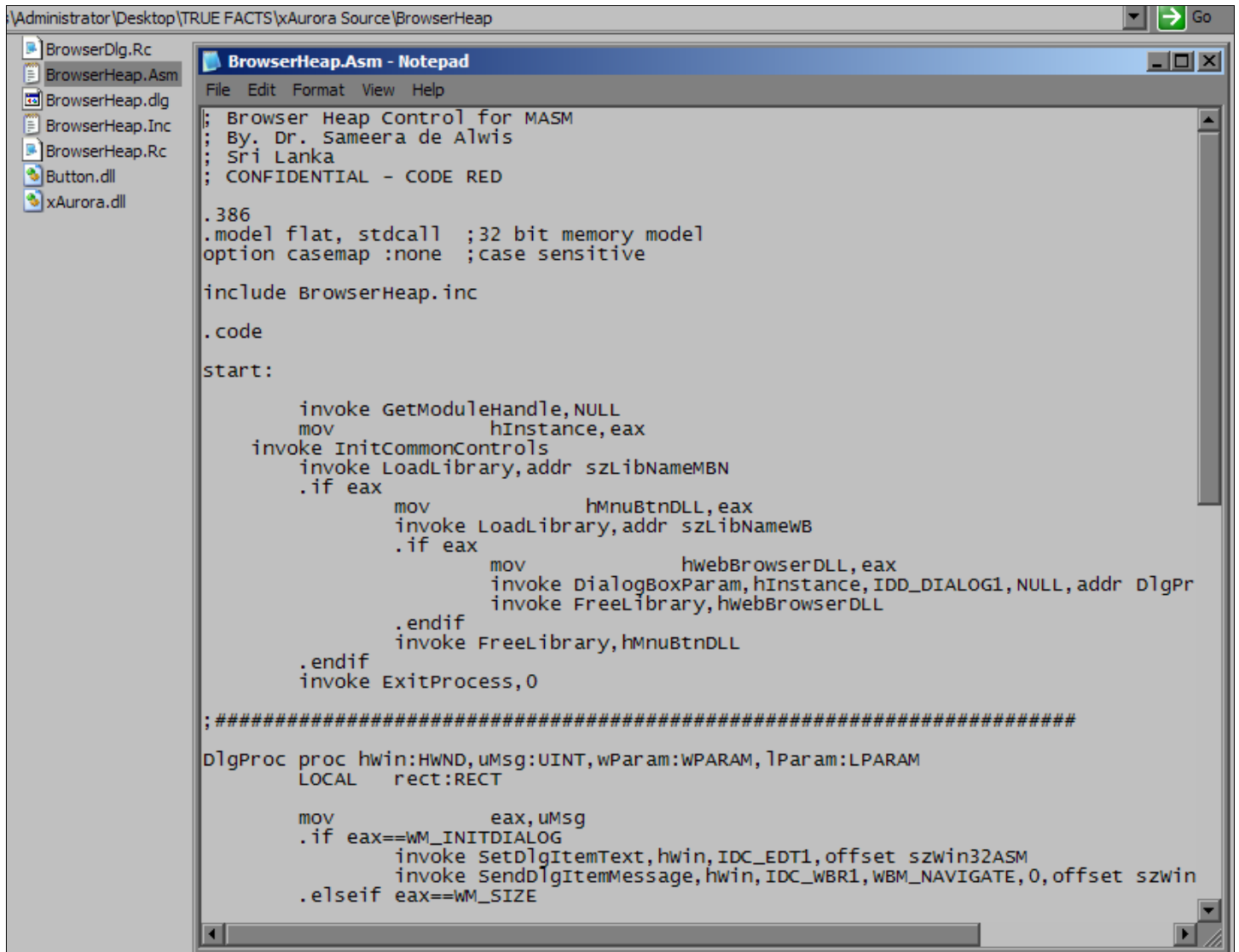
.CODE

START:
nop
RET
END START
:make
if exist *.res del *.res
if exist *.obj del *.obj
if exist *.exe del *.exe
if exist *.rc goto rc
for %%f in (*.bat) do \masm32\bin\ml /nologo /c /coff /Cp %%f
\masm32\bin\link /nologo /SUBSYSTEM:WINDOWS /LIBPATH:\masm32\lib *.obj
goto exit
:rc
for %%f in (*.bat) do \masm32\bin\ml /nologo /c /coff /Cp %%f
for %%f in (*.rc) do \masm32\bin\rc %%f
\masm32\bin\link /nologo /SUBSYSTEM:WINDOWS /LIBPATH:\masm32\lib *.obj *.res
del *.res
:exit
del *.obj
echo.
pause
cls
```

## 4. Resource Directory Root



## 5. Browser HEAP Control Stack



```
Administrator\Desktop\TRUE FACTS\xAurora Source\BrowserHeap
BrowserDlg.Rc
BrowserHeap.AsM
BrowserHeap.dlg
BrowserHeap.Inc
BrowserHeap.Rc
Button.dll
xAurora.dll

BrowserHeap.AsM - Notepad
File Edit Format View Help

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

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

include BrowserHeap.inc

.code

start:

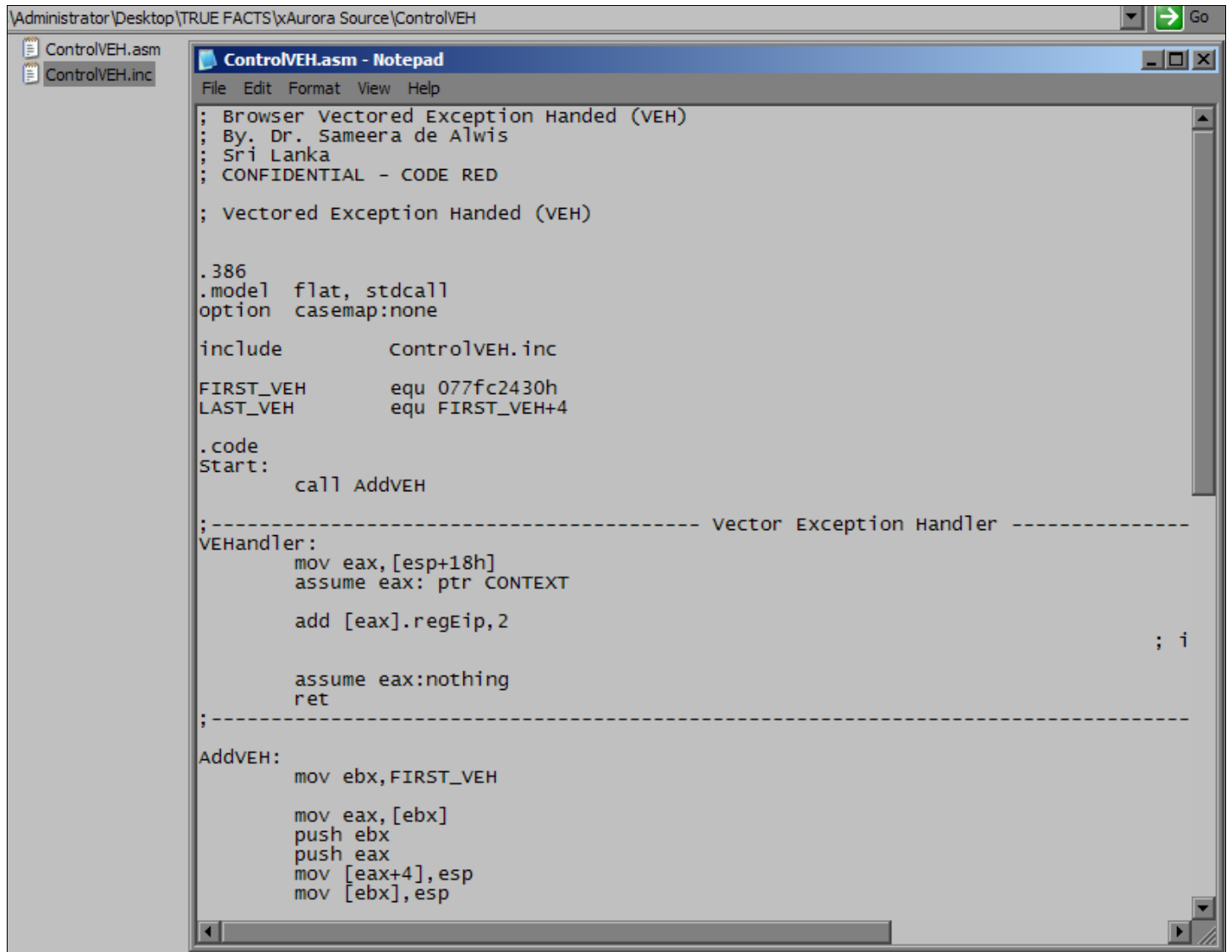
    invoke GetModuleHandle,NULL
    mov     hInstance,eax
    invoke InitCommonControls
    invoke LoadLibrary,addr szLibNameMBN
    .if eax
        mov     hMnuBtnDLL,eax
        invoke LoadLibrary,addr szLibNameWB
        .if eax
            mov     hWebBrowserDLL,eax
            invoke DialogBoxParam,hInstance,IDD_DIALOG1,NULL,addr DlgPr
            invoke FreeLibrary,hWebBrowserDLL
        .endif
        invoke FreeLibrary,hMnuBtnDLL
    .endif
    invoke ExitProcess,0

;#####

DlgProc proc hwin:HWND,uMsg:UINT,wParam:WPARAM,lParam:LPARAM
    LOCAL    rect:RECT

    mov     eax,uMsg
    .if eax==WM_INITDIALOG
        invoke SetDlgItemText,hwin,IDC_EDT1,offset szwin32ASM
        invoke SendDlgItemMessage,hwin,IDC_WBR1,WBM_NAVIGATE,0,offset szwin
    .elseif eax==WM_SIZE
```

## 6. Browser VEH (Vector Exceptions Handler)



```
Administrator\Desktop\TRUE FACTS\Aurora Source\ControlVEH
ControlVEH.asm
ControlVEH.inc

ControlVEH.asm - Notepad
File Edit Format View Help

; Browser Vectored Exception Handed (VEH)
; By. Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

; Vectored Exception Handed (VEH)

.386
.model flat, stdcall
option casemap:none

include ControlVEH.inc

FIRST_VEH equ 077fc2430h
LAST_VEH equ FIRST_VEH+4

.code
Start:
    call AddVEH

;----- Vector Exception Handler -----
VEHandler:
    mov eax,[esp+18h]
    assume eax: ptr CONTEXT

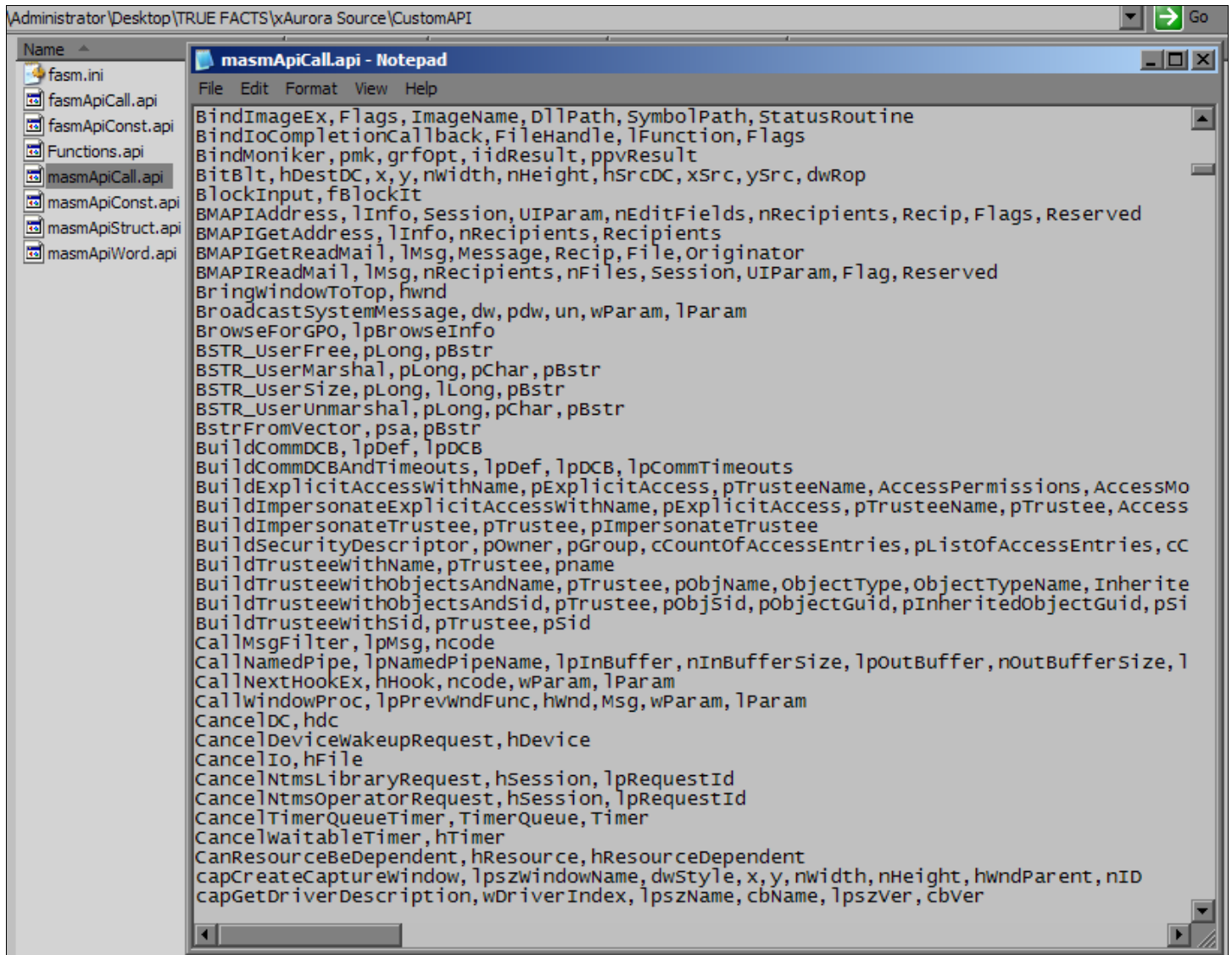
    add [eax].regEip,2
                                     ; i

    assume eax:nothing
    ret
;-----

AddVEH:
    mov ebx,FIRST_VEH

    mov eax,[ebx]
    push ebx
    push eax
    mov [eax+4],esp
    mov [ebx],esp
```

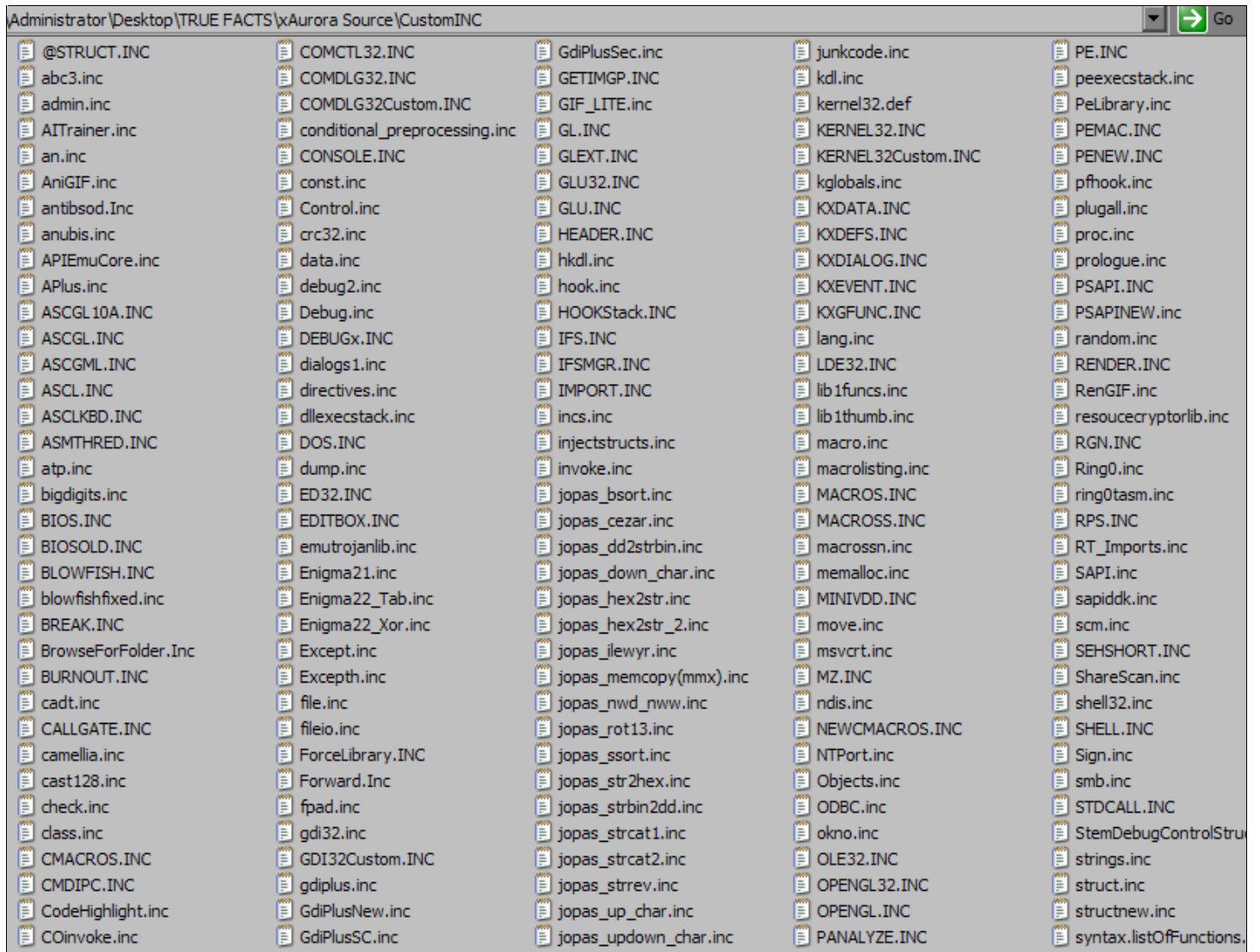
## 7. Custom API for MASM/FASM - Modified & Optimized



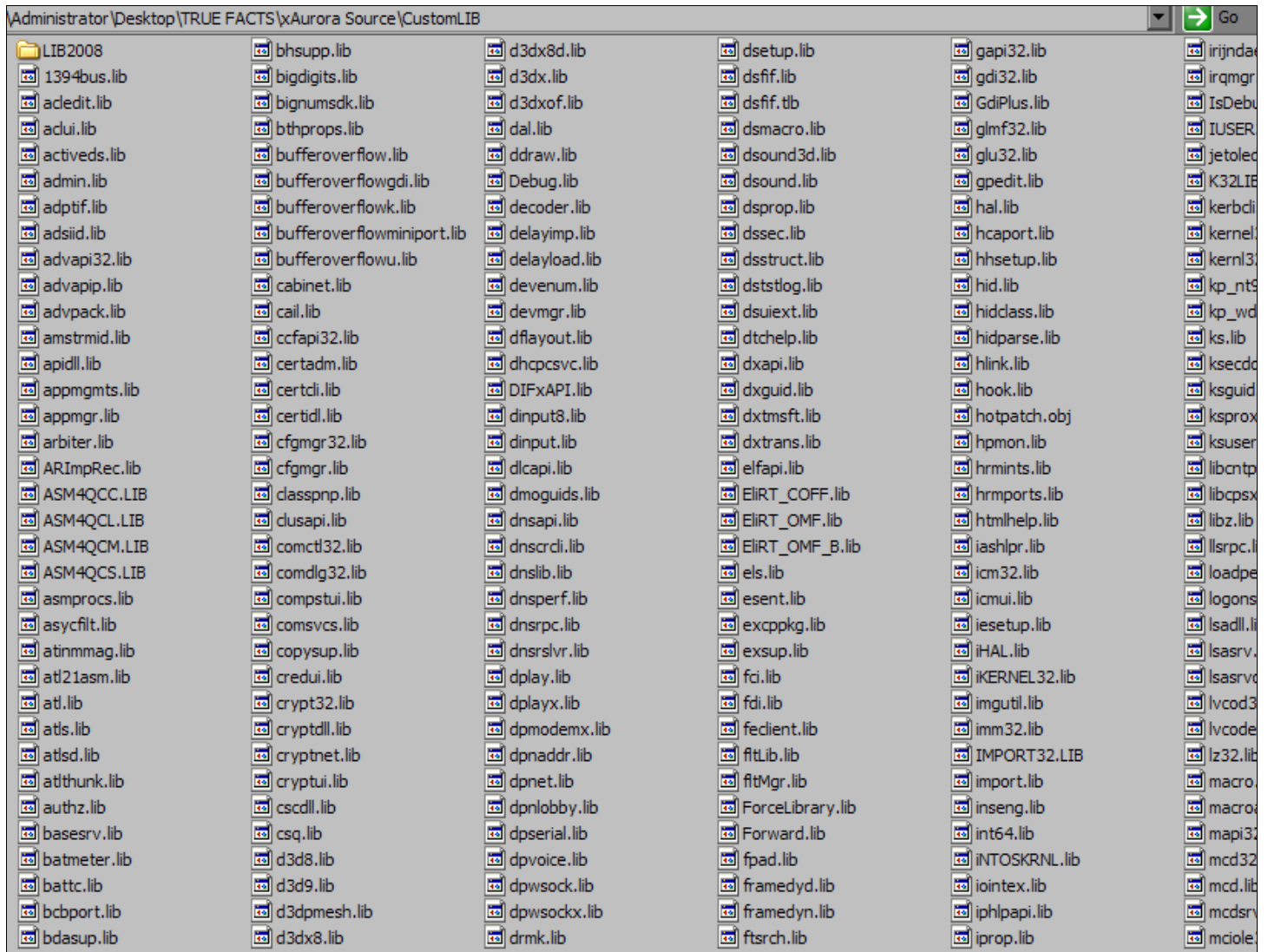
The image shows a Windows Explorer window with the address bar set to 'Administrator\Desktop\TRUE FACTS\Aurora Source\CustomAPI'. The left pane shows a list of files: 'fasm.ini', 'fasmApiCall.api', 'fasmApiConst.api', 'Functions.api', 'masmApiCall.api' (selected), 'masmApiConst.api', 'masmApiStruct.api', and 'masmApiWord.api'. The right pane shows a Notepad window titled 'masmApiCall.api - Notepad' containing a list of API names and their parameters, such as 'BindImageEx, Flags, ImageName, DllPath, SymbolPath, StatusRoutine' and 'BroadcastSystemMessage, dw, pdw, un, wParam, lParam'.

```
File Edit Format View Help
BindImageEx, Flags, ImageName, DllPath, SymbolPath, StatusRoutine
BindIoCompletionCallback, FileHandle, lFunction, Flags
BindMoniker, pmk, grfOpt, iidResult, ppvResult
BitBlt, hDestDC, x, y, nwidth, nHeight, hSrcDC, xSrc, ySrc, dwRop
BlockInput, fBlockIt
BMAPIAddress, lInfo, Session, UIParam, nEditFields, nRecipients, Recip, Flags, Reserved
BMAPIGetAddress, lInfo, nRecipients, Recipients
BMAPIGetReadMail, lMsg, Message, Recip, File, Originator
BMAPIReadMail, lMsg, nRecipients, nFiles, Session, UIParam, Flag, Reserved
BringWindowToTop, hwnd
BroadcastSystemMessage, dw, pdw, un, wParam, lParam
BrowseForGPO, lpBrowseInfo
BSTR_UserFree, pLong, pBstr
BSTR_UserMarshal, pLong, pchar, pBstr
BSTR_UserSize, pLong, lLong, pBstr
BSTR_UserUnmarshal, pLong, pChar, pBstr
BstrFromVector, psa, pBstr
BuildCommDCB, lpDef, lpDCB
BuildCommDCBAndTimeouts, lpDef, lpDCB, lpCommTimeouts
BuildExplicitAccessWithName, pExplicitAccess, pTrusteeName, AccessPermissions, AccessMo
BuildImpersonateExplicitAccessWithName, pExplicitAccess, pTrusteeName, pTrustee, Access
BuildImpersonateTrustee, pTrustee, pImpersonateTrustee
BuildSecurityDescriptor, pOwner, pGroup, cCountOfAccessEntries, pListOfAccessEntries, cC
BuildTrusteeWithName, pTrustee, pname
BuildTrusteeWithObjectsAndName, pTrustee, pObjName, ObjectType, ObjectTypeName, Inherite
BuildTrusteeWithObjectsAndSid, pTrustee, pObjSid, pObjGuid, pInheritedObjGuid, psi
BuildTrusteeWithSid, pTrustee, pSid
CallMsgFilter, lpMsg, ncode
CallNamedPipe, lpNamedPipeName, lpInBuffer, nInBufferSize, lpOutBuffer, nOutBufferSize, l
CallNextHookEx, hHook, ncode, wParam, lParam
CallWindowProc, lpPrevWndFunc, hwnd, Msg, wParam, lParam
CancelDC, hdc
CancelDeviceWakeUpRequest, hDevice
CancelIo, hFile
CancelNtmsLibraryRequest, hSession, lpRequestId
CancelNtmsOperatorRequest, hSession, lpRequestId
CancelTimerQueueTimer, TimerQueue, Timer
CancelWaitableTimer, hTimer
CanResourceBeDependent, hResource, hResourceDependent
capCreateCaptureWindow, lpszWindowName, dwStyle, x, y, nwidth, nHeight, hwndParent, nID
capGetDriverDescription, wDriverIndex, lpszName, cbName, lpszVer, cbVer
```

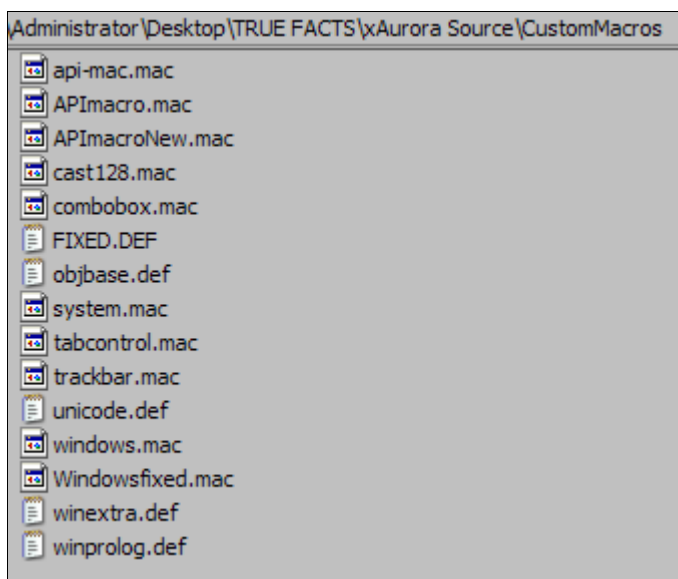
## 8. Custom HEADER Files Root for MASM



## 9. Custom LIBRARY Files Root for MASM



## 9. Custom MACRO Files Root for MASM



## 10. Wrap DLL Advanced Procedure

```
Administrator\Desktop\TRUE FACTS\Aurora Source\DLLCodeWrappingEmbedded
BrowserWrapDLLAdvProcForEmbeddedDLLStacks.asm
DLLWrap.asm
DLLWrap.def

; Browser wrap DLL Advanced Procedure for Embedded DLL Stacks
; By. Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

; DEBUG_BUILD = TRUE
; DEBUG_BUILD = FALSE

MAX_APIS =1000h

.586
.model flat, STDCALL

extrn strlenA : proc
extrn GetCommandLineA : proc
extrn ExitProcess : proc
extrn GetLastError : proc
extrn GetModuleHandleA : proc
extrn GetProcAddress : proc
extrn LoadLibraryA : proc
extrn CreateFileA : proc
extrn CreateFileMappingA : proc
extrn MapViewOfFile : proc
extrn MapViewOfFileEx : proc
extrn UnmapViewOfFile : proc
extrn CloseHandle : proc
extrn GetFullPathNameW : proc
extrn GlobalAlloc : proc
extrn GlobalFree : proc
extrn lstrcatA : proc

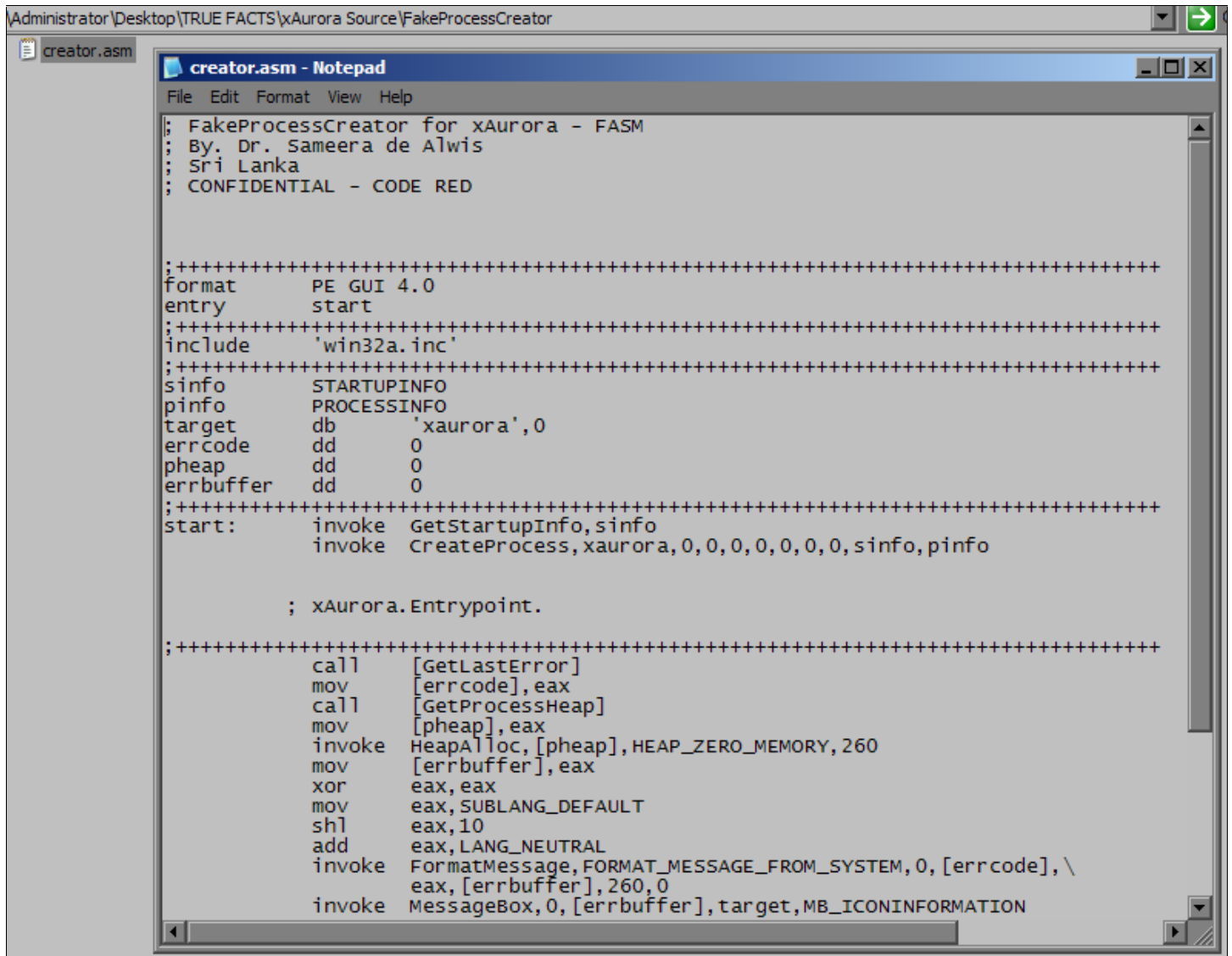
include incs\mz.inc
include incs\pe.inc
include incs\win32api.inc

IMAGE_SIZEOF_NT_HEADERS EQU SIZE IMAGE_NT_HEADERS

.data

APINAME_PREFIX equ 'wrapped_'
```

## 11. Browser Protection – Fake Process Creation Stub



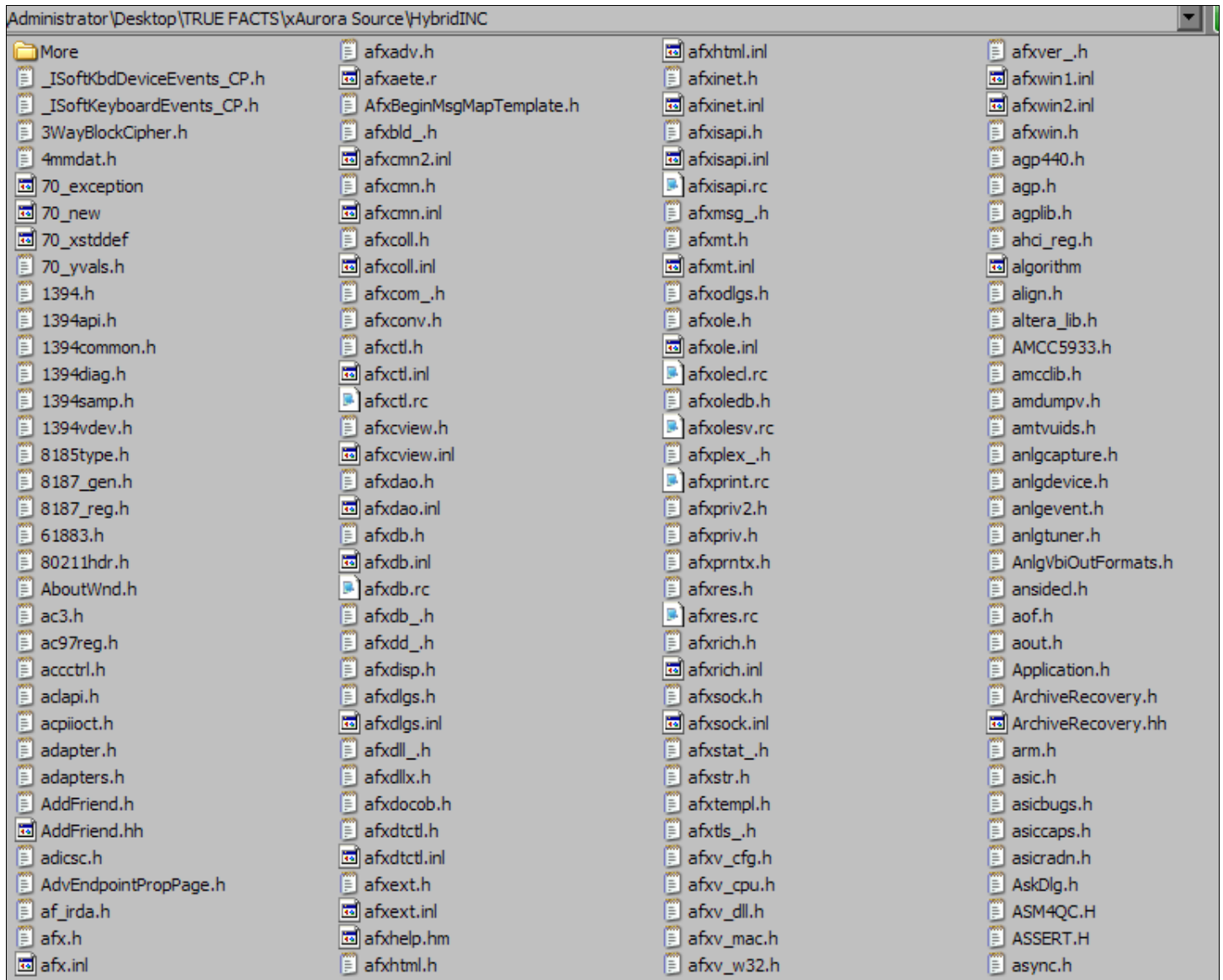
```
Administrator\Desktop\TRUE FACTS\xAurora Source\FakeProcessCreator
creator.asm
creator.asm - Notepad
File Edit Format View Help
; FakeProcessCreator for xAurora - FASM
; By. Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

;+++++
format      PE GUI 4.0
entry       start
;+++++
include     'win32a.inc'
;+++++
sinfo       STARTUPINFO
pinfo       PROCESSINFO
target      db      'xaurora',0
errcode     dd      0
pheap       dd      0
errbuffer   dd      0
;+++++
start:      invoke  GetStartupInfo, sinfo
             invoke  CreateProcess, xaurora, 0, 0, 0, 0, 0, 0, 0, sinfo, pinfo

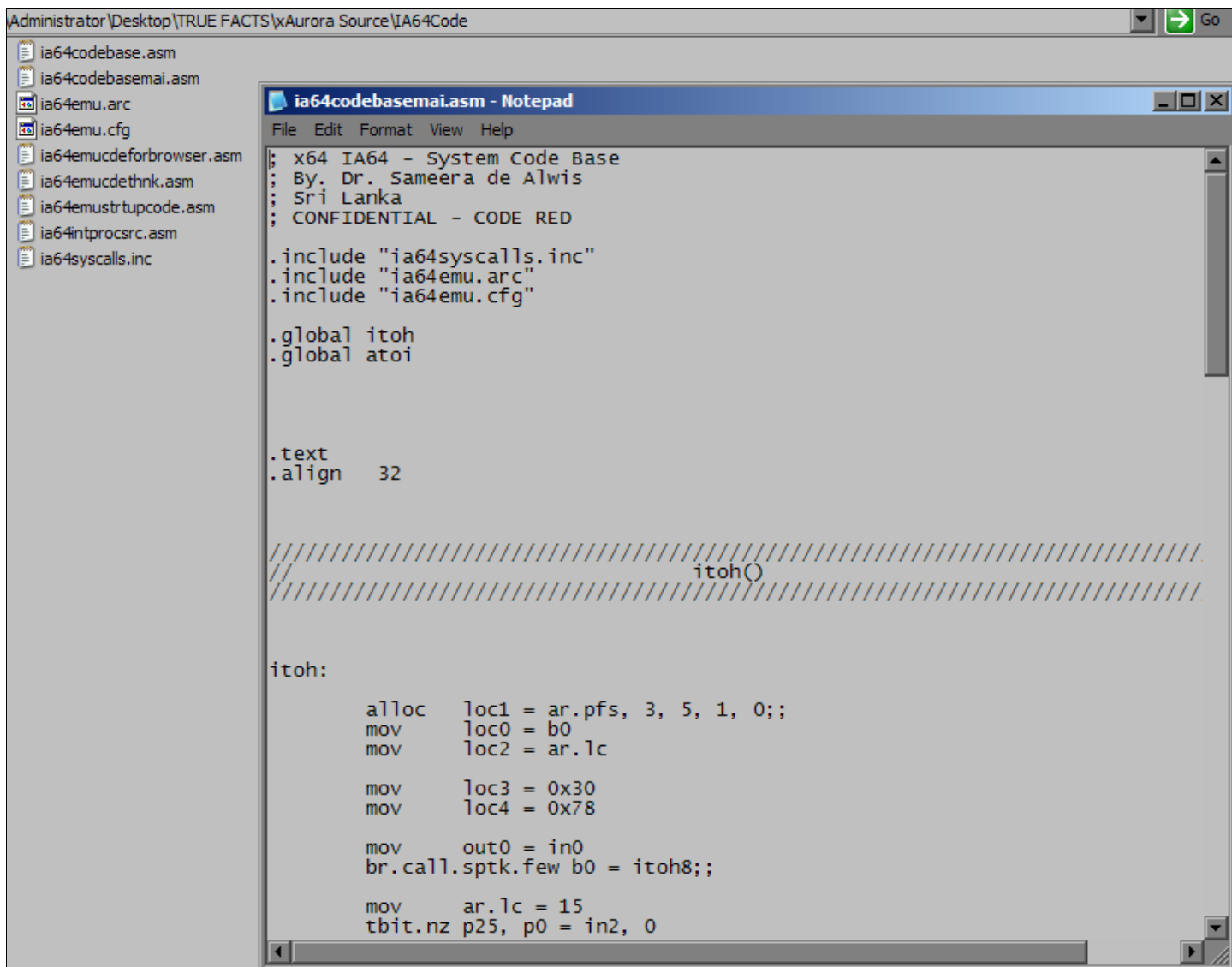
             ; xAurora.Entrypoint.

;+++++
             call    [GetLastError]
             mov     [errcode], eax
             call    [GetProcessHeap]
             mov     [pheap], eax
             invoke  HeapAlloc, [pheap], HEAP_ZERO_MEMORY, 260
             mov     [errbuffer], eax
             xor     eax, eax
             mov     eax, SUBLANG_DEFAULT
             shl     eax, 10
             add     eax, LANG_NEUTRAL
             invoke  FormatMessage, FORMAT_MESSAGE_FROM_SYSTEM, 0, [errcode], \
             eax, [errbuffer], 260, 0
             invoke  MessageBox, 0, [errbuffer], target, MB_ICONINFORMATION
```

## 12. Hybrid - Cross Programming Control Headers POD



### 13. x64 Bit Code for Intel Itanium True 64 Bits & AMD Opteron Code for xAurora



```
Administrator\Desktop\TRUE FACTS\xAurora Source\IA64Code
ia64codebase.asm
ia64codebasemai.asm
ia64emu.arc
ia64emu.cfg
ia64emucdeforbrowser.asm
ia64emucdethnk.asm
ia64emustrtupcode.asm
ia64intprosrc.asm
ia64syscalls.inc

; x64 IA64 - System Code Base
; By. Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

.include "ia64syscalls.inc"
.include "ia64emu.arc"
.include "ia64emu.cfg"

.global itoh
.global atoi

.text
.align 32

//////////////////////////////////////
//                                     itoh()
//////////////////////////////////////

itoh:

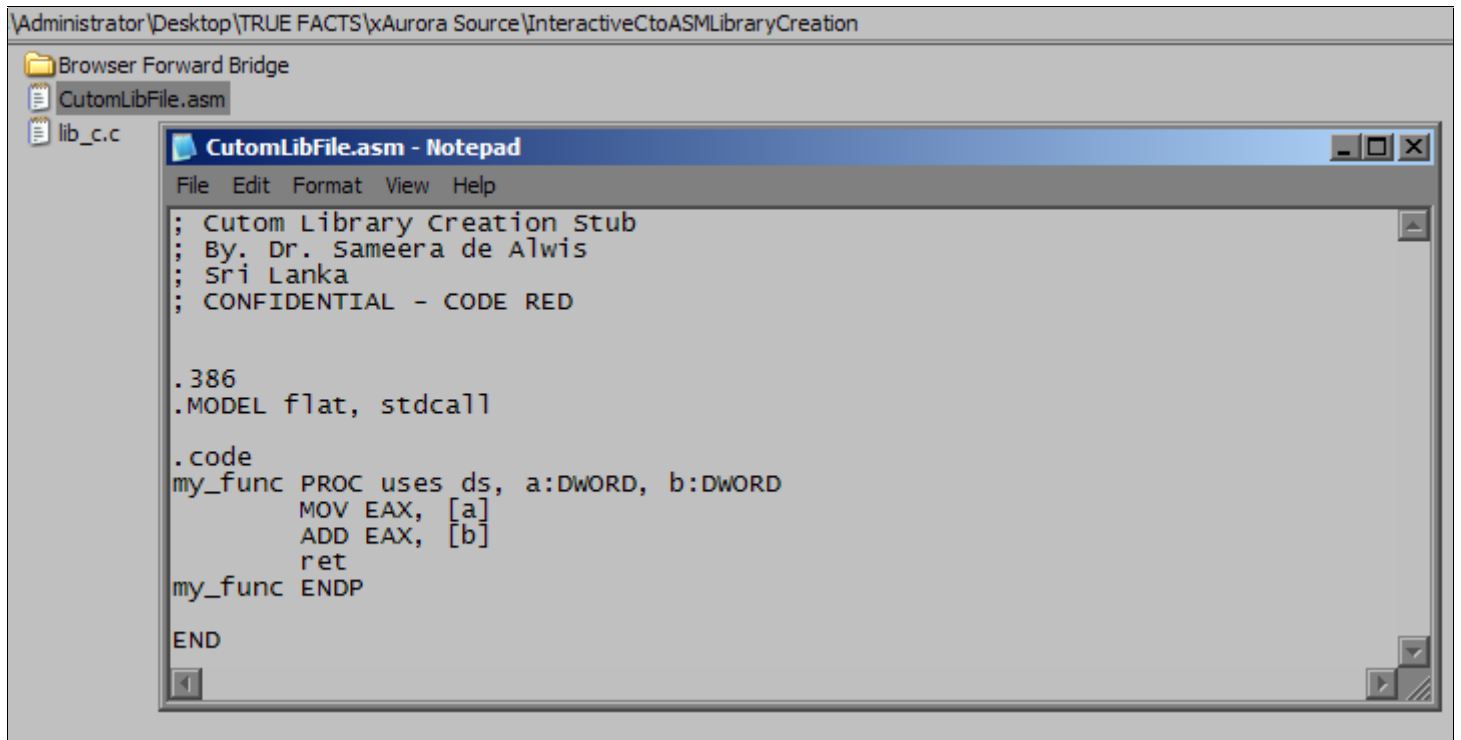
    alloc    loc1 = ar.pfs, 3, 5, 1, 0;;
    mov     loc0 = b0
    mov     loc2 = ar.lc

    mov     loc3 = 0x30
    mov     loc4 = 0x78

    mov     out0 = in0
    br.call.sptk.few b0 = itoh8;;

    mov     ar.lc = 15
    tbit.nz p25, p0 = in2, 0
```

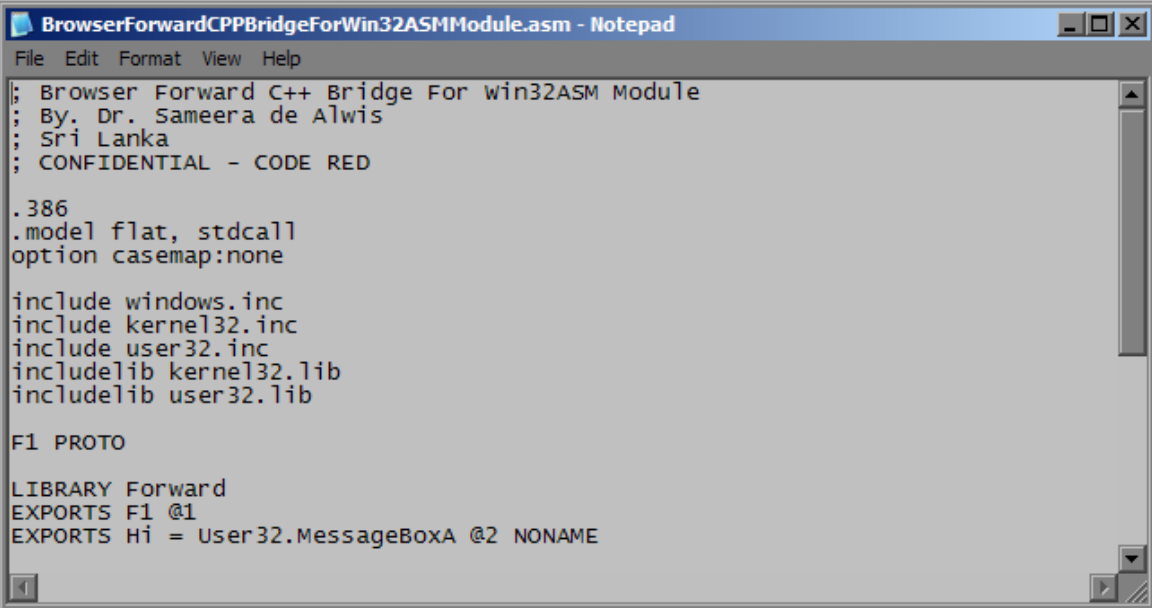
## 14. Interactive C++ to Win32 Assembly Language Cross Library



The image shows a Notepad window titled "CutomLibFile.asm - Notepad" with a menu bar (File, Edit, Format, View, Help). The window contains the following assembly code:

```
; Cutom Library Creation Stub  
; By. Dr. Sameera de Alwis  
; Sri Lanka  
; CONFIDENTIAL - CODE RED  
  
.386  
.MODEL flat, stdcall  
  
.code  
my_func PROC uses ds, a:DWORD, b:DWORD  
    MOV EAX, [a]  
    ADD EAX, [b]  
    ret  
my_func ENDP  
  
END
```

\* Browser Forward Bridging Control Library for C++ 2 Win32 Assembly x32 - i386



```
Administrator\Desktop\TRUE FACTS\xAurora Source\InteractiveCtoASMLibraryCreation\Browser Forward Bridge
BrowserForwardBridgeMain.cpp
BrowserForwardCPPBridgeForWin32ASModule.asm

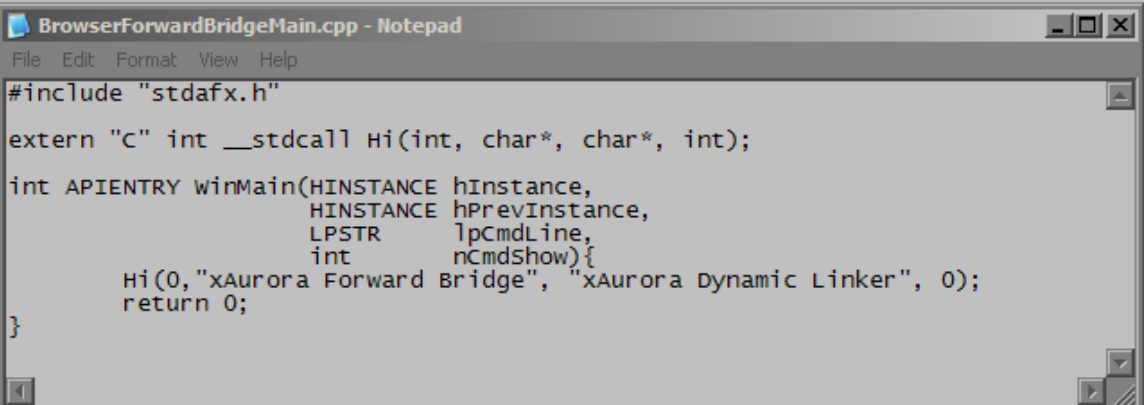
BrowserForwardCPPBridgeForWin32ASModule.asm - Notepad
File Edit Format View Help
; Browser Forward C++ Bridge For win32ASM Module
; By. Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

.386
.model flat, stdcall
option casemap:none

include windows.inc
include kernel32.inc
include user32.inc
includelib kernel32.lib
includelib user32.lib

F1 PROTO

LIBRARY Forward
EXPORTS F1 @1
EXPORTS Hi = User32.MessageBoxA @2 NONAME
```

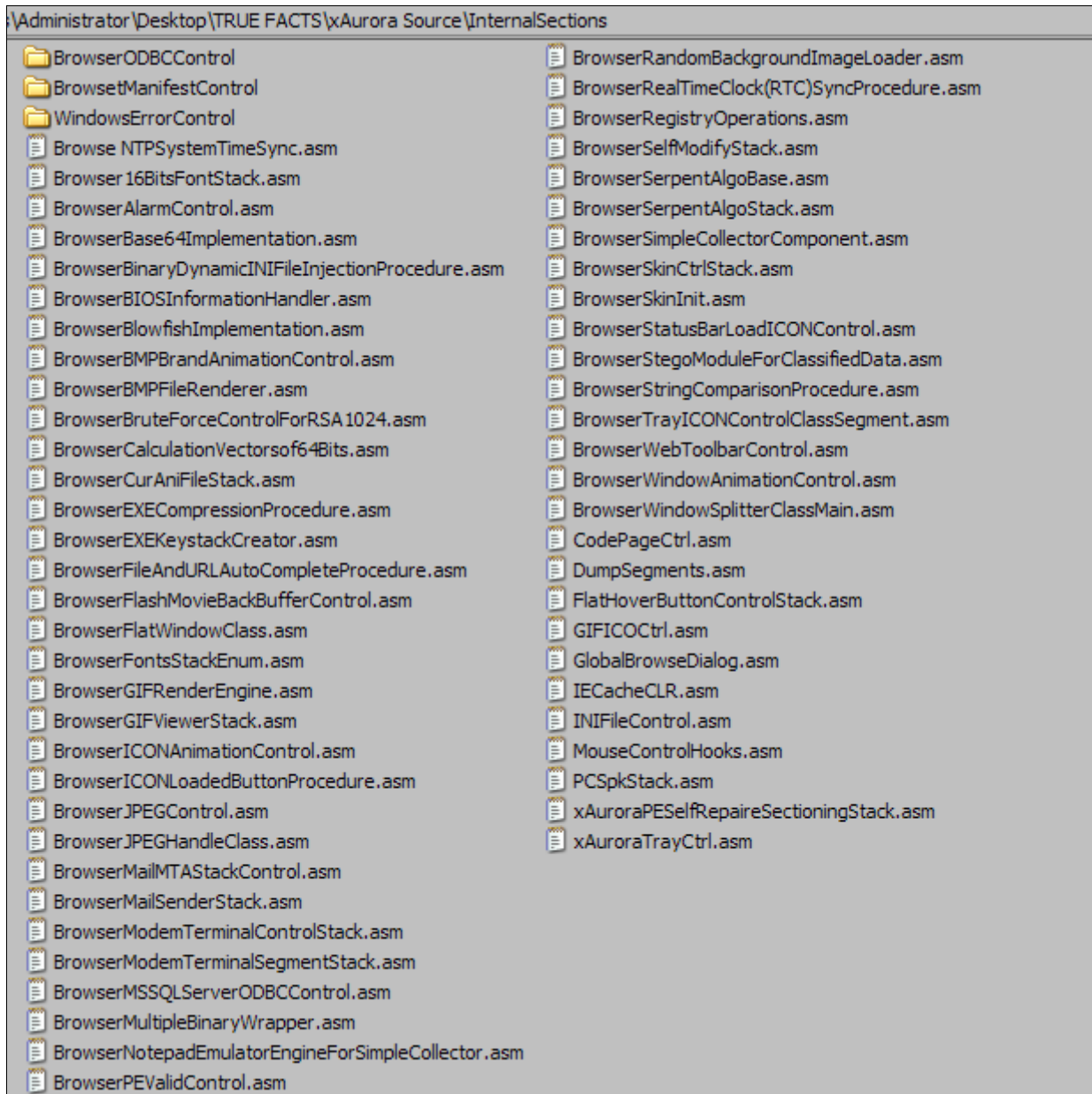


```
BrowserForwardBridgeMain.cpp - Notepad
File Edit Format View Help
#include "stdafx.h"

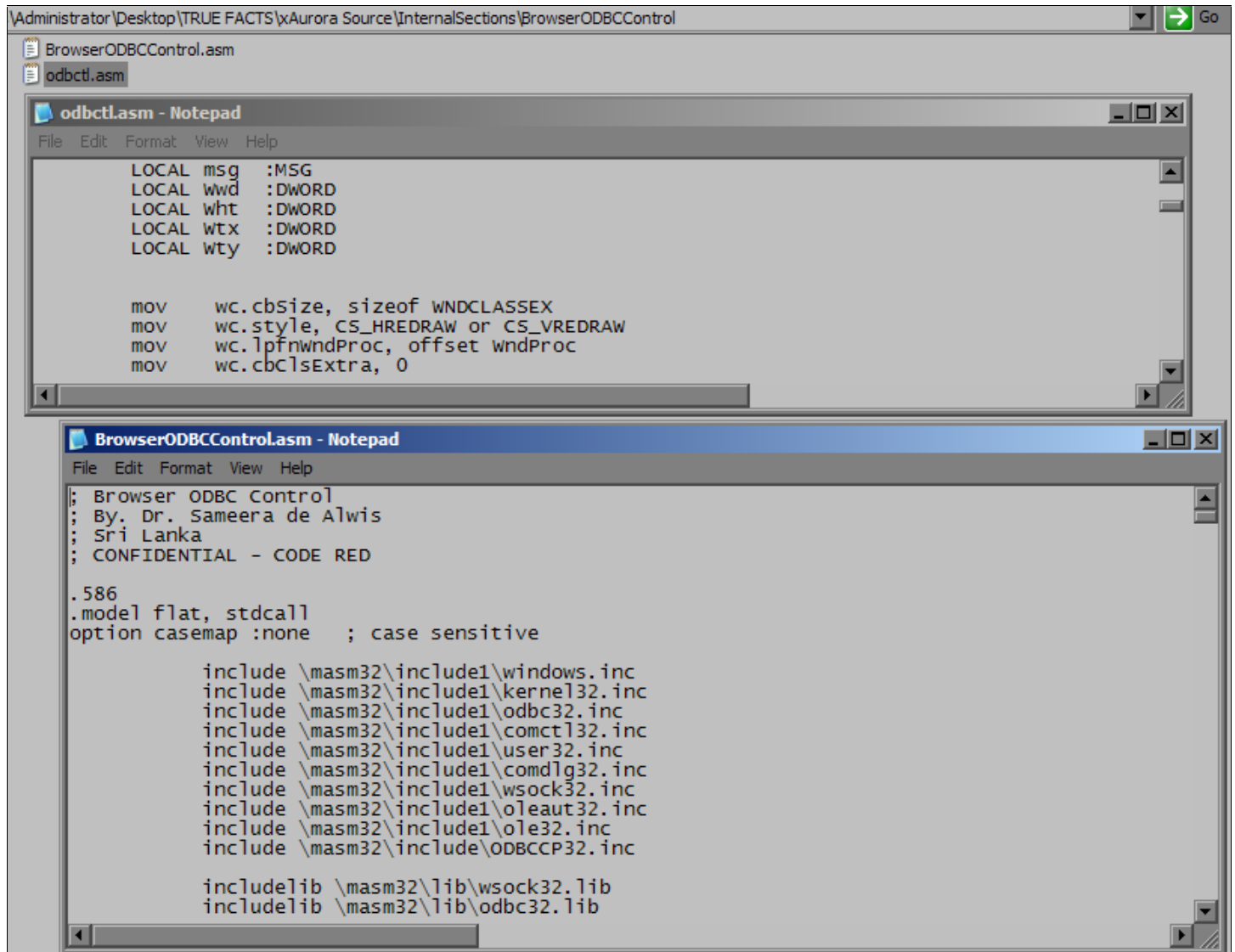
extern "C" int __stdcall Hi(int, char*, char*, int);

int APIENTRY WinMain(HINSTANCE hInstance,
                    HINSTANCE hPrevInstance,
                    LPSTR lpCmdLine,
                    int nCmdShow){
    Hi(0, "xAurora Forward Bridge", "xAurora Dynamic Linker", 0);
    return 0;
}
```

## 15. xAurora Internal Core Stacks & Handler Library Stacks



\* ODBC Control Stack for xAurora



The image shows two Notepad windows. The top window, titled 'odbctl.asm - Notepad', contains assembly code for a control stack. The bottom window, titled 'BrowserODBCControl.asm - Notepad', contains the main assembly code for the control stack, including headers, model settings, and include directives.

```
LOCAL msg :MSG
LOCAL wwd :DWORD
LOCAL wht :DWORD
LOCAL wtx :DWORD
LOCAL wty :DWORD

mov wc.cbSize, sizeof WNDCLASSEX
mov wc.style, CS_HREDRAW or CS_VREDRAW
mov wc.lpfnWndProc, offset wndProc
mov wc.cbClsExtra, 0
```

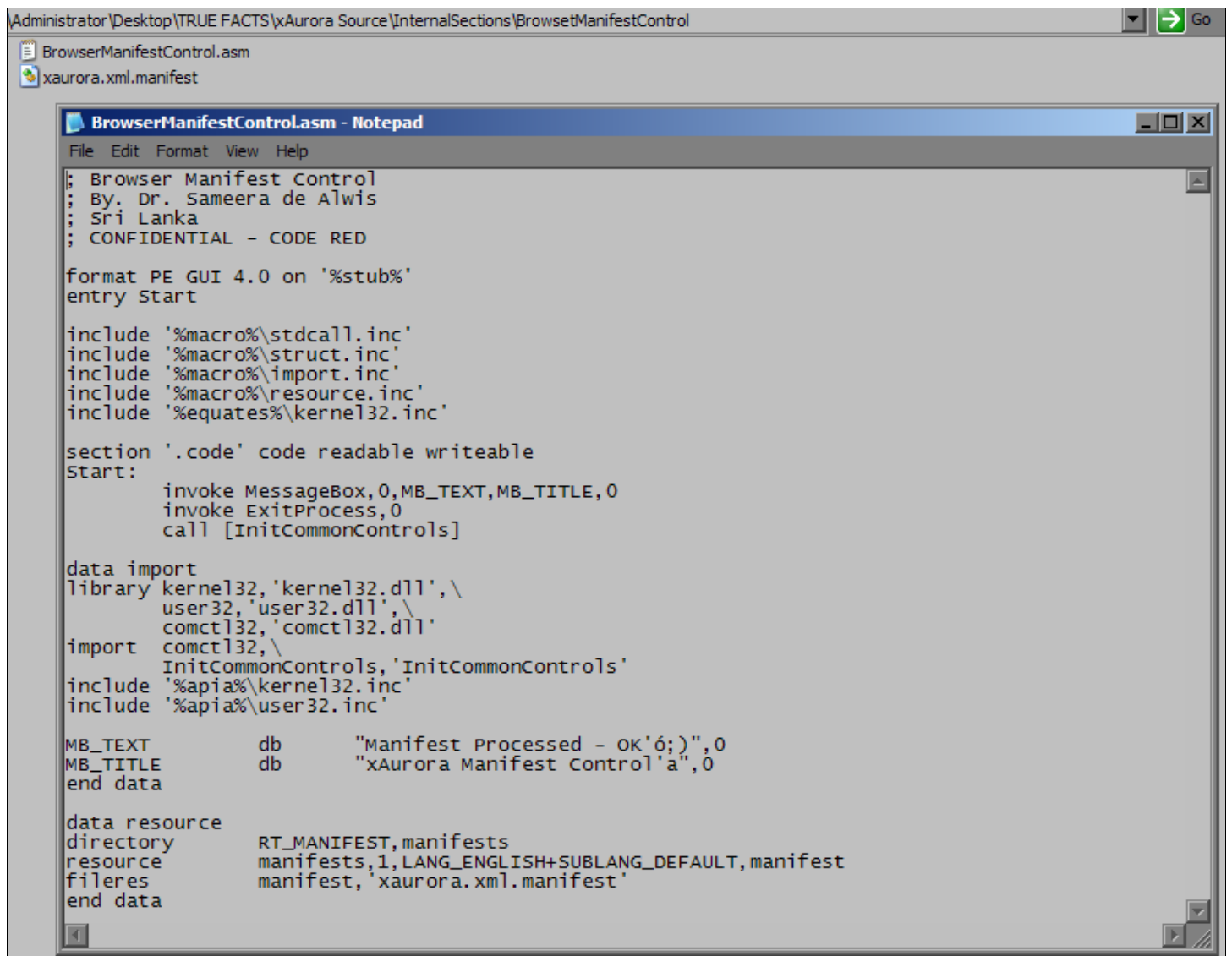
```
; Browser ODBC Control
; By. Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

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

include \masm32\include1\windows.inc
include \masm32\include1\kernel32.inc
include \masm32\include1\odbc32.inc
include \masm32\include1\comctl32.inc
include \masm32\include1\user32.inc
include \masm32\include1\comdlg32.inc
include \masm32\include1\wsock32.inc
include \masm32\include1\oleaut32.inc
include \masm32\include1\ole32.inc
include \masm32\include\ODBCCP32.inc

includelib \masm32\lib\wsock32.lib
includelib \masm32\lib\odbc32.lib
```

## \* Win32 XP/VISTA Browser Manifest Control Stack



```
Administrator\Desktop\TRUE FACTS\xAurora Source\InternalSections\BrowserManifestControl
BrowserManifestControl.asm
xaurora.xml.manifest

BrowserManifestControl.asm - Notepad
File Edit Format View Help

; Browser Manifest Control
; By. Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

format PE GUI 4.0 on '%stub%'
entry Start

include '%macro%\stdcall.inc'
include '%macro%\struct.inc'
include '%macro%\import.inc'
include '%macro%\resource.inc'
include '%equates%\kernel32.inc'

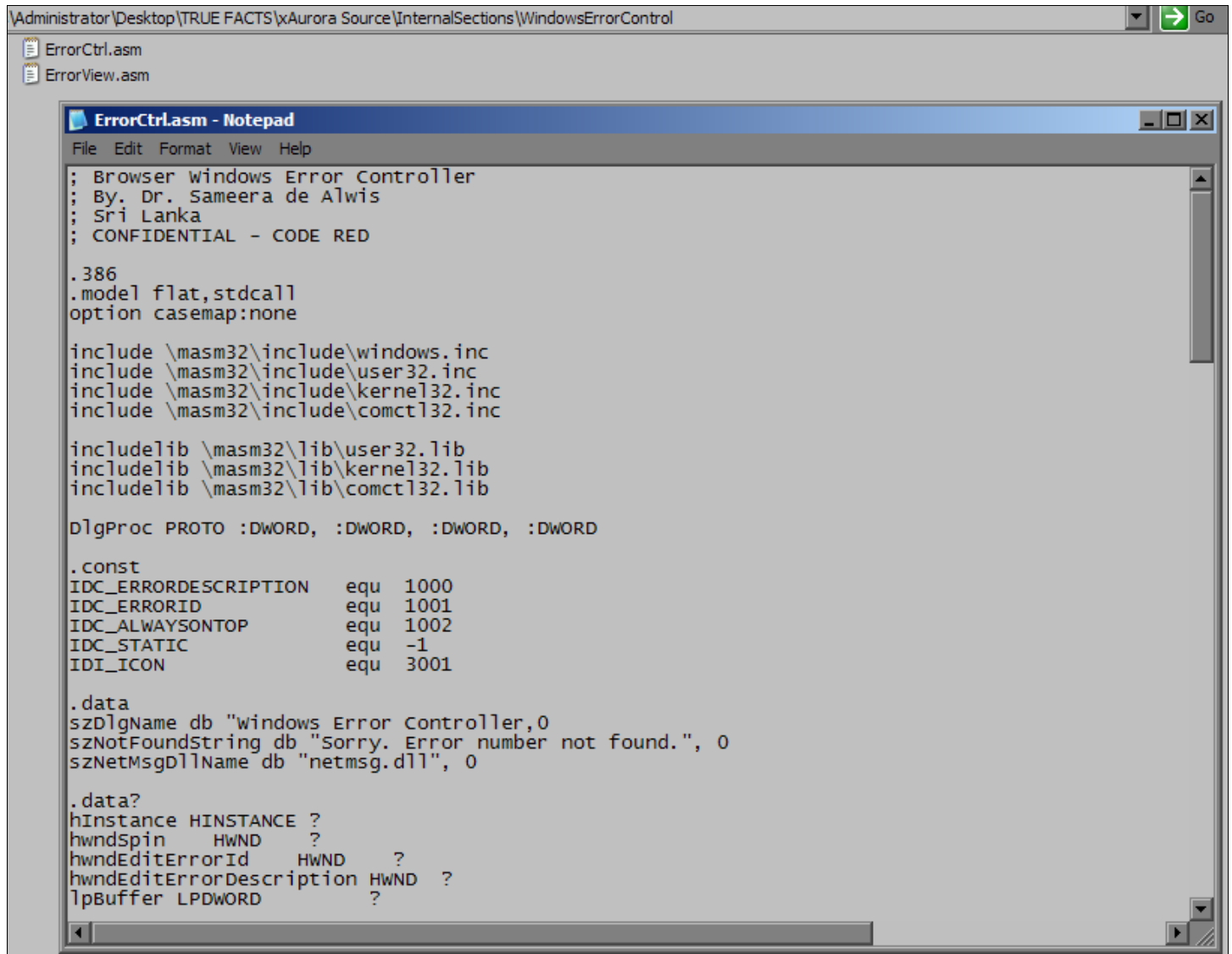
section '.code' code readable writeable
Start:
    invoke MessageBox,0,MB_TEXT,MB_TITLE,0
    invoke ExitProcess,0
    call [InitCommonControls]

data import
library kernel32,'kernel32.dll',\
        user32,'user32.dll',\
        comctl32,'comctl32.dll'
import comctl32,\
        InitCommonControls,'InitCommonControls'
include '%apia%\kernel32.inc'
include '%apia%\user32.inc'

MB_TEXT      db      "Manifest Processed - OK'ó;)",0
MB_TITLE     db      "xAurora Manifest Control'a",0
end data

data resource
directory    RT_MANIFEST,manifests
resource     manifests,1,LANG_ENGLISH+SUBLANG_DEFAULT,manifest
fileres     manifest,'xaurora.xml.manifest'
end data
```

\* xAurora Windows Error Control Library Stack



```
Administrator\Desktop\TRUE FACTS\xAurora Source\InternalSections\WindowsErrorControl
ErrorCtrl.asm
ErrorView.asm

ErrorCtrl.asm - Notepad
File Edit Format View Help

; Browser Windows Error Controller
; 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\comctl32.inc

includelib \masm32\lib\user32.lib
includelib \masm32\lib\kernel32.lib
includelib \masm32\lib\comctl32.lib

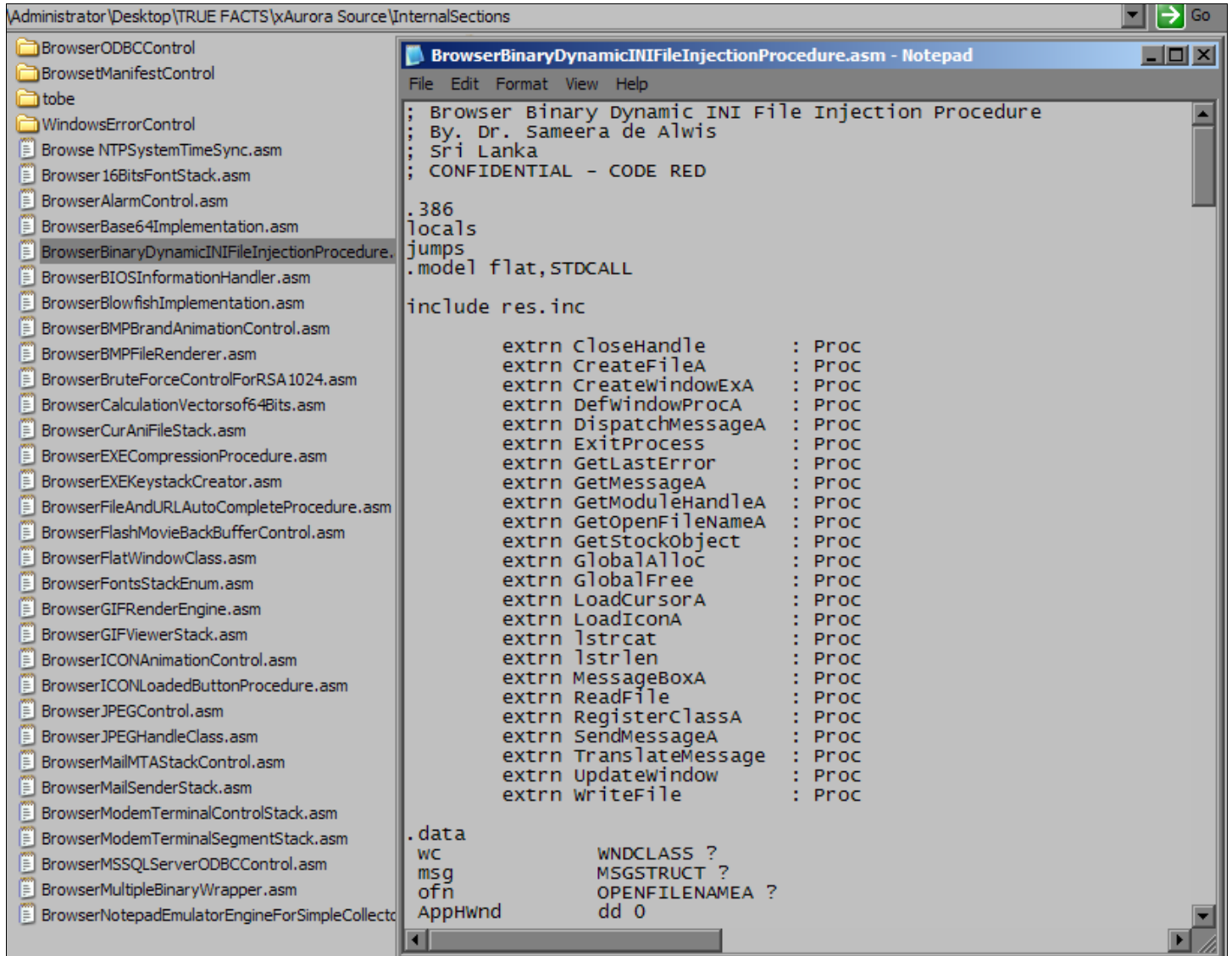
DlgProc PROTO :DWORD, :DWORD, :DWORD, :DWORD

.const
IDC_ERRORDESCRIPTION equ 1000
IDC_ERRORID equ 1001
IDC_ALWAYSONTOP equ 1002
IDC_STATIC equ -1
IDI_ICON equ 3001

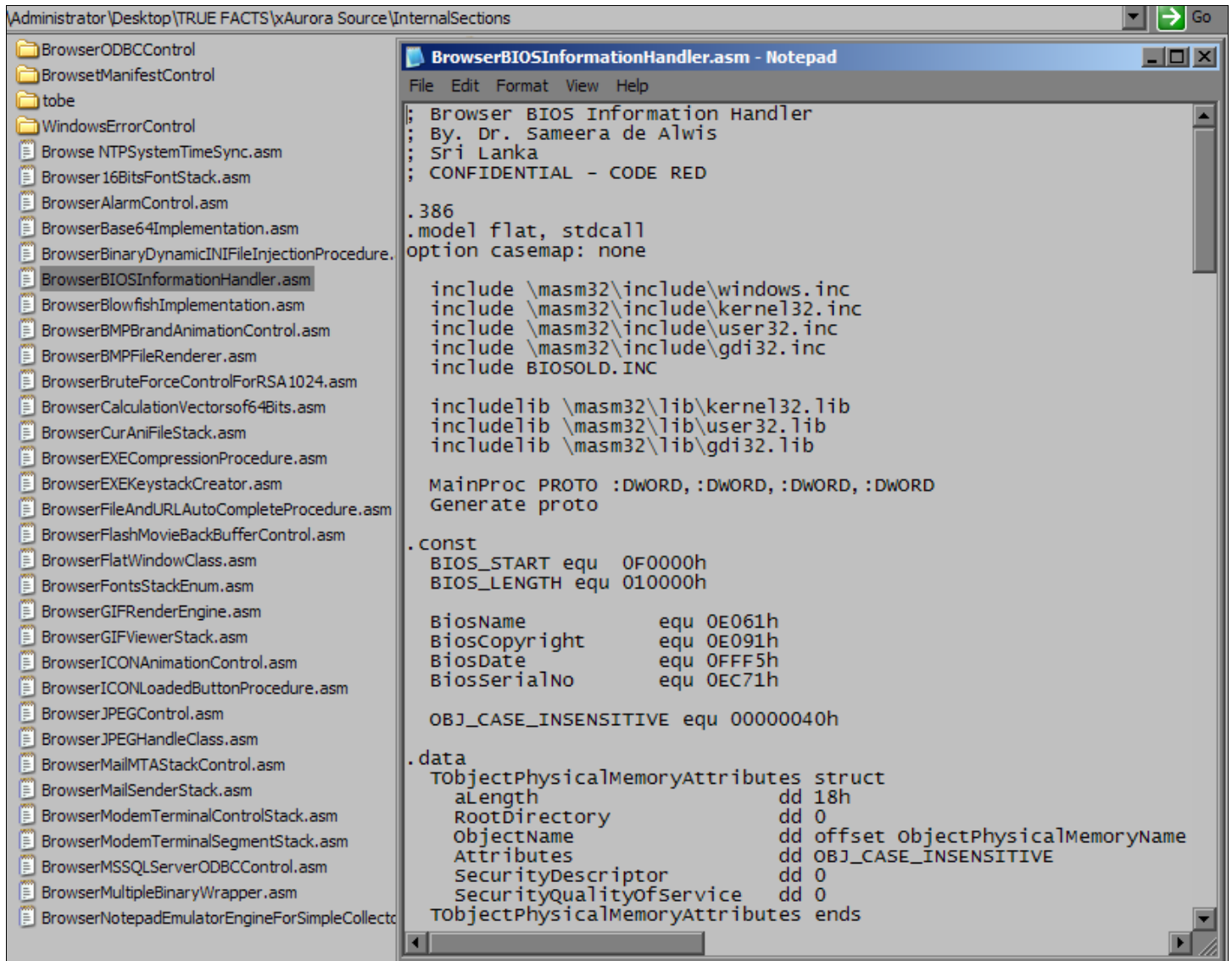
.data
szDlgName db "windows Error Controller,0
szNotFoundString db "Sorry. Error number not found.", 0
szNetMessageName db "netmsg.dll", 0

.data?
hInstance HINSTANCE ?
hwndSpin HWND ?
hwndEditErrorId HWND ?
hwndEditErrorDescription HWND ?
lpBuffer LPDWORD ?
```

\* xAurora Dynamic INI File Injection Procedure



\* xAurora Low Level BIOS Information Handler



The image shows a Windows Explorer window with the address bar set to "Administrator\Desktop\TRUE FACTS\xAurora Source\InternalSections". The left pane displays a tree view of folders and files, including "BrowserODBCControl", "BrowserManifestControl", "tobe", "WindowsErrorControl", and numerous ".asm" files. The file "BrowserBIOSInformationHandler.asm" is selected. The right pane shows a Notepad window titled "BrowserBIOSInformationHandler.asm - Notepad" containing the following assembly code:

```
; Browser BIOS Information Handler
; 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
include \masm32\include\gdi32.inc
include BIOSOLD.INC

includelib \masm32\lib\kernel32.lib
includelib \masm32\lib\user32.lib
includelib \masm32\lib\gdi32.lib

MainProc PROTO :DWORD, :DWORD, :DWORD, :DWORD
Generate proto

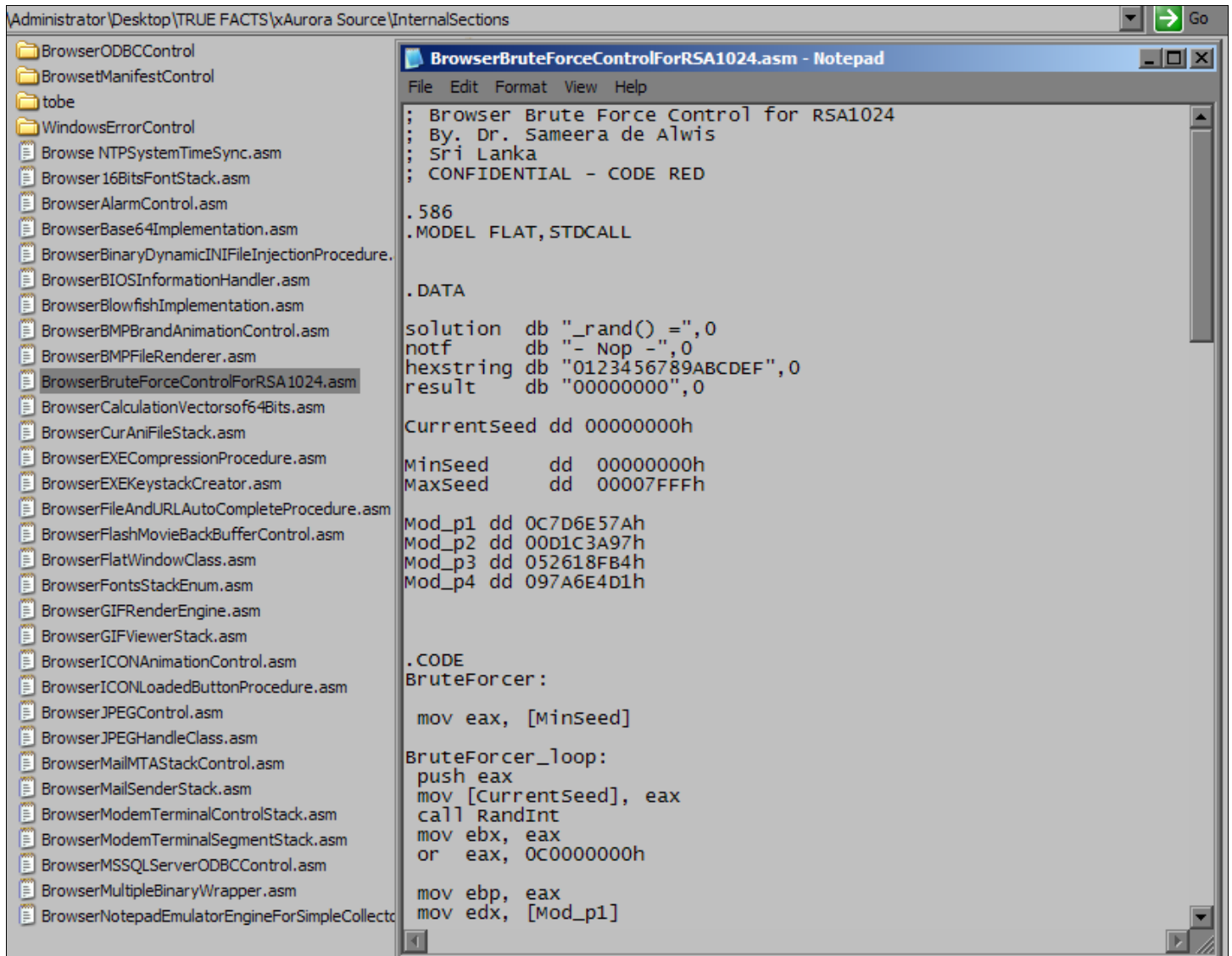
.const
BIOS_START equ 0F0000h
BIOS_LENGTH equ 010000h

BiosName equ 0E061h
BiosCopyright equ 0E091h
BiosDate equ 0FF5h
BiosSerialNo equ 0EC71h

OBJ_CASE_INSENSITIVE equ 00000040h

.data
TobjectPhysicalMemoryAttributes struct
aLength dd 18h
RootDirectory dd 0
ObjectName dd offset objectPhysicalMemoryName
Attributes dd OBJ_CASE_INSENSITIVE
SecurityDescriptor dd 0
SecurityQualityofService dd 0
TobjectPhysicalMemoryAttributes ends
```

## \* Browser Brute Force Control Stack for RSA 1024 Algorithm



The image shows a Windows Explorer window with the following directory structure:

- Administrator\Desktop\TRUE FACTS\Aurora Source\InternalSections
  - BrowserODBCControl
  - BrowsetManifestControl
  - tobe
  - WindowsErrorControl
  - Browse NTPSystemTimeSync.asm
  - Browser16BitsFontStack.asm
  - BrowserAlarmControl.asm
  - BrowserBase64Implementation.asm
  - BrowserBinaryDynamicINIFileInjectionProcedure.
  - BrowserBIOSInformationHandler.asm
  - BrowserBlowfishImplementation.asm
  - BrowserBMPBrandAnimationControl.asm
  - BrowserBMPFileRenderer.asm
  - BrowserBruteForceControlForRSA1024.asm**
  - BrowserCalculationVectorsof64Bits.asm
  - BrowserCurAniFileStack.asm
  - BrowserEXECompressionProcedure.asm
  - BrowserEXEKeystackCreator.asm
  - BrowserFileAndURLAutoCompleteProcedure.asm
  - BrowserFlashMovieBackBufferControl.asm
  - BrowserFlatWindowClass.asm
  - BrowserFontsStackEnum.asm
  - BrowserGIFRenderEngine.asm
  - BrowserGIFViewerStack.asm
  - BrowserICONAnimationControl.asm
  - BrowserICONLoadedButtonProcedure.asm
  - BrowserJPEGControl.asm
  - BrowserJPEGHandleClass.asm
  - BrowserMailMTAStackControl.asm
  - BrowserMailSenderStack.asm
  - BrowserModemTerminalControlStack.asm
  - BrowserModemTerminalSegmentStack.asm
  - BrowserMSSQLServerODBCControl.asm
  - BrowserMultipleBinaryWrapper.asm
  - BrowserNotepadEmulatorEngineForSimpleCollect

The Notepad window displays the assembly code for 'BrowserBruteForceControlForRSA1024.asm':

```
; Browser Brute Force Control for RSA1024
; By. Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

.586
.MODEL FLAT, STDCALL

.DATA

solution db "_rand() =",0
notf     db "- Nop -",0
hexstring db "0123456789ABCDEF",0
result  db "00000000",0

CurrentSeed dd 00000000h

MinSeed     dd 00000000h
MaxSeed     dd 00007FFFh

Mod_p1 dd 0C7D6E57Ah
Mod_p2 dd 00D1C3A97h
Mod_p3 dd 052618FB4h
Mod_p4 dd 097A6E4D1h

.CODE
BruteForcer:

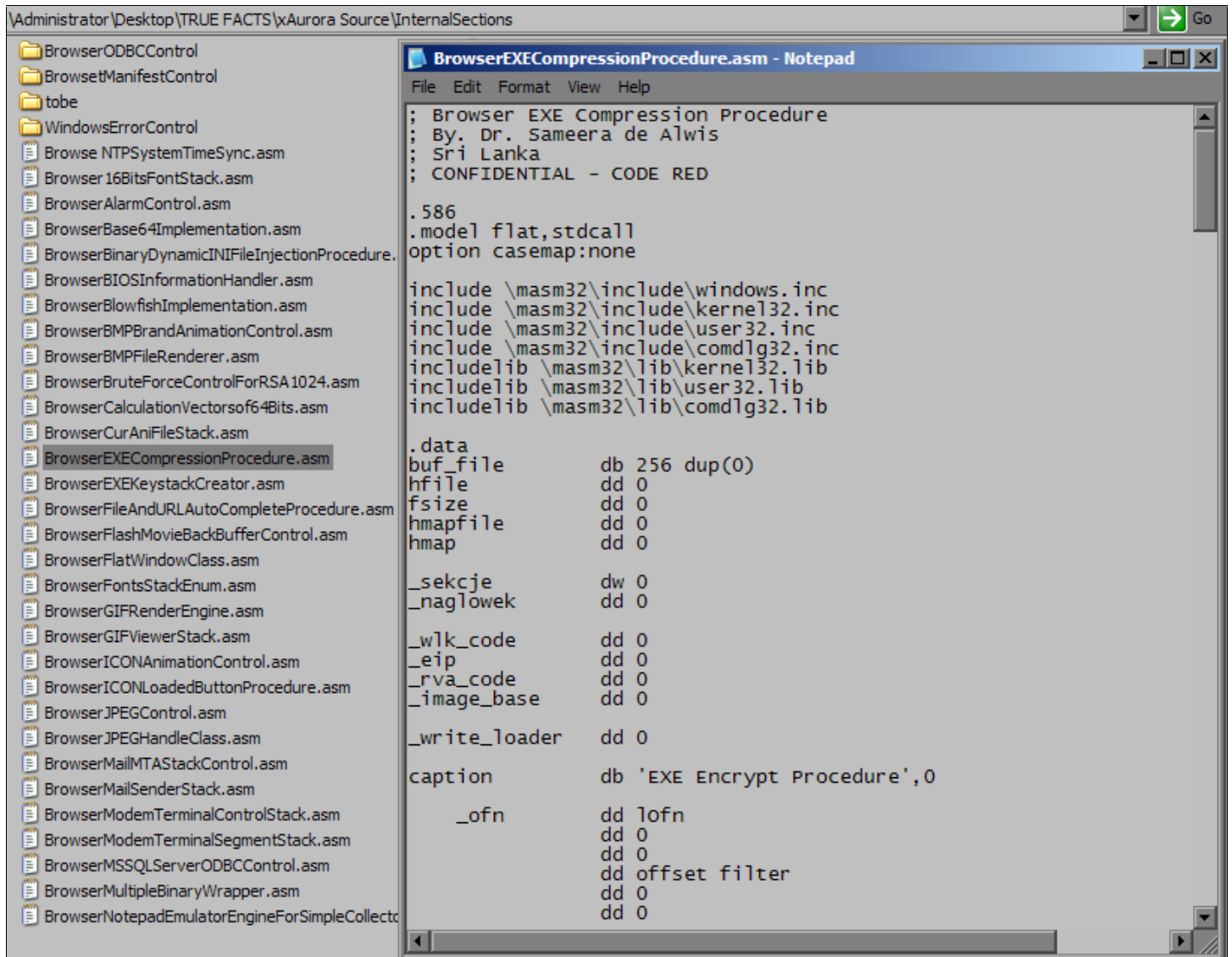
    mov eax, [MinSeed]

BruteForcer_loop:
    push eax
    mov [CurrentSeed], eax
    call RandInt
    mov ebx, eax
    or  eax, 0C0000000h

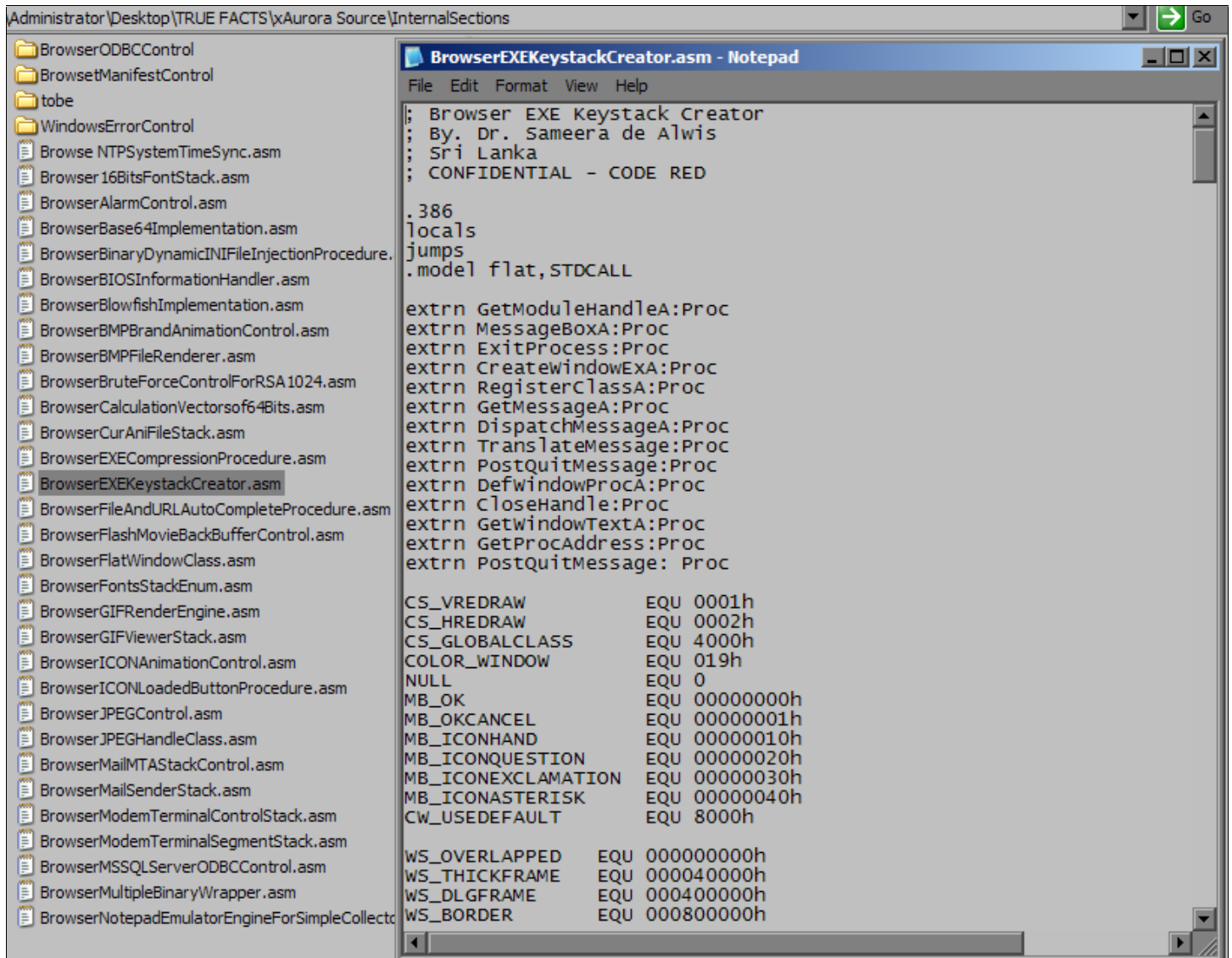
    mov ebp, eax
    mov edx, [Mod_p1]
```



\* xAurora EXE Compression/Encryption Stub



## \* EXE Key Stack Control Vectors



Administrator\Desktop\TRUE FACTS\Aurora Source\InternalSections

BrowserODBCControl  
BrowserManifestControl  
tobe  
WindowsErrorControl  
Browse NTPSystemTimeSync.asm  
Browser16BitsFontStack.asm  
BrowserAlarmControl.asm  
BrowserBase64Implementation.asm  
BrowserBinaryDynamicINIFileInjectionProcedure.  
BrowserBIOSInformationHandler.asm  
BrowserBlowfishImplementation.asm  
BrowserBMPBrandAnimationControl.asm  
BrowserBMPFileRenderer.asm  
BrowserBruteForceControlForRSA1024.asm  
BrowserCalculationVectorsof64Bits.asm  
BrowserCurAniFileStack.asm  
BrowserEXECompressionProcedure.asm  
BrowserEXEKeystackCreator.asm  
BrowserFileAndURLAutoCompleteProcedure.asm  
BrowserFlashMovieBackBufferControl.asm  
BrowserFlatWindowClass.asm  
BrowserFontsStackEnum.asm  
BrowserGIFRenderEngine.asm  
BrowserGIFViewerStack.asm  
BrowserICONAnimationControl.asm  
BrowserICONLoadedButtonProcedure.asm  
BrowserJPEGControl.asm  
BrowserJPEGHandleClass.asm  
BrowserMailMTAStackControl.asm  
BrowserMailSenderStack.asm  
BrowserModemTerminalControlStack.asm  
BrowserModemTerminalSegmentStack.asm  
BrowserMSSQLServerODBCControl.asm  
BrowserMultipleBinaryWrapper.asm  
BrowserNotepadEmulatorEngineForSimpleCollect

BrowserEXEKeystackCreator.asm - Notepad

```
File Edit Format View Help
; Browser EXE Keystack Creator
; By. Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

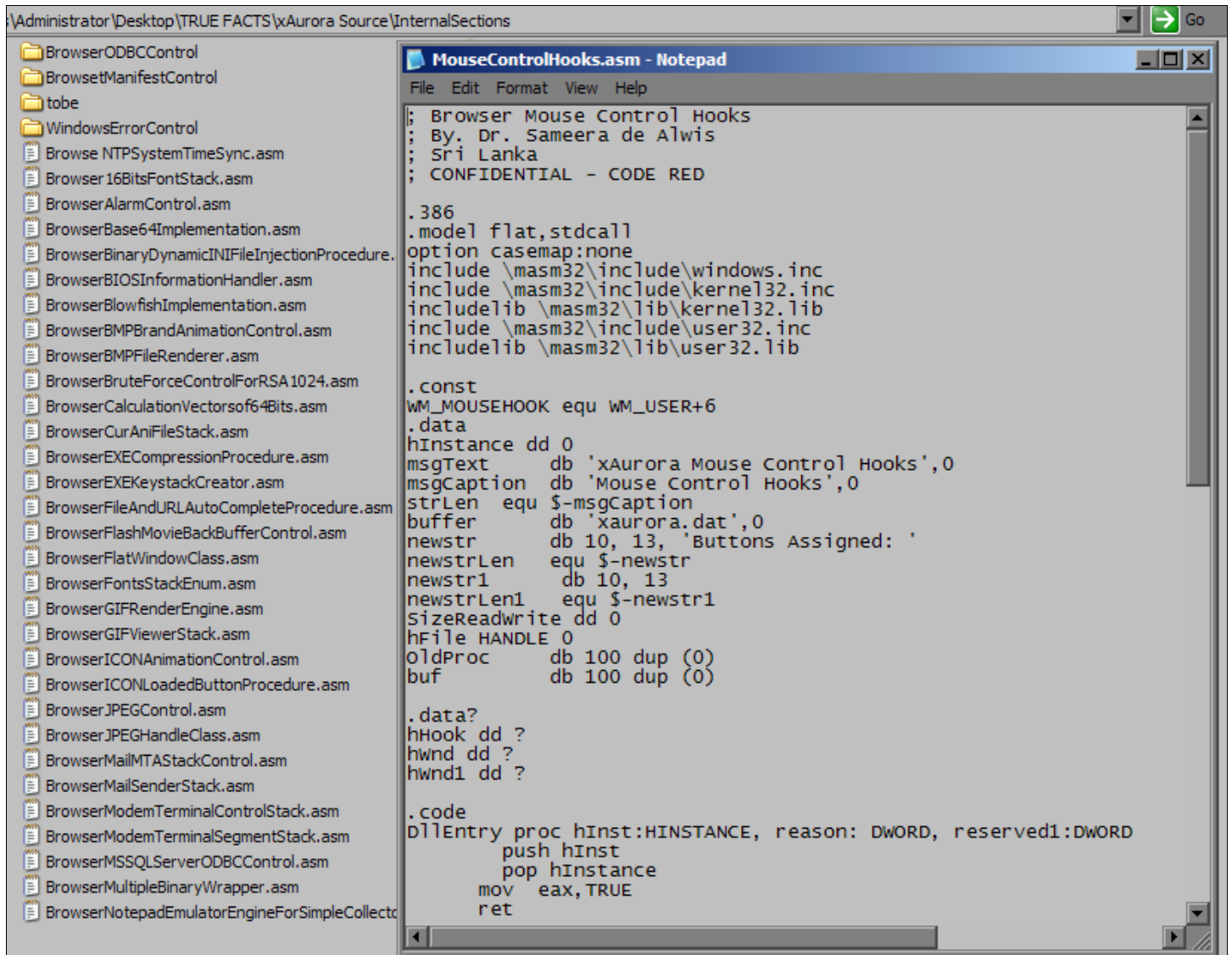
.386
locals
jumps
.model flat, STDCALL

extrn GetModuleHandleA:Proc
extrn MessageBoxA:Proc
extrn ExitProcess:Proc
extrn CreateWindowExA:Proc
extrn RegisterClassA:Proc
extrn GetMessageA:Proc
extrn DispatchMessageA:Proc
extrn TranslateMessage:Proc
extrn PostQuitMessage:Proc
extrn DefWindowProcA:Proc
extrn CloseHandle:Proc
extrn GetWindowTextA:Proc
extrn GetProcAddress:Proc
extrn PostQuitMessage: Proc

CS_VREDRAW EQU 0001h
CS_HREDRAW EQU 0002h
CS_GLOBALCLASS EQU 4000h
COLOR_WINDOW EQU 019h
NULL EQU 0
MB_OK EQU 00000000h
MB_OKCANCEL EQU 00000001h
MB_ICONHAND EQU 00000010h
MB_ICONQUESTION EQU 00000020h
MB_ICONEXCLAMATION EQU 00000030h
MB_ICONASTERISK EQU 00000040h
CW_USEDEFAULT EQU 8000h

WS_OVERLAPPED EQU 00000000h
WS_THICKFRAME EQU 00004000h
WS_DLGFAME EQU 00040000h
WS_BORDER EQU 00080000h
```

## \* Mouse Control Hooks



The image shows a Windows Explorer window with the following directory structure:

- Administrator\Desktop\TRUE FACTS\xAurora Source\InternalSections
  - BrowserODBCControl
  - BrowseManifestControl
  - tobe
  - WindowsErrorControl
  - Browse NTPSystemTimeSync.asm
  - Browser16BitsFontStack.asm
  - BrowserAlarmControl.asm
  - BrowserBase64Implementation.asm
  - BrowserBinaryDynamicINIFileInjectionProcedure.
  - BrowserBIOSInformationHandler.asm
  - BrowserBlowfishImplementation.asm
  - BrowserBMPBrandAnimationControl.asm
  - BrowserBMPFileRenderer.asm
  - BrowserBruteForceControlForRSA1024.asm
  - BrowserCalculationVectorsof64Bits.asm
  - BrowserCurAniFileStack.asm
  - BrowserEXECompressionProcedure.asm
  - BrowserEXEKeystackCreator.asm
  - BrowserFileAndURLAutoCompleteProcedure.asm
  - BrowserFlashMovieBackBufferControl.asm
  - BrowserFlatWindowClass.asm
  - BrowserFontsStackEnum.asm
  - BrowserGIFRenderEngine.asm
  - BrowserGIFViewerStack.asm
  - BrowserICONAnimationControl.asm
  - BrowserICONLoadedButtonProcedure.asm
  - BrowserJPEGControl.asm
  - BrowserJPEGHandleClass.asm
  - BrowserMailMTAStackControl.asm
  - BrowserMailSenderStack.asm
  - BrowserModemTerminalControlStack.asm
  - BrowserModemTerminalSegmentStack.asm
  - BrowserMSSQLServerODBCControl.asm
  - BrowserMultipleBinaryWrapper.asm
  - BrowserNotepadEmulatorEngineForSimpleCollect

The Notepad window, titled "MouseControlHooks.asm - Notepad", contains the following assembly code:

```
; Browser Mouse Control Hooks
; By. Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

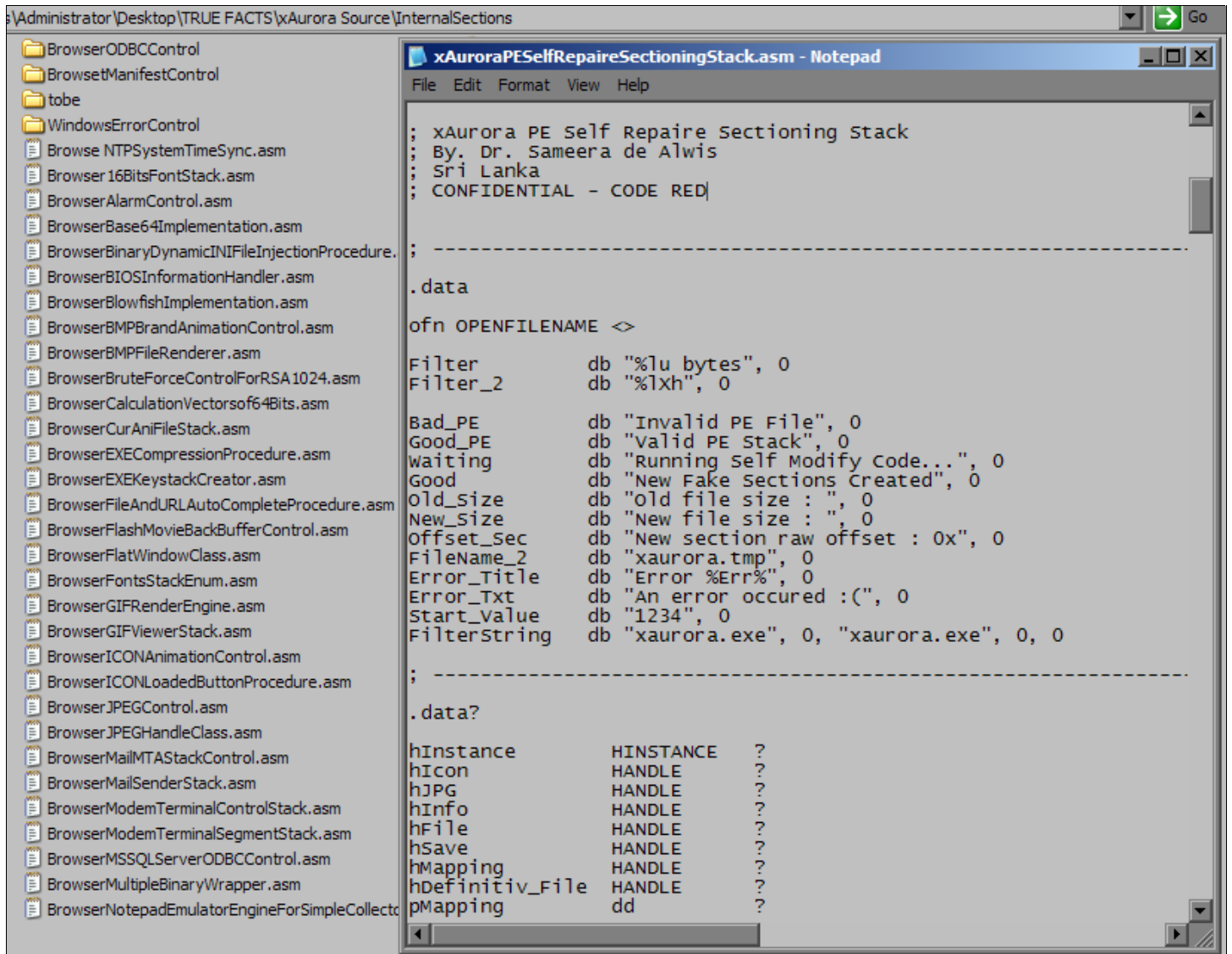
.386
.model flat,stdcall
option casemap:none
include \masm32\include\windows.inc
include \masm32\include\kernel32.inc
includelib \masm32\lib\kernel32.lib
include \masm32\include\user32.inc
includelib \masm32\lib\user32.lib

.const
WM_MOUSEHOOK equ WM_USER+6
.data
hInstance dd 0
msgText db 'xAurora Mouse Control Hooks',0
msgCaption db 'Mouse Control Hooks',0
strLen equ $-msgCaption
buffer db 'xaurora.dat',0
newstr db 10, 13, 'Buttons Assigned: '
newstrLen equ $-newstr
newstr1 db 10, 13
newstrLen1 equ $-newstr1
SizeReadwrite dd 0
hFile HANDLE 0
oldProc db 100 dup (0)
buf db 100 dup (0)

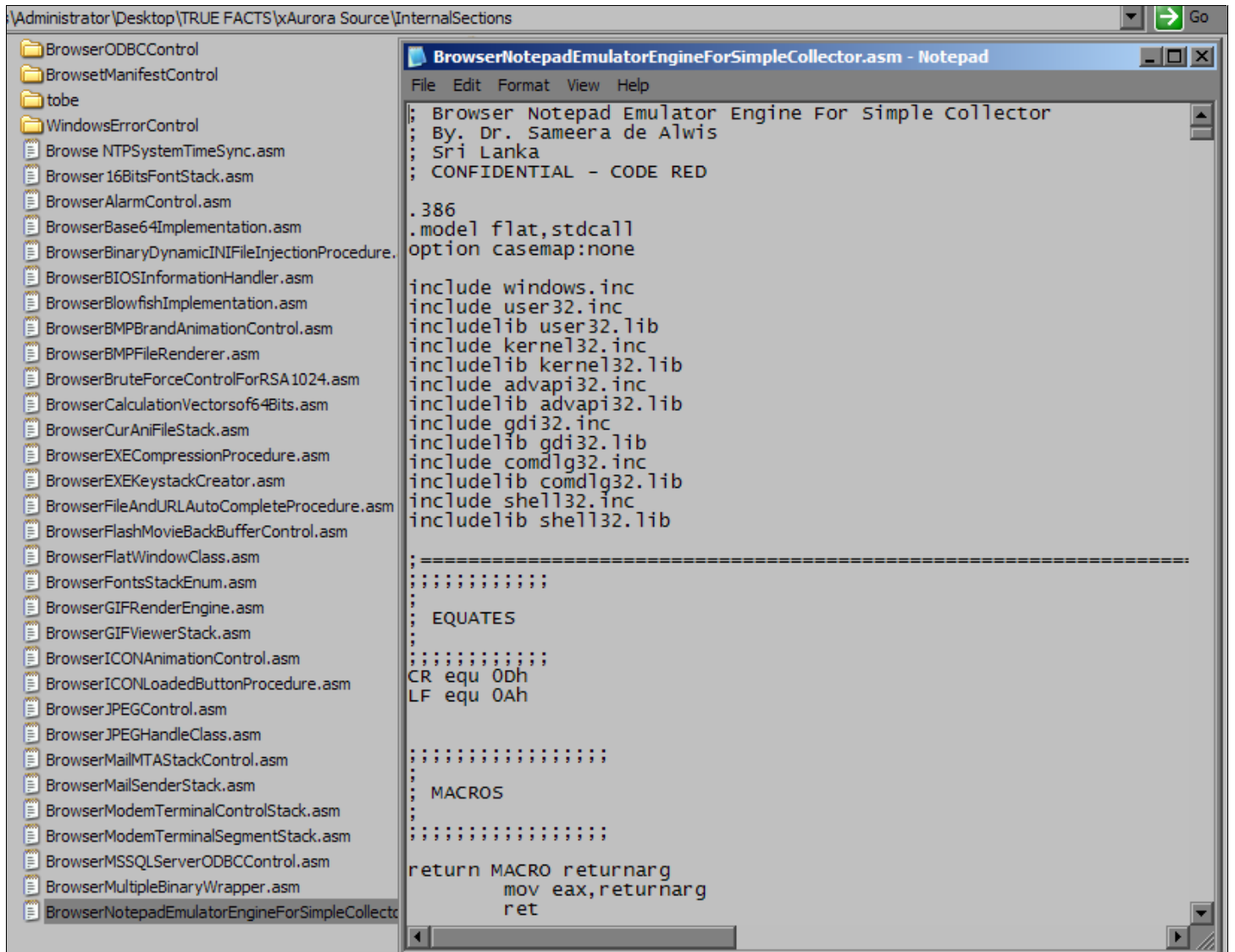
.data?
hHook dd ?
hwnd dd ?
hwnd1 dd ?

.code
DllEntry proc hInst:HINSTANCE, reason: DWORD, reserved1:DWORD
    push hInst
    pop hInstance
    mov eax,TRUE
    ret
```

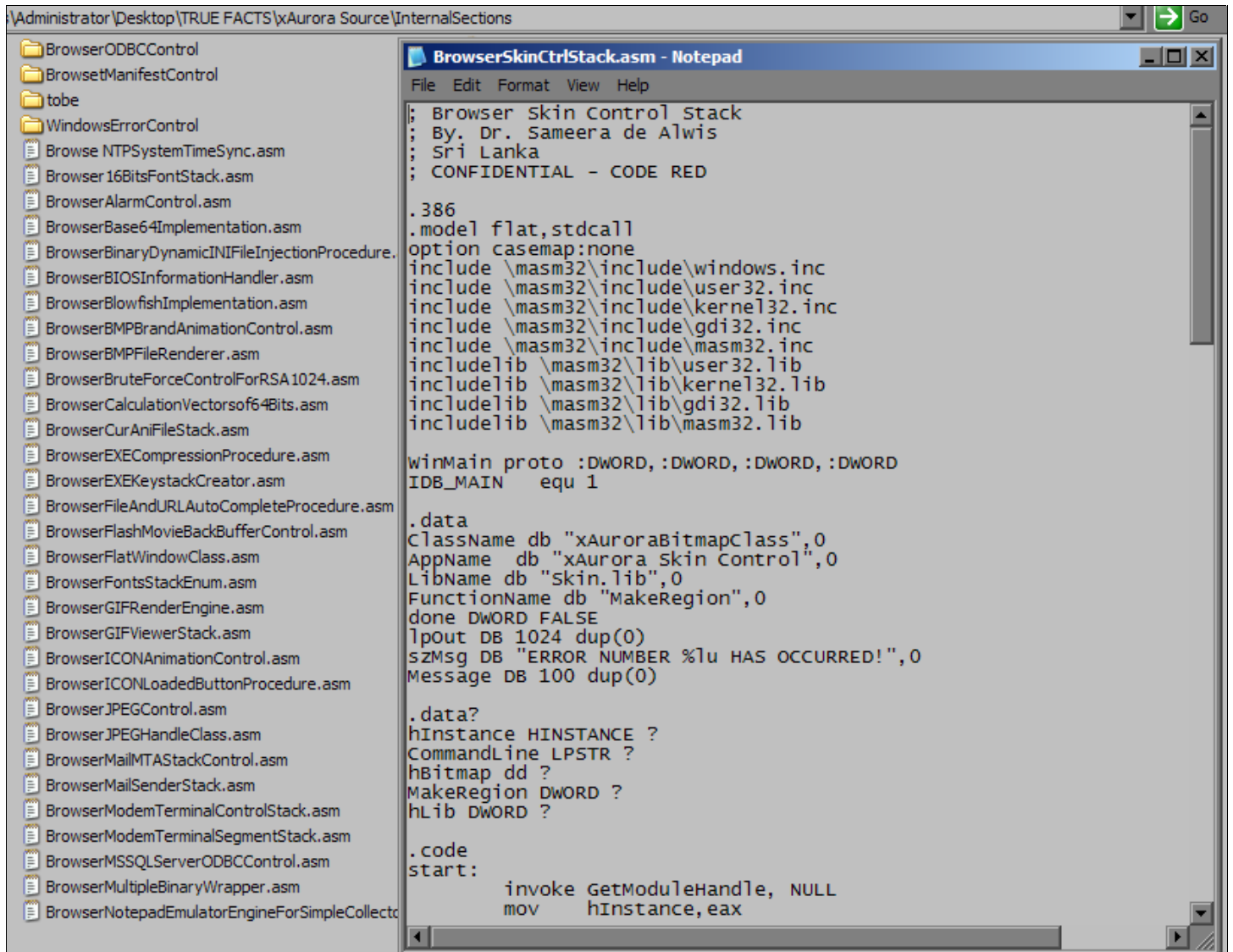
\* xAurora EXE Self Repair Section



\* Simple Collector - Embedded Mini Notepad Control



## \* Skin Control Stack



```
Administrator\Desktop\TRUE FACTS\xAurora Source\InternalSections
BrowserODBCControl
BrowsetManifestControl
tobe
WindowsErrorControl
Browse NTPSystemTimeSync.asm
Browser16BitsFontStack.asm
BrowserAlarmControl.asm
BrowserBase64Implementation.asm
BrowserBinaryDynamicINIFileInjectionProcedure.asm
BrowserBIOSInformationHandler.asm
BrowserBlowfishImplementation.asm
BrowserBMPBrandAnimationControl.asm
BrowserBMPFileRenderer.asm
BrowserBruteForceControlForRSA1024.asm
BrowserCalculationVectorsof64Bits.asm
BrowserCurAniFileStack.asm
BrowserEXECompressionProcedure.asm
BrowserEXEKeystackCreator.asm
BrowserFileAndURLAutoCompleteProcedure.asm
BrowserFlashMovieBackBufferControl.asm
BrowserFlatWindowClass.asm
BrowserFontsStackEnum.asm
BrowserGIFRenderEngine.asm
BrowserGIFViewerStack.asm
BrowserICONAnimationControl.asm
BrowserICONLoadedButtonProcedure.asm
BrowserJPEGControl.asm
BrowserJPEGHandleClass.asm
BrowserMailMTAStackControl.asm
BrowserMailSenderStack.asm
BrowserModemTerminalControlStack.asm
BrowserModemTerminalSegmentStack.asm
BrowserMSSQLServerODBCControl.asm
BrowserMultipleBinaryWrapper.asm
BrowserNotepadEmulatorEngineForSimpleCollect

BrowserSkinCtrlStack.asm - Notepad
File Edit Format View Help
; Browser Skin Control Stack
; 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\gdi32.inc
include \masm32\include\masm32.inc
includelib \masm32\lib\user32.lib
includelib \masm32\lib\kernel32.lib
includelib \masm32\lib\gdi32.lib
includelib \masm32\lib\masm32.lib

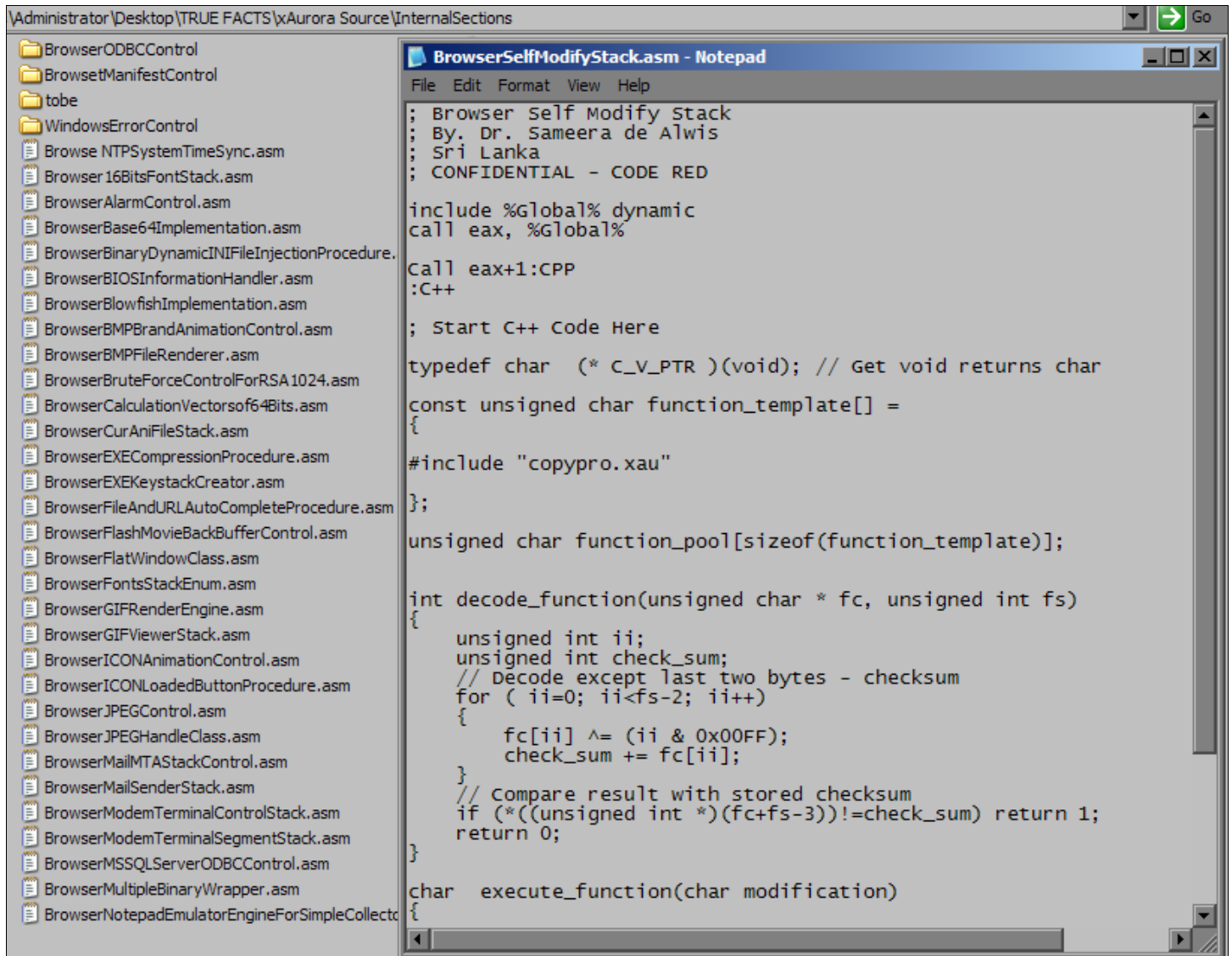
winMain proto :DWORD, :DWORD, :DWORD, :DWORD
IDB_MAIN equ 1

.data
ClassName db "xAuroraBitmapClass",0
AppName db "xAurora Skin Control",0
LibName db "skin.lib",0
FunctionName db "MakeRegion",0
done DWORD FALSE
lpout DB 1024 dup(0)
szMsg DB "ERROR NUMBER %!u HAS OCCURRED!",0
Message DB 100 dup(0)

.data?
hInstance HINSTANCE ?
CommandLine LPSTR ?
hBitmap dd ?
MakeRegion DWORD ?
hLib DWORD ?

.code
start:
invoke GetModuleHandle, NULL
mov hInstance, eax
```

## \* Self Modify Procedure - Hybrid C++ & Win32 Assembler Stack



```
Administrator\Desktop\TRUE FACTS\Aurora Source\InternalSections
BrowserODBCControl
BrowserManifestControl
tobe
WindowsErrorControl
Browse NTPSystemTimeSync.asm
Browser16BitsFontStack.asm
BrowserAlarmControl.asm
BrowserBase64Implementation.asm
BrowserBinaryDynamicINIFileInjectionProcedure.
BrowserBIOSInformationHandler.asm
BrowserBlowfishImplementation.asm
BrowserBMPBrandAnimationControl.asm
BrowserBMPFileRenderer.asm
BrowserBruteForceControlForRSA1024.asm
BrowserCalculationVectorsof64Bits.asm
BrowserCurAniFileStack.asm
BrowserEXECompressionProcedure.asm
BrowserEXEKeystackCreator.asm
BrowserFileAndURLAutoCompleteProcedure.asm
BrowserFlashMovieBackBufferControl.asm
BrowserFlatWindowClass.asm
BrowserFontsStackEnum.asm
BrowserGIFRenderEngine.asm
BrowserGIFViewerStack.asm
BrowserICONAnimationControl.asm
BrowserICONLoadedButtonProcedure.asm
BrowserJPEGControl.asm
BrowserJPEGHandleClass.asm
BrowserMailMTAStackControl.asm
BrowserMailSenderStack.asm
BrowserModemTerminalControlStack.asm
BrowserModemTerminalSegmentStack.asm
BrowserMSSQLServerODBCControl.asm
BrowserMultipleBinaryWrapper.asm
BrowserNotepadEmulatorEngineForSimpleCollecto

BrowserSelfModifyStack.asm - Notepad
File Edit Format View Help
; Browser Self Modify Stack
; By. Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

include %Global% dynamic
call eax, %Global%

Call eax+1:CPP
:C++

; Start C++ Code Here

typedef char (* C_V_PTR )(void); // Get void returns char

const unsigned char function_template[] =
{
#include "copypro.xau"
};

unsigned char function_pool[sizeof(function_template)];

int decode_function(unsigned char * fc, unsigned int fs)
{
    unsigned int ii;
    unsigned int check_sum;
    // Decode except last two bytes - checksum
    for ( ii=0; ii<fs-2; ii++)
    {
        fc[ii] ^= (ii & 0x00FF);
        check_sum += fc[ii];
    }
    // Compare result with stored checksum
    if (*((unsigned int *)(fc+fs-3))!=check_sum) return 1;
    return 0;
}

char execute_function(char modification)
{
```

\* xAurora Registry Control Stack

Administrator\Desktop\TRUE FACTS\xAurora Source\InternalSections

BrowserRegistryOperations.asm - Notepad

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

.486
.model flat, stdcall
option casemap :none

include c:\masm32\include\windows.inc
include c:\masm32\include\gdi32.inc
include c:\masm32\include\user32.inc
include c:\masm32\include\kernel32.inc
include c:\masm32\include\advapi32.inc

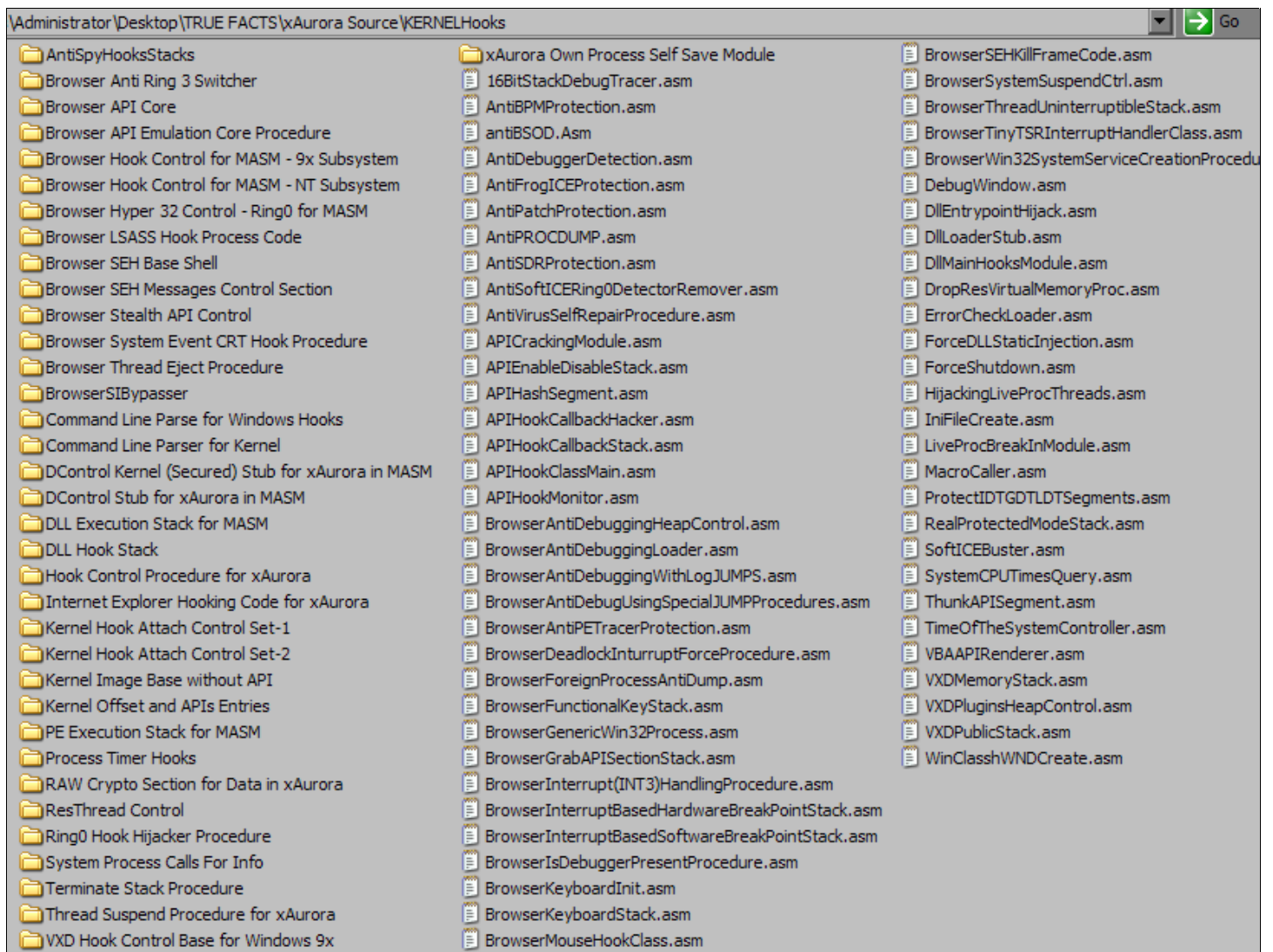
includelib c:\masm32\lib\gdi32.lib
includelib c:\masm32\lib\user32.lib
includelib c:\masm32\lib\kernel32.lib
includelib c:\masm32\lib\advapi32.lib

IDD_DIALOG      equ 101
IDADD           equ 1000
IDDELETE       equ 1001
IDC_LIST       equ 1002
IDLOAD         equ 1003
IDSAVE         equ 1004
IDC_EDIT       equ 1005

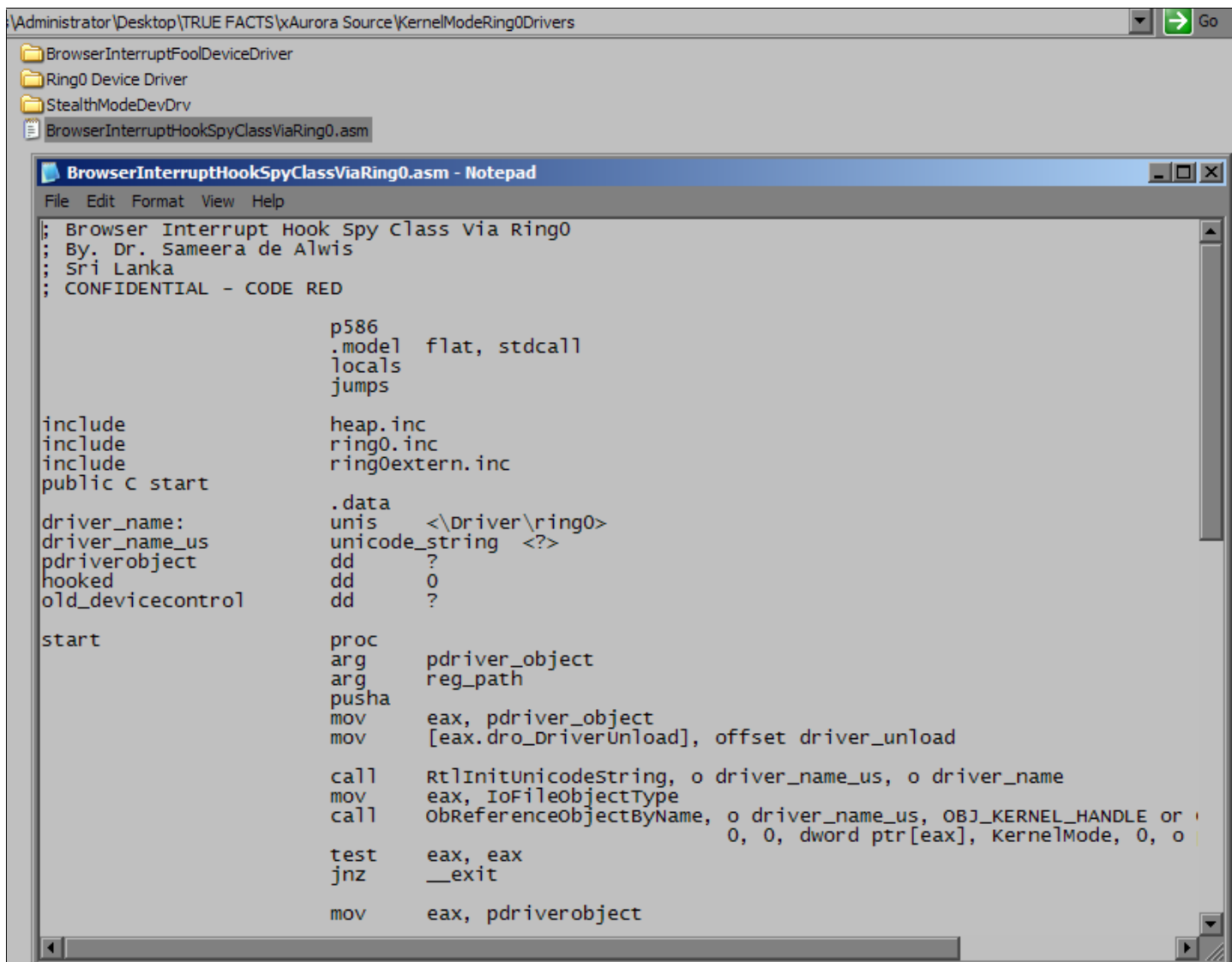
.const
  szSubKey      db 'set the xAurora Registry Keys key\Sub key',0
  szFormat      db '[Item %02d]',0

.data
  hwndDlg      HWND NULL
  hwndAdd      HWND NULL
  hwndDelete   HWND NULL
  hwndList     HWND NULL
  hwndLoad     HWND NULL
  hwndSave     HWND NULL
  hwndEdit     HWND NULL
  bmultisel    DWORD 0
  oldwndproc   DWORD NULL
```

## 16. xAurora Highly Confidential KERNEL MODE INTERNAL CODE HOOKS/STACKS



## 17. Browser Interrupt Hook Spy Class via Ring0



The image shows a Windows Explorer window with the address bar displaying the path: `Administrator\Desktop\TRUE FACTS\Aurora Source\KernelModeRing0Drivers`. The file explorer view shows a folder structure with `BrowserInterruptFoolDeviceDriver`, `Ring0 Device Driver`, `StealthModeDevDrv`, and `BrowserInterruptHookSpyClassViaRing0.asm`. A Notepad window is open over the Explorer, displaying the assembly code for `BrowserInterruptHookSpyClassViaRing0.asm`. The code includes headers, defines data fields, and implements a `start` procedure that initializes a driver object and hooks the `IoFileObjectType`.

```
; Browser Interrupt Hook Spy Class via Ring0
; By. Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

                p586
                .model flat, stdcall
                locals
                jumps

include        heap.inc
include        ring0.inc
include        ring0extern.inc
public C start

driver_name:   .data
                unis    <\Driver\ring0>
driver_name_us unicode_string <?>
pdriverobject dd    ?
hooked        dd    0
old_devicecontrol dd    ?

start         proc
                arg    pdriver_object
                arg    reg_path
                pusha
                mov    eax, pdriver_object
                mov    [eax.dro_DriverUnload], offset driver_unload

                call   RtlInitUnicodeString, o driver_name_us, o driver_name
                mov    eax, IoFileObjectType
                call   ObReferenceObjectByName, o driver_name_us, OBJ_KERNEL_HANDLE or
                0, 0, dword ptr[eax], KernelMode, 0, o

                test   eax, eax
                jnz    __exit

                mov    eax, pdriverobject
                endp
```



## 19. Browser Stealth Mode Device Driver Stack

```
Administrator\Desktop\TRUE FACTS\Aurora Source\KernelModeRing0Drivers\StealthModeDevDrv\StealthModeDeviceDriver
BrowserStealthModeDeviceDriverStack.asm
REG.BAT
RUN.BAT

BrowserStealthModeDeviceDriverStack.asm - Notepad
File Edit Format View Help

;-----
; Browser Stealth Mode Device Driver stack
; By. Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED
;-----

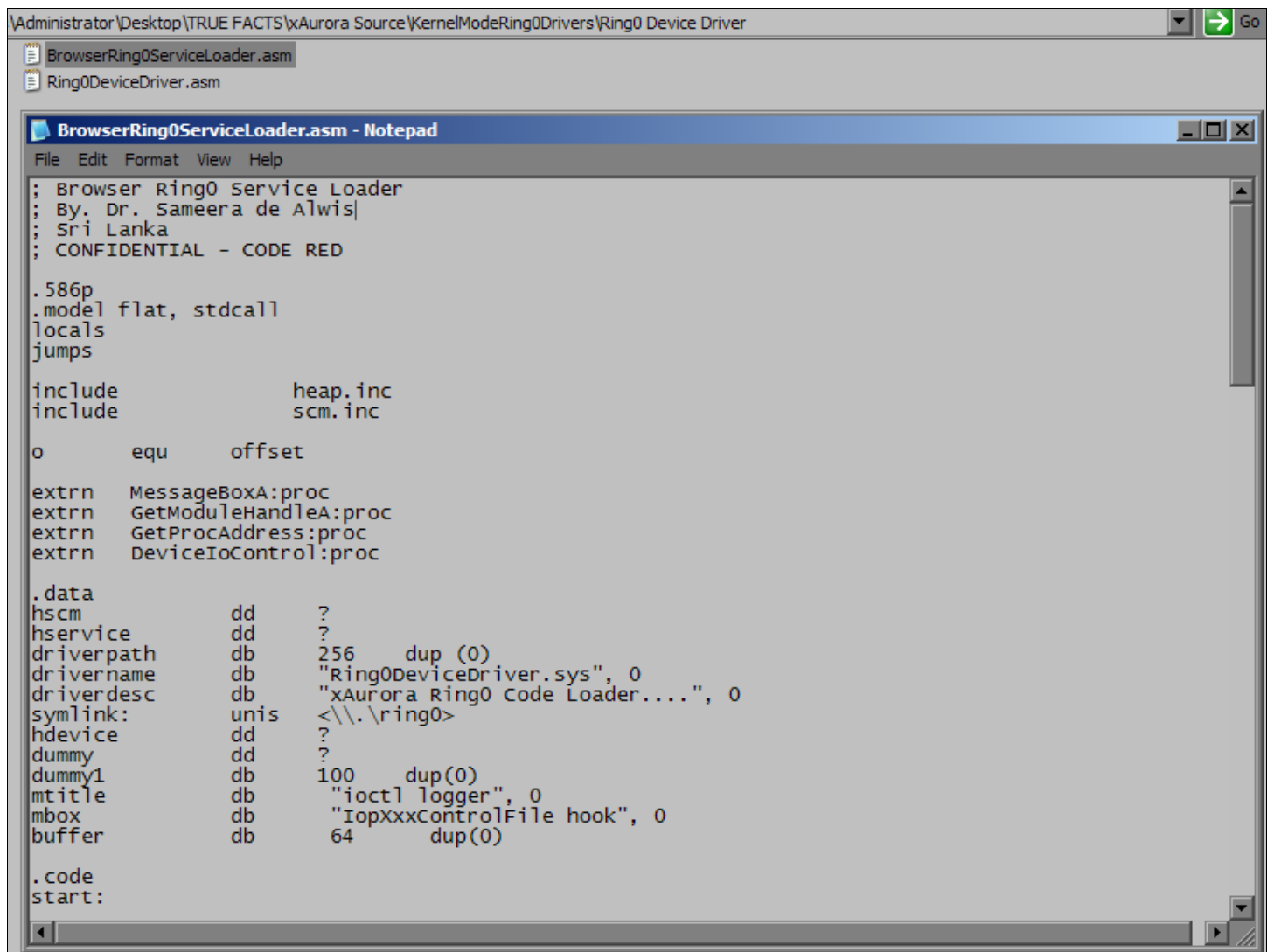
CLIENT_ID          STRUCT          ;NTDDK
UniqueProcess      DWORD ?
UniqueThread       DWORD ?
CLIENT_ID          ENDS

;-----
OBJ_INHERIT        = 00000002H
OBJ_PERMANENT      = 00000010H
OBJ_EXCLUSIVE      = 00000020H
OBJ_CASE_INSENSITIVE = 00000040H
OBJ_OPENIF         = 00000080H
OBJ_OPENLINK       = 00000100H
OBJ_VALID_ATTRIBUTES = 000001F2H

OBJECT_ATTRIBUTES  STRUCT          ;NTDDK
Length_           DWORD ?
RootDirectory     DWORD ?
ObjectName         DWORD ?
Attributes         DWORD ?
SecurityDescriptor  DWORD ?
SecurityQualityOfService  DWORD ?
OBJECT_ATTRIBUTES ENDS

;-----
TIME_FIELDS        STRUC  DWORD          ;NTDDK
Year               WORD  ? ;range [1601...]
Month              WORD  ? ;range [1..12]
Day                WORD  ? ;range [1..31]
Hour               WORD  ? ;range [0..23]
Minute             WORD  ? ;range [0..59]
```

## 20. Browser Ring0 Service Loader



```
Administrator\Desktop\TRUE FACTS\xAurora Source\KernelModeRing0Drivers\Ring0 Device Driver
BrowserRing0ServiceLoader.asm
Ring0DeviceDriver.asm

BrowserRing0ServiceLoader.asm - Notepad
File Edit Format View Help

; Browser Ring0 Service Loader
; By. Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

.586p
.model flat, stdcall
.locals
.jumps

include          heap.inc
include          scm.inc

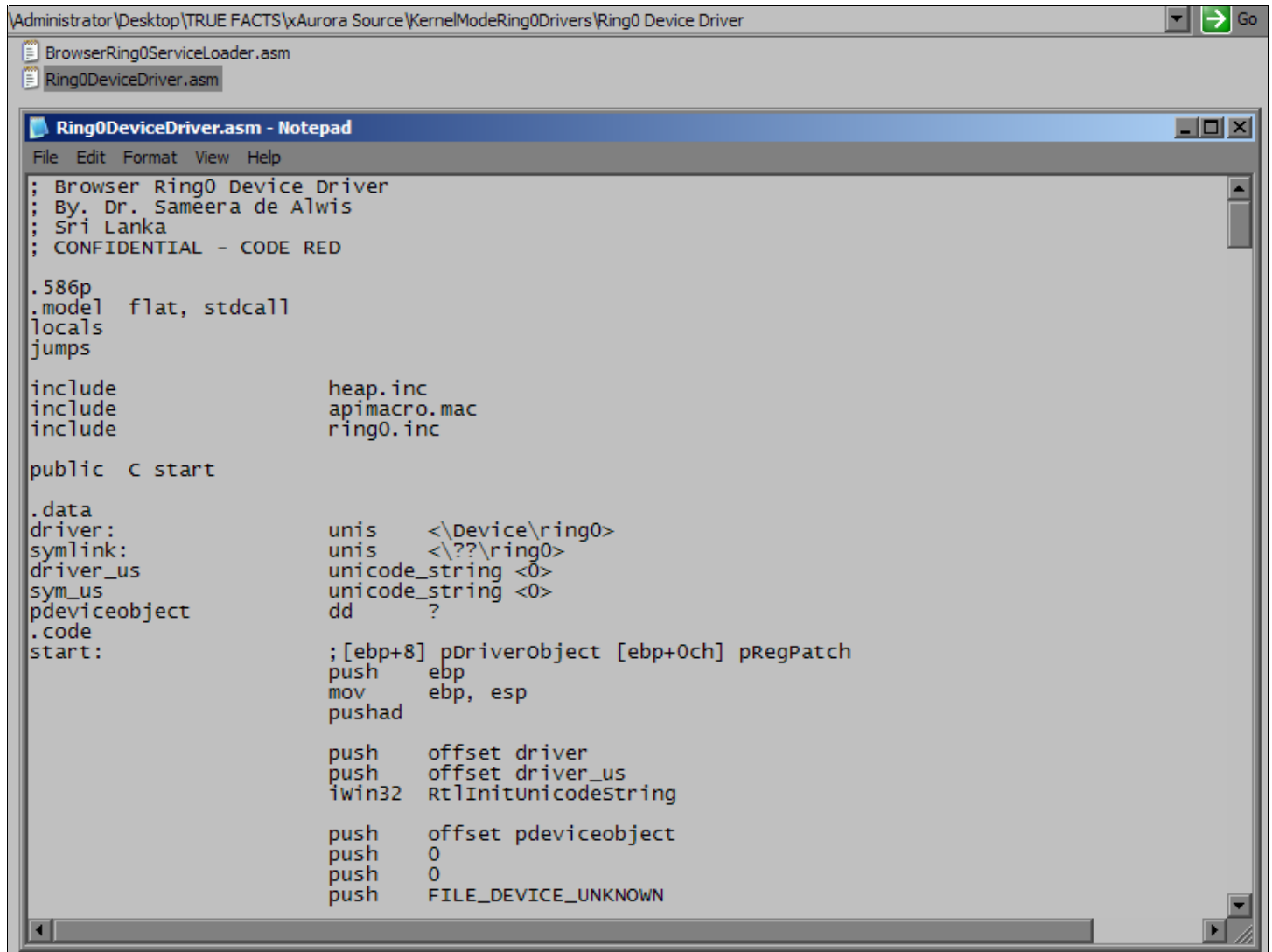
o      equ      offset

extrn  MessageBoxA:proc
extrn  GetModuleHandleA:proc
extrn  GetProcAddress:proc
extrn  DeviceIoControl:proc

.data
hscm          dd      ?
hservice      dd      ?
driverpath    db      256      dup(0)
drivername    db      "Ring0DeviceDriver.sys", 0
driverdesc    db      "xAurora Ring0 Code Loader....", 0
symlink:      unis    <\\.ring0>
hdevice       dd      ?
dummy         dd      ?
dummy1        db      100      dup(0)
mtitle        db      "ioctl logger", 0
mbox          db      "IopxxxControlFile hook", 0
buffer        db      64      dup(0)

.code
start:
```

## 21. Browser Ring0 Device Driver



```
Administrator\Desktop\TRUE FACTS\Aurora Source\KernelModeRing0Drivers\Ring0 Device Driver
BrowserRing0ServiceLoader.asm
Ring0DeviceDriver.asm

Ring0DeviceDriver.asm - Notepad
File Edit Format View Help

; Browser Ring0 Device Driver
; By. Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

.586p
.model flat, stdcall
locals
jumps

include          heap.inc
include          apimacro.mac
include          ring0.inc

public C start

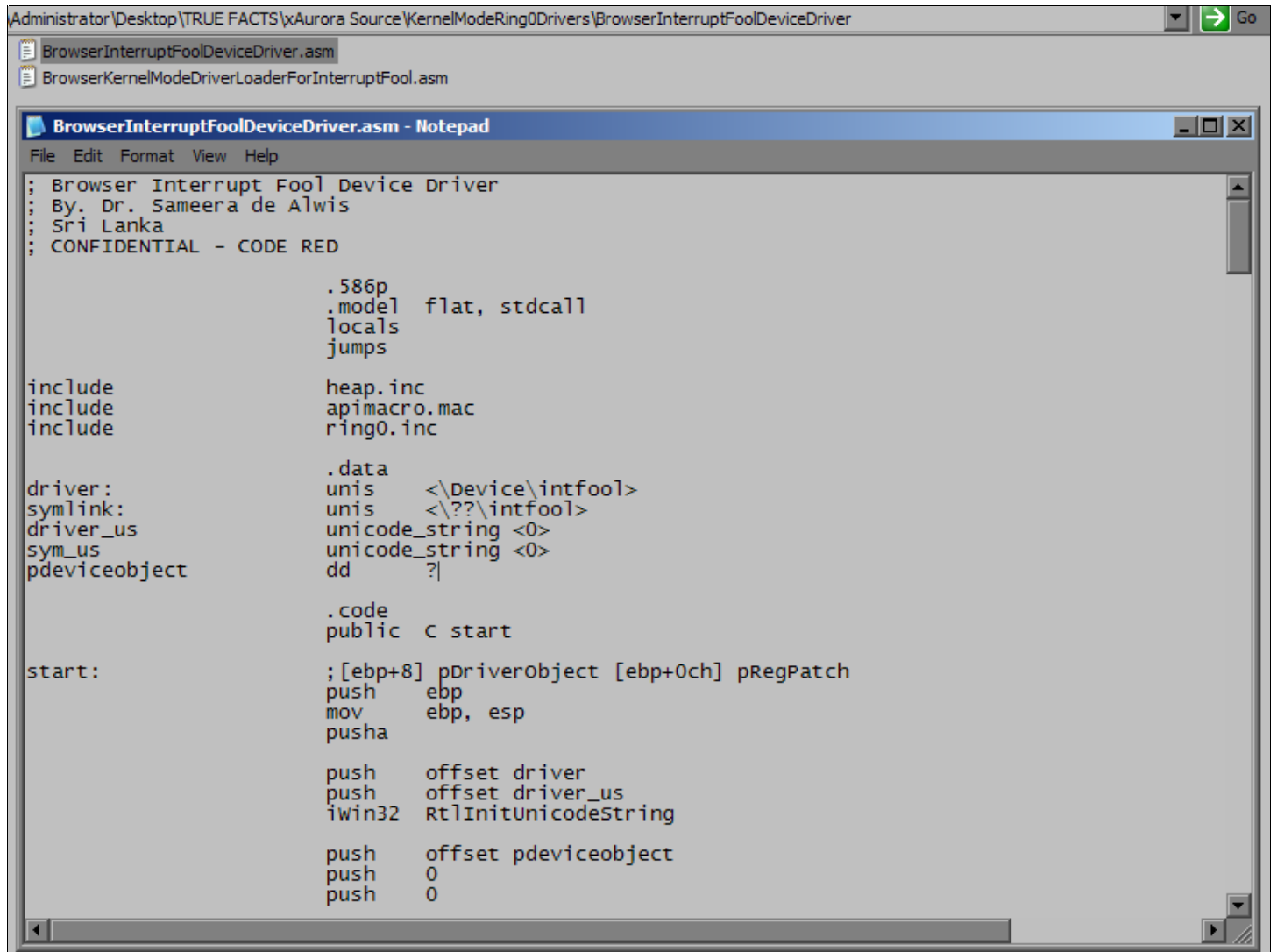
.data
driver:          unis    <\Device\ring0>
symlink:        unis    <\\??\ring0>
driver_us       unicode_string <0>
sym_us          unicode_string <0>
pdeviceobject   dd      ?

.code
start:          ;[ebp+8] pDriverObject [ebp+0ch] pRegPatch
               push    ebp
               mov     ebp, esp
               pushad

               push    offset driver
               push    offset driver_us
               iwin32  RtlInitunicodeString

               push    offset pdeviceobject
               push    0
               push    0
               push    FILE_DEVICE_UNKNOWN
```

## 22. Browser Interrupt Fool Device Driver



```
Administrator\Desktop\TRUE FACTS\Aurora Source\KernelModeRing0Drivers\BrowserInterruptFoolDeviceDriver
BrowserInterruptFoolDeviceDriver.asm
BrowserKernelModeDriverLoaderForInterruptFool.asm

BrowserInterruptFoolDeviceDriver.asm - Notepad
File Edit Format View Help

; Browser Interrupt Fool Device Driver
; By. Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

                                .586p
                                .model flat, stdcall
                                locals
                                jumps

include                          heap.inc
include                          apimacro.mac
include                          ring0.inc

                                .data
driver:                          unis <\Device\intfool>
symlink:                         unis <\\?\intfool>
driver_us                        unicode_string <0>
sym_us                           unicode_string <0>
pdeviceobject                    dd ?

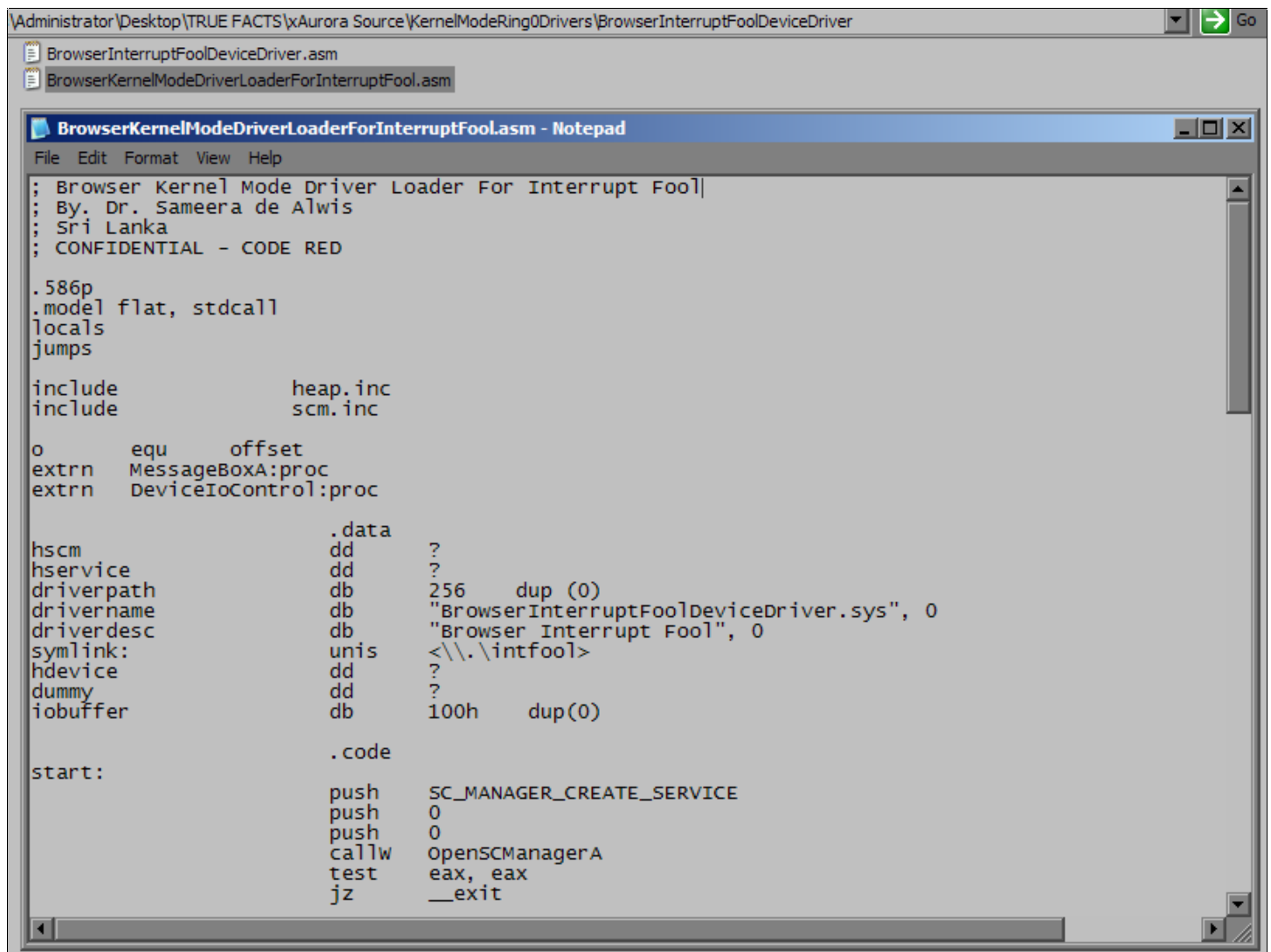
                                .code
                                public C start

start:                            ;[ebp+8] pDriverObject [ebp+0ch] pRegPatch
                                push ebp
                                mov ebp, esp
                                pusha

                                push offset driver
                                push offset driver_us
                                iwin32 RtlInitUnicodeString

                                push offset pdeviceobject
                                push 0
                                push 0
```

## 23. Browser Kernel Mode Driver Loader for Interrupt Fool



```
Administrator\Desktop\TRUE FACTS\Aurora Source\KernelModeRing0Drivers\BrowserInterruptFoolDeviceDriver
BrowserInterruptFoolDeviceDriver.asm
BrowserKernelModeDriverLoaderForInterruptFool.asm

BrowserKernelModeDriverLoaderForInterruptFool.asm - Notepad
File Edit Format View Help

; Browser Kernel Mode Driver Loader For Interrupt Fool
; By. Dr. Sameera de Alwis
; Sri Lanka
; CONFIDENTIAL - CODE RED

.586p
.model flat, stdcall
.locals
.jumps

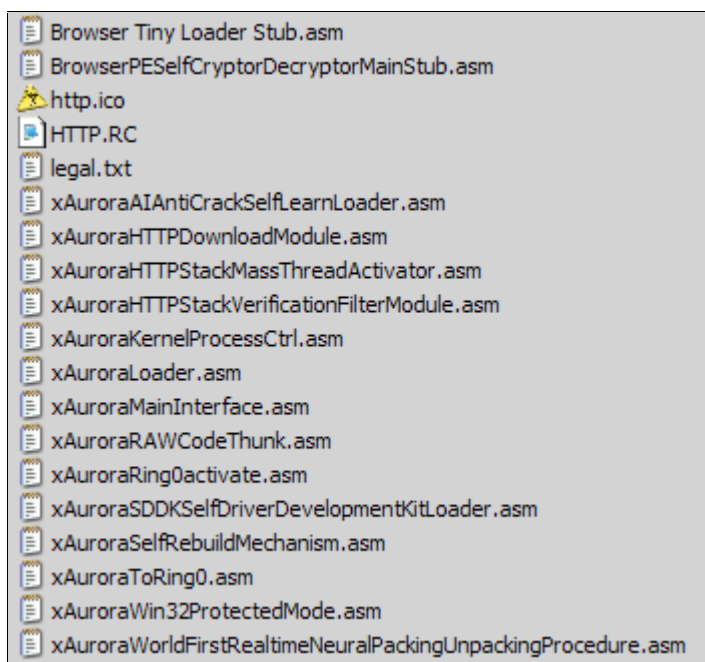
include          heap.inc
include          scm.inc

o          equ          offset
extrn     MessageBoxA:proc
extrn     DeviceIoControl:proc

                .data
hscm            dd          ?
hservice        dd          ?
driverpath      db          256          dup (0)
drivername      db          "BrowserInterruptFoolDeviceDriver.sys", 0
driverdesc      db          "Browser Interrupt Fool", 0
symlink:        unis        <\\.\intfool>
hdevice         dd          ?
dummy           dd          ?
iobuffer        db          100h          dup(0)

                .code
start:
                push     SC_MANAGER_CREATE_SERVICE
                push     0
                push     0
                callw   OpenSCManagerA
                test     eax, eax
                jz       __exit
```

## 24. Root Core Files



## 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.

xAurora Developers Pod Revealed – Visual Approach – PART 2 will be available soon on Gotaimbara's Blog.

Kind Regards

Dr. Sameera de Alwis

Founder – Team xAurora 2009