Program Code Analyzers – Agenda

- The Problem
- Dynamic and Static Tools
- Examples of Tools

The Problems

- Programmers make errors when coding
- The Compiler usually only finds syntax errors, not memory or logical errors

- These bugs show up at run time
- But sometimes only rarely, and may seem invisible
- We need help to find them!

- Does the code have a reasonable amount of comments?
- How long and complex are the functions/methods?

Dynamic and Static Tools

Dynamic Tools

- Run-time testing
- Detection of memory errors, such as leaks or memory writes
- Memory efficiency
- Detection of race conditions
- Construction of run-time call graphs

Static Tools

- Before run-time
- Detect common errors
- Detect potental problems, such as methods often used incorrectly or unreachable code
- Calculate metrics for program code
- Construction of call graphs
- Assist in writing test programs

Examples of Tools

- IDA Pro
- Purify
- Resource Standard Metric (RSM)
- Valgrind

Resource Standard Metric (RSM)

- http://msquaredtechnologies.com/
- Static source code analyzer

Resource Standard Metrics Wizard

File Edit Action Help

Guided Process Steps

? Help | Free Play | 1 - Load or Name Solution | 2- Choose or Modify Files | 3 - Load or Name Output File | 4 - Select/Create Reports | 5 - Execute RSM

Selection Tree of Path or Files

Acquistion Mode: Path / Files ?

C:\Documents and Settings\mop\Desktop\GenericProgramming\assigi — Path Recurse

h,c,cpp,java,cs,hpp — Ext. +Filter — .gui.cs,.ui.cpp — Pattern -Filter

temp,tmp,test,CVS,SCCS — Directory -Filter

Set Path | Path To List | Acquire Files | Files To List | Clear Tree

- C:\Documents and Settings\mop\Desktop\GenericProgramming\assignment4
  - main.cpp

RSM Input File List

Count 1 — Append — Load — Save — Clear ?

File List: grafik.lst ±

C:\Documents and Settings\mop\Desktop\GenericProgramming\assignment4\main.cpp

RSM Wizard Solution

graphic.rsm ± Load Save ?

RSM Output File

Format: Text / HTML (-H) / CSV (-C) / XML (-X) ? Open

output.htm ± Set

RSM Reports, Switches, Options & Compound Options

New Report | Load | Save | New | Reset | ?

new_report.rpt ±

RSM Reports | Switch a - f | Switch i - k | Switch l - s | Switch T | Switch w | Switch u - z | Help

Resource Standard Metrics™ — RSM Wizard

Delete | Support | Reload | Help

Select Single Click, Execute Double Click a Report

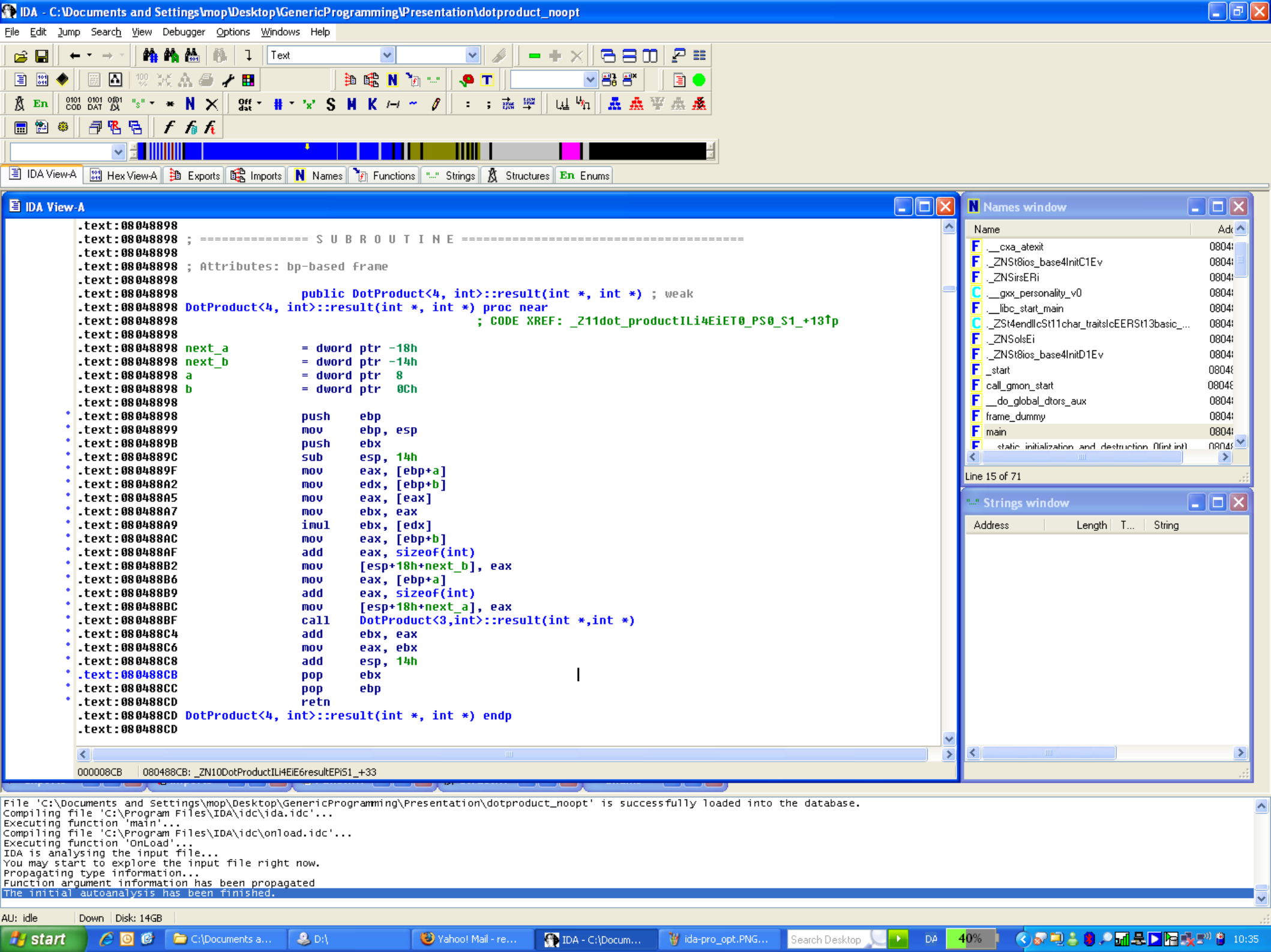
- M2 - Print Format For Source Code (Text)
- M2 - Source Code Functional Metrics and Analysis (CSV)
- M2 - Source Code Functional Metrics and Analysis (HTML)
- M2 - Source Code Functional Metrics and Analysis (Text)
- M2 - Total All Metrics with Title (HTML)
- M2 - Total LOC Summary Metrics (CSV)
- M2 - Total LOC Summary Metrics (HTML)
- M2 - Total LOC Summary Metrics (Text)
- M2 - Total Quality Analysis By File (HTML)
- M2 - Total Quality Profile (HTML)
- M2 - Total Summary Metrics (HTML)
- M2 - Verbose Source Code Metrics (HTML)
- M2 - Verbose Source Code Metrics (Text)
- New Report
- New Report 1

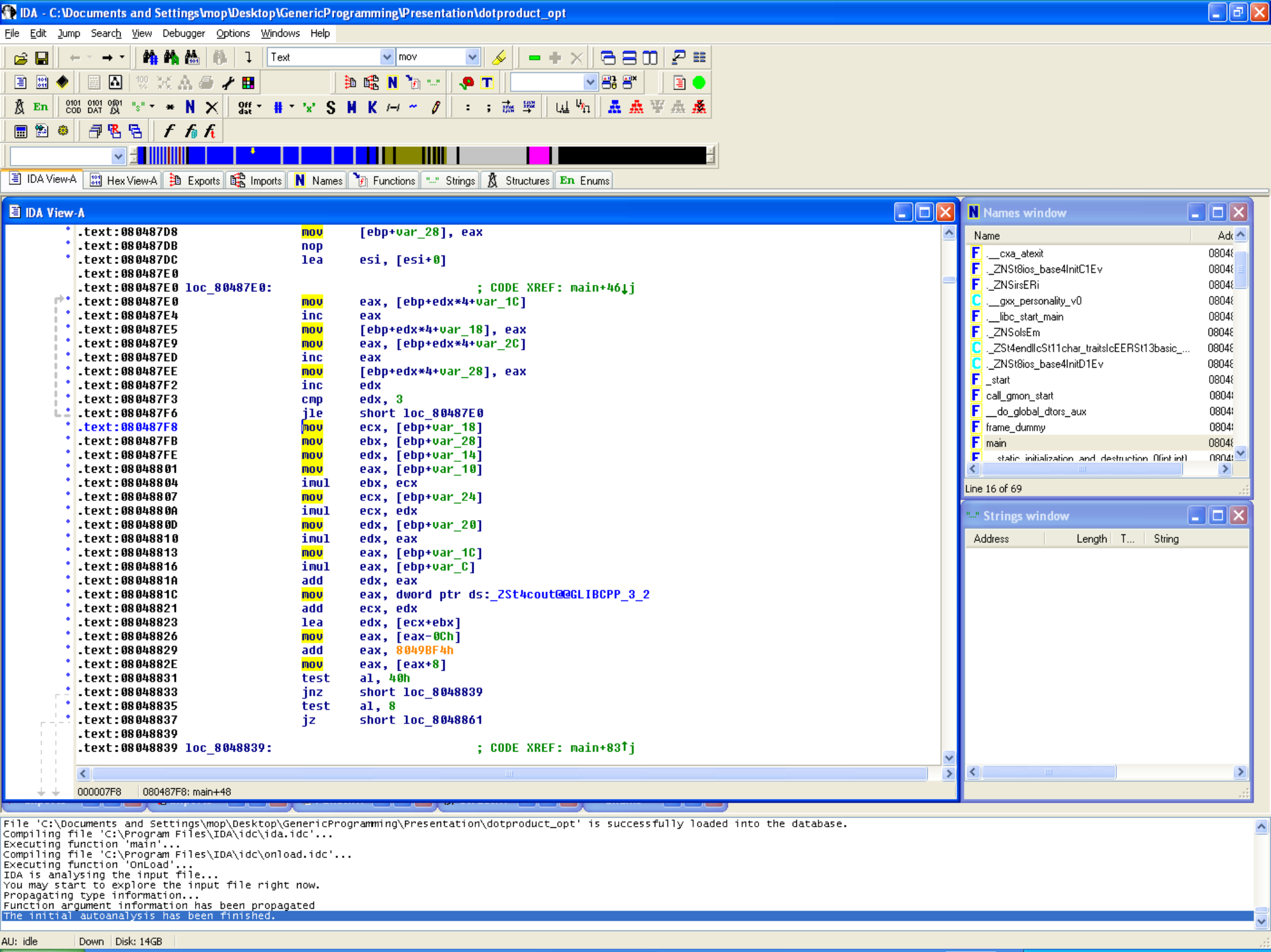
RSM Command Line

Auto — -H -O"C:\Documents and Settings\mop\M2 RSM Wizard\output\output.htm" -a -c -n -F"C:\Documents and Settings\mop\M2 RSM Wizard\input\grafik.lst" ? Execute

Interactive Disassembler Pro (IDA Pro)

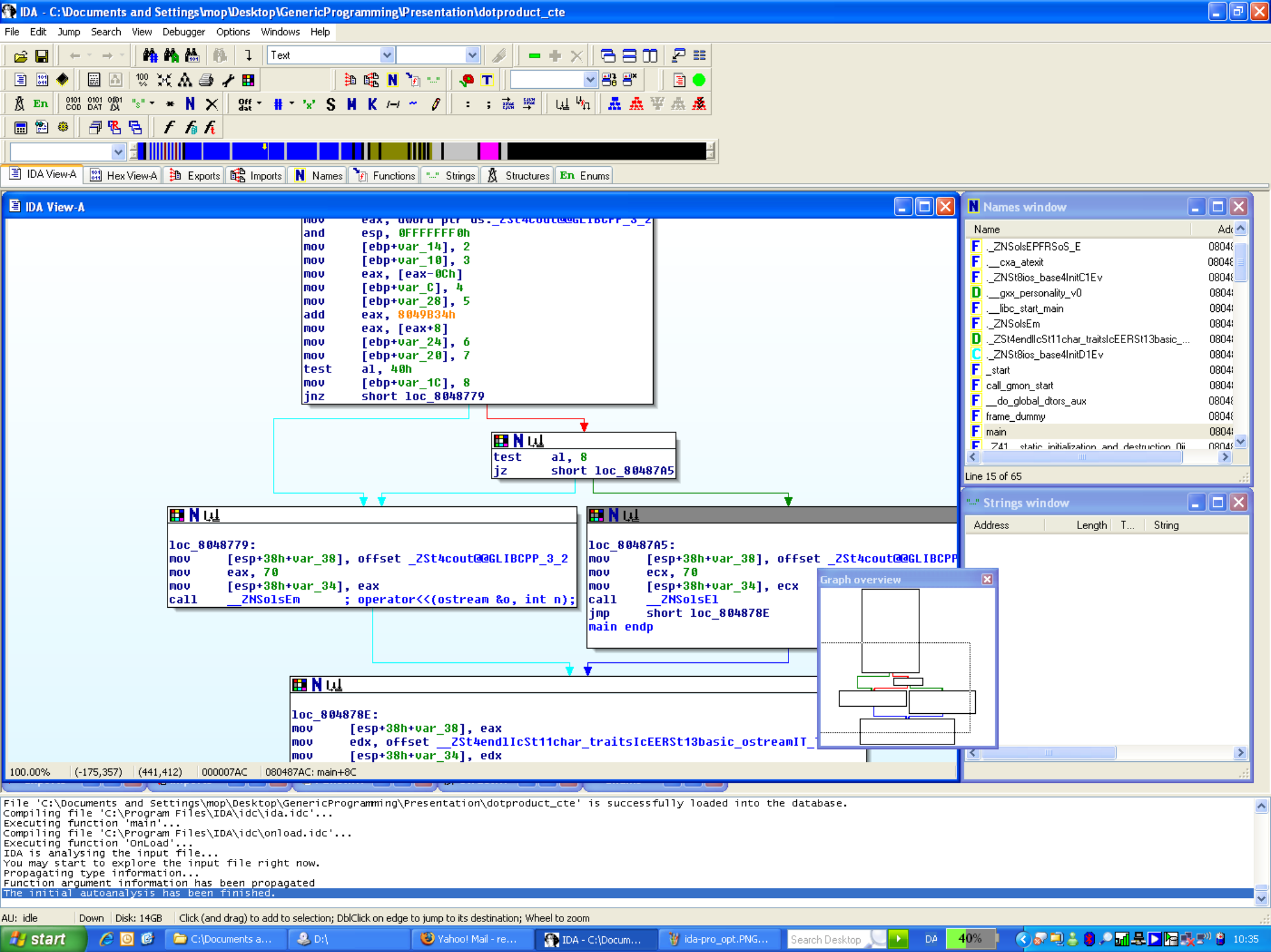
- http://www.datarescue.com/idabase
- Disassembler with extensive plugin interface


IDA - C:\Documents and Settings\mop\Desktop\GenericProgramming\Presentation\dotproduct_noopt
File Edit Jump Search View Debugger Options Windows Help
IDA View-A Hex View-A Exports Imports Names Functions Strings Structures Enums
IDA View-A
.text:08048898
.text:08048898 ; =============== S U B R O U T I N E =======================================
.text:08048898
.text:08048898 ; Attributes: bp-based frame
.text:08048898
.text:08048898 public DotProduct<4, int>::result(int *, int *) ; weak
.text:08048898 DotProduct<4, int>::result(int *, int *) proc near
.text:08048898 ; CODE XREF: _Z11dot_productILi4EiET0_PS0_S1_+13↑p
.text:08048898
.text:08048898 next_a = dword ptr -18h
.text:08048898 next_b = dword ptr -14h
.text:08048898 a = dword ptr 8
.text:08048898 b = dword ptr 0Ch
.text:08048898
.text:08048898 push ebp
.text:08048899 mov ebp, esp
.text:0804889B push ebx
.text:0804889C sub esp, 14h
.text:0804889F mov eax, [ebp+a]
.text:080488A2 mov edx, [ebp+b]
.text:080488A5 mov eax, [eax]
.text:080488A7 mov ebx, eax
.text:080488A9 imul ebx, [edx]
.text:080488AC mov eax, [ebp+b]
.text:080488AF add eax, sizeof(int)
.text:080488B2 mov [esp+18h+next_b], eax
.text:080488B6 mov eax, [ebp+a]
.text:080488B9 add eax, sizeof(int)
.text:080488BC mov [esp+18h+next_a], eax
.text:080488BF call DotProduct<3,int>::result(int *,int *)
.text:080488C4 add ebx, eax
.text:080488C6 mov eax, ebx
.text:080488C8 add esp, 14h
.text:080488CB pop ebx
.text:080488CC pop ebp
.text:080488CD retn
.text:080488CD DotProduct<4, int>::result(int *, int *) endp
.text:080488CD
000008CB 080488CB: _ZN10DotProductILi4EiE6resultEPiS1_+33
Names window
Name Ad
F .__cxa_atexit 0804
F ._ZNSt8ios_base4InitC1Ev 0804
F ._ZNSirsERi 0804
C .__gxx_personality_v0 0804
F .__libc_start_main 0804
C ._ZSt4endlIcSt11char_traitsIcEERSt13basic_... 0804
F ._ZNSolsEi 0804
F ._ZNSt8ios_base4InitD1Ev 0804
F _start 0804
F call_gmon_start 0804
F __do_global_dtors_aux 0804
F frame_dummy 0804
F main 0804
Line 15 of 71
Strings window
Address Length T... String
File 'C:\Documents and Settings\mop\Desktop\GenericProgramming\Presentation\dotproduct_noopt' is successfully loaded into the database.
Compiling file 'C:\Program Files\IDA\idc\ida.idc'...
Executing function 'main'...
Compiling file 'C:\Program Files\IDA\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished.
AU: idle Down Disk: 14GB
start
C:\Documents a...
D:\
Yahoo! Mail - re...
IDA - C:\Docum...
ida-pro_opt.PNG...
Search Desktop
DA
40%
10:35


IDA - C:\Documents and Settings\mop\Desktop\GenericProgramming\Presentation\dotproduct_opt
File Edit Jump Search View Debugger Options Windows Help
IDA View-A
Hex View-A
Exports
Imports
Names
Functions
Strings
Structures
Enums
.text:080487D8 mov [ebp+var_28], eax
.text:080487DB nop
.text:080487DC lea esi, [esi+0]
.text:080487E0
.text:080487E0 loc_80487E0: ; CODE XREF: main+46↓j
.text:080487E0 mov eax, [ebp+edx*4+var_1C]
.text:080487E4 inc eax
.text:080487E5 mov [ebp+edx*4+var_18], eax
.text:080487E9 mov eax, [ebp+edx*4+var_2C]
.text:080487ED inc eax
.text:080487EE mov [ebp+edx*4+var_28], eax
.text:080487F2 inc edx
.text:080487F3 cmp edx, 3
.text:080487F6 jle short loc_80487E0
.text:080487F8 mov ecx, [ebp+var_18]
.text:080487FB mov ebx, [ebp+var_28]
.text:080487FE mov edx, [ebp+var_14]
.text:08048801 mov eax, [ebp+var_10]
.text:08048804 imul ebx, ecx
.text:08048807 mov ecx, [ebp+var_24]
.text:0804880A imul ecx, edx
.text:0804880D mov edx, [ebp+var_20]
.text:08048810 imul edx, eax
.text:08048813 mov eax, [ebp+var_1C]
.text:08048816 imul eax, [ebp+var_C]
.text:0804881A add edx, eax
.text:0804881C mov eax, dword ptr ds:_ZSt4cout@@GLIBCPP_3_2
.text:08048821 add ecx, edx
.text:08048823 lea edx, [ecx+ebx]
.text:08048826 mov eax, [eax-0Ch]
.text:08048829 add eax, 8049BF4h
.text:0804882E mov eax, [eax+8]
.text:08048831 test al, 40h
.text:08048833 jnz short loc_8048839
.text:08048835 test al, 8
.text:08048837 jz short loc_8048861
.text:08048839
.text:08048839 loc_8048839: ; CODE XREF: main+83↑j
000007F8 080487F8: main+48
Names window
Name
__cxa_atexit
_ZNSt8ios_base4InitC1Ev
_ZNSirsERi
__gxx_personality_v0
__libc_start_main
_ZNSolsEm
_ZSt4endlIcSt11char_traitsIcEERSt13basic_...
_ZNSt8ios_base4InitD1Ev
_start
call_gmon_start
__do_global_dtors_aux
frame_dummy
main
Line 16 of 69
Strings window
Address
Length
T...
String
File 'C:\Documents and Settings\mop\Desktop\GenericProgramming\Presentation\dotproduct_opt' is successfully loaded into the database.
Compiling file 'C:\Program Files\IDA\idc\ida.idc'...
Executing function 'main'...
Compiling file 'C:\Program Files\IDA\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished.
AU: idle
Down
Disk: 14GB

```
int main()
{
  int a[4] = {1,2,3,4};
  int b[4] = {5,6,7,8};

  cout << dot_product<4>(a, b) << endl;
  return 0;
}
```


IDA - C:\Documents and Settings\mop\Desktop\GenericProgramming\Presentation\dotproduct_cte
File Edit Jump Search View Debugger Options Windows Help
IDA View-A
Hex View-A
Exports
Imports
Names
Functions
Strings
Structures
Enums
and esp, 0FFFFFFF0h
mov [ebp+var_14], 2
mov [ebp+var_10], 3
mov eax, [eax-0Ch]
mov [ebp+var_C], 4
mov [ebp+var_28], 5
add eax, 8049B34h
mov eax, [eax+8]
mov [ebp+var_24], 6
mov [ebp+var_20], 7
test al, 40h
mov [ebp+var_1C], 8
jnz short loc_8048779
test al, 8
jz short loc_80487A5
loc_8048779:
mov [esp+38h+var_38], offset _ZSt4cout@@GLIBCPP_3_2
mov eax, 70
mov [esp+38h+var_34], eax
call __ZNSolsEm ; operator<<(ostream &o, int n);
loc_80487A5:
mov [esp+38h+var_38], offset _ZSt4cout@@GLIBCPP
mov ecx, 70
mov [esp+38h+var_34], ecx
call __ZNSolsEl
jmp short loc_804878E
main endp
loc_804878E:
mov [esp+38h+var_38], eax
mov edx, offset __ZSt4endlIcSt11char_traitsIcEERSt13basic_ostreamIT_
mov [esp+38h+var_34], edx
Names window
Name
._ZNSolsEPFRSoS_E
.__cxa_atexit
._ZNSt8ios_base4InitC1Ev
.__gxx_personality_v0
.__libc_start_main
._ZNSolsEm
._ZSt4endlIcSt11char_traitsIcEERSt13basic_...
._ZNSt8ios_base4InitD1Ev
._start
.call_gmon_start
.__do_global_dtors_aux
.frame_dummy
.main
Line 15 of 65
Strings window
Address
Length
T...
String
Graph overview
100.00%
(-175,357)
(441,412)
000007AC
080487AC: main+8C
File 'C:\Documents and Settings\mop\Desktop\GenericProgramming\Presentation\dotproduct_cte' is successfully loaded into the database.
Compiling file 'C:\Program Files\IDA\idc\ida.idc'...
Executing function 'main'...
Compiling file 'C:\Program Files\IDA\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished.
AU: idle
Down
Disk: 14GB
Click (and drag) to add to selection; DblClick on edge to jump to its destination; Wheel to zoom
start
C:\Documents a...
D:\
Yahoo! Mail - re...
IDA - C:\Docum...
ida-pro_opt.PNG...
Search Desktop
DA
40%
10:35