From TCT to the Adaptability of Computer Forensic Tools

Haohao Zhai
Renmin University of China

OUTLINE

1 Introduction

2 The Problems

3 Analyzing Reasons of the Problems

4 Solutions to the Problems

5 Implementation and Test

6 Related work and Conclusions

Introduction

Introduction

Introduction

- Computer forensics tools
  - Hardware tools
    - Copying, erasure, conversion of disk interfaces, etc.
    - Product from Logicube (American).
  - Software tools
    - Live investigation, key words searching, anti-deletion of files, evidence analysis, etc.
    - Encase, FTK(Forensics Toolkit)
    - Winhex
    - TCT(The Coroner's Toolkit)，TSK（The Sleuth Kit）

The Problems

The Problems

- TCT
  - D.Farmer and W. Venema
  - Open source
  - Released in 2000
  - 19 versions by now, the latest one is TCT-1.19
  - FreeBSD, OpenBSD, BSD/OS, SunOS, Linux, FFS, Ext2, Ext3, etc.
  - FFS, Ext2, Ext3, etc.
  - Perl 5.004 or later version and a C complier
  - Main functions

Function	Program	Description
Data Gathering	grave-robber	Automatically collecting static and dynamic data from the system
Time Analysis	mactime	Collecting and handling MAC time attributes of files
Low-Level File System Utilities	unrm	Accessing a disk block by its disk number
	icat	Accessing file content by its inode number
	ils	Accessing file attributes by its inode number
File Reconstruction	lazarus	Reconstructing the structure of deleted file content
Low-Level Memory Utilities	pcat	Dumping the memory of a running process
Other C Program	file	Determining file type
	major_minor	Listing device major and minor number
	md5	Computing the md5 checksum for each file
	lastcomm	Showing last commands executed in reverse order (applied to BSD operating system)

The Problems

- Our experiments
  - Linux 2.* operation system
    - Debian：Ubuntn9.04、Ubuntn9.10、Ubuntn10.04、Ubuntn10.10、Ubuntn11.04
    - Red Hat：Fedora13、Fedora14、Fedora15
  - File System
    - Ext3/Ext4
  - 16 experiment platforms ,more than 10,000 lines of source code

The Problems

OS Release (Kernel Version)	Release Date	Perl Version	File System	Testing Results of TCT Tool
Ubuntu9.04 (2.6.28)	2009.04	5.10.0	Ext3	Installable. Running results of icat and ils programs incorrect. Lazarus program not able to run.
			Ext4	
Ubuntu9.10 (2.6.31)	2009.10	5.10.0	Ext3	Failed to be installed. Errors appear in file /usr/include/linux/ext2_fs.h when compiling
			Ext4	
Ubuntu10.04 (2.6.32)	2010.04	5.10.1	Ext3	Failed to be installed. Errors appear in file /usr/include/linux/ext2_fs.h when compiling
			Ext4	
Ubuntu10.10 (2.6.35)	2010.10	5.10.1	Ext3	Failed to be installed. Errors appear in file /usr/include/linux/ext2_fs.h when compiling
			Ext4	
Ubuntu11.04 (2.6.38)	2011.04	5.10.1	Ext3	Failed to be installed. Errors appear in file /usr/include/linux/ext2_fs.h when compiling
			Ext4	
Fedora13 (2.6.32)	2010.04	5.10.1	Ext3	Failed to be installed. Errors appear in file /usr/include/linux/ext2_fs.h when compiling
			Ext4	
Fedora14 (2.6.35)	2010.10	5.10.1	Ext3	Failed to be installed. Errors appear in file /usr/include/linux/ext2_fs.h when compiling
			Ext4	
Fedora15 (2.6.38)	2011.04	5.10.1	Ext3	Failed to be installed. Errors appear in file /usr/include/linux/ext2_fs.h when compiling
			Ext4	

Analyzing Reasons of the Problems

Preliminary Analysis

- Ubuntu9.04：
  - Installable. Program icat, ils and lazarus have some problem.
  - icat, ils
    - Running results incorrect
    - Inspecting the internal working process of the programs and the structure of the low-level file system.
  - Lazarus
    - "$*" variable in source code of lazarus is unsupported.
    - Inspecting the Perl language and its version update state.

Running Problems

- Ubuntu9.10-11.04, Fedora 13-15：
  - Failed to be installed. The /usr/include/linux/ext2_fs.h file is said to be incorrect in compilation.
  - Inspecting the update state of the file in the operating systems.

Installation Problems

Analysis of Installation Problems

- Installing a software tool involves a large number of files and data.

  Configuration files and system environments must be taken into account.

- Taking Ubuntu 9.10 as an example to do analysis in three steps

  1. Compare.

  Reslut: Ubuntu 9.10 had updated ext2_fs.h.

  2. Modify.

  Result: problems that occur in the compiling period can be solved.

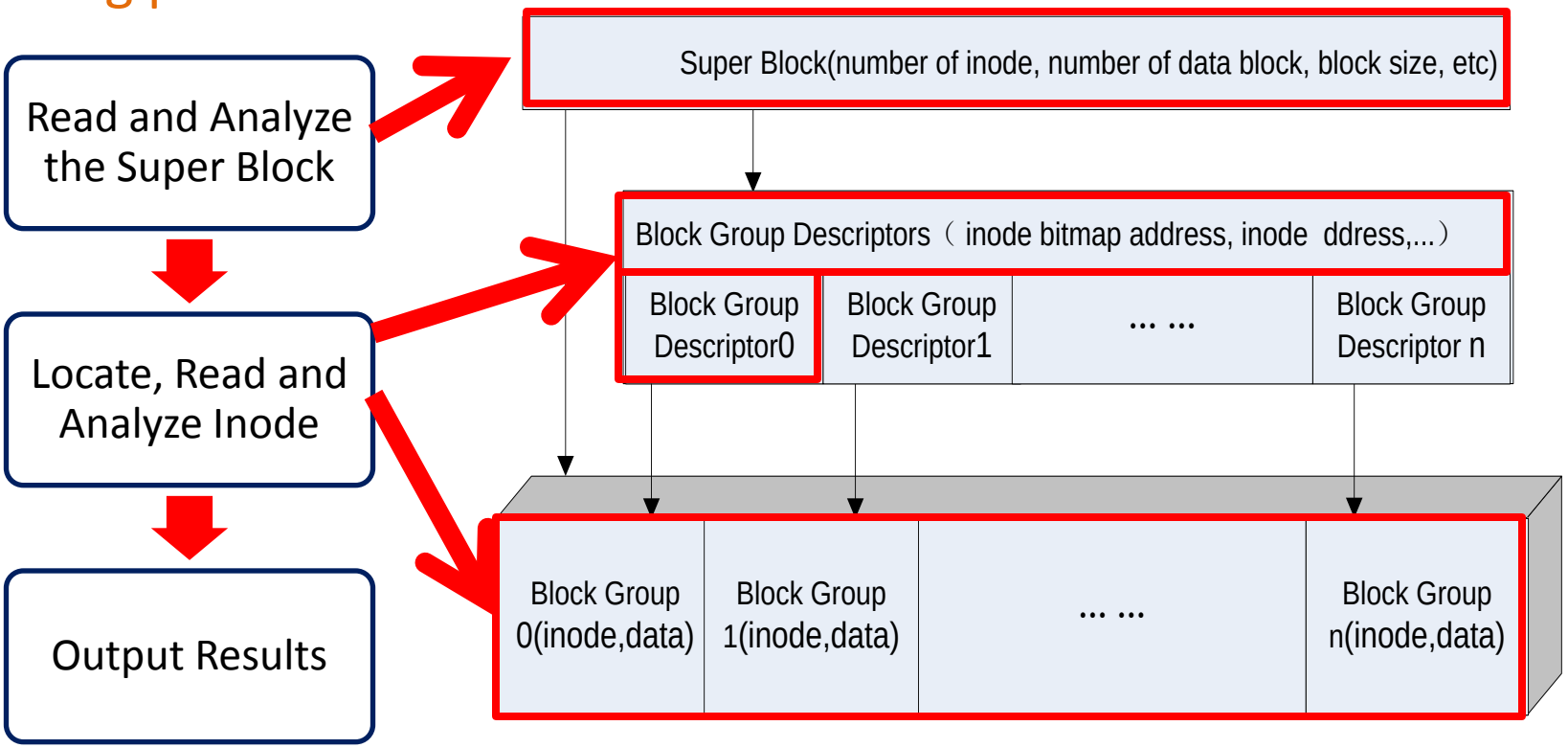
  3. Test.

  Reslut: successfully installed ,but icat and ils produce incorrect results, while lazarus can not run.

Analysis of Running Problems

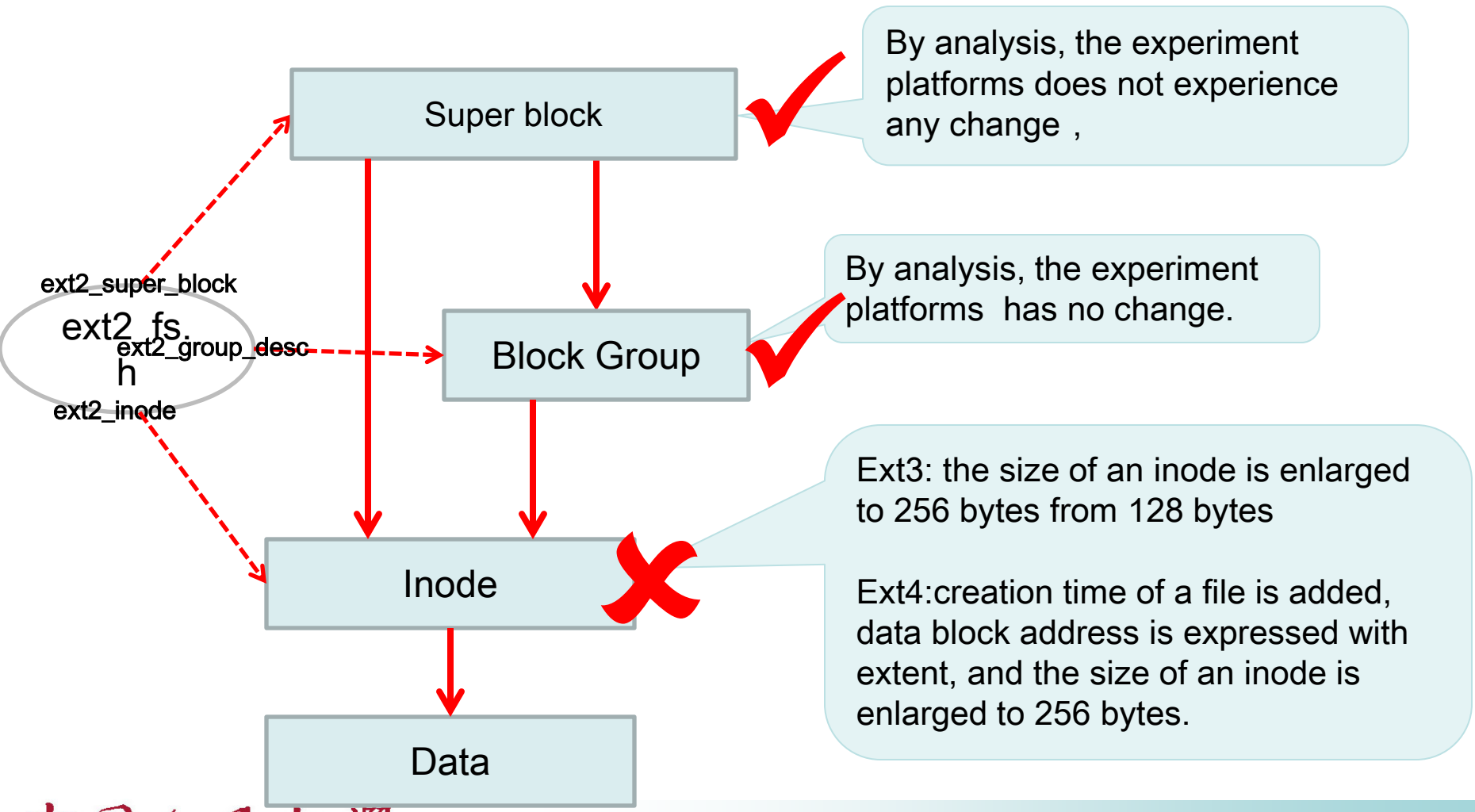
- Problems Related to File Systems: icat, ils

  Working process:



Analysis of Running Problems

- Problems Related to File Systems: icat, ils



Analysis of Running Problems

- Problems Related to Compiling Environments

Need : 5.004 or later versions.

Experiment platforms :Perl 5.10.0 or later versions.

By analyzing Perl compilers of 5.10.0 or later versions, the "$*"variable has been removed.

So, cancelation of the variable causes malfunction of the lazarus program.

Solutions to the Problems

Solutions to the Problems

Solutions to the problems have to be reasonably put forward according to reasons that cause the problems. They should be able to guide people to modify source codes of relevant programs if necessary.

Solutions to the Problems

Installation Problems:

TCT depends on certain files of the operating system. → Add a new ext_fs.h header file.

Running Problems

TCT uses system header files to determine the size of an inode. → Change the way to calculate the size of an inode.

TCT uses system header files to analyze an inode. → Add a new method to analyze inodes.

TCT need Perl compilers of earlier versions. → Substitute the "$*" variable for multiline matching.

Implementation and Test

Implementation and Test

Code Modification

The main points of our work:

(1)Add the new ext_fs.h header file to the tct-1.19/src/fstool directory.

(2)Modify the tct-1.19/src/fstools/fs_tools.h file.

(3)Modify the tct-1.19/src/fstools/ext2fs.c file.

(4)Substitute ext2 in all files with ext.

(5)Modify the tct-1.19/lazarus/lazarus file.

Implementation and Test

Testing and Results

Testing :16 platforms mentioned above.

Result: TCT tool can be properly installed at all the platforms and all the programs run correctly.

Related work and Conclusions

Related work and Conclusions

Related work

Developers: update program codes, re-analyze lower level data structures, add new functions

CFTT(Computer Forensics Tool Testing):test computer forensic tools,2003.

B. Carrier(developer of The Sleuth Kit), put forward a concept to deduce possible problems of forensics tools by using abstraction layer.

However, to solve the adaptability problems of computer forensic tools, there is still a long way to go.

Related work and Conclusions

Our work:

Take the open source TCT tool as a representative.

Anatomize the adaptability problems of software forensic tools.

Figure out the very reasons that cause the problems.

Establish solutions to the problem.

Related work and Conclusions

Conclusions

A general way to handle adaptability problems:

1. Perform preliminary analysis according to error status messages.

Identify the type of the problem.

Narrow the scope of the problem space.

Locate the target of the problem.

2. Perform detailed analysis according to the type of the problem.

Key issues: system configuration files , lower level data structures, compiler.

Thank you !
Q&A

zhaihaohao520@126.com