The LogReport Annual Report 2004

Joost van Baal

Wytze van der Raay

Table of Contents

1. Introduction **1**

2. Activities in 2004 .... **1**

2.1. Introduction 2

2.2. People 2

2.3. The LogReport server 2

2.4. Lire Software Releases 3

2.5. Statistics 6

2.6. Looking back, looking ahead 8

1. Introduction

Log files are often treated like a wasteful by-product of IT activity: they sit somewhere in a dark corner of a computer system and are only examined occasionally, usually in case of after-the-fact reactive problem solving. This is unfortunate. Log files contain the traces of computer activity, and by intelligently analyzing these traces one can learn a lot about the behavior of a system and its users.

Log file analysis is both an essential and tedious part of system administration. It is essential because it's the best way of profiling the usage of the service installed on the network. It's tedious because programs generate a lot of data and tools to report on this data are unavailable or incomplete and when such tools exist, they are specific to one product, which means that you can't compare your Qmail and Exim mail servers.

The Stichting LogReport Foundation, a non-profit foundation, founded August 2000, detected this flaw in system administration and chose to serve a dual purpose: developing and maintaining Lire, our Open Source reporting and analysis software, and serving as a nexus of documentation, ideas, and thought on the topic of log files and their potential applications.

2. Activities in 2004

2.1. Introduction

We report on the activities of the LogReport team during 2004, the LogReport Foundation's fourth and last full year.

A more in-depth overview of what's presented in this document, specifically on Lire development, can be found in the Lire NEWS[1] file, as well as in the various Lire roadmap documents, as shipped with the Lire releases during the year[2]. A *very* detailed journal of changes in Lire is in the Lire ChangeLog[3] file. Some highlights can be found on the LogReport history page[4] too.

2.2. People

The main task of the LogReport team is maintenance and development on Lire, LogReport's Free Software tool for performing an integrated analysis of all ones Internet and Intranet Services. Lire does this by automatically generating useful reports from raw logfiles from various services. Next to this work, the team has taken care of administering the LogReport server, hibou.logreport.org. The following changes in the LogReport staff have occured during the year.

Since August 19, 2003, Francis Lacoste together with Wolfgang Sourdeau are paid for their work on Lire; the contract specifies a Lire 2.0 release, and is valid till full completion of such a release.

Next to these people, involved in the LogReport project by having access to the LogReport server, or being on the <`logreport@logreport.org`> alias, are: Joost van Baal, Wessel Dankers, Wytze van der Raay, and Egon Willighagen. (In September 2003, Josh Koenig left the project.)

During 2004, the LogReport board consisted of Joost van Baal (chairman), Wytze van der Raay (treasurer) and Jakob Schripsema (secretary). Teus Hagen is an advisor to the board.

2.3. The LogReport server

The machine hibou.logreport.org hosts our website http://logreport.org/, provides the public LogReport Online Responder service, handles our email, and hosts the 4 public mailinglists <`commit@logreport.org`>, <`announcement@logreport.org`>, <`questions@logreport.org`> and <`development@logreport.org`>. Furthermore, it hosts a CVS repository for version control of non-public documents and hibou's configuration data. The Lire code development is done using CVS on SourceForge.

Since March 2004, hibou is offering its services via IPv6 too.

The server is hosted in Amsterdam, The Netherlands: The NLnet Labs foundation[6] has offered LogReport a space in their machine room and free access over NLnet Labs' high-speed internet connection.

Until late November 2004, Guus Sliepen hosted download.logreport.org. It is now hosted on the LogReport server (hibou) itself.

2.4. Lire Software Releases

Lire is available in .tar.gz source package format, as RPM package to facilitate installation on RPM-based systems like Red Hat Linux[7] and Mandrake Linux[8], as Debian package for installation on Debian GNU/Linux[9], and as a FreeBSD port package[10].

It is possible to install/upgrade Lire RPMS using apt-rpm[11] from the LogReport server.

Wolfgang Sourdeau maintains the Lire Debian package[12]. Lire will very likely get shipped with the Debian 'sarge' release. Edwin Groothuis[13] maintains the Lire FreeBSD port[14], and Oden Eriksson from mandrakesoft.com maintains the Mandrake Linux RPM. Lire will get shipped with Mandrake Linux 10.2.

Lire is free in both senses of the word: it is available gratis for download from the internet, and it is Free Software: it is licensed using the GNU General Public License[15]. This means, among other things, anybody is free to study how the program works, and adapt it to ones needs; anybody is free to redistribute copies; and anybody is free to make modifications to the code, and to publish these modifications. During 2004, the copyright on the major part of the code was held by Stichting LogReport Foundation. See also the Lire Contributor Guidelines[16] for more information on licensing related issues.

In the year 2004, the following Lire versions have been released:

Table 1. Lire releases

release date	version (filename)
January 7, 2004	Lire 1.4.1: Bugfix release for Lire 1.4 (`lire-1.4.1.tar.gz`, RPM packages for Red Hat Linux 8.0 and Red Hat Linux 9.0, Debian GNU/Linux packages for Debian unstable and sarge)
February 29, 2004	Lire 1.4.1 FreeBSD port
March 10 - March 12, 2004	Lire 1.4.1-2, 1.4.1-3 and 1.4.1-4: Debian package bugfixes

release date	**version (filename)**
April 12, 2004	Lire 1.5 (`lire-1.5.tar.gz`, RPM packages for Red Hat Linux 9.0, Debian GNU/Linux packages (1.5-1 - 1.5-4), FreeBSD port)
June 30, 2004	Lire 1.5-5: Debian package bugfixes
August 30 - September 3, 2004	Lire 2.0rc1, Lire 2.0rc2, Lire 2.0 (`lire-2.0.tar.gz`, RPM packages for Fedora Core 2, Debian GNU/Linux packages for Debian unstable and sarge)
October 9, 2004	Lire 2.0.1: bugfix release (`lire-2.0.1.tar.gz`, RPM packages for Fedora Core 2, Debian GNU/Linux packages for Debian unstable and sarge)
October 11 - October 15, 2004	Lire 2.0 and 2.0.1 FreeBSD port
December 2, 2004	Lire 2.0.1 is shipped with development snapshots of the upcoming Mandrake Linux 10.2 releases, in the contrib section. `lire-2.0.1-1mdk.noarch.rpm`, `lire-docs-2.0.1-1mdk.noarch.rpm` (No source RPMs seem to be available from the mandrake mirrors.)

We list the main improvements in the various releases, as posted on the LogReport Announcement list[17]. A more detailed overview is in the NEWS file, as distributed with Lire.

Within Lire, we use the term *service*. A service coincides with one well-defined log file format. So, a service generally coincides with one application: the *sendmail* service handles sendmail log files. However, a lot of webservers use W3C defined formats, and a lot of commercial firewalls use the WELF format. Therefore, *w3c_extended* and *welf* are services. Each service has its *2dlf-convertor*, to convert the log file to the more generic Lire DLF format. We provide e.g. **sendmail2dlf** and **w3c_extended2dlf**. A *superservice* is a class of services which share the same DLF format, and which will generally give the same reports.

Lire 1.5

Lire 1.5 came with completed Internationalisation support, and offered a Lire Store configuration framework.

- Store configuration is done with the new Curses-based command: lire. (This replaces the old lr_config command.)

- Lire 1.5 has a full fledged internationalisation framework. One nice side-effect of i18n is that Lire now supports non-ascii log files. Furthermore (and of course) many Lire commands are internationalised, so that translation user output to native languages is much easier.
- The configuration framework is more flexible.

Support for RTF output was dropped in 1.5. See the Lire 1.5 release page[18] for more information.

Lire 2.0

With release 2.0, Lire no longer needs DocBook and other extra XML tools for any output format. Furthermore:

- New output formats LaTeX, DVI and PS added.
- Much better looking HTML output.
- Three new chart types are supported; charts are much more configurable through the lire(1) command.
- All report configurations are editable through the lire(1) command.
- It is now possible to report on more than one superservice in a single report.
- As always, lots of bugfixes and documentation updates and improvements.

Support for DocBookXML output was dropped. The Lire 2.0 release has undergone extensive testing on Debian, Fedora[19], and Solaris 2.9. See the Lire 2.0 release page[20] for more information.

Lire 2.0.1 was mainly a bugfix release. As previous versions, this version supports up to 39 different log file formats. The complete list of supported output formats for Lire 2.0.1 is:

- Excel 95 spreadsheet
- PDF, PostScript
- HTML, XHTML
- Plain ASCII
- LaTeX, DVI
- XML

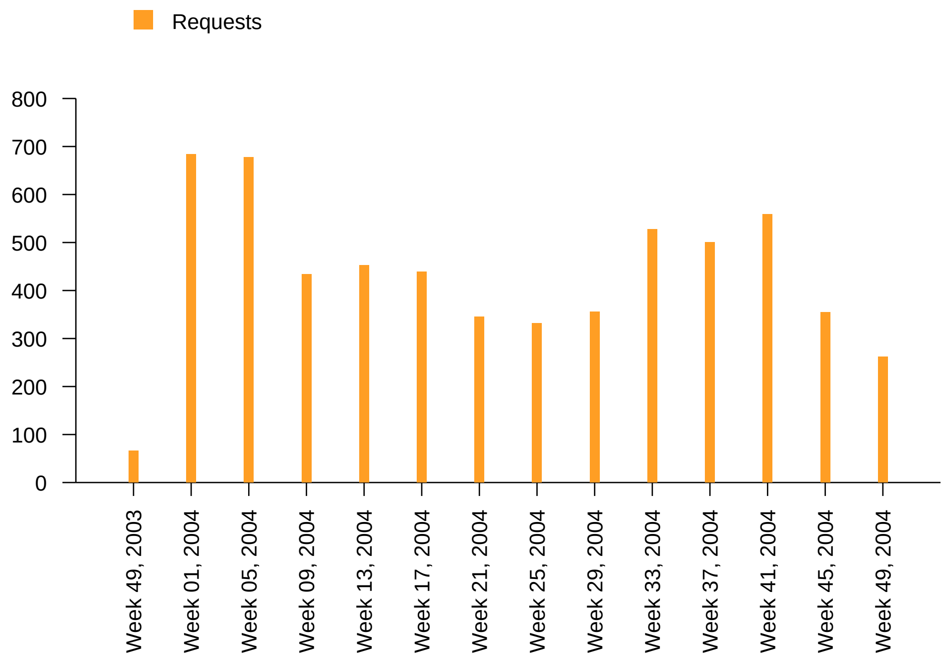
For XML, (X)HTML, PostScript and PDF, images in PNG, JPG, EPS or GIF can be included (depending on ploticus support).

2.5. Statistics

We show some statistics, giving some indications about the work done by the LogReport team, as well as about the effectiveness of this work.

2.5.1. Downloads and installs

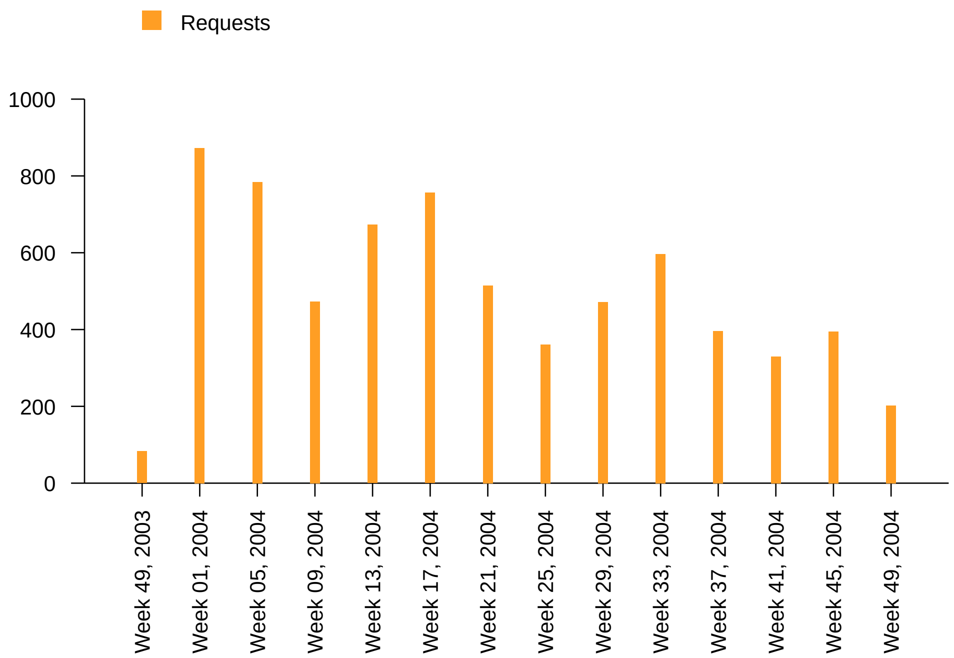
We do have figures about the number of downloads from our webserver. They're depicted in the graphic.



Number of Lire tarball downloads from http://logreport.org/ in 4-week periods during 2004.

The number of tarball downloads was reasonably steady during the year. We have been doing slightly better in 2003 though: in that year, all 4-week periods had more than 500 downloads, and in that year, we've had 2 periods with more than 1000 downloads. However, beware: we've seen some IPs downloading *all* files from our server: spam-like behaviour. Very likely, this is not traffic caused by interested Lire users. We've filtered the obvious non-legitimate traffic from our logs before generating the statistics.

RPM downloads



Number of Lire RPM package downloads from http://logreport.org/ in 4-week periods during 2004.

The number of RPM downloads was slightly less than in 2003, but still very substantial. Like in 2003, we've had more than 300 downloads in every period. However, in 2003 we've had over 800 downloads during 3 periods while in 2004 we've had this happening in only one of the 4-week periods.

Based on number supplied by the Debian Popularity Contest[21], combined with subscribtion numbers[22] of Debian mailing lists , the number of people who've installed a Lire Debian package has been between 500 and 600 during 2004.

The number of downloads of Lire package directly from SourceForge during 2004 was not substantial.

2.5.2. Submits to the LogReport Online Responder

During the entire year, we've been running a so called Online Responder on <`log@<service>.logreport.org`>. People can send their log files via email or submit them via a web page, and get a report back.

Due to abuse by spammers of this service, it's not possible to give reliable statistics on its legitimate usage.

2.5.3. CVS Commits to the Lire code

There are between 100 and 300 commits on the Concurrent Version System holding the Lire code done monthly during 2004, for a total of 1540 (was 1148 in 2003). This number represents the number of changes to the Lire code. (Beware: the size and impact of one change can vary a lot! Therefore, these number are to be interpreted cum grano salis.)

2.5.4. Traffic on the LogReport mailing lists

During the year, the number of external people subscribed to the announcement mailing list grew from about 200 to about 300. (Early 2002, we had 24 announcement subscribers, early 2003: 90.) Subscribers on the development list grew from 40 to 50 (30 early 2003), while the number of subscribers on the questions list grew from 90 to 100 (was 50 early 2003). The steady growth in interest in LogReport and Lire achieved in 2003, has been continued in 2004. We're very happy with these numbers: this surely gives confidence in Lire's future!

Via the lists, The LogReport developers have been contacted by lots of ISP's, network hardware manufacturers, players in the Financial and Industry markets as well as people working for Educational institutions and Universities, suggesting improvements and reporting bugs. See the questions[23] and development list archives[24] for the raw data.

Unfortunately, no substantial contributions of code have been received in 2004.

2.6. Looking back, looking ahead

2.6.1. Comparing 2003 and 2004

As in 2003, in 2004, LogReport development was mainly done by two developers: nearly all code contributions were done by Francis and Wolfgang, while the rest of the team was very much in the background. Most of the activities in 2004 were as agreed upon late 2003 in the Lire 2.0 roadmap, and layed down later in a formal contract. As said, the extended community did not supply as much code contributions as in 2003. We will not speculate about the causes for this in this document.

Still the LogReport community was vivid: the number of mailing list subscribers is still growing. The LogReport board is very grateful and would like to thank the 2004 LogReport team, for this amazing achievement.

2.6.2. LogReport Future

At the November 11, 2004 Board meeting, it was decided the LogReport Foundation will be dismantled at December 30, 2004: a formal foundation framework is deemed no longer needed after the 2.0 release. Indeed, requirements for 2.0, as layed down in the last contract made by the foundation, were aimed at making it even more easy to extend Lire for one's own site-specific needs.

With the dismantling having taken effect, no activities from the formal LogReport Foundation are expected after the release of Lire 2.0. However, with the Lire 2.0 framework in place, and given the stable and growing Lire user base, we foresee a bright future for the Lire Free Software product. We look forward to see further community-contributed evolution, but also to see e.g. consultants offering tailor-made solutions based on the Lire 2.0 framework.

Notes

1. http://download.logreport.org/pub/current/NEWS
2. http://download.logreport.org/pub/archive/
3. http://download.logreport.org/pub/current/ChangeLog
4. http://logreport.org/oldnews.php
5. http://logreport.org/
6. http://www.nlnetlabs.nl/
7. http://www.redhat.com/
8. http://www.mandrakelinux.com/
9. http://www.debian.org/
10. http://www.freebsd.org/ports/
11. http://apt4rpm.sourceforge.net/
12. http://packages.debian.org/lire
13. http://www.mavetju.org/

14. http://www.freebsd.org/cgi/cvsweb.cgi/ports/sysutils/lire/
15. http://www.gnu.org/copyleft/gpl.html
16. http://logreport.org/dev/guidelines.php
17. http://logreport.org/contact/lists/announcement/
18. http://www.logreport.org/lire/lire15.php
19. http://fedora.redhat.com/
20. http://www.logreport.org/lire/lire20.php
21. http://popcon.debian.org/
22. http://lists.debian.org/stats/
23. http://logreport.org/contact/lists/questions/
24. http://logreport.org/contact/lists/development/

3. Official Information

Stichting LogReport Foundation has been established on August 21, 2000 in Eindhoven, The Netherlands. The goal of the foundation is:

a. to develop, maintain and distribute tools and knowledge for processing log files of network/computer system applications and for generating reports based on such log files;

b. to stimulate the use of the tools and knowledge mentione above for the management of information systems;

c. to stimulate authors of network/computer system applications to incorporate provisions in these applications for generating useful standardised and automatically processable information in log files;

d. to contribute to the development and implementation of product-independent log file formats (standards);

e. to create a forum for system administrators and software developers in the area of the application and analysis of log file information; and

f. anything which is directly or partly related to the above, or can be beneficial to the above, in the widest sense.

3.1 Board

The board of Stichting LogReport Foundation consists of three members:

Joost van Baal	chairman
Jakob Schripsema	secretary
Wytze van der Raay	treasurer

Teus Hagen (chairman and board member until mid-2003) was retained as advisor to the board, and attended all board meetings.

Three board meetings were held in 2004:

date	*place*
January 15, 2004	Ede
June 10, 2004	Eindhoven
November 11, 2004	Ede

3.2 Employees

The foundation has not employed any staff during 2004. But a number of freelancers abroad have performed paid remote development work for the foundation:

Francis Lacoste	Canada	June 2001 - October 2004
Wolfgang Sourdeau	Canada	September 2003 - May 2004

In addition, a number of volunteers have performed various tasks for the foundation.

3.3 Administration

The responsibility for day-to-day administration, handling of payments and other similar activities rests with Joost van Baal. The bookkeeping function has been taken care of by Wytze van der Raay, treasurer of the foundation.

3.4 Fiscal year

The fiscal year of Stichting LogReport Foundation coincides with the calendar year. Thus the (fifth) fiscal year of the foundation ran from January 1, 2004 until December 31, 2004.

3.5 Fiscal position

Based on its current activities, the foundation is not taxable for Dutch corporate tax ("vennootschapsbelasting") or value-added tax ("BTW").

On November 28, 2000, Stichting LogReport Foundation has been recognised by the Dutch fiscal authories as an organisation working for the general benefit ("algemeen nut beogende instelling") as meant in article 24, paragraph 4 of the Dutch Inheritance Act 1956.

3.6 Termination of foundation

In the board meeting of November 11, 2004, the board has decided to dissolve Stichting LogReport Foundation per December 30, 2004. Joost van Baal has been nominated as keeper of the administration of the foundation. Thus this is the last annual report of Stichting LogReport Foundation.

In order to fullfil the goals of the foundation in the best way after its termination, the board decided to:

- transfer the copyright ownership, logreport.org domain name and fully depreciated LogReport server hardware to Stichting NLnet, who has enabled LogReport to achieve what it has achieved in the past five years, and who can be trusted to continue and protect the free LogReport software and service in the best possible way;
- donate the remaining funds of € 346.43 to SPI (Software in the Public Interest) in support of the Debian project, the primary free software development platform for the LogReport software.

4. Financial Statements

4.1 Balance Sheet per December, 31 2004 (after result allocation)

	2004		2003	
	€	€	€	€
Fixed assets				
Material fixed assets				
Computer equipment		0.00		428.39
Current assets				
Accounts receivable				
Interest to be received		0.00		0.00
Costs paid in advance		0.00		0.00
Cash		0.00		31,213.64
		0.00		31,642.03
Own capital		0.00		31,455.83
Short-term liabilities				
Accounts payable	0.00		116.48	
Taxes and social charges	0.00		(1.68)	
Other liabilities	0.00		71.40	
		0.00		186.20
		0.00		31,642.03

4.2 Profit and Loss Account 2004

	2004		2003	
	€	€	€	€
Other income				
Donations received		0.00		43,000.00
Other expense				
Payroll expenses	0.00		9,760.98	
Depreciation of material fixed assets	428.39		161.76	
Other operational expenses	31,282.50		26,472.02	
		31,710.89		36,394.76
		(31,710.89)		6,605.24
Interest earned	255.37		125,84	
Interest paid	(0.31)		0.00	
		255.06		125,84
Gross result from regular operations before tax		(31.455.83)		6,371.08
Tax		0.00		0.00
Net result		(31.455.83)		6,371.08

4.3 General explanations

4.3.1 Basis for valuation and result determination

Assets and liabilities
Unless stated otherwise, assets and liabilities have been stated at their nominal values.

Material fixed assets
Material fixed assets have been stated at historical cost price, reduced with depreciation calculated linearly based on the estimated total useful life of the corresponding fixed asset.

4.3.2 Result determination

General
The following holds with respect to items included in the operational result: profits are only included if and for the part they have been realized in the reporting period, and losses and risks have been taken into account inasmuch they originate before the end of the reporting period.

4.4 Amplification of the Balance Sheet 2004

4.4.1 Material fixed assets

The material fixed assets can be specified as follows:

	Inventory	Computer-equipment	Total
	€	€	€
January 1, 2004			
Procurement costs	0.00	3,476.89	3,476.89
Cumulative depreciation	0.00	(3,048.50)	(3,048.50)
Book value	0.00	428.39	428.39
Changes			
Desinvestments	0.00	0.00	0.00
Investments	0.00	0.00	0.00
Depreciation	0.00	(428.39)	(428.39)
Depreciation desinvestments	0.00	0.00	0.00
		(428.39)	(428.39)
December 31, 2004			
Procurement costs	0.00	3,476.89	3,476.89
Cumulative depreciation	0.00	(3,476.89)	(3,476.89)
Book value	0.00	0.00	0.00
Depreciation percentage	20%	33-50%	

4.4.2 Cash

Cash is kept on a business giro account and an associated savings account ("Kapitaalrekening") at Postbank N.V.

	2004	2003
	€	€
Postbank giro account	0.00	31,213.64
Postbank Kapitaalrekening	0.00	0.00
	0.00	31,213.64

As a result of the termination of the foundation, all its bank accounts have been closed.

4.4.3 Own capital

Reserve fund

The course is as follows:

	2004	2003
	€	€
Value per January 1	31,455.83	24,724.75
Plus: net result	(31,455.83)	6,731.08
Value per December 31	0.00	31,455.83

4.4.4 Short-term liabilities

Taxes and social charges

	2004	2003
	€	€
Salary tax	0.00	0.00
Social charges bedrijfsvereniging	0.00	(1.68)
	0.00	(1.68)

Other liabilities

	2004	2003
	€	€
Salary administration expenses	0.00	71.40
	0.00	71.40

4.4.5 Liabilities not shown in the balance sheet

None.

4.5 Amplification of the Profit and Loss Account 2004

4.5.1 Income

The only income over 2004 was obtained from interest payment on a Postbank savings account. Due to the pending termination of operations, no new donations have been pursued in 2004.

4.5.2 Payroll expenses

	2004	2003
	€	€
Staff salaries	0.00	8,510.60
Social charges	0.00	1,250.38
	0.00	9,760.98
Staff salaries		
Salaries	0.00	7,866.00
Salary tax on savings salary	0.00	15.32
Holiday allowances	0.00	629.28
	0.00	8,510.60
Social charges		
Social charges	0.00	1,076.69
ARBO service	0.00	173.69
	0.00	1,250.38

4.5.3 Other operational expenses

	2004	2003
	€	€
Other staff expenses	30,400.00	22,388.10
Office expenses	5.50	3,139.65
General expenses	877.00	944.27
	31,282.50	26,472.02
Other staff expenses		
Travel expenses volunteers	0.00	25.10
Cost of freelancers	30,400.00	22,363.00
	30,400.00	22,388.10

	2004	**2003**
	€	€
Office expenses		
Forwarding charges	5.50	0.00
Internet expenses	0.00	3,139.65
	5.50	3,139.65

General expenses		
Subscriptions & contributions	28.10	28.39
Accountancy fees	0.00	452.15
Travel expenses board	161.98	297.88
Other board expenses	225.75	72.20
Representation costs	17.64	0.00
Donations	346.43	0.00
Bank expenses	95.41	94.23
Calculation differences	1.68	(0.58)
Payment differences	0.01	0.00
	877.00	944.27

4.5.4 Interest earned

	2004	**2003**
	€	€
Credit interest Postbank Kapitaalrekening	255.37	125.84
	255.37	125.84

4.5.5 Interest paid

	2004	**2003**
	€	€
Debet interest Postbank giro account	0.31	0.00
	0.31	0.00

4.6 Allocation of net result 2004

The net loss over 2004 ad € 31,455.83 has been subtracted from the reserve fund. The reserve fund has thus reached a value of zero.

4.7 Profit and Loss Account 2000 - 2004

We include a consolidated profit and loss account over the lifetime of Stichting LogReport Foundation to provide a complete picture of its financial operations history.

		2000 - 2004	
		€	€
Other income			
Donations received			291,554.32
Other expense			
Staff salaries	92,496.88		
Social charges	12,784.87		
Payroll expenses		105,281.75	
Travel expenses staff	3,494.85		
Travel expenses volunteers	607.04		
Compensation volunteers	76.00		
Cost of freelancers	152,973.00		
Other staff expenses		157,150.89	
Office expenses	14,190.85		
General expenses	13,673.17		
Other operational expenses		27,864.02	
Depreciation of material fixed assets		3,476.89	
			293,773.55
			(2,219,23)
Interest earned	2,220.39		
Interest paid	(1.16)		
			2,219.23
Gross result from regular operations before tax			0.00
Tax			0.00
Net result			0.00