ANÁLISE DE PROGRAMAS: ESTUDO DE CASO DA FERRAMENTA CASE OPEN SOURCE

Nathalia Lais Mazotti, Sarah Mansur Resende de Miranda, Caroline Vilela Momenté, Shigueo Nomura
Universidade Federal de Uberlândia, Faculdade de Engenharia Elétrica, Uberlândia- MG
nathalia.lmazotti@hotmail.com, sarahmansur94@hotmail.com, carol_momente@hotmail.com, shigueonomura@feelt.ufu.br

***Resumo* - O objetivo deste trabalho é estudar e analisar tecnicamente as ferramentas CASE para análise de programas destacando-se o ClamWin Free Antivirus. O trabalho visa também difundir o conhecimento a respeito da análise de programas, seus conceitos, aplicações e benefícios que o seu usuário pode usufruir. Programas de limpeza e antivírus são apresentados como bons exemplos de sistemas que realizam a tarefa de analisar, avaliar e/ou verificar um conteúdo desejado pelo usuário. A ferramenta escolhida ClamWin Free Antivirus é um software que possui propostas interessantes com relação à manutenção do computador e ao bom funcionamento do sistema. A aplicação prática da ferramenta e a análise e discussão dos resultados levaram a concluir que o produto possui muitas vantagens em relação aos concorrentes como facilidade de instalação e manuseio, utilização de pouco espaço de memória, oferecimento de código aberto e alta popularidade entre vários usuários.**

***Palavras-Chave* - Análise de programas, antivírus, ferramentas CASE, programa de limpeza, software.**

PROGRAM ANALYSIS: A CASE STUDY FOR OPEN SOURCE CASE TOOL

***Abstract* - The objective of this work is to study and analyze the CASE tools for program analysis focusing on ClamWin Free Antivirus. Also, the work aims for spreading the knowledge on program analysis, its concepts, applications and benefits to be enjoyed by users. Cleaning programs and antivirus are presented as good examples for systems that perform tasks of analyzing, evaluating and/or searching for the desired content by the user. The selected ClamWin Free Antivirus tool is software with interesting purposes related to the computer maintenance and good work of system. The practical application of the tool and the analysis/discussion of results led to conclude that the product has several advantages in relation to its competition products such as easy installation and utilization, a little memory space requirement, open source providing and high popularity among various users.** 1

***Keywords* – Antivirus, CASE tools, cleaning program, program analysis, software.**

NOMENCLATURA

CASE *Computer- Aided Software Engineering*.
HD *Hard Disk*.
USB *Universal Serial Bus*.

I. INTRODUÇÃO

Analisar um programa é uma tarefa extremamente importante quando se preza o bom funcionamento do computador. Existem males que podem danificar até o *hardware* e acarretar um alto custo de conserto, ou até mesmo impossibilitar o uso de alguma peça, fazendo com que ela seja substituída.

Infelizmente, não é possível prever com exatidão o momento em que o computador irá apresentar algum problema de funcionamento. A utilidade das ferramentas CASE em questão está no objetivo de manter o bom funcionamento desse computador como um todo.

As ferramentas CASE para Análise de Programas [1] verificam os componentes desejados e buscam erros que comprometem o bom funcionamento dos programas ou do computador como um todo.

Essa análise pode ser feita em um arquivo específico do computador escolhido pelo usuário, ou também se pode analisar o computador totalmente, todos os seus programas e arquivos. As ferramentas que desenvolvem essa análise podem, além de analisar, fornecer ao usuário soluções viáveis para a correção do problema encontrado.

Existem ferramentas desenvolvidas para este fim que precisam ser acionadas para poderem funcionar, ou seja, a ferramenta não irá analisar um determinado arquivo sem que essa análise seja solicitada, falha essa que pode gerar problemas para o computador [2].

II. FUNDAMENTOS TEÓRICOS

A busca por erros é feita através de comparações dos arquivos suspeitos com os arquivos ruins que já foram detectados. O antivírus, por exemplo, é uma ferramenta CASE que utiliza essa comparação para detectar os vírus através da sequência de códigos que identifica cada arquivo [3].

Os antivírus possuem um banco de dados, onde ficam armazenadas as "assinaturas" dos vírus já conhecidos. Para identificar um vírus, o antivírus compara a sequência de códigos do arquivo suspeito com os códigos dos vírus que estão no banco de dados, e se o código do arquivo possuir

XI CEEL – ISSN 2178-8308
25 a 29 de novembro de 2013
Universidade Federal de Uberlândia – UFU
Uberlândia – Minas Gerais – Brasil

alguma semelhança com os que estão no banco de dados, esse arquivo será considerado uma ameaça [3].

Novos tipos de vírus vão surgindo com o tempo, e por esse motivo é importante que o antivírus seja atualizado sempre que necessário, pois podem surgir vírus cujo código não esteja no banco de dados, fazendo com que o programa não os reconheça.

O tema em questão aqui é ferramentas CASE que analisam programas. Essas ferramentas são responsáveis pela análise desde uma busca por erros no computador, arquivos que foram duplicados ocupando espaço desnecessário no HD, *cookies* e *caches* de Internet armazenados, *logs*, arquivos infectados por vírus, *malwares, spywares*, enfim, tudo o que pode ser desnecessário para o seu computador, deixando seu processamento mais lento. A maioria dos programas ainda exibe um relatório com tudo que foi vasculhado em seu sistema e oferece a solução para alguns dos problemas encontrados.

III. CARACTERÍSTICAS DAS FERRAMENTAS CASE

A. Programa de Limpeza

O computador cria arquivos novos diariamente para armazenar informações do sistema, registros de programas instalados e desinstalados, e dados de *backup*. Esses arquivos temporários de funcionamento muitas vezes não são excluídos após o uso e acabam sobrecarregando o disco rígido, tornando o processamento lento. Erros de programas, *cookies* de navegador, desinstalações mal sucedidas e arquivos que foram removidos, mas que ainda ocupam espaço no HD também fazem partes desse pacote de arquivos e programas que comprometem o bom funcionamento do sistema [4].

Para solucionar esse problema foram criados programas de limpeza, que tem como principal função fazer uma varredura no computador, excluindo tudo que não é necessário, assim, abre-se espaço para armazenamento de dados e aumentando a velocidade de processamento [5].

Atualmente o mercado está repleto de grandes sistemas como o CCleaner, PrivaZer, Registry Winner**,** MVRegClean e Glary Utilities.

O CCleaner é um dos exemplos mais completos desse tipo de *software*, com suporte operacional para Windows e Mac e por isso acabou sendo um dos programas de limpezas mais recomendados em fóruns da Internet. Sua principal função é a eliminação de conteúdos desnecessários que foram mantidos pelo sistema operacional, tais como histórico de navegação, arquivos duplicados, programas que não foram desinstalados completamente e também a exclusão de todos os arquivos deletados que continuam ocupando espaço no HD [6].

A "limpeza" que o CCleaner faz no sistema operacional, deixa o computador mais rápido e elimina quase que totalmente tudo que não é necessário no sistema [4].

B. Antivírus

Diferentemente dos programas de limpeza, que fazem varreduras no HD procurando arquivos sobressalentes e desnecessários, os antivírus são programas que tem o intuito de prevenir, detectar e às vezes eliminar vírus, que são programas maliciosos, que fazem cópias de si mesmo e tentam se espalhar para outros computadores invadindo o sistema operacional [7].

Existem muitos produtos no mercado, onde o diferencial está no suporte técnico oferecido e nas camadas de proteção. Nenhum antivírus é totalmente seguro, visto que os vírus podem sofrer "mutações" e vírus novos surgem constantemente. Por isso a manutenção e o *backup* são de extrema importância se o usuário presa por segurança [7].

Alguns exemplos de antivírus altamente competentes no mercado são o Avast! Antivírus, Eset Nod32, Norton e ClamWin [8].

O único modo de ficar imune aos *malwares* é isolando totalmente o computador, ou seja, não usar a Internet e dispositivos externos, como CDs, DVDs e *pendrives*.

IV. COMPARAÇÃO ENTRE FERRAMENTAS CASE

Os programas de limpeza têm como principal propósito remover itens desnecessários ou redundantes presentes no computador. Enquanto isso, os antivírus em geral são programas que têm como função primordial a identificação de ataques de vírus e muitas vezes sua remoção. Cada programa de limpeza possui sua peculiaridade, apesar de suas funções principais serem as mesmas na maioria dos casos, assim como acontece com os antivírus. Ambas as ferramentas realizam varreduras no sistema, melhorando seu desempenho e aumentando sua velocidade de processamento, além de melhorar a vida dos usuários e lhes permitir maiores facilidades e segurança. A Tabela I resume as características das ferramentas CASE em questão.

Tabela I - Comparação entre as Ferramentas CASE

Itens comparados	***Antivírus***	***Programa de limpeza***
Realização de varreduras no computador	X	X
Prevenção contra vírus	X	
Eliminação de vírus	X	
Aumento da velocidade de processamento	X	X
Melhoria da qualidade de vida do usuário	X	X
Detecção de vírus	X	
Eliminação de programas e arquivos desnecessários		X

V. JUSTIFICATIVAS DA ESCOLHA DE UMA DAS FERRAMENTAS CASE

O exemplo de ferramenta CASE escolhida é o antivírus *ClamWin Free Antivírus* devido à facilidade de instalação e manuseio. Ainda, ele possui código aberto, podendo ser aprimorado por qualquer usuário. Também, utiliza pouco espaço de memória. Devido a essas vantagens, a ferramenta foi escolhida para análise neste trabalho.

Uma outra razão da escolha se deve ao grande número de usuários dessa ferramenta. Assim, surge a motivação para

verificar a sua eficiência, através de estudos e testes simples como um escaneamento, por exemplo.

Além disso, um antivírus é fundamental para a proteção contra ações de programas malignos, conservação do bom funcionamento do sistema operacional e proteção das informações armazenadas no computador. Dessa forma, com a aplicação adequada do antivírus se consegue maior confiabilidade e menor vulnerabilidade dos sistemas.

VI. DETALHAMENTO TÉCNICO DA FERRAMENTA CASE ESCOLHIDA

O *ClamWin Free Antivírus* é um programa de *software* livre, ou seja, de código aberto, onde qualquer pessoa pode enviar os vírus detectados e as amostras de *spyware*, testar a versão mais recente do programa, encontrar os erros e enviar os *bugs* e as solicitações de recursos, melhorar sua documentação e promovê-lo na Internet e na imprensa. Caso o usuário seja um desenvolvedor *C++* ou *Python*, ele poderá juntar-se ao projeto do programa e ajudar a melhorá-lo [8].

Ocupando cerca de 45.8 Mb na memória do computador, ele tem como base o código-fonte do programa ClamAV, implementando uma interface gráfica sobre este. Além disso, funciona gratuitamente para o Windows Vista/ Server XP/ Me/ 2000/ 98/ 7/ 2008 e 2003 [8].

O programa possui guia e documentos para que os usuários possam usá-lo e integrá-lo com outros programas, por exemplo, recursos Anti Malware, WinZip ClamWin e o programa na versão portátil em uma unidade USB ou removível [8].

O programa também realiza uma busca minuciosa com altas taxas de detecção de vírus e *spyware*; possui *Scanning Scheduler*, que funciona como um agendador de tarefas; *upgrades* automáticos de banco de dados de vírus atualizados constantemente; realiza escaneamento de vírus autônomo e integração com a *Microsoft Windows Explorer*; *Addin* é um controle *Activex* que trabalha dentro do *Microsoft Outlook* para remover vírus anexos infectados automaticamente. É importante lembrar que o *ClamWin Free Antivírus* não trabalha em tempo real, ou seja, você precisa procurar manualmente um arquivo para que ele possa passar por análise de vírus ou *spyware* [8].

VII. MANUAL DE USO DA FERRAMENTA

O manual de uso da ferramenta se encontra na versão em inglês, e é disponibilizado no momento em que você instala o programa. Por ser um programa simples e de fácil compreensão, seu manual é rico em informações citadas e explicadas para todas as funções existentes nas ferramentas.

Existem várias maneiras de usar ClamWin:

- Executar no menu Iniciar;
- Executar a partir do ícone da bandeja do sistema;
- Verificações agendadas;
- Integração com o *Outlook*;
- Integração do *Windows Explorer*.

Esta seção irá discutir cada uma das maneiras:

A. Executado a Partir do Menu Iniciar

Por padrão, durante a instalação, um grupo de programas chamado "ClamWin Antivirus" é criado, que contém *Virus Scanner help* / manual e *uninstaller*. A seleção de *Virus Scanner* vai começar ClamWin com a janela principal aberta como mostrado na Figura 1 [8].

Para escanear um arquivo ou uma pasta, basta selecioná-lo na janela principal como é mostrado na Figura 1, e clicar no botão *Scan* (ou clique em "*File*" "*Scan File*" no menu ou clicar no último ícone na barra de ferramentas). Os múltiplos arquivos / pastas também podem ser selecionados. Para verificar todos os programas carregados que estão atualmente na memória, basta selecionar "*File Scan Memory*". A varredura de memória pode ser iniciada através do ícone também em terceiro lugar na barra de ferramentas [8].

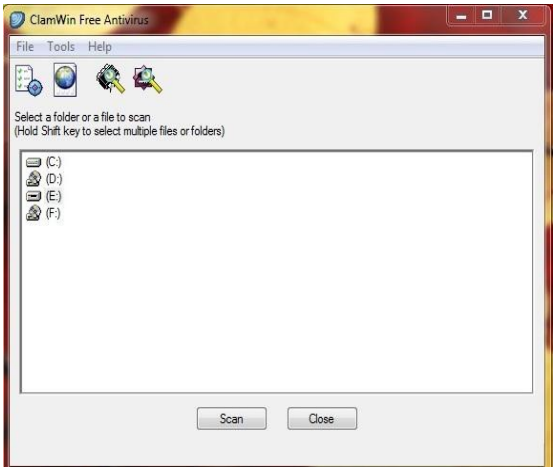

Fig. 1. Página de inicialização do programa *ClamWin Free Antivírus*, selecionada a opção do USB *Flash Drive*.

B. Executado a Partir do Ícone da Bandeja do Sistema

Para executar ClamWin a partir do ícone da bandeja do sistema, basta clicar duas vezes no ícone ou botão direito do mouse e selecionar "*Open ClamWin*". O programa será iniciado com a janela principal aberta, como na Figura 1 [8].

O ícone da bandeja do sistema permite outras opções para ser selecionada no botão direito do mouse como observamos na Figura 2 [8].

Fig. 2. Menu oferecido a partir do ícone da bandeja do sistema.

1) Download da atualização do banco de dados

Isso fará com que o ClamWin verifique se há atualizações para o banco de dados de vírus e baixe as atualizações que estão disponíveis, como mostrado na Figura 3 [8].

Fig. 3. Janela inicial do programa *ClamWin Free Antivírus*.

2) Configuração do ClamWin

Esta opção exibe a janela de preferências do programa onde as configurações ClamWin podem ser alteradas. Nessa opção é encontrada por exemplo a configuração para escanear um email, verificar atualizações, agendar escaneamento, como mostrada na Figura 4 [8].

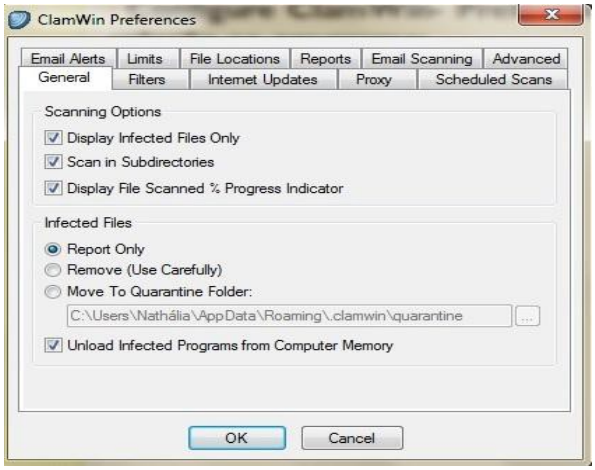

Fig. 4. Página de configuração/alteração do *programa ClamWin Free Antivírus.*

3) Agendamento

A Figura 5 ilustra o conteúdo deste guia. Através desse guia, verificações agendadas podem ser configuradas, programadas e executadas, ou ainda, interrompidas. O agendamento de escaneamento permite ao usuário a facilidade de manter seu computador sempre seguro [8].

4) Exibir relatórios

Ao escolher esta opção, uma janela como a ilustrada na Figura 6 é apresentada. O "Relatório de Atualização do Banco de Dados" ou "Relatório de Verificação de Vírus" pode ser visto, como o exemplo da Figura 6 [8].

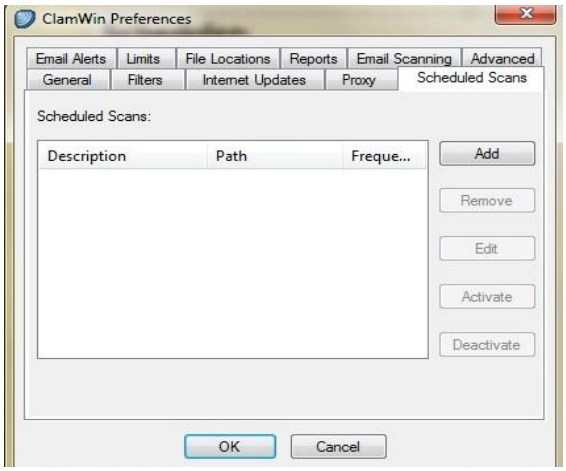

Fig. 5. Página do programa *ClamWin Free Antivírus* ao ser selecionada a opção "*Scheduled Scans*".

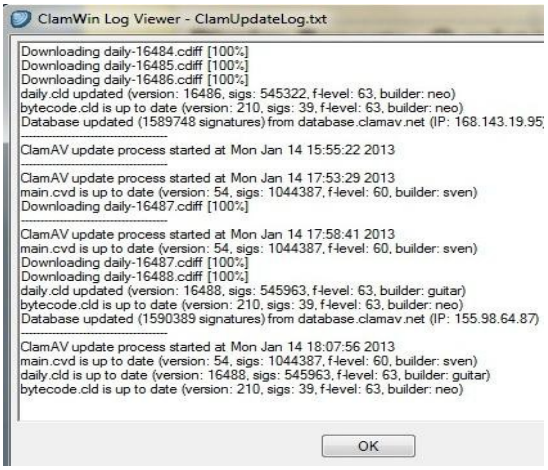

Fig. 6. Página de exibição de relatório do programa *ClamWin Free Antivírus.*

5) Verificar versões mais recentes

Esta opção irá abrir o navegador padrão no site ClamWin como mostrado na Figura 7 e permitirá verificar a versão instalada do ClamWin. A página irá exibir uma mensagem mostrando a versão mais recente disponível. Caso o usuário deseje baixar a nova versão, um endereço do *download* estará disponível na página [8].

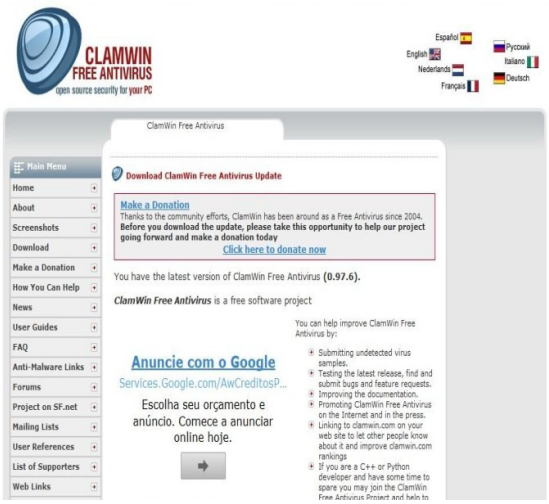

Fig. 7. Site do *software ClamWin Free Antivírus.*

C. Verificações Agendadas

Verificações agendadas podem ser configuradas na janela de preferências ("Ferramentas", "Preferências" e "Verificações agendadas") ou a partir do sistema de bandeja de ícones ("*Scheduler*" e "Configurar *Scheduler*"). Se uma verificação agendada é criada, será executado o escaneamento ClamWin com o tempo especificado, sem interromper o usuário. Se um vírus for encontrado, um balão de notificação será exibido acima do ícone da bandeja do sistema (nota: o recurso de notificação de balão não funciona no Windows 98). A ação tomada pelo ClamWin na detecção de um vírus será determinada pelo que tem sido especificado no guia geral da janela de preferências, como apresentado na Figura 5 [8].

D. Integração com MS Outlook

Se o *Outlook* estiver instalado no computador e a integração foi selecionada durante a instalação do ClamWin, ele irá escanear todas as entradas e saídas de e-mails que tenham vírus. Isto é feito totalmente automático, sem que a intervenção do usuário seja necessária. Se um *e-mail* recebido tem um vírus anexado, este é substituído por um arquivo de relatório [8].

E. Integração com Windows Explorer

Se essa opção foi selecionada durante a instalação do ClamWin, uma opção extra (*Scan For Viruses With ClamWin*) será adicionada no menu do botão direito do *Windows Explorer*. Para isso, apertar o botão direito do mouse em um arquivo ou pasta e selecionar na pasta a opção que irá escanear o arquivo ou pasta para o vírus, proporcionando uma maneira rápida e simples para a varredura dos arquivos suspeitos [8].

VIII. APLICAÇÃO PRÁTICA DA FERRAMENTA

Utilizando o antivírus ClamWin como exemplo de ferramenta CASE de Análise de Programas, um teste será realizado para demonstrar o seu funcionamento básico e analisar se realmente ele cumpre todas as vantagens que diz possuir e o quão seguro é sua utilização. Como o escaneamento é uma das partes mais importantes num programa de antivírus, a varredura pela procura por vírus e *spywares* presentes no sistema é essencial, além de apontá-los e propor uma solução.

No escaneamento, o usuário pode escolher qual pasta deseja fazer a varredura. Escolhido o destino, o programa começa a procurar e detectar as possíveis ameaças presentes no sistema operacional. Após o término do escaneamento, o programa aponta os resultados e o local onde o vírus está inserido. A opção de remoção e mover para a quarentena é definida pelo usuário.

Abaixo, serão mostrados os passos do escaneamento da ferramenta.

A. Escolha da Pasta Destinada ao Escaneamento

No exemplo da Figura 8, utilizamos uma memória USB *Flash Drive* para a análise. Para o teste, a pasta E correspondente à opção do USB *Flash Drive* é escolhida para o escaneamento conforme se verifica na Figura 8.

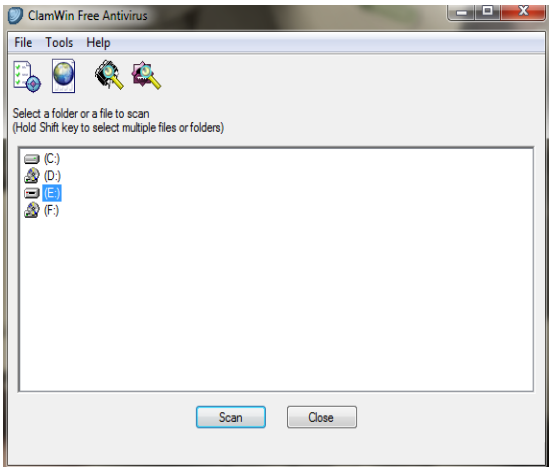

Fig. 8. Página de inicialização do programa *ClamWin Free Antivírus*, estando selecionada a opção do USB *Flash Drive*.

B. Escaneamento da Pasta Escolhida

Há uma procura por vírus e *spywares* como mostrada na tela da Figura 9.

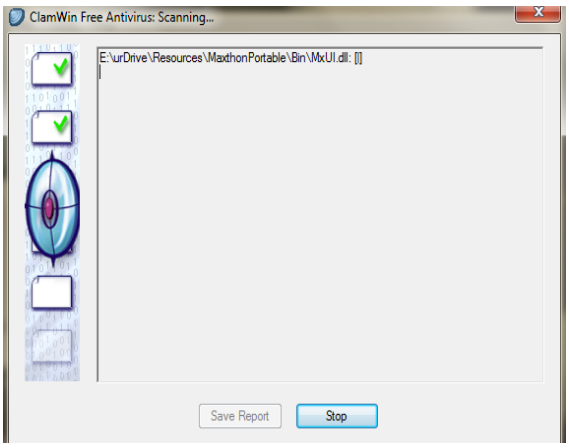

Fig. 9. Inicialização da varredura do USB *Flash Drive.*

C. Escaneamento Concluído

O programa apresenta o total de arquivos escaneados e os que foram encontrados infectados, como mostra a Figura 10. Após isso, os arquivos infectados são excluídos ou movidos para quarentena.

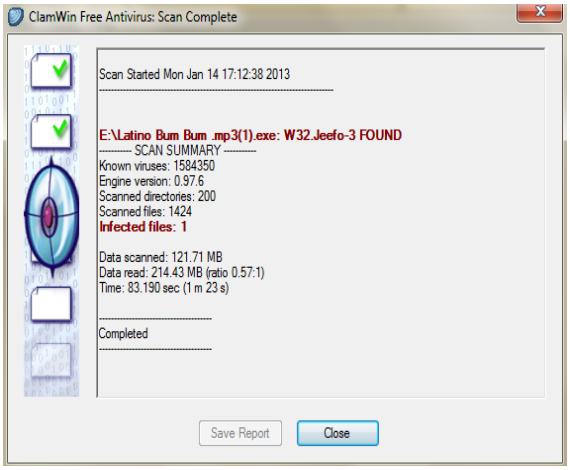

Fig. 10. Relatório completo do escaneamento. Foi detectado apenas um arquivo infectado.

IX. ANÁLISE E DISCUSSÃO DOS RESULTADOS

O *ClamWin Free Antivírus* é um programa simples, de fácil utilização que não oferece complicações quanto à execução e realmente cumpre o que diz ter de vantagem.

Através de sua fácil interface, varreduras podem ser realizadas por todo o sistema operacional e drives externos para buscar os vírus e *spywares* nos arquivos e propor soluções para esses arquivos infectados. Como aspectos negativos apareceram o fato de ter visual limitado e simples e o fato de não alertar em tempo real quando o sistema é atacado.

Um ponto positivo para a ferramenta é o fato dela ser um *software* portátil, facilitando a vida do usuário devido a sua leveza e facilidade de uso, além da grande compatibilidade com a maioria dos sistemas.

X. CONCLUSÃO

Neste trabalho foi proposto um estudo técnico pormenorizado de ferramentas CASE para análise de programas. Foram escolhidos o programa de limpeza (CCleaner) e o antivírus (ClamWin) como exemplos dessas ferramentas.

Para uma análise técnica pormenorizada escolheu-se o *software ClamWin Free Antivírus*, por ser de código aberto e possuir muitos usuários pelo mundo. Para o *software* escolhido foi desenvolvido um manual prático de uso da ferramenta e foi construído um tutorial de aplicação da ferramenta para o escaneamento de um diretório de programas em busca de arquivos infectados.

Os resultados da análise técnica levaram a concluir que o *software* atingiu plenamente as vantagens que ele propõe, sendo de fácil instalação e manuseio, ocupando pouco espaço de memória, possuindo um manual rico em informações e oferecendo a grande vantagem de ser gratuito. Além disso, verificou-se que por ser de código aberto, o referido *software* se encontra bem revisado, não apresentando falhas que possam comprometer o seu funcionamento.

O *software ClamWin Free Antivírus* como uma ferramenta CASE mostrou ser uma opção bastante interessante principalmente para confirmação secundária de segurança, garantindo o bom funcionamento do computador pelas suas vantagens de oferecer facilidades de instalação e uso além da eficiência no combate aos vírus sem acarretar custos.

REFERÊNCIAS

[1] C. Gane, T. Sarson, "Análise Estruturada de Sistemas", 1ª Edição, Rio de Janeiro, 1987.

[2] A. S. Tanenbaum, M. V. Steen, "Sistemas Distribuídos, Princípios e Paradigmas", 2ª Edição, São Paulo, 2008.

[3] Enigma Software Group (2009). *Vírus e outras ameaças: Como lidar com eles*. Acessado em 7 de Janeiro de 2013, em: http://www.enigmasoftware.com/pt/virus-e-outras-ameacas-como-lidar-com-eles/.

[4] Baixaki (2013). *Ccleaner*. Acessado em 10 de Janeiro de 2013, em: http://www.baixaki.com.br/download/ccleaner.htm.

[5] Rocha (2011). *Dez programas gratuitos para limpeza e otimização do Windows*. Acessado em 8 de janeiro de 2013, em: http://www.oblogdoseupc.com.br.

[6] Piriform® (2013). *Get that new computer feel with CCleaner*. Acessado em 10 de Janeiro de 2013, em: http://www.piriform.com.

[7] Wikipédia (2013). *Antivírus*. Acessado em 5 de Janeiro de 2013, em: http://pt.wikipedia.org/wiki/Antiv%C3%ADrus.

[8] ClamWin Free Antivirus (2013). *Segurança OpenSource para seu PC*. Acessado em 10 de Janeiro de 2013, em: http://www.clamwin.com.