DOI: 10.5769/C2012011 or http://dx.doi.org/10.5769/C2012011

Tornando Pública a Navegação "In Private"

Rodrigo de S. Ruiz [1], Fernando Pompeo Amatte [2] , Kil Jin Brandini Park D. Sc. [3]
1, 2 Divisão de Segurança de Sistemas da Informação (DSSI)
Centro de Tecnologia da Informação Renato Archer (CTI)
Campinas – SP, Brasil.
3 Faculdade de Computação (FACOM) – Universidade Federal de Uberlândia
Monte Carmelo – MG, Brasil
rodrigo.ruiz@dssi.cti.gov.br, famatte@gmail.com, kil@facom.ufu.br

Resumo — A crescente preocupação dos usuários com o sigilo dos dados gerados pelas atividades desenvolvidas no decorrer da navegação pelas páginas web fomentou o desenvolvimento de opções de navegação que ofertassem maior grau de segurança e sigilo para estes dados.
Se por um lado tal recurso, em caso de funcionamento perfeitamente alinhado as diretrizes de segurança, fornece ao usuário privacidade em suas atividades online, por outro lado fica claro que em caso de ilícitos cometidos, os agentes da lei têm que lidar com mais esta dificuldade para obter dados que forneçam provas necessárias durante uma investigação.
Independente do caso é importante verificar se as diferentes ofertas de mecanismo de navegação privada realmente funcionam.
A metodologia proposta mostrou que, dependendo do navegador utilizado, é possível recuperar dados em formato de texto sobre páginas visitadas durante a navegação sigilosa e até mesmo figuras que constituem essa página, em clara violação ao requisito funcional básico deste recurso.
Palavras-chave: Navegação sigilosa, Segurança de navegadores, Análise forense em navegadores.

Abstract — The growing concern of users about the confidentiality of data generated by web browsing activities made browser developers include options for safer and confidential browsing in their products.
For users those options, when functionally compliant with data security guidelines, guarantee online privacy. For law enforcement agents, this functionality introduces another obstacle for data acquisition towards evidence gathering.
It is important to assess and validate private browsing techniques no matter which case.
The presented methodology shows that for some browsers it is possible to recover text and graphical data related to pages visited during private navigation, in clear violation of this tool basic functional requirement.
Keywords: Private browsing, Browser safety, Browser forensics.

I. Introdução

A crescente preocupação dos usuários com o sigilo dos dados gerados pelas atividades desenvolvidas no decorrer da navegação pelas páginas web fomentou o desenvolvimento de opções de navegação que ofertassem maior grau de segurança e sigilo destes dados.

A promessa dos desenvolvedores em relação ao funcionamento desse recurso é impedir que outros consigam reconstruir os passos que o usuário tomou durante suas atividades online.

Se por um lado tal recurso, em caso de funcionamento perfeitamente alinhado as diretrizes de segurança, fornece ao usuário privacidade em suas atividades online, por outro lado fica claro que em caso de ilícitos cometidos, os agentes da lei têm que lidar com mais esta dificuldade para obter dados que forneçam provas necessárias durante uma investigação.

Em ambos os casos, é importante verificar a funcionalidade real de tal recurso, se as implementações disponíveis realmente oferecem o sigilo ofertado, ou se existem falhas que possibilitem a obtenção de dados das atividades online mesmo com esta opção em uso.

Assim, o presente trabalho se estrutura nos seguintes tópicos:

Metodologia de Testes, onde se apresenta a metodologia aplicada aos testes efetuados da funcionalidade de navegação privada.

Resultados e Discussão, onde se apresenta os resultados obtidos pelos testes adotados e discute-se o tratamento apresentado para esses resultados.

Finalizando, seguem as conclusões e referências bibliográficas utilizadas.

II. Metodologia de Testes

Ao testar uma funcionalidade de segurança, faz-se necessário definir os requisitos funcionais da mesma, além do perfil do atacante que tentará desabilitar ou sobrepujar tal funcionalidade.

Em um trabalho sobre análise da funcionalidade de navegação privada, [1] lista os perfis de possíveis atacantes, além dos modelos de segurança a serem verificados e os objetivos a serem cumpridos pelos navegadores que implementam a navegação privada.

No presente trabalho, parte-se do arcabouço metodológico apresentado por [1], para a construção do seguinte modelo metodológico:

O perfil do atacante considerado parte do pressuposto que este possui acesso local a maquina do usuário. Portanto, as tentativas de burlar o sistema de navegação privada ocorrerão a partir de uma imagem extraída da máquina do usuário.

Como o foco é avaliar a funcionalidade de navegação privada de modo isolado, considera-se que o usuário não adota técnicas de segurança que potencialmente influenciariam no acesso aos dados gerados durante a navegação. Assim, considera-se a não utilização de métodos criptográficos no disco da máquina do usuário.

Além disso, o presente trabalho foca a prospecção de dados na máquina do usuário em formato de texto ou figuras que tragam informações a respeito de páginas visitadas por este. Portanto, não é efetuada análise específica de alterações em arquivos utilizados por navegadores tais como histórico, cookies, cache, certificados e outros, cuja análise pode ser observada em [1] e [2].

Para os testes efetuados, criou-se uma máquina virtual "guest" padrão, com a instalação do sistema operacional Windows XP SP3 sobre uma máquina "host" executando o sistema operacional Ubuntu 10.04 e o virtualizador VirtualBox [3].

Um "snapshot" da máquina Windows recém instalada foi criado, considerando a possível necessidade de comparação futura da máquina base com as máquinas que executam os diferentes navegadores instalados.

Os navegadores testados foram o Internet Explorer 8 e o Firefox 8.0.1. Após cada teste, a máquina virtual Windows é levada ao seu estado inicial, imediatamente após a instalação do navegador em questão. Dessa forma, garante-se que todos os testes são efetuados sobre a mesma base.

Com base nestas premissas, efetuaram-se quatro testes diferentes para cada um dos navegadores em modo de navegação privada:

Teste 1: Visitar um site disponível na internet, sem efetuar operações de interação com o site. Finalizar corretamente o navegador, gerar a imagem da máquina virtual para análise.

Teste 2: Visitar um site disponível na internet, sem efetuar operações de interação com o site. Com o navegador ainda ativo, gerar a imagem da máquina virtual para análise.

Teste 3: Visitar um site disponível na internet, sem efetuar operações de interação com o site. Requisitar que o sistema operacional interrompa o navegador, gerar a imagem da máquina virtual para análise.

Teste 4: Visitar um site disponível na internet , sem efetuar operações de interação com o site. Requisitar que o virtualizador desligue a máquina virtual, simulando uma queda de energia, gerar a imagem da máquina virtual para análise.

Entende-se por imagem da máquina virtual, os arquivos separados de memória e disco da mesma.

Para cada teste efetuado, a imagem da máquina virtual gerada será analisada através da aplicação do programa strings [4] encontrado nas distribuições Linux, para a prospecção de cadeias de caracteres que tenham relação com a página web visitada.

Além disso, a imagem da máquina virtual também será analisada para a prospecção de arquivos gráficos associados à página visitada, através da utilização do programa scalpel [5], uma reconhecida ferramenta forense para extração de arquivos ("data carving") de diferentes formatos.

Esta ferramenta funciona da seguinte forma: Ela lê um bloco de dados - memória, disco ou arquivos - e procura por assinaturas relacionadas a arquivos de formatos conhecidos.

Como essas assinaturas são uma seqüência de bytes, existe a chance de ocorrência de falso-positivos e, portanto, a não captura do arquivo correto.

Além disso, é importante salientar a existência de diversos problemas conhecidos relacionados ao uso de ferramentas de "data carving", como, por exemplo, suas limitações para o tratamento de dados não contíguos. Assim, é possível que uma imagem cuja seqüência de bytes esteja dispersa não seja recuperada integralmente, apesar de sua possível existência no bloco de dados analisado.

III. Resultados e Discussão

Visando simular uma visita real a um site qualquer disponível na internet, uma seleção aleatória foi realizada, e o site escolhido para o experimento foi o [6]. Dado que algumas informações do site são proprietárias, as figuras recuperadas durante o teste, mesmo aquelas que foram completamente recuperadas serão reproduzidas apenas parcialmente no presente trabalho. O status de recuperação (parcial / total) será indicado na legenda associada à figura.

Para o navegador Internet Explorer 8, parte dos resultados obtidos foram:

A. Teste 1

1) Strings

<title>Simpsons.com.br </title>

<link rel="stylesheet" href="http://www.simpsons.com.br/wp-content/themes/the_simpsons_theme/style.css" type="text/css" media="screen" />

<link rel="alternate" type="application/rss+xml" title="Simpsons.com.br RSS Feed" href="http://www.simpsons.com.br/?feed=rss2" />

<link rel="pingback" href="http://www.simpsons.com.br/xmlrpc.php" />

<link rel="stylesheet" type="text/css" href="http://www.simpsons.com.br/wp-content/themes/the_simpsons_theme/style.css" />

<link rel="stylesheet" type="text/css" href="http://www.simpsons.com.br/wp-content/themes/the_simpsons_theme/style_ie.css" />

<link rel=”stylesheet” type=”text/css” href=”http://www.simpsons.com.br/wp-content/themes/the_simpsons_theme/style_ie6.css” />

<link rel=”stylesheet” href=”http://www.simpsons.com.br/wp-content/plugins/share-buttons/css/share-buttons-user.css” type=”text/css” />

seu voto:.. ..http://thesimpsons.com/nedna/...” />

seu voto:.. ..http://thesimpsons.com/nedna/...” />

<script type=’text/javascript’ src=’http://www.simpsons.com.br/wp-includes/js/l10n.js?ver=20101110’></script>

<script type=’text/javascript’ src=’http://www.simpsons.com.br/wp-content/plugins/share-buttons/js/share-buttons.js?ver=3.2.1’></script>

Theme Name: The Simpsons Theme

Description: The Simpsons Theme is a unique Widget ready WordPress theme with 2 columns, right sidebar and fixed width. Tested on Firefox, Internet Explorer 6, 7 and Opera.

É possível verificar que o navegador, mesmo em modo de navegação privada, deixou no sistema informações a respeito da página visitada. Ao analisar o conteúdo completo gerado pelo programa strings, percebe-se que existe a possibilidade de reconstrução uma fração considerável da página visitada apenas com esses dados.

2) Figuras

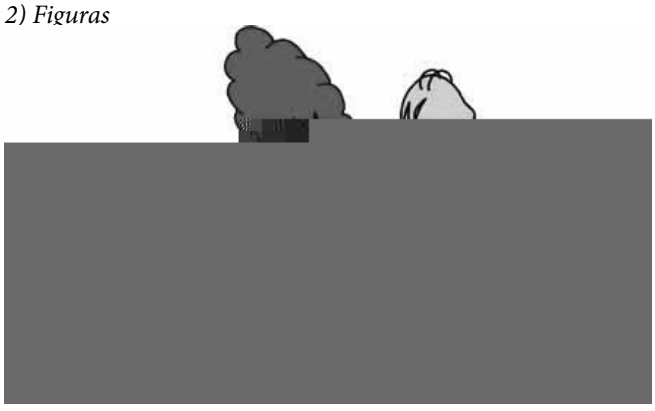

Figura 1 – Figura Parcialmente Recuperada do Sistema pelo Scalpel

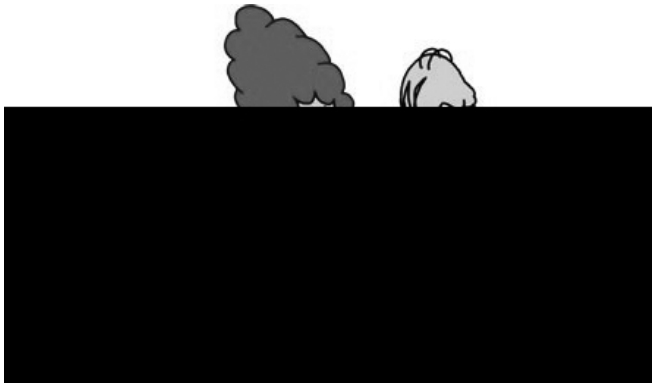

Figura 2 – Parte da Figura Original Encontrada na Página Visitada

Figura 3 – Parte da Figura Totalmente recuperada do Sistema pelo Scalpel

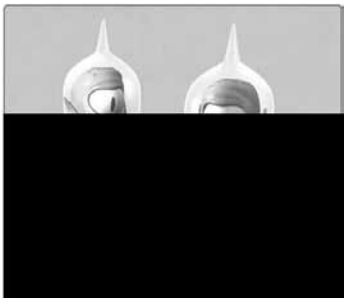

Figura 4 – Parte da Figura Original Encontrada na Página Visitada

Novamente, é possível verificar que o navegador, mesmo em modo de navegação privada, deixou no sistema informações suficientes a respeito de figuras existentes na página visitada para possibilitar a identificação e até mesmo recuperação de algumas delas.

B. Teste 2

3) Strings

Simpsons.jpg HTTP/1.1

simpsons`

ww.simpsonsE

www.simpsonsF

simpsons@-

eferer: http://www.simpsons.com.

simpsons.com.br/

simpsons@-

simpsons.com.br/

simpsons@-

simpsonsF

erer: http://www.simpsons.com.br

www.simpsons.com.br

simpsons.#

.simpsons.com.br%2F&extra_2=

: www.simpsons.c

simpsons.com.br

_simpsons_th@

http:www.simpsons.com.br

simpsons@[

_url=”http://www.simpsons.com.br /?p=148”>S@

Os Simpsons

simpsons.com.br

simpsons@-

http://www.simpsons.com.br/favic

simpsons.#

Simpsons

Simpsons

www.simpsonsI

tp://thesimpsons.com/nedna/c

sidades sobre os Simpsons’ class

w.simpsons.com.br%2F&extr

Os Simpsons

simpsons@-

Os Simpsons

simpsons@-

simpsons@-

Pode-se observar que seria possível recuperar informações suficientes para identificar a página visitada.

4) Figuras

Figura 5 - Figura Parcialmente Recuperada do Sistema pelo Scalpel

Figura 6 - Parte da Figura Original Encontrada na Página Visitada

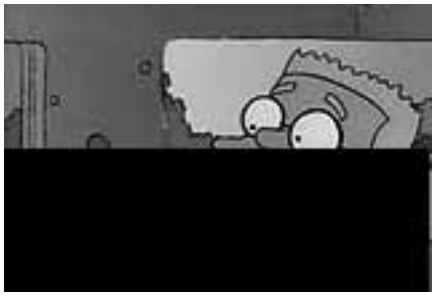

Figura 7 - Parte da Figura Totalmente recuperada do Sistema pelo Scalpel

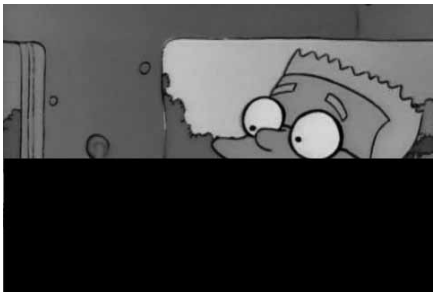

Figura 8 - Parte da Figura Original Encontrada na Página Visitada

Novamente, é possível verificar que o navegador, mesmo em modo de navegação privada, deixou no sistema informações suficientes a respeito de figuras existentes na página visitada para possibilitar a identificação e até mesmo a recuperação de algumas delas.

C. Teste 3

5) Strings

w.simpsonsDr

ww.simpsonsE

simpsons.&W

simpsons`

simpsons@R

simpsons@-

www.simpsonsK

www.simpsonsE

p://www.simpsons.com.br/

www.simpsonsF

: http://www.simpsona

Referer: http://www.simpson

: http://www.simpsonsE

Simpsons.jpg HTTP/1.1

.simpsons.com.br%2F&extra_2=

dades sobre os Simpsons.

simpsons.#

sidades sobre os Simpsons' class

w.simpsons.com.br%2F&extra_2

www.simpsons.com.br

src="http://thesimpsons.com/nedn

www.simpsonsHu

ia Simpsons tem 3 re (

www.simpsons@(.br/?p=129

Os Simpsons

www.simpsons.com.br

Simpsons

Os Simpsons

%2F%2Fwww.simpsons.com.br

mporada dos Simpsons.

re Steve Jobs e Homer Simpson</b

www.simpsons.com.br

www.simpsons.com.br

www.simpsonsA

simpsons

http://www.simpsons.com.br/wp-co

title>Simpsons.com.br </

simpsons@-

dios de "Os Simpsons

simpsons@-

de Homer Simpson e sua fam

simpsons@-

u Simpsons - Escolha.

Novamente, pode-se observar que seria possível recuperar informações suficientes para identificar a página visitada.

6) Figuras

Figura 9 - Figura Parcialmente Recuperada do Sistema pelo Scalpel

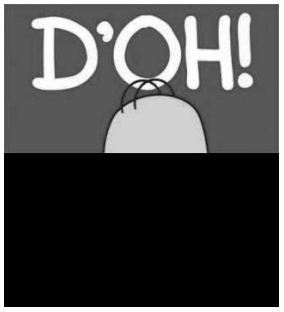

Figura 10 - Parte da Figura Original Encontrada na Página Visitada

Figura 11 - Parte da Figura Totalmente recuperada do Sistema pelo Scalpel

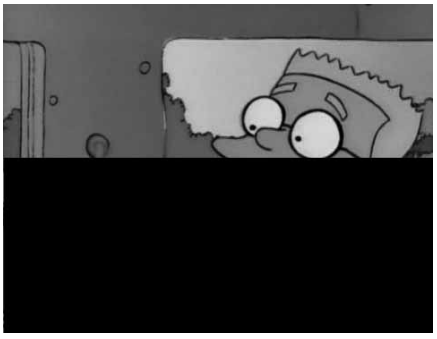

Figura 12 - Parte da Figura Original Encontrada na Página Visitada

É possível verificar que o navegador, mesmo em modo de navegação privada, deixou no sistema informações suficientes a respeito de figuras existentes na página visitada para possibilitar a identificação e até mesmo a recuperação de algumas delas.

D. Teste 4

7) Strings

Theme Name: The Simpsons Theme

Description: The Simpsons Theme is a unique Widget ready WordPress theme with 2 columns, right sidebar and fixed width. Tested on Firefox, Internet Explorer 6, 7 and Opera. Theme is XHTML/CSS valid and SEO friendly.

curtiu Globo adapta "Os Simpsons" para hor

e outras 2 pessoas curtiram isso.2 curtiram. <a href=”/campaign/landing.php?campaign_id=137675572948107&partner_id=simpsons.com.br&placement=like_button&(

<link rel=”EditURI” type=”application/rsd+xml” title=”RSD” href=”http://www.simpsons.com.br/xmlrpc.php?rsd” />

<link rel=”wlwmanifest” type=”application/wlwmanifest+xml” href=”http://www.simpsons.com.br/wp-includes/wlwmanifest.xml” />

<link rel=’index’ title=’Simpsons.com.br’ href=’http://www.simpsons.com.br’ />

<h1>Simpsons.com.br</h1>

s dos Simpsons

<h2>Ned Flanders e Edna Krabappel</h2>

Autor: Felipe | Categoria: <a href=”http://www.simpsons.com.br/?cat=5” title=”Ver todos os posts em Informa

<ahref=”http://thesimpsons.com/nedna/”>

http://thesimpsons.com/nedna/

Tweet Share to FB <!--End Share Buttons http://sbuttons.ru -->

<iframe src=”http://www.facebook.com/plugins/like.php?href=http://www.simpsons.com.br/?p=148&layout=standart&show_faces=1&width=450&action=like&font=tahoma&colorscheme=light&height=70” scrolling=”no” frameborder=”0” style=”border:none; overflow:hidden; width:450px; height:70px;” allowTransparency=”true”></iframe>

Pode-se verificar que neste teste, o resultado gerado pelo programa strings gera informações que permitiriam não apenas identificar como também reconstruir parcialmente a página visitada.

8) Figuras

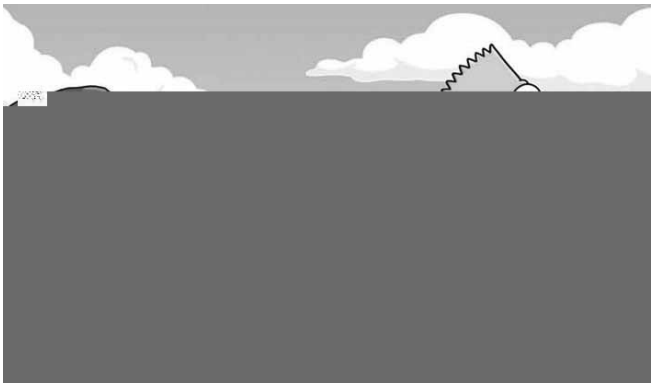

Figura 13 - Figura Parcialmente Recuperada do Sistema pelo Scalpel

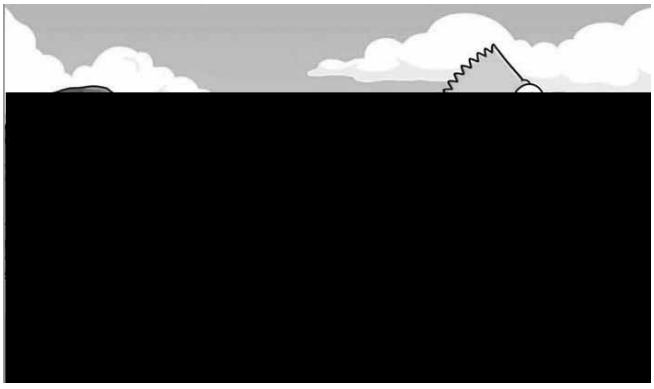

Figura 14 - Parte da Figura Original Encontrada na Página Visitada

Figura 15 - Parte da Figura Totalmente recuperada do Sistema pelo Scalpel

Figura 16 - Parte da Figura Original Encontrada na Página Visitada

Novamente, é possível verificar que o navegador, mesmo em modo de navegação privada, deixou no sistema informações suficientes a respeito de figuras existentes na página visitada para possibilitar a identificação e até mesmo a recuperação de algumas delas.

Para o navegador Firefox, alguns dos resultados obtidos foram:

E. Teste 1

9) Strings

Nenhum resultado relevante

10) Figuras

Nenhum resultado relevante

F. Teste 2

11) Strings

Simpsons.com.br

thesimpsons

www.simpsons.com.br

http://thesimpsons.com/nedna/

www.simpsons.c

www.simpsons.com.br/wp-(

thesimpson

www.simpsons.com

www.simpsons.com.br

www.simpsons.com.br/?feed=rss2

simpsons@-

http://www.simpsons.com.br/wp-co

simpsonsC,

http://thesimpsons.com/nedna/col

HTTP:http://www.simpsons.com.br/

HTTP:http://www.simpsons.com.br/

simpsons@-

http://www.simpsonsAX!Q

dio dos Simpsons demor

www.simpsons.com.br

simpsons@-

/www.simpsons.com.br/wp-content/

www.simpsons.com.br/wp-includ%

a tema dos Simpsons.

www.simpsonsF

www.simpsons.com.br

www.simpsons.com.br

www.simpsonsC

ost: thesimpsons.com

/03/RockBottomSimpsons.jpg

www.simpsonsD[

r: http://www.simpsons.com.br/

www.simpsonsA;

www.simpsons.com.br

Pode-se observar que seria possível recuperar informações suficientes para identificar a página visitada.

12) Figuras

Figura 17 - Figura Parcialmente Recuperada do Sistema pelo Scalpel

Figura 18 - Parte da Figura Original Encontrada na Página Visitada

É possível verificar que o navegador, mesmo em modo de navegação privada, deixou no sistema informações suficientes a respeito de figuras existentes na página visitada para possibilitar a identificação das mesmas.

G. Teste 3

13) Strings

www.simpsons.com.br

Referer: http://www.simpsona;

.simpsons.

www.simpsonsD`

Referer: http://www.simpsonsAY

thesimpsons.com

www.simpsons.com.br

Referer: http://www.simpsonsA;

simpsons@-

Referer: http://www.simpsonsA;

content/uploads/2010/03/simpsons

Host: www.simpsons.com.br

simpsonsA

simpsons@-

r: http://www.simpsons.com.br/

Pode-se observar que seria possível recuperar informações suficientes para identificar a página visitada.

14) Figuras

Não foram recuperadas figuras relativas a página visitada.

H. Teste 4

15) Strings

Não foram recuperadas strings de texto referentes a página visitada.

16) Figuras

Não foram recuperadas figuras referentes a página visitada.

Agrupando os resultados obtidos, tem-se:

Tabela 1 – Resultados para o navegador Internet Explorer

	Teste 1	Teste 2	Teste 3	Teste 4
Recuperação de endereço da página visitada	Sim	Sim	Sim	Sim
Recuperação de figuras parciais	Sim	Sim	Sim	Sim
Recuperação de figuras completas	Sim	Sim	Sim	Sim

Tabela 2 – Resultados para o navegador Firefox

	Teste 1	Teste 2	Teste 3	Teste 4
Recuperação de endereço da página visitada	Não	Sim	Sim	Não
Recuperação de figuras parciais	Não	Sim	Não	Não
Recuperação de figuras completas	Não	Não	Não	Não

Pode-se verificar que a função de navegação privada, tal como implementada, apresenta-se funcionalmente mais adequada no navegador Firefox.

IV. Conclusão

Nos quatro tipos de testes realizados, é possível verificar que a versão testada do Internet Explorer possui sérias falhas em sua funcionalidade de navegação privada, ao deixar disponível no sistema uma série de informações que possibilitariam não apenas identificar páginas visitadas como também reconstruí-las.

Já o navegador Firefox apresenta dados relativos à página visitada apenas nas análises desenvolvidas tanto com o navegador executando (teste 2) quanto logo após o sistema ter interrompido sua execução (teste 3).

Assim, pode-se concluir que para a metodologia adotada, a funcionalidade de navegação privada implementada no Firefox mostra-se mais adequada que aquela encontrada no Internet Explorer.

Se por um lado isso representa um ponto negativo para o usuário, por outro facilita o trabalho de perícia dos navegadores por agentes da lei nos casos em que esta tarefa se faz necessária.

V. Referências Bibliográficas

[1] AGGARVAL, G. BURSZTEIN, E. JACKSON, C. BONEH, An Analisys of Private Browsing Modes in Modern Browsers. USENIX 2010, Disponível em: http://crypto.stanford.edu/~dabo/pubs/papers/privatebrowsing.pdf. Acesso em: 30 jun 2012.

[2] MAHENDRAKAR, A. IRVING, J. PATEL, S. Forensic Analisys of Private Browsing Mode in Popular Browsers. Disponível em: http://mocktest.net/paper.pdf. Acesso em: 30 jun 2012.

[3] VirtualBox. Disponível em: https://www.virtualbox.org/. Acesso em: 30 jun 2012.

[4] Strings manpage. Disponível me: http://linux.die.net/man/1/strings. Acesso em 30 jun 2012.

[5] Scalpel. Disponível em: http://www.digitalforensicssolutions.com/Scalpel/. Acesso em 30 jun 2012.

[6] Simpsons.com.br. Disponível em: http://www.simpsons.com.br/. Acesso em 30 jun 2012.

Rodrigo de Souza Ruiz é servidor do Centro de Tecnologia da Informação Renato Archer. "Agradeço ao empenho dos meus amigos Fernando e Kil que tornaram possível essa pesquisa e especialmente a minha mulher, Gilce Ganzert Ruiz, pela inspiração e apoio ao meu trabalho."

Fernando Pompeo Amatte, com mais de 20 anos de experiência na área de segurança da informação, possui as certificações profissionais CISSP, GCIH e MCSO. Com experiências em provedores de acesso, empresas multinacionais de telecomunicação e setor financeiro.
Atua como consultor de segurança da informação e como professor nos cursos de Pós-Graduação da Veris Educacionals (IBTA) e SENAC em Campinas. Pesquisador de malwares, é também perito de informática para o Tribunal Regional do Trabalho de Campinas.

Kil Jin Brandini Park, D. Sc., é especialista em segurança da informação, engenheiro de computação pela UNICAMP e doutor pela mesma instituição. Atua como professor adjunto da faculdade de computação - FACOM, da universidade federal de Uberlândia - UFU, Campus Monte Carmelo.