Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

SERGIO ROSA DA SILVA JUNIOR

Uso de Aplicações Open Source na Prática de Perícia Forense Computacional

Assis

2012

SERGIO ROSA DA SILVA JUNIOR

Uso de Aplicações Open Source na Prática de Perícia Forense Computacional

Trabalho de Conclusão de Curso apresentado ao curso de Bacharelado em Ciência da Computação do Instituto Municipal de Ensino Superior de Assis – IMESA e a Fundação Educacional do Município de Assis – FEMA, como requisito parcial à obtenção do Certificado de Conclusão.

Orientador: Me. Fabio Eder Cardoso

Assis

2012

FICHA CATALOGRÁFICA

JUNIOR, Sergio Rosa da Silva

Uso de Aplicações Open Source na Prática de Perícia Forense Computacional / Sergio Rosa da Silva Junior. Fundação Educacional do Município de Assis – FEMA --Assis, 2012.

40p.

Orientador: Me Fabio Eder Cardoso

Trabalho de Conclusão de Curso - Instituto Municipal de Ensino Superior de Assis - IMESA

1 – Pericia Forense Computacional; 2 – FDTK; 3 – Segurança.

CDD:001.6
Biblioteca da FEMA

SERGIO ROSA DA SILVA JUNIOR

Uso de Aplicações Open Source na Prática de Perícia Forense Computacional

Trabalho de Conclusão de Curso apresentado ao curso de Bacharelado em Ciência da Computação do Instituto Municipal de Ensino Superior de Assis – IMESA e a Fundação Educacional do Município de Assis – FEMA, como requisito parcial à obtenção do Certificado de Conclusão.

Orientador: Me. Fabio Eder Cardoso.

Analisador: Me. Douglas Sanches da Cunha.

Assis

2012

DEDICATÓRIA

Dedico este trabalho as pessoas que dia após dia estão ao meu lado, transmitindo fé, amor, alegria, determinação, paciência, e coragem. A minha noiva Thaís Regina Fontana Porto, meus pais, Sergio e Silvana, a minha irmã Caroline e aos meus companheiros de serviço.

AGRADECIMENTOS

Primeiramente agradeço a Deus por tudo, por estar sempre me guiando em minhas decisões, por ter me abençoado com o dom da vida e sempre me ouvir em minhas orações.

A minha noiva Thaís por ser compreensiva, paciente, me incentivar e não deixar eu nunca desistir.

Aos meus pais por darem a oportunidade de estudo, pela minha educação, formação de caráter e por estarem dia após dia ao meu lado, me cobrando, fazendo com que eu siga sempre em frente apesar da dificuldade.

Ao meu grande amigo, professor e orientador Fabio Eder Cardoso, por me apresentar ao mundo da pericia forense computacional e me auxiliar sempre que necessário.

Aos meus amigos pelas eternas risadas e lembranças e em especial ao meu amigo Claudinei Roberto da Cunha que compreendeu minhas necessidades, me ajudou nessa reta final e sempre me deu bons conselhos.

RESUMO

A Computação Forense na área de criminalística visa determinar toda a relação, causas, meios, autoria e consequências de um incidente que envolve computador, o estudo aqui apresentado levantará conceitos sobre pericia forense computacional e simulará uma pericia tecnicamente.

A distribuição Linux FDTK é uma excelente ferramenta voltado a pericia forense computacional que, em seu conteúdo, possui mais de cem ferramentas open source, além de ser totalmente em português. Assim, nesse trabalho abordará conceitos, área de atuação, técnicas, procedimentos, importância do trabalho da área e a extrema necessidade de conscientização de segurança e vulnerabilidade que estão expostos os computadores e notebooks.

Palavras-chaves: Computação Forense, FDTK, Segurança, Pericia Computacional, Ferramentas Open Source.

.

ABSTRACT

The Computer Forensics in the area of criminology aims to determine any relationship, causes, media authoring and consequences of an incident that involves computer, the study presented here raise skill concepts about computer forensics and simulate a skill technically.

A Linux distribution is an excellent tool FDTK oriented computer forensics expertise, in its content, has over a hundred open source tools, and is entirely in Portuguese. Thus, this paper will discuss concepts, practice area, techniques, procedures, importance of the work area and the extreme need for security awareness and vulnerability are exposed to computers and laptops.

Keywords: Computer Forensics, FDTK, Security, Computer Skill, Open Source Tools.

LISTA DE IMAGENS

SUMÁRIO

1 – Introdução.

Devido a crescente demanda de crimes virtuais no mundo, surgiu a necessidade de uma eficiente ferramenta para identificação de tais crimes, criminosos e redução de riscos de acontecer o mesmo.

De acordo com Freitas (2006) a Forense Computacional é o ramo da criminalística que compreende a aquisição, prevenção, restauração e análise de evidências computacionais, quer sejam os componentes físicos ou dados que foram processados eletronicamente e armazenados em mídias computacionais, a grande diferença entre os crimes tradicionais e os crimes virtuais, é o modo de operação, pois crimes virtuais utilizam de dispositivos eletrônicos, computadores, redes e da internet para a ação ou omissão do crime.

Contudo, a tarefa de identificação, julgamento e penalização se torna cada vez mais complexa devido à possibilidade de anonimato dos contraventores e ao fato de que as evidências do crime poderem estar distribuídas em diversos servidores espalhados pela Internet, tornando-se assim a prática de pericia forense computacional cada vez mais desafiador.

O presente trabalho fará abordará conceitos sobre Pericia Forense Computacional na investigação e esclarecimento de ocorrências no mundo cibernético, será feito uma simulação de pericia em uma imagem usando o FDTK v2.01.

A redução de custo, fez com que haja uma grande acessibilidade a computadores, notebooks, mídias digitais, porém, a conscientização de segurança, não aumentou junto com a informatização, fazendo com que estelionatários e pessoas de má fé que visam obter ganhos a base de pessoas mal informadas sobre segurança. O papel do perito forense computacional é, após ter ocorrido a fraude, o delito, o mesmo vai a busca de evidencias a fim de levantar, relação, meios, causas, autoria e consequências do delito, ou seja, buscar informações de como ocorreu, o por que ocorreu, consequências sofridas no sistema, banco de dados, computadores, recuperação de arquivos, documentos importantes para a vitima, ajudando na investigação e apontando a falha, erro, para que o incidente não ocorra

mais.

Quando se fala em mercado de trabalho para peritos forenses computacionais ainda têm-se o pensamento em trabalhar apenas em parceria com fóruns, advogados, no anonimato, porém, essa realidade esta mudando, no Brasil muitas empresas estão surgindo com foco em pericia forense computacional, visando trabalhar lado-a-lado com empresas.

Ao se falar em pericia forense computacional e investigação, ainda não se têm uma regulamentação especifica sobre o valor judicial de uma prova eletrônica, mostrando o quão o assunto ainda é recente no Brasil, então para uma prova eletrônica poder ser aceita em um tribunal são feitos alguns procedimentos (coleta, exame, análise e relatórios) adaptados de outras áreas, sendo que, no final, todo o trabalho árduo de um perito, pode não ser aceito em um tribunal como evidencia.

No Brasil, pode-se citar o FDTK - Ubuntubr como uma grande distribuição Linux de apoio aos peritos da área, o mesmo possui um conjunto de mais de cem ferramentas open source, totalmente em português (BR) que em seu menu, distingui todas as etapas(coleta, exame, analise e relatórios) de uma pericia forense computacional, porém, não se deve achar que o trabalho de um perito da área é fácil, a cada nova pericia, surge um novo desafio, a cada dia que se passa novas técnicas anti-forese são criadas então o perito tem que sempre estar buscando conhecimento e estar disposto a se deparar com algo novo a cada pericia.

1.2 - Objetivo.

O presente trabalho abordará conceitos sobre Perícia Forense Computacionais na investigação e esclarecimento de ocorrências no mundo cibernético.

Serão Abordados exemplos de métodos de analise forense e como objetivo principal haverá um estudo comparativo entre estes métodos, viabilizando a melhor técnica em torno das mais variadas formas de análise, sendo assim, o presente trabalho não visa esgotar o assunto e sim estimular o leitor a aprender mais sobre o mesmo e buscar novos conhecimentos e conceitos.

Contudo usaremos a ferramenta FTDK(Forense digital Toolkit), uma distribuição livre UbuntuBR que possui em seu conteúdo um conjunto de mais de 100(cem) ferramentas voltadas a pericia forense computacional, sendo assim, simularemos o uso da ferramenta coletando dados, examinando, analisando e recuperando arquivos.

1.3 - Justificativa.

Com o grande crescimento de ataques cibernéticos, há uma grande necessidade de levantamentos de informações que permitirão a recuperação de dados perdidos de forma acidental ou maliciosa, depois de um levantamento rigoroso, seguido das boas praticas do processo de recuperação, existe a possibilidade de identificar o roubo de informações (como e quem roubou).

1.4 - Motivação.

O crescente aumento na demanda de crimes virtuais e a pequena quantidade de profissionais na área, no mundo todo, são 1 milhão de pessoas atingidas diariamente. Anualmente, o prejuízo global é de U$$ 388 bilhões, enquanto somente no Brasil esse valor chega a U$$ 63,3 bilhões, equivalente a R$ 104,8 bilhões.

1.5 - Perspectivas de Contribuição.

A perspectiva é de que invistam mais nessa área que no Brasil, a área de combate, identificação, julgamento e penalização do crime virtual, pois a realidade hoje ainda esta longe do ideal, além de futuramente servir como uma fonte a mais de pesquisa.

1.6 - Metodologias de pesquisa

Para o desenvolvimento do artigo estará sendo utilizados artigos de outros autores que serão pesquisados na Internet, Trabalhos de Conclusões de Cursos, Apostilas, Livros e o uso do FDTK-UbuntoBR(Forense digital Toolkit) simulando a coleta, exame e analise de dados e recuperando arquivos danificados, ou seja, simulando uma pericia forense computacional em um determinado arquivo.

.

1.7 – Recursos necessários.

Os recursos necessários para a elaboração da simulação da pericia nesse trabalho são: Computador e FDTK-UbuntuBR v2.01.

1.8- Estrutura do Trabalho.

Este trabalho foi organizado em cinco capítulos, sendo o primeiro esta introdução. No segundo capítulo será apresentada a computação forense. No terceiro capítulo, será apresentado o conjunto de ferramentas FDTK. No quarto capítulo, será apresentada a simulação e no quinta a conclusão.

2 – Computação Forense.

Convencionalmente é comum definir a Computação Forense como um conjunto de técnicas e ferramentas utilizadas para encontrar evidências em um computador (CALOYANNIDES, 2001), portanto, um dos principais objetivos deste tipo de perícia forense pode ser definido como a coleta de vestígios relacionados ao crime investigado, os quais possibilitem, depois de uma completa investigação, a formulação de conclusões sobre o caso (REIS, 2003).

A Computação Forense na área de criminalística visa determinar toda a

relação, causas, meios, autoria e consequências de um incidente que envolve computador.

Uma análise vem sempre impulsionada por um fato que ocorreu, sendo assim seu objetivo é ligado a tal fato.

A computação forense visa reunir provas, informações, identificar, rastrear e comprovar a autoria de ações criminosas, ou seja, auxiliar na investigação.

Com o crescente aumento de crimes, evidencias podem ser encontradas em vários recursos computacionais como, por exemplo, mídias digitais, que são usadas como ferramentas para auxiliar na execução do crime, de um ponto de vista geral, a computação acabou servindo como um apoio na execução de crimes comuns como estelionato e fraudes.

A Computação Forense exige um amplo conhecimento, pois em uma investigação é comum se deparar com o desconhecido, como por exemplo, arquivos criptografados que necessita técnicas de criptoanálise e outros eventos que justificam o uso de conhecimento em outras áreas.

É de extrema importância dos profissionais da área de pericia forense computacional a determinação na atenção aos detalhes, tanto no procedimento quanto as escolhas de melhores praticas.

A figura abaixo ilustra o mapa mental do conhecimento necessário que envolve um perito forense computacional.

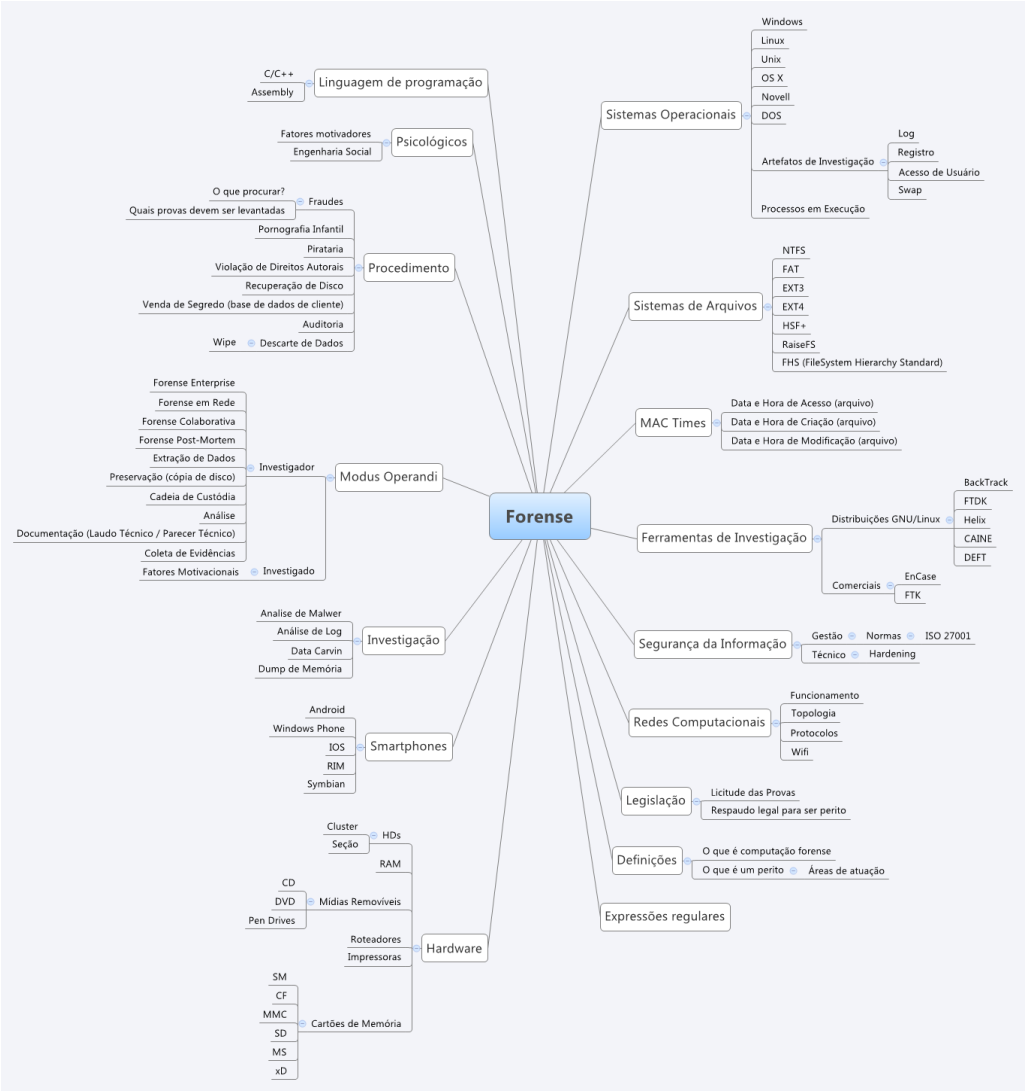

Figura 1 – Mapa mental conhecimento perito forense computacional

***Fonte*: (<** http://4en6br.files.wordpress.com/2012/05/forense1.png**>)**

Em uma investigação em que envolva recursos computacionais, é de extrema importância uma copia integral (e fiel) das mídias feita bit por bit, dessa maneira é possível a coleta de dados (arquivos) apagados e *Slack Spaces.*

Uma digital no mundo do crime faz com que identificamos a pessoa, porém, uma quantidade enorme de informações pode ser adquirida através de uma analise de um computador, através de um simples arquivo, a historia completa de um crime pode ser contada.

A busca incansável por provas, pode muitas vezes ter motivos específicos, como por exemplo, a busca por e-mails, arquivos relacionados a navegadores

(cookies, históricos), logs entre outros.

É comum se deparar com procuras em mídias para se obter dados como arquivos, números, frases , palavras chaves, ou seja, nem sempre é apenas envolvido em um crime, uma pericia forense computacional também é usada na recuperação de dados.

A grande diferença entre os crimes convencionais e os crimes virtuais pode-se dizer que nos convencionais o auto muitas vezes necessita usar armas, arquitetar planos e fugas mirabolantes, se defrontar em situações de risco de vida, enquanto que nos crimes virtuais não há nenhuma dessas necessidades, sendo muitas vezes cometidos por pessoas a milhares de quilômetros de distancia da vitima.

Informações podem ser armazenadas em discos sem a utilização de um sistema de arquivos, ou seja, informações valiosas podem estar armazenadas também em diversas áreas do disco que não são acessíveis por meios normais, uma destas técnicas de armazenamento em nível de camada de sistemas de arquivos é o *Slake Spaces*, que basicamente se resume em utilizar espaços subaproveitados de um ou mais blocos de sistema de arquivos para ocultar dados/informações.

Os sistemas de arquivos armazenam as informações utilizando blocos de tamanho fixo (1 Kb, 2 Kb ou 4 Kb). Entretanto, os arquivos podem ter tamanhos variados. Desta maneira, é muito raro o tamanho de um arquivo ser múltiplo do tamanho de um bloco, o que impede seu armazenamento ideal, ou seja, é comum que o último bloco de um arquivo não seja totalmente utilizado por ele, permitindo que dados excluídos possam ser capturados e analisados.

A figura abaixo ilustra um bloco de 4 Kb com um *Slack Space* com mais de um setor de 512 bytes:

Figura 2 - Slake Space

***Fonte*: (<** http://www.dicas-l.com.br/arquivo/tecnicas_anti-forense_para_ocultacao_de_dados.php#.T-fL5cXmAmc **>)**

Não se pode afirmar que os *Slack Spaces* são espaços livres para armazenamento de dados de forma convencional.

Os blocos de dados marcados como *Slack Spaces* serão vistos pelo sistema operacional como usados e só serão sobrescritos pelo sistema caso o arquivo seja expandido.

Para o armazenamento, detecção e recuperação de informações em *Slack Spaces*, é preciso conhecimento e o uso de ferramentas especializadas, como por exemplo, o bmap para sistemas de arquivos ext2/ext3 ou o slacker para NTFS.

Como se tem uma falta de regulamentação especifica sobre o valor judicial de uma prova eletrônica, é feito um paralelo com métodos tradicionais, sendo de extrema importância ao perito à compreensão do Código de Processo Penal - "Capitulo II - Do Exame do Corpo de Delito, e das Pericia em Geral".

Art. 170 do Código de Processo Penal Capitulo II - Do Exame do Corpo de Delito, e das Pericia em Geral - “Nas perícias de laboratório, os peritos guardarão material suficiente para a eventualidade de nova perícia. Sempre que conveniente, os laudos serão ilustrados com provas fotográficas, ou microfotográficas, desenhos ou esquemas.”.

É importante na forense computacional saber diferenciar dados, informações e evidencias. Dados: podem ser descritos como Bits, Blocos, setores em forma bruta.

Informações é um conjunto de dados que juntos formam um contexto ou uma mensagem e evidencias: são conjuntos de informações que conseguem comprovar

a ocorrência de um incidente.

A preservação das evidencias deve ser crucial, alterar dados pode-se igualar a alterar uma cena de crime no mundo real, deve-se impedir a alteração da media original antes, durante e depois dos procedimentos de aquisição, convencionalmente são usados Assinaturas *hash* para garantir a integridades dos dados coletados.

No tratamento das evidencias, a extração é o processo de extrair informações disponíveis das mídias e recuperação é o processo de buscar dados apagados totalmente ou parcialmente. Existem casos que a manipulação dos mesmos poderá ser efetuada por um perito a parte contrato pelos advogados que contestarem os laudos.

Existe sempre a cautela de se usar ferramentas especializadas para a realização do trabalho do perito, isso deve-se ao fato de haver uma extrema necessidade de não haver qualquer alteração no sistema em que está sendo feita a análise, qualquer alteração feita prejudicará toda a investigação.

Existem várias técnicas para se ocultar dados como a citada acima a *Slake Spaces,* porém não podemos deixar de citar a esteganografia, que consiste basicamente em mascarar informações com a finalidade de evitar a sua descoberta. O processo de esteganografia se resume a esconder uma informação através de uma mensagem de cobertura, ou seja, esconder uma informação através de outra de menor importância.

Não podemos deixar de citar as técnicas, a arte anti-forense, sempre que um invasor quer manter seu acesso a um sistema, ele terá que esconder o seu rastro, ou seja, técnicas anti-forense são utilizadas a fim de vagar por um sistema sem ser detectado, dificultando ainda mais o trabalho do perito.

Citamos acima a técnica de *Slake Space*, porém não podemos deixar de falar de esteganografia, criptografia dos dados, *rootkits* e ocultação de dados em camada de hardware.

Em ocultação de dados em nível de camada de hardware temos que citar os discos rígidos, independentemente dos sistemas operacionais, aparentam ser um excelente local para o armazenamento de dados confidenciais, uma das áreas não acessadas por usuários comuns que é possível fazer isso é a MBR.

Normalmente, quando se particiona um disco rígido, as tabelas de partições começam sempre na cabeça, o primeiro setor de uma partição começa na cabeça 1,setor 1 do cilindro, sendo assim, como consequência dessa pratica, tem-se a existência de setores sem utilização entre o setor da tabela de partições até o inicio da primeira partição.

Ao invadir um sistema, o invasor tende a deixar arquivos, ficheiros nele, porém ao ocultar tais ficheiros, deve-se admitir que os mesmos possam ser encontrados, dessa forma o invasor utiliza de ferramentas de criptografia para caso haja a descoberta dos arquivos ocultas, seja bem difícil a descoberta do conteúdo dos mesmo.

Conseguindo invadir o sistema, o primeiro passo do invasor é garantir seu acesso posterior, os *rootkits* visão isso, é um conjunto de ferramentas que contém softwares necessários para apagar os rastros do atacante.

Ocultar informações de tal forma que seja impossível detectar sua existência é o caso da Esteganografia.

Arquivos de som e imagem que possuem áreas de dados não usadas ou pouco significativas, essas áreas são trocadas por informações, isso é esteganografia.

Esteganografia e criptografias são duas áreas bem diferentes, enquanto a criptografia se baseia em impedir que as pessoas descubram seu o conteúdo da mensagem, a esteganografia visa impedir a existência da mensagem.

2.1- Procedimentos Forenses.

Cada vez mais advogados utilizam evidências digitais em tribunais e cortes. Entretanto, para que sejam consideradas provas válidas o perito deve realizar o processo de investigação cuidadosa e sistematicamente, desse modo preservando as evidências e as documentando detalhadamente, com a finalidade de autenticá-las (PEREIRA, 2007).

As provas eletrônicas baseadas em computador apresentam grandes desafios

únicos para que assegure a sua admissão no tribunal. É indispensável que sejam usados procedimentos forenses, tais procedimentos incluem quatro palavras: coleta, exame, análise e relatórios.

A fase de coleta envolve buscar, reconhecer, recolher a documentação e o computador baseados em provas. A fase de coleta pode ser em tempo real (ainda com o computador ligado), pois existem informações armazenadas que podem ser perdidas caso haja o desligamento do computador, assim, é imprescindível que sejam tomadas precauções no local.

O processo de exame contribui para que a evidência permaneça visível, tenha significado e origem, portanto deve ser realizada de forma correta e conter as seguintes informações: deve documentar o conteúdo e o estado dos elementos em sua totalidade. Incluído neste processo é a busca de informações que podem ser escondidas ou não reveladas. Uma vez que todas as informações são visíveis, o processo de redução de dados pode começar.

A Fase de analise analisa seu significado e o valor probatório do processo. O laudo é uma análise técnica.

Relatórios definem o processo de análise, os dados recuperados e completa o exame. As anotações devem ser muito bem preservadas para fins de divulgação ou até de depoimento.

Não podemos deixar de falar da cadeia de custodia.

A cadeia de custódia é necessária para documentar a história cronológica da evidência, para rastrear a posse e o manuseio da amostra, um controle de onde, quem e quando foram manuseadas as possíveis evidencias.

De acordo com Sampaio (2006), todos os procedimentos relacionados à evidência, desde a coleta, o manuseio e análise, sem os devidos cuidados e sem a observação de condições mínimas de segurança, podem acarretar na falta de integridade da prova, provocando danos irrecuperáveis no material coletado, comprometendo a idoneidade do processo e prejudicando a sua rastreabilidade.

O fato de assegurar a memória de todas as fases do processo constitui um protocolo legal que possibilita garantir a idoneidade do caminho que a amostra percorreu. (NÓBREGA, 2006). Por isso a necessidade da cadeia de custodia.

EVIDÊNCIA ELETRÔNICA

FORMULÁRIO DE CADEIA DE CUSTÓDIA

Caso Num.: 001	Pag.:	De: Sergio R.S.JR

MÍDIA ELETRÔNICA/DETALHES EQUIPAMENTO

Item:	Descrição:		
1	PEN DRIVE 16 GB		
Fabricante:	Modelo:	Num. de serie:	
KINGSTON	DATATRAVELER 100 / OEM	NÃO ENCONTRADO	

DETALHES SOBRE A IMAGEM DOS DADOS

Data/Hora:	Criada por:	Método usado:	Nome da Imagem:	Partes:
06/10/2012 14:30	SERGIO R. S.JUNIOR	ENCASE(DD)	TCC.E01	1
Drive:	HASH:			
C	C955E69296EA0FE8F55259B995F4B43F			

CADEIA DE CUSTÓDIA

Destino:	Data/Hora:	Origem:	Destino	Motivo:
PERICIA	Data: 05/10/2012	Nome/Org.: LOCAL APREENSÃO	Nome/Org.: SERGIO	Apreensão do equipamento envio para a perícia.
	Hora: 21h05m	Assinatura:	Assinatura:	
	Data:	Nome/Org.:	Nome/Org.:	
	Hora:	Assinatura:	Assinatura:	
	Data:	Nome/Org.:	Nome/Org.:	
	Hora:	Assinatura:	Assinatura:	
	Data:	Nome/Org.:	Nome/Org.:	
	Hora:	Assinatura:	Assinatura:	
	Data:	Nome/Org.:	Nome/Org.:	
	Hora:	Assinatura:	Assinatura:	
	Data:	Nome/Org.:	Nome/Org.:	
	Hora:	Assinatura:	Assinatura:	
	Data:	Nome/Org.:	Nome/Org.:	
	Hora:	Assinatura:	Assinatura:	

Figura 3 – Cadeia de Custodia.

3- FDTK-UbuntuBR v2.01.

FDTK(Forense Digital Toolkit) é um sistema operacional baseado no Ubuntu linux, é voltado inteiramente para a prática Forense Computacional, uma ferramenta

de uso prático e que apresente resultados precisos, que além de utilizar softwares livres para obter resultados, é totalmente em português.

A ideia de criar a FDTK surgiu em um trabalho de monografia, a ideia principal era esclarecer e trazer a tona técnicas utilizadas na prática forense computacional.

Segundo PAULO NEUKAMP em "a verdadeira historia do distro fdtk" durante a fase de pesquisa, surgiu um desafio lançado por seu orientado Prof. Msc. Leonardo Lemes “Será que é muito difícil fazer uma distribuição Linux focada em Forense Computacional?”, e o desse desafio surgiu o sucesso em que se tornou a ferramenta FDTK.

Havia três problemas na época, além da falta de atualização, todas as distribuições focadas neste assunto estavam a mais de dois anos desatualizadas, porém o que afastavam os profissionais da área eram a barreira com o idioma estrangeiro, a falta de menção nas etapas de pericia e a necessidade de um profunde conhecimento nas ferramentas.

A possibilidade de efetuar customizações necessárias, facilidade de utilização, disponibilidade de documentação e a regularidade de lançamentos de novas atualizações/versões foi os critérios usados para que o Linux fosse escolhido como base para o projeto, porém, na época, nenhuma distribuição focada em forense utilizava essa plataforma como base, sendo assim foi um diferencial na época. A interface escolhida foi a Gnome, pois a mesma, além de ser a mais utilizada no mundo, ainda possui uma série de qualidades.

Inicialmente sua divulgação foi feita em um canal Linux em 2007, e segunda as estimativas, nos primeiros 15 dias foram feitos mais de 7 mil downloads.

Passado um ano, foi então lançada a versão 2.0 com atualizações dos pacotes, melhorias e agora com logo e vários detalhes personalizados.

No lançamento da versão 3.0 não poderia ser diferente, 13 mil downloads apenas na primeira semana, mostrando o sucesso da ferramenta e a adoção maciça da mesmo na área.

Sobre as ferramentas selecionadas para fazerem parte do FDTK, foram escolhidas praticamente 100, todas open source, das quais, todas serão listadas abaixo separadas por etapas:

Coleta de Dados:

Formulário: Formulário referente a Cadeia de Custódia

gnome-screenshot: Tirar “prints” da área de trabalho.

aimage: Geração de imagem das mídias utilizando o padrão aff.

air: Interface gráfica para dd/dcfldd.

dc3ddgui : Interface gráfica para O DC3DD, imagens forense.

dcfldd : Versão melhorada pelo DOD-Departament of Defense do dd.

dd : Geração de imagem dos dados.

ddrescue : Ferramenta para recuperação de dados de hds com setores defeituosos.

mondoarquive : Copiar dados de nsf, fitas,hd’s ou cd's.

mondorestore : Restaurar dados de nsf, fitas, hd’s ou cd's..

rdd : Versão um pouco mais robusta do dd.

rddi : Prompt interativo do rdd.

sdd : Ferramenta dd desenvolvida para fitas.

memdump : Dumper de memória para UNIX-like.

md5sum : Gerar hash md5.

sha1sum : Gerar hash sha 160bits.

discover : Levantamento de informações sobre Hardware

hardinfo : Testes do Sistema e informações.

lshw-gráfico : Lista em formato HTML todos dispositivos de hardware

sysinfo : Mostra informações do sistema e do computador.

wipe : Remover dados das Mídias.

Exame dos Dados:

cabextract : Acessar arquivos .cab.

orange : manipular arquivos .cab.

p7zip : Ferramenta de acesso a arquivos zip.

unace : Descompactar extensões .ace.

unrar-free : Descompactar arquivos rar.

unshield : Ferramenta feita para descompactação de arquivos CAB da MS.

xarchiver : Visualizar, modificar e criar arquivos compactados.

zoo : Ferramenta para acessão de arquivos .zoo compactados.

dcraw : Acesso a imagens cruas de câmeras.

exif : Informações EXIF de arquivos jpeg.

exifprobe : Exame do conteúdo e da estrutura de imagens JPEG.

exiftran : Transformar imagens raw de câmeras digitais.

exiftags : Adquirir informações sobre a câmera e as imagens por ela produzidas.

exiv2 : Manipular metadados de imagens.

jhead : Visualizar e manipular os dados de cabeçalhos de imagens jpeg.

jpeginfo : Ferramenta para coletar informações sobre imagens jpeg.

antiword : Ferramenta para ler arquivos do MS-Word.

dumpster : Acessar os arquivos da lixeira do Windows.

fccu-docprob : Ferramenta para visualizar as propriedades de arquivos OLE.

mdb-hexdump : Ferramenta para manipulação de arquivos MDB.

readpst : Ferramenta para ler arquivos do MS-Outlook.

reglookup : Utilitário para leitura e resgate de dados do registro do Windows.

regp : Acessar o conteúdo de arquivos .dat.

tnef : Acessar anexos de email's MS.

bcrypt : Encriptar e decriptar arquivos usando o algoritmo blowfish.

ccrypt : Encriptar e decriptar arquivos e streams.

outguess : Detectar dados ocultos em imagens JPG.

stegcompare : Comparar imagens jpeg e detectar a existência de steganografia.

stegdimage : Detectar a existência de steganografia em imagens jpeg.

stegdetect : Detectar a existência de steganografia em imagens jpeg.

xsteg : Ferramenta gr fica para detectar steganografia em imagens jpeg.

ghex2 : Ferramenta de visualização de arquivos em formato HEX.

hexcat : Ferramenta de visualização de arquivos em formato HEX.

ghexdump : Visualizar arquivos em formato HEX.

affcat : Verificar conteúdo de arquivos .aff sem montar.

afcompare : Comparar dois arquivos .aff.

afconvert : Converte aff -> raw, raw -> aff, aff -> aff recompactando-o.

afinfo : Visualizar estatísticas sobre um ou mais arquivos aff.

afstats : Visualizar estatísticas sobre um ou mais arquivos aff.

afxml : Exportar metadados de arquivos aff para um arquivo xml.
dcat : Localizar dados dentro de arquivos dd, aff, ewf.
glark : Ferramenta semelhante ao grep para localizar dados.
gnome-search-tool : Ferramenta gráfica de localização de arquivos.
slocate : Localiza arquivos e indexa os disco
mac-robber : Coletar dados de arquivos para criar a linha de tempo (timeline).
mactime : Cria uma linha do tempo ASCII das atividades dos arquivos.
ntfscat : Concatenar arquivos e visualizá-los sem montar a partição NTFS.
ntfsclone : Clonar um sistema de arquivos NTFS ou somente parte dele.
ntfscluster : Localizar arquivo dentro de cluster ou de v rios clusters NTFS.
ntfsinfo : Obter informações sobre partições NTFS.
ntfslabel : Verificar ou alterar a descrição de partições NTFS.
ntfsls : Lista o conteúdo de diretórios em partições NTFS sem montá-los.
fcrackzip : Quebrar as senhas de arquivos compactados em ZIP.
john the ripper : Ferramenta para localizar senhas de usuários.
medussa : Crack de senhas.
ophcrack : Crack de senhas do Windows.
e2undel : Ferramenta para recuperar arquivos em partições ext2.
fatback : Ferramenta para recuperar dados de sistemas de arquivos FAT.
foremost : Ferramenta para recuperação de imagens a partir dos cabeçalhos.
gzrecover : Ferramenta para extrair dados de arquivos gzip corrompidos.
magicrescue : Recuperação de imagens RAW, baseando-se nos cabeçalhos.
ntfsundelete : Recuperar arquivos deletados em partições NTFS.
recover : Ferramenta para recuperar todos inodes deletados de um disco.
recoverjpg : Ferramenta para recuperar imagens jpg.
scrounge-ntfs : Ferramenta para recuperar dados de partições NTFS.
chkrookit : Ferramenta para identificar a presença de rootkits no sistema.
rkhunter : Ferramenta para identificar a presença de rootkits no sistema.
fspot : Organizador de imagens fotos.
gthumb : Visualizar e organizar imagens.
imageindex : Gera galeria de imagens em html.
Análise das Evidências:

coockie_cruncher : Analisar coockies.

eindeutig : Analisar arquivos .dbx.

fccu-evtreader : Script perl para visualizar arquivos de eventos da MS (EVT).

galleta : Analisar coockies do Windows.

GrocEVT : Coleção de scripts construídos para ler arquivos de eventos do Windows.

mork : Script perl para visualizar arquivos history.dat do Firefox.

pasco : Analisar cache do IExplorer.

rifiuti : Analisar arquivos INF2 da MS.

xtraceroute : Tracerouter gráfico.

autopsy : Ferramenta browser para realizar Perícias Forenses.

4 – Simulação.

A simulação será feita usando as ferramentas disponíveis no FDTK versão 2.01, entretanto, deve-se ter em mente o seguinte cenário: Foi entregue ao perito uma pen drive para que seja realizada a pericia, ao receber a possível prova, o mesmo iniciou-se o processo de Geração de imagem de dados (DD) com o auxilio da ferramenta Encase junto com três peritos garantindo a integridade da cópia.

Dentro da pen drive há dois arquivos, ambos com extensões .jpg(Pordosol.jpg e POrdosol.jpg) inicialmente aparentando ser duas simples imagens.

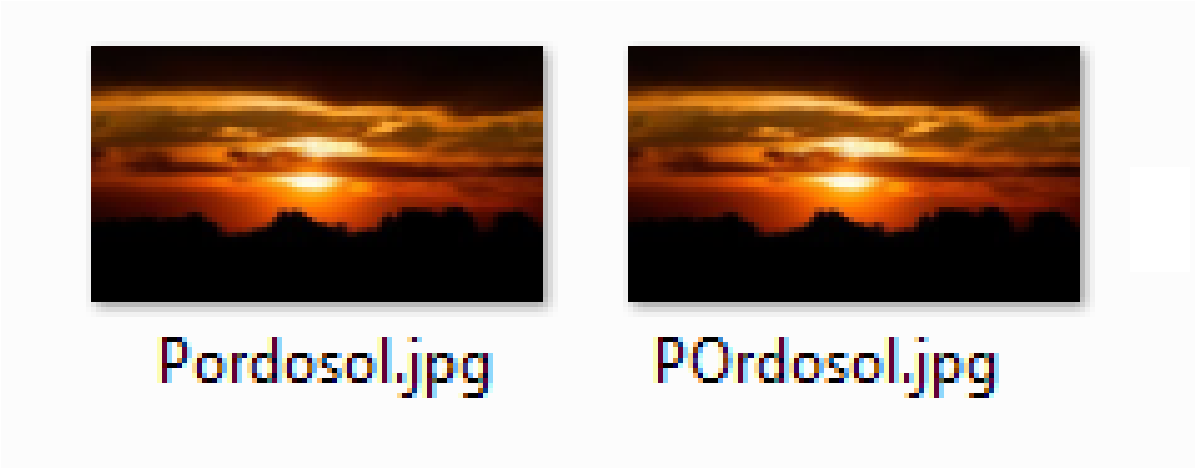

Figura 4 - Arquivos dentro da pen drive.

A simulação sempre será feita primeiramente no arquivo POrdosol.jpg e depois no Pordosol.jpg.

A primeira ferramenta a ser usada na análise é a exif. Exif(Exchangeable image file format), pode-se dizer que refere-se a uma padronização estipulada por fabricantes de câmeras digitais que armazenam informações técnicas de captura da foto junto ao arquivo da imagem. As etiquetas no padrão Exif incluem informações de interesse do fotógrafo, ou seja, dados de suas fotografias como data e hora e especificações sobre a câmera.

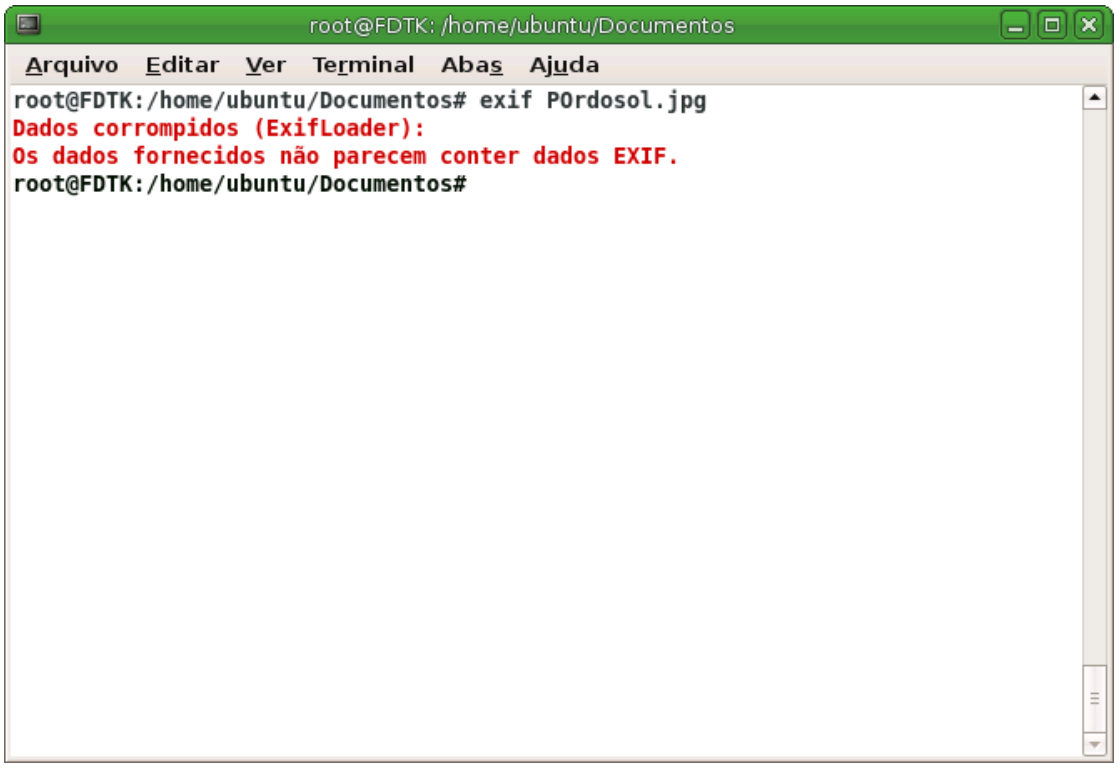

Figura 5 - Utilizando a ferramenta exif no arquivo POrdosol.jpg

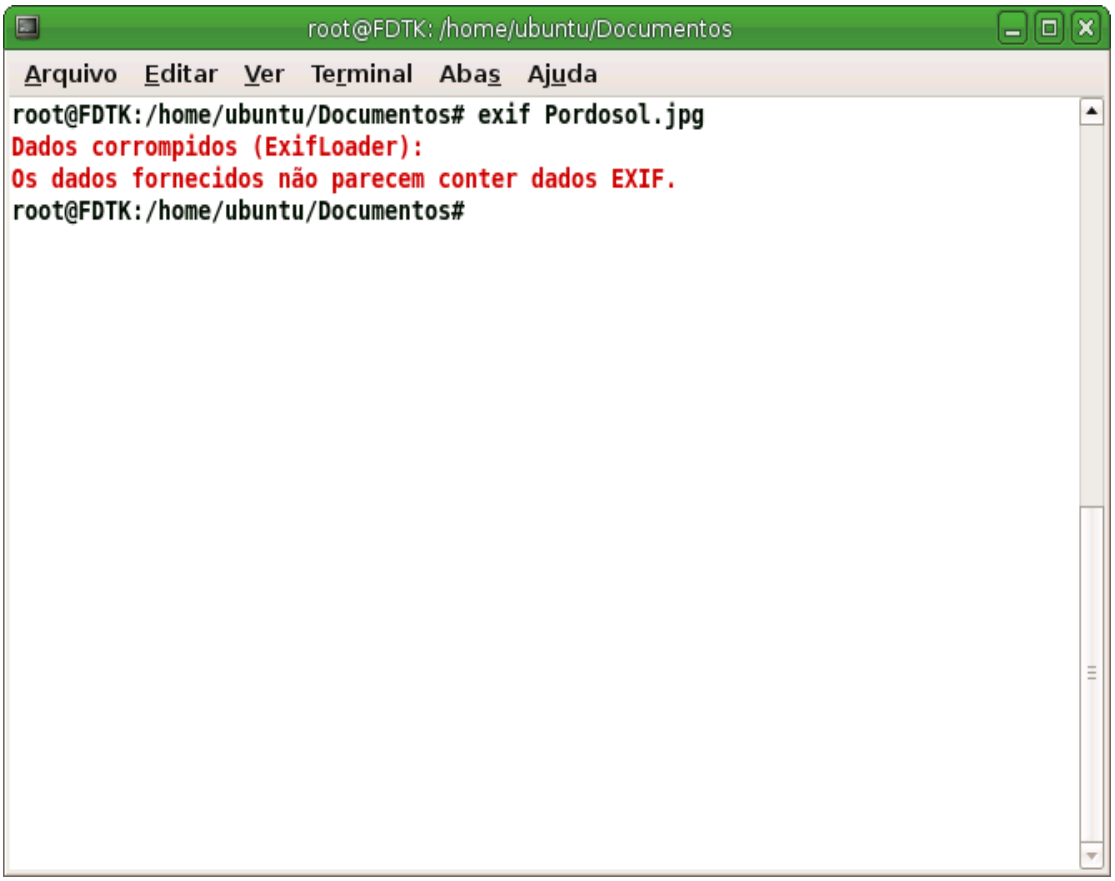

Figura 6 - Utilizando a ferramenta exif no arquivo Pordosol.jpg

Os dois arquivos aparentam não conter dados EXIF, mesmo assim usaremos a ferramenta exifprobe nas imagens para uma verificação mais profunda.

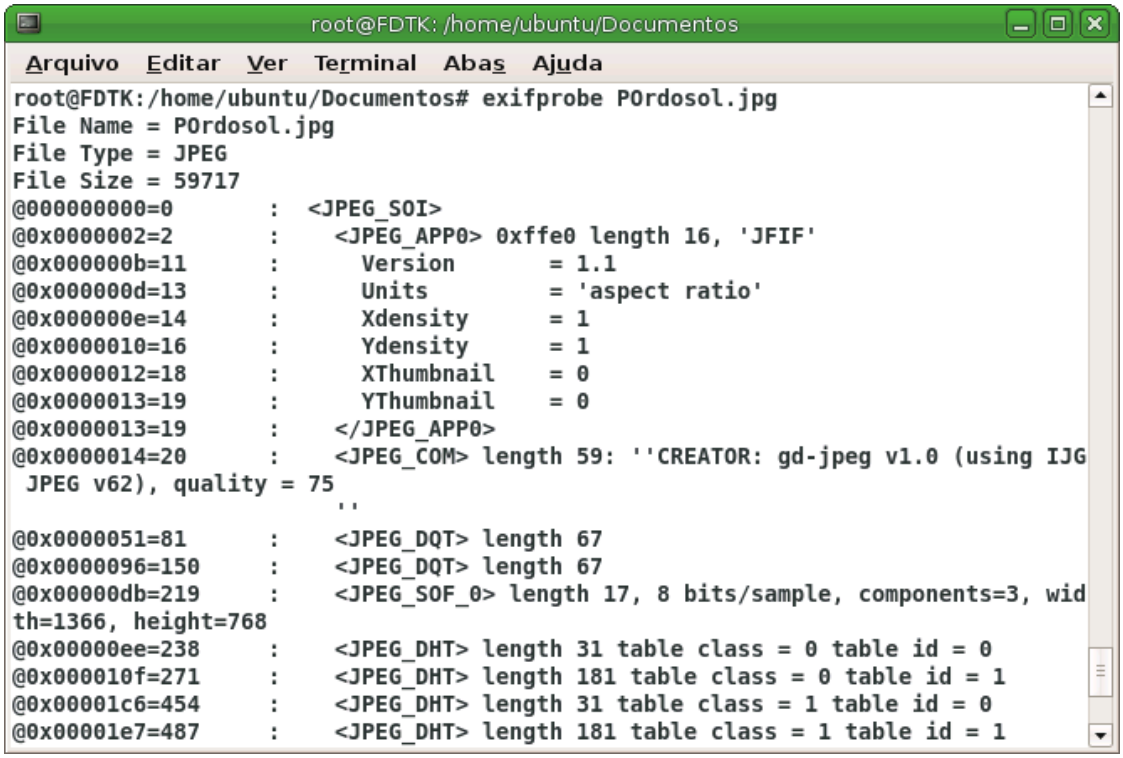

Figura 7 - Utilizando a ferramenta exifprobe no arquivo POrdosol.jpg pt1.

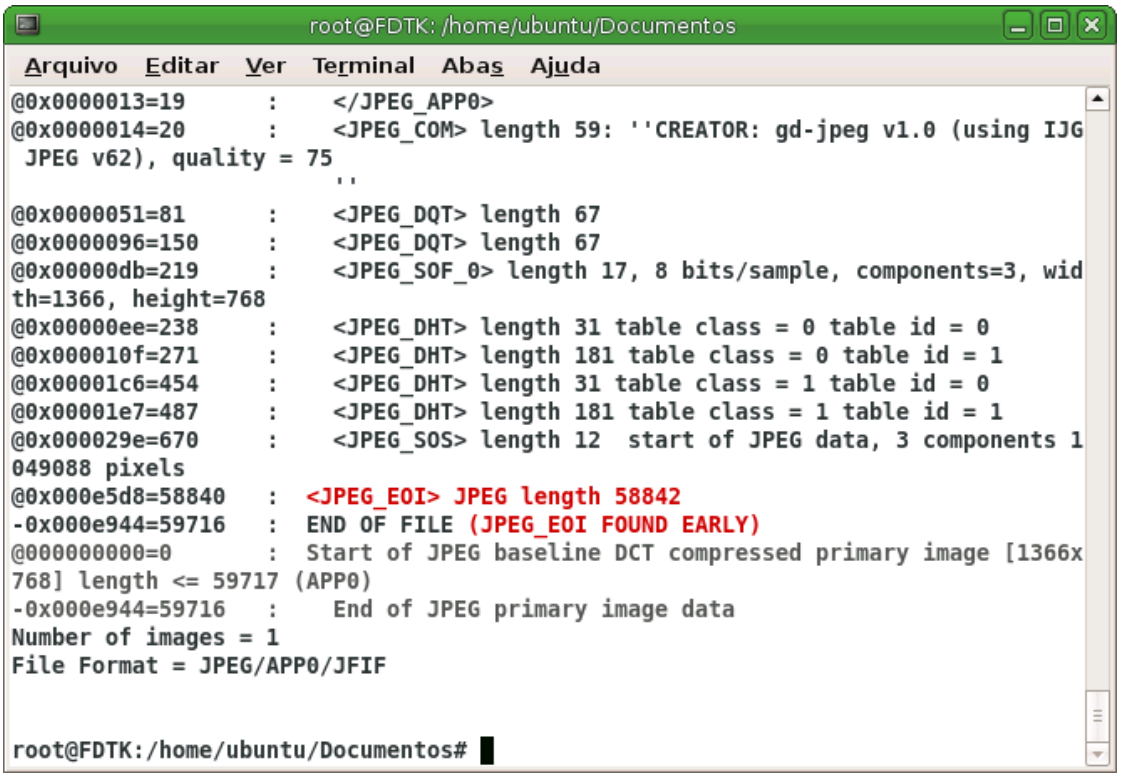

Figura 8 - Utilizando a ferramenta exifprobe no arquivo POrdosol.jpg pt2.

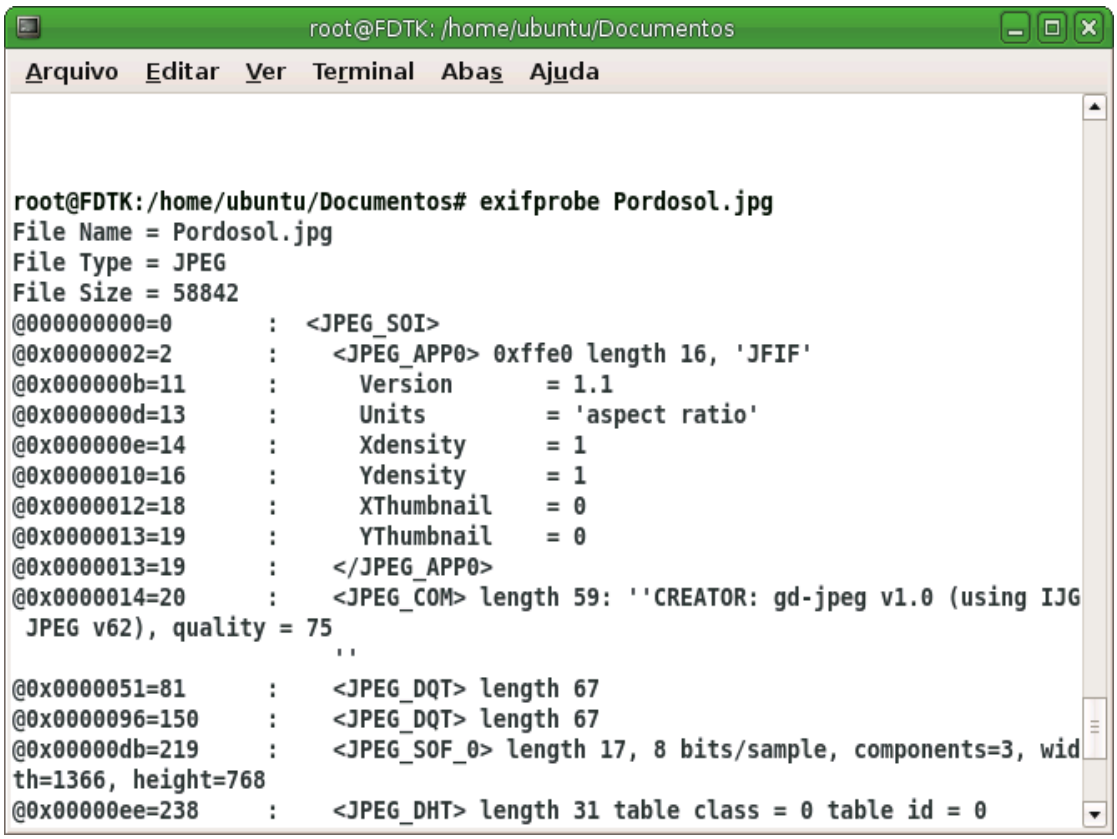

Figura 9 - Utilizando a ferramenta exifprobe no arquivo Pordosol.jpg pt1.

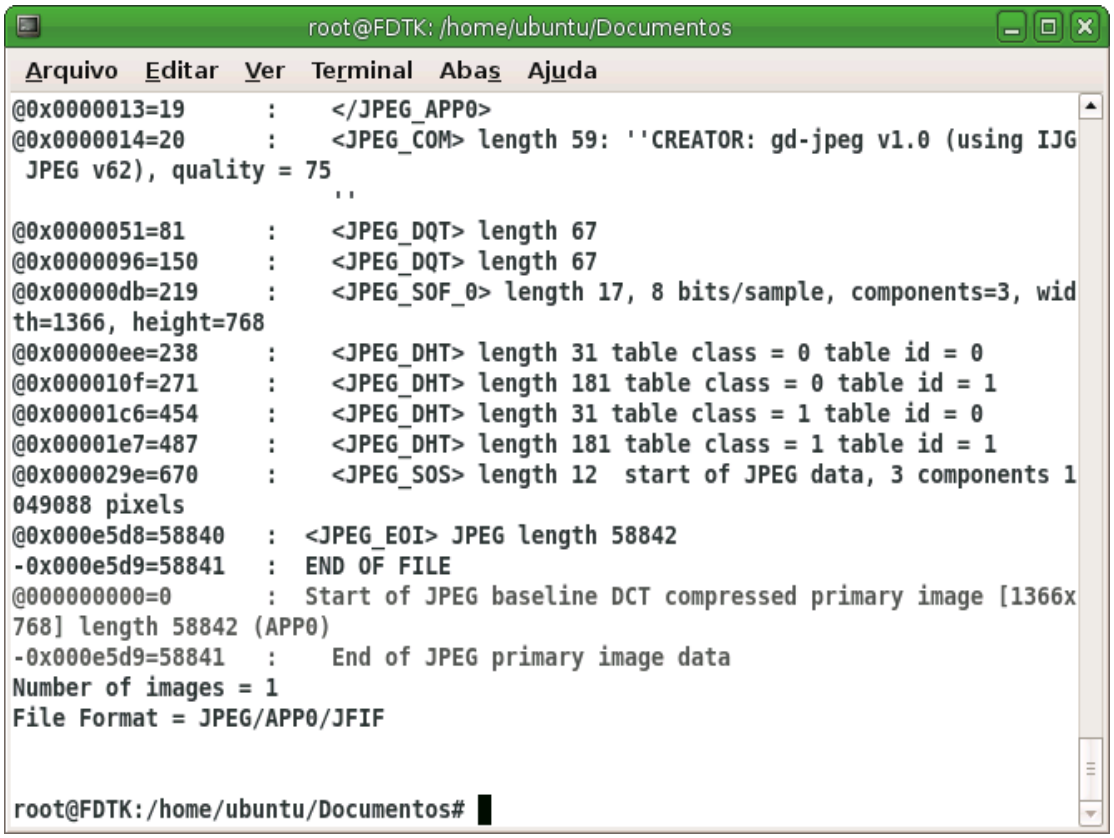

Figura 10 – Utilizando a ferramenta exifprobe no arquivo Pordosol.jpg pt2.

Com a ferramenta exifprobe obtêm-se mais características do arquivo com relação a sua estrutura, porém sem sinal de arquivos exif.

Neste primeiro momento nota-se algo um pouco estranho no arquivo POrdosol.jpg devido ao alerta em vermelho “(JPEG_EOI FOUND EARLY)”, JPEG_EOI encontrado cedo, antes da hora. Sendo assim buscaremos mais dados sobre esses arquivos. Com o jhead podemos obter algumas características como nome do arquivo, tamanho, data e resolução da imagem.

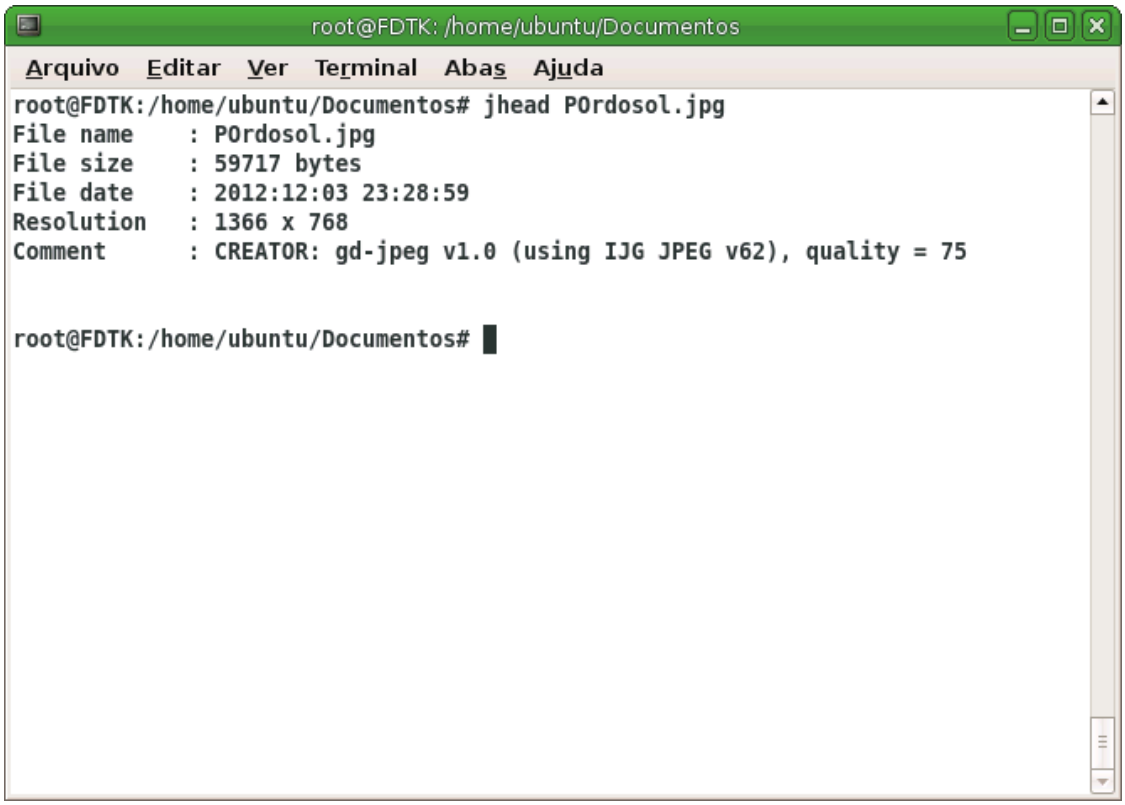

Figura 11– Utilizando a ferramenta jhead no arquivo POrdosol.jpg.

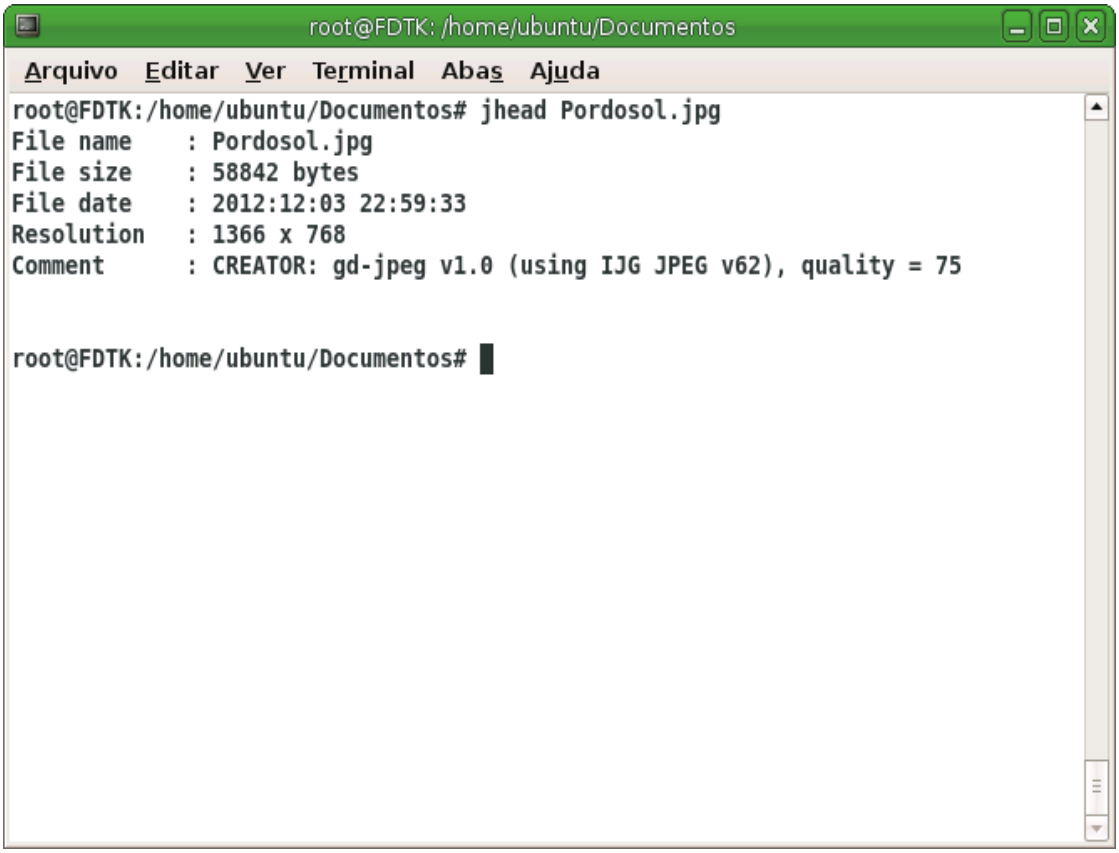

Figura 12 - Utilizando a ferramenta jhead no arquivo Pordosol.jpg.

Aprofundando na busca de mais informações sobre o arquivo podemos ver a sobre a integridade em que o mesmo se encontra com o uso da ferramenta jpeginfo.

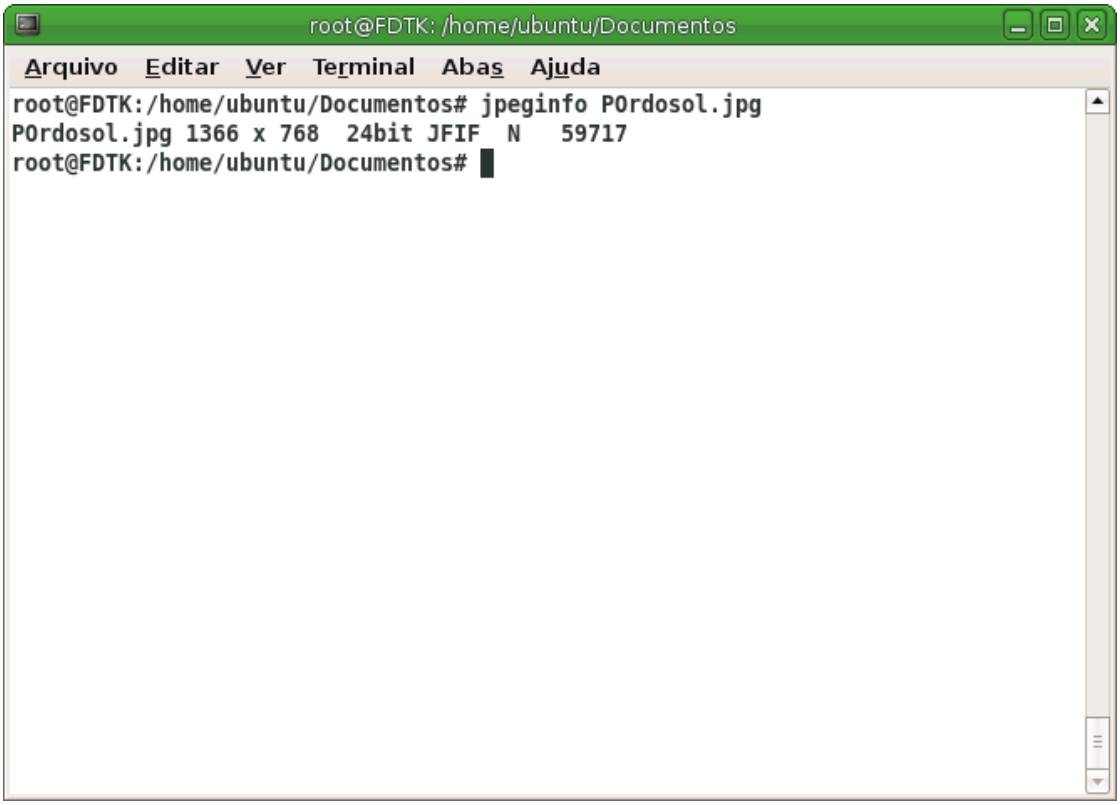

Figura 13 – Utilizando a ferramenta jpeginfo no arquivo POrdosol.jpg

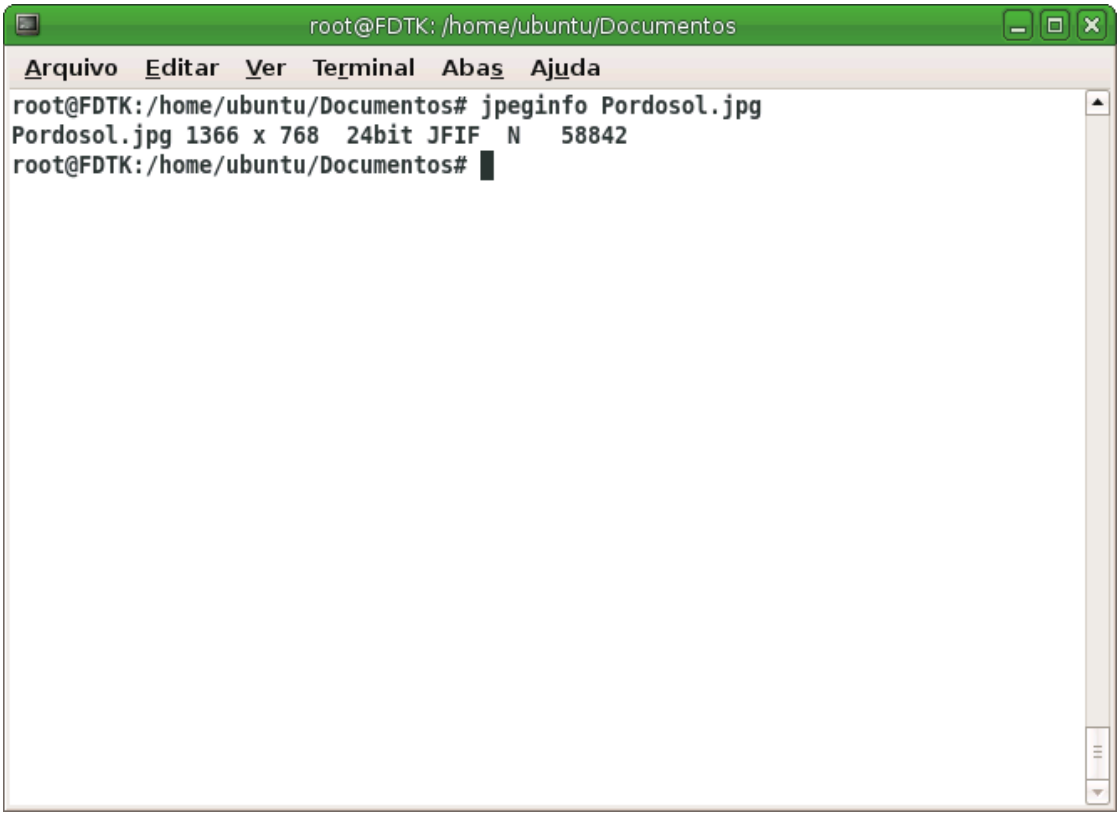

Figura 14 – Utilizando a ferramenta jpeginfo no arquivo Pordosol.jpg

A integridade dos dois arquivos esta ok, porém, nota-se desde o uso da ferramenta exifprobe que os arquivos apesar de aparentar serem iguais ambas têm tamanhos totalmente diferentes, enquanto o arquivo Pordosol.jpg tem 58.842 bytes o POrdosol.jpg tem 59.779 bytes, devido a essa diferença de tamanho há indícios de se tratar de esteganografia.

A ferramenta stegdetect tem a função de determinar se o arquivo se trata de esteganografia e caso seja, com o auxilio da ferramenta xsteg pode-se determinar a possível ferramenta utilizada para a criação do arquivo esteganografado.

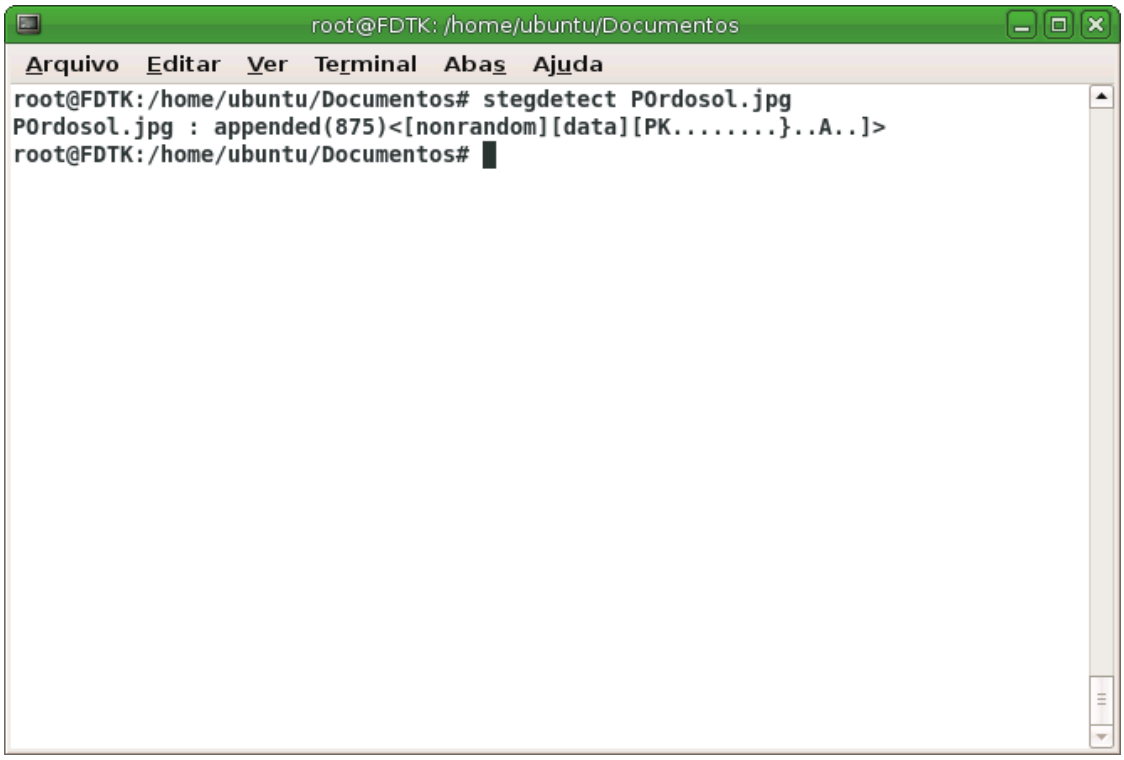

Figura 15 – Utilizando a ferramenta stegdetect no arquivo POrdosol.jpg

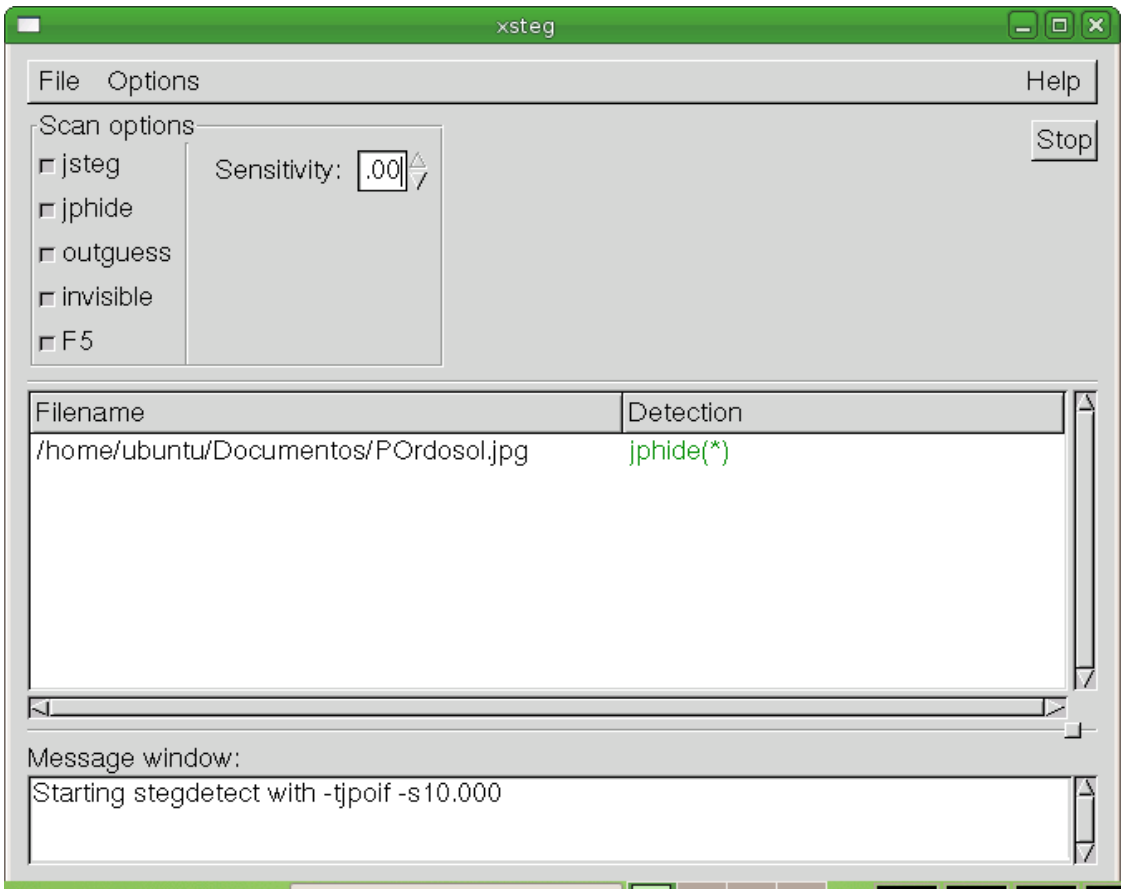

Figura 16 – Utilizando a ferramenta gráfica xsteg no arquivo POrdosol.jpg

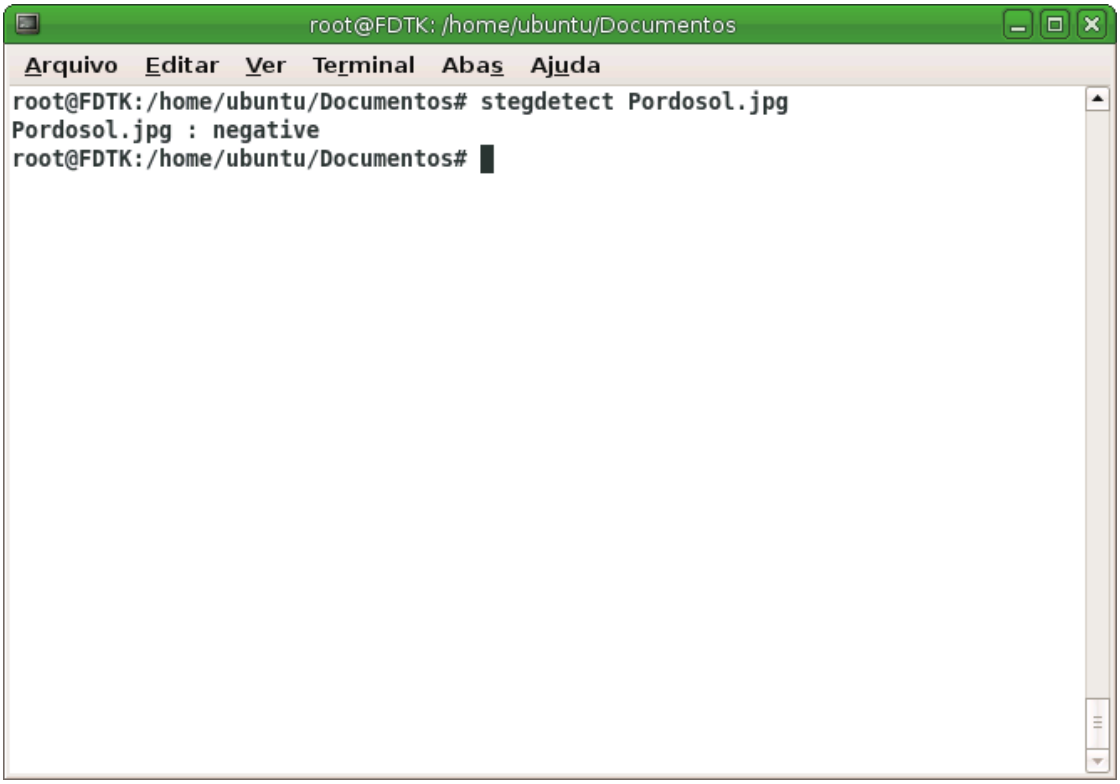

Figura 17– Utilizando a ferramenta stegdetect no arquivo Pordosol.jpg

Como esperado, com o uso do comando stegdetect no arquivo POrdosol.jpg o mesmo deu a resposta que tem anexado dentro do arquivo outro arquivo de tamanho de 937 bytes, exatamente a diferença entre o arquivo POrdosol.jpg e o Pordosol.jpg (59.779 bytes – 58.842 bytes = 937 bytes), ao executar o xsteg no arquivo POrdosol.jpg o mesmo retorna a mensagem gráfica que o possível programa utilizado na esteganografia do arquivo foi o JPHIDE, enquanto que, ao executar o stegdetect no arquivo Pordosol.jpg o mesmo retorna a mensagem “negative”, ou seja, o arquivo não foi esteganografado.

Sabe-se que o arquivo POrdosol.jpg tem omitido dentro dele outro arquivo devido a esteganografia, usando o comando *strings* é feito uma varredura em todo o arquivo binário com o intuito de extrair sequencias de caracteres de seu conteúdo, caso seja uma esteganografia simples entre uma imagem .jpg e um arquivo texto, com o comando strings, todo o conteúdo do arquivo texto seria impresso.

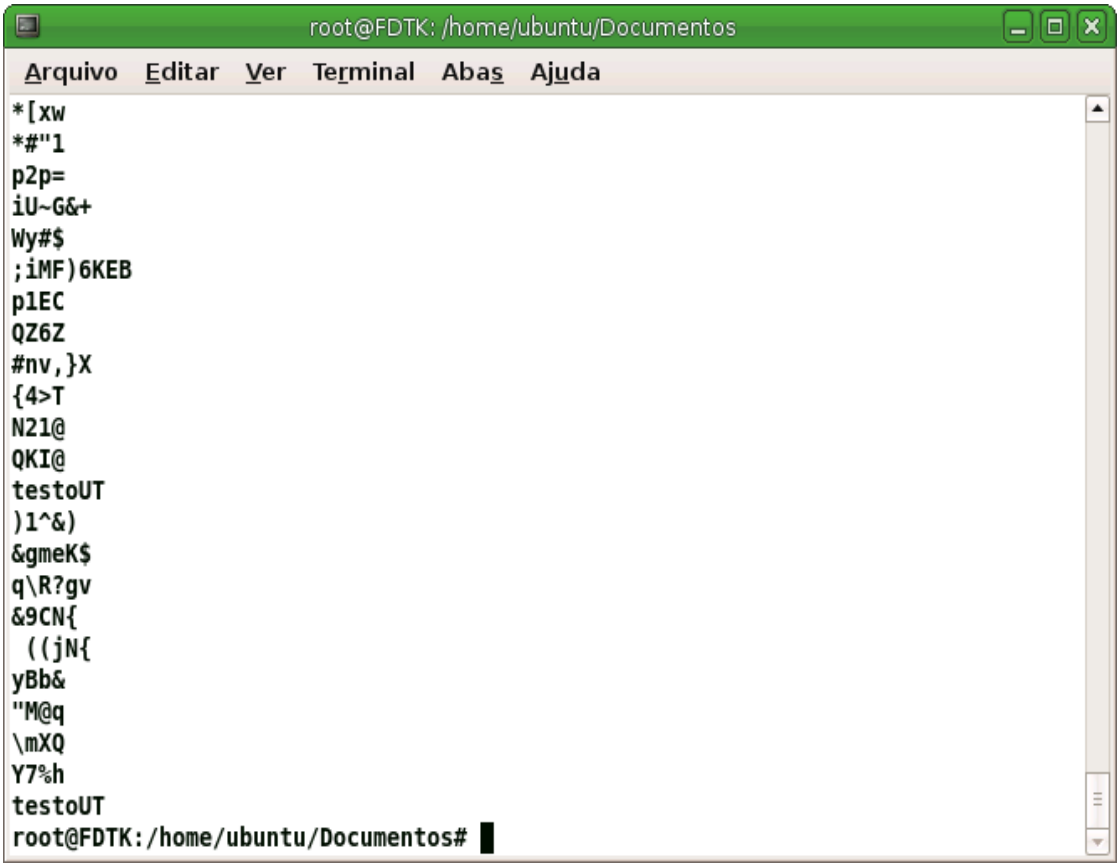

Figura 18 – Utilizando o comando strings no arquivo POrdosol.jpg

Ao utilizar o comando strings no arquivo POrdosol.jpg observa-se que a sequencia de caracteres “testoUT” se destaca entre as demais, além de se repetir e parecer formar uma palavra, sendo assim, com o uso de raciocínio logico, experiência e atenção aos detalhes entende-se que existe um arquivo com nome testo e pelo fato de ser a ultima sequencia de caracteres provavelmente trata-se de um arquivo .zip (a posição que aparece a sequencia de caracteres com o provável nome do arquivo depende da extensão da compactação).

Ao contrario do comando CAT usado na concatenação de arquivos, o comando Split é totalmente o oposto, o mesmo tem como objetivo dividir arquivos. Após usado o comando Split no arquivo POrdosol.jpg, ao dar o comando ls no diretório, o arquivo xaa foi “criado”, por padrão o Split “cria” o arquivo com a extensão aa, ab, ac, acima foi citado que provavelmente seria um arquivo compresso .zip, então nesse momento iremos renomear o arquivo xaa para x.zip, em seguida daremos o comando unzip no arquivo x.zip.

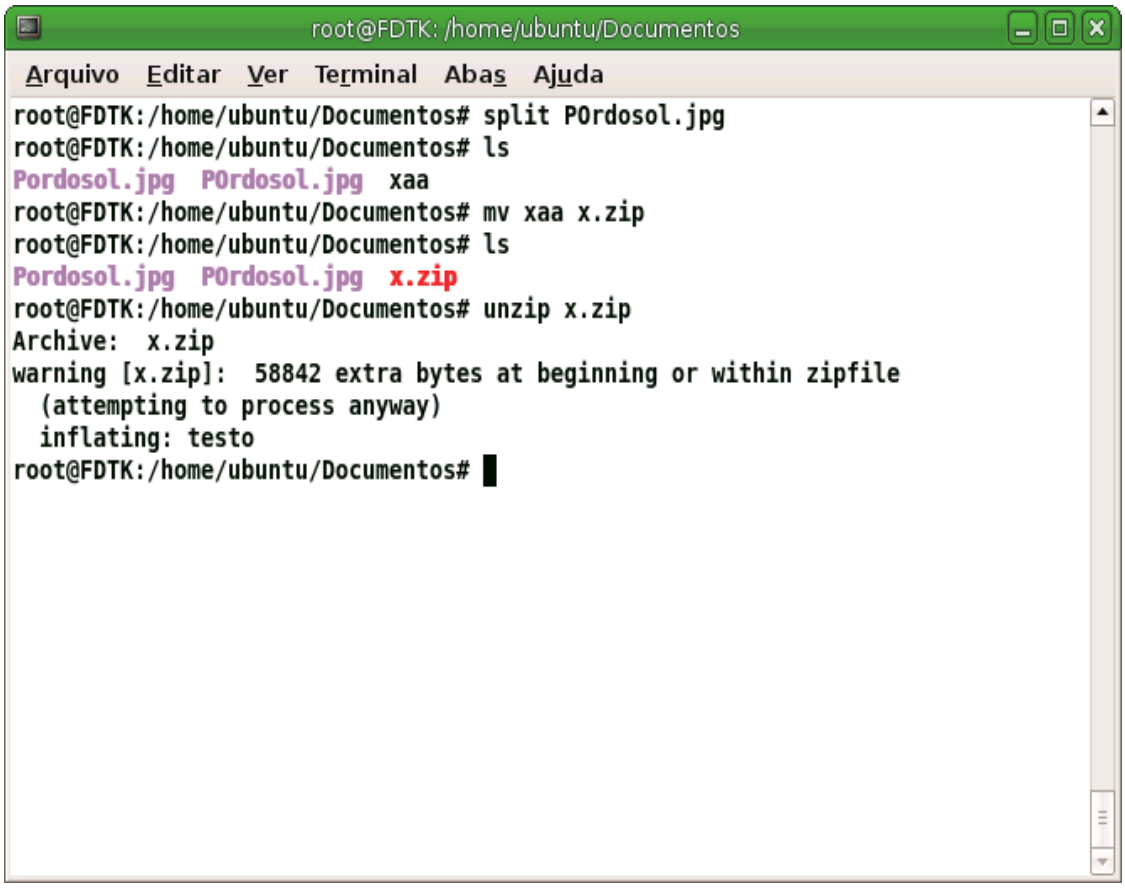

Figura 19 – Utilizando o comando Split, renomeando e extraindo o arquivo zipado do arquivo POrdosol.jpg.

Após usar o comando unzip, o arquivo oculto é então revelado “testo”, em seguida vamos utilizar o comando cat para a impressão do arquivo na tela.

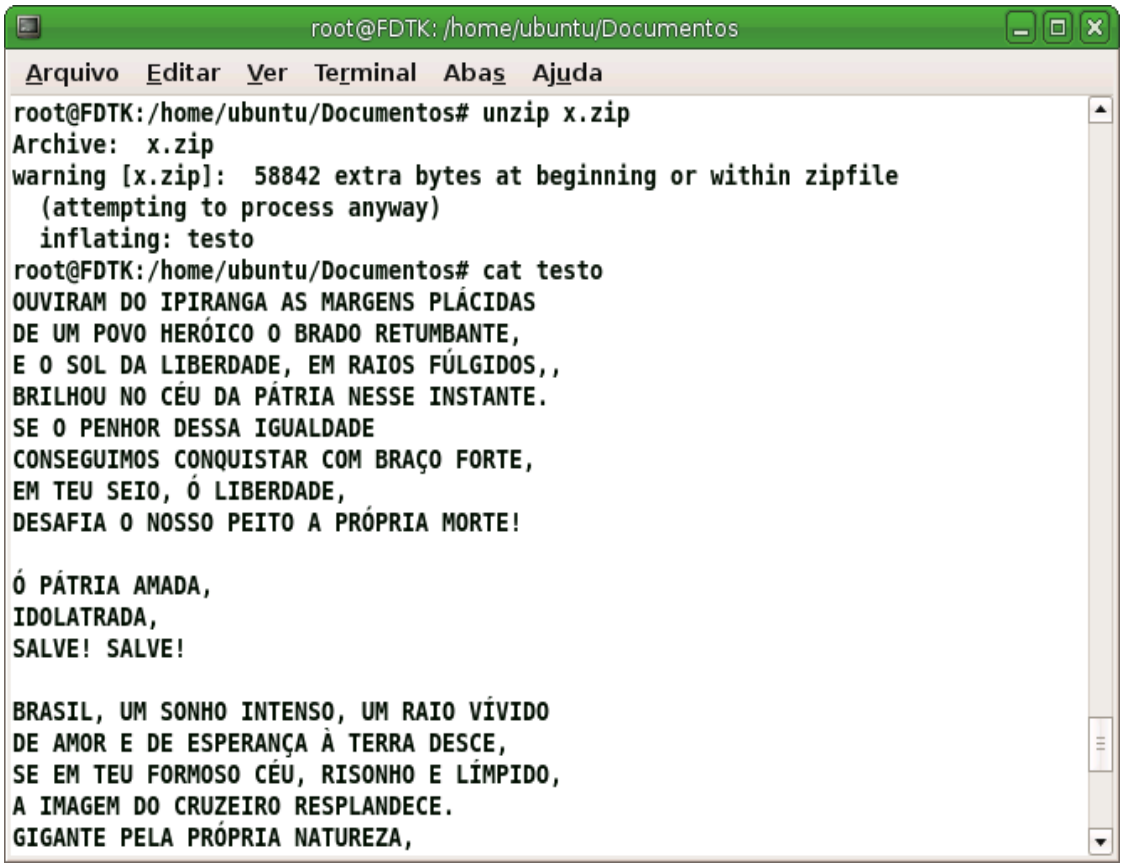

Figura 20 – Utilizando o comando cat no arquivo testo.

O conteúdo do arquivo foi impresso, o arquivo se tratava de um arquivo texto com o nome “testo" e tinha em seu conteúdo a letra do Hino Nacional Brasileiro.

Ao terminar a perícia deve-se fazer um laudo para apresentação ao tribunal, como nesse caso é uma simulação para estudo, indicarei então os itens necessários em um laudo.

O laudo varia muito o modelo, cada perito segue um modelo, porém em todos os modelos são indicados o(s) perito(s) envolvido(s), a descrição das partes envolvidas, solicitante da pericia, cadeia de custodia, objeto submetido (individuo com indícios em possível envolvimento com crimes, objetos e arquivos a serem periciados), metodologia usada na analise, analise do evento e resultados obtidos.

5 - Conclusão.

Diante do que foi apresentado neste trabalho, percebe-se a importância da área de forense computacional, os desafios vividos a cada nova pericia, a importância de os peritos estarem sempre atualizados e os prejuízos anuais causados pelos crimes virtuais, que a cada dia aumentam devido a facilidade com que se tem acesso a notebooks, computadores, mídias e o pouco conhecimento em segurança dos mesmos.

Verifica-se que a pericia forense computacional não é focada somente na área de investigação e criminalista, grandes empresas estão surgindo com o proposito de recuperar dados valiosos que foram perdidos de forma acidental ou maliciosa.

Ainda é necessário uma conscientização da população brasileira sobre segurança em seus aparelhos digitais (computadores, notebooks, smartphones) pois a cultura da mesma demostra com sua historia que só se preocupam com o assunto após o mesmo ocorrer, ou seja, após ter acontecido, sendo inevitável uma atenção preventiva em segurança afim de ser alvo de fraudes e estelionatários.

Ao simular a pericia na imagem compreende-se que conhecimento, experiência e muita atenção são necessárias nas buscas por evidências.

A distribuição FDTK-UbuntuBR mostrou-se bastante eficaz na simulação da pericia feita nas imagens, sua facilidade de uso, suas qualidades são inúmeras (atualizações, lançamentos de novas versões, o menu separado por etapas, totalmente em português e a não necessidade de um conhecimento profundo das ferramentas), sendo assim, a ferramenta faz jus a sua fama, tornando-se um fato real sua e verídico sua aceitação pelos peritos e seus numerosos downloads, sendo assim, recomendada a profissionais ingressantes e experientes na área.

Conclui-se também que é Insensato fazer um comparativo entre técnicas e ferramentas sendo que quanto mais ferramentas e métodos forem usados, mais segura será a pericia.

Por fim, tendo em vista que o tema em questão ainda é novo no Brasil, seria interessante a continuidade deste trabalho, de modo a mostrar novas tecnologias e ferramentas na área de pericia forense computacional.

REFERÊNCIAS BIBLIOGRAFICAS.

ARAUJO, José Mariano. **Cyber Crimes** – Delegado Mariano. Weblogger sobre crimes eletrônicos no mundo. Disponível em: <http://mariano.delegadodepolicia.com/>. Acesso em: 12/09/2012.

Daraya, vanessa. **Crimes Virtuais atingem 80% dos Brasileiros.** Disponível em:<http://info.abril.com.br/noticias/seguranca/crimes-virtuais-atingem-80-de-brasileiros-20092011-23.shl >Acesso em: 03/04/2012.

FARMER, Dan; VENEMA, Wietse.Pericia Forense Computacional:teoria e práticaaplicada. São Paulo: Pearson Prentice Hall, 2007

FREITAS, Andrey Rodrigues. **Perícia Forense Aplicada à Informática**. Rio de Janeiro: Brasport, 2006.

GARRISON, Clint P. Digital forensics for Network, Internet, and Cloud Computing: A forensic evidence guide for moving targets and data. Burlington: Syngress, 2010.

GALVÃO, Ricardo Kléber M.. **Perícia Forense Computacional.** Disponível em:<www.cefetrn.br/~rk/seginfo2009_2_rk.pdf> Acesso em: 02/04/2012.

GUIMARÃES, Célio Cardoso. OLIVEIRA, Flávio de Souza. REIS, Marcelo Abdalla dos. GEUS, Paulo Lício de**. Forense Computacional: Aspectos Legais e Padronização.**Disponível em:<*labcom.inf.ufrgs.br/ceseg/anais/2001/14.pdf* >Acesso em: 03/04/2012.

HEISER, Jay G.; KRUSE, Warren G. II; Computer Forensics Incident Response Essentials. Addison-Wesley: New York, 2001.

KENNEALLY, Erin. **Computer Forensics – Beyond the Buzzword**. Volume: 27, n. 4, agosto, 2002. Pág.. 8-11.

MELO, Sandro. **Computação Forense com Software Livre**. Rio de Janeiro: Alta. Books, 2009. 1ª edição.

MERCURI, Rebecca T. **Challenges in Forensic Computing**. Communications of the ACM. ACM, 2005.

OLIVEIRA, Flávio de Souza; GUIMARÃES, Célio Cardoso; de GEUS, Paulo Lício.Resposta a incidentes para ambientes corporativos baseados em windows, 2002. Disponível em: <http://www.las.ic.unicamp.br/paulo/papers/2002-WSeg-flavio.oliveira-resposta.incidentes.pdf> Acesso em: 21/08/2012.

OLIVEIRA, Flávio de Souza. Metodologias de análise forense para ambientes baseados em NTFS, 2001. Disponível em: <http://www.las.ic.unicamp.br/paulo/papers/2001-SSI-flavio.oliveira-forense.ntfs.pdf>Acesso em 12/07/2012

PHILIPP, Aaron. Hacking Exposed Computer Forensics, Second Edition: ComputerForensics Secrets & Solutions - McGraw-Hill Osborne Media– Segunda Edição- 2009.

QUEIROZ, Claudemir; VARGAS, Raffael. Investigação e Perícia Forense Computacional: certificações, Leis processuais e estudos de caso. Rio de Janeiro:Brasport, 2010.

RAMOS, Rodrigo. **Cenário Proposto I**. Evidência Digital, v. 3, julho, agosto e setembro, 2004. p. 49-51.

RODRIGUES, Thalita Scharr, Foltran Jr, Dierone César**. Analise de Ferramentas Forenses na Investigação Digital.** Disponível em: <http://ri.uepg.br:8080/riuepg/bitstream/handle/123456789/530/ARTIGO_AnaliseFerramentasForenses.pdf?sequence=1 > Acesso em: 03/04/2012

US-CERT. **Computer Forensics**. Disponível em: <http://www.us-cert.gov/>. 2012.

TOCHETTO, D., GALANTE, H., ZARZUELA, J., et al. (1995). Tratado de Perícias Criminalísticas. Editora Sragra-DC Luzzatto, 1ª Edição, 1995.