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

CAIO AUGUSTO MARTINS FRANCISCONI

UTILIZAÇÃO DE FERRAMENTAS DE PERÍCIA FORENSE NA SOLUÇÃO DE CRIMES DIGITAIS EM IMAGENS.

Assis
2014

CAIO AUGUSTO MARTINS FRANCISCONI

UTILIZAÇÃO DE FERRAMENTAS DE PERÍCIA FORENSE NA SOLUÇÃO DE CRIMES DIGITAIS EM IMAGENS.

Projeto de Conclusão de Curso apresentado ao Curso de Análise e Desenvolvimento de Sistemas, do Instituto Municipal de Ensino Superior de Assis – IMESA e à Fundação Educacional do Município de Assis – FEMA, como requisito parcial à obtenção do Certificado de Conclusão.

Orientando: Caio Augusto Martins Francisconi
Orientador: Me. Fábio Eder Cardoso

Assis
2014

FICHA CATALOGRÁFICA

FRANCISCONI, Caio Augusto Martins

Utilização de ferramentas de perícia forense na solução de crimes digitais em imagens/ Caio Augusto Martins Francisconi. Fundação Educacional do Município de Assis – Fema – Assis, 2014 70p.

Orientador: Msc. Fabio Eder Cardoso.

Trabalho de conclusão de curso

Instituto Municipal de ensino Superior de Assis – IMESA

1 – Investigação Digital de Imagens; 2 – FDTK; 3 – CAINE; 4 – BACKTRACK; 5 – FDTK;

CDD: 001.6

Biblioteca da FEMA

AGRADECIMENTOS

Em primeiro lugar agradeço a Deus, por ter chegado até aqui, pois sem ele nenhum sonho teria a possibilidade de ser concretizado, em segundo lugar a minha família que sempre esteve presente, me apoiando e incentivando em todos os sentidos.

Agradeço aos meus professores e ao meu orientador Me. Fábio Eder Cardoso, pelas sugestões e ensinamento durante todo esse trabalho. Aos alunos que compartilharam desse sonho durante esses anos e que hoje se tornaram grandes amigos.

A todos os amigos que souberam compreender a minha ausência e por todo apoio que me deram.

Orgulho-me por estar me formando nesse curso, é gratificante, é prova de que todo meu esforço valeu a pena. Sei que a trajetória não acaba por aqui, é apenas o começo, e que é por intermédio da conclusão desta etapa que outras possibilidades serão abertas em minha vida.

RESUMO

A Computação Forense Digital é uma ciência que vem crescendo anualmente, entretanto faltam orientações para informar qual a maneira mais fácil e ágil de se realizar uma perícia digital.

São diversas as ferramentas de utilização para se realizar um estudo de perícia forense. Dessa maneira, o mesmo processo pode ser repetido, utilizando diferentes técnicas e ferramentas, podendo se obter resultado semelhante ou diferente.

Sendo assim, o presente estudo propõe um processo de realização de perícia digital, ou seja, um processo criado e executado desde o início, que poderá ser realizado por qualquer pessoa ou empresa que tenha interesse na área.

Palavras Chaves: Computação Forense, Perícia Forense, Perícia Digital.

ABSTRACT

The Digital Computer Forensics is a science that is growing annually. However lacking guidelines to inform which is the easiest and fast way to make a digital expertise.

In addition, there are various tools used to conduct a study of forensics. Thus, the same process can be repeated with other techniques and tools, and the obtained result is different or the like.

Thus, this study proposes a method of performing digital expertise, ie, a process created and executed from the beginning, which can be performed by which person or company who has an interest in the area.

Keywords: Computer Forensic, Forensics Expertise, Digital Expertise.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT – NBR ISSO/IEC 27002 – Tecnologia da Informação: código de prática para a gestão da segurança da informação - 2001

IOCE - Organização Internacional de Evidência Digital – 1995

SPYWARES - Programa automático de computador, que recolhe informações sobre o usuário.·.

F.R.E.D. - Forensic Recovery Evidency Device – Sistemas otimizados para aquisição laboratório estacionária e análise.

FDTK – Software utilizado para varredura de disco rígido.

EDRM - Electronic Discovery Reference Model.

LINK – Palavras que ligam páginas de um mesmo site.

WEB – Palavra em Inglês que significa Teia, na informática pode se referir a WWW (Word, Wide, Web).

FTP - Protocolo de Transferência de Arquivos.

CRIMEWARE – Classe de programa malicioso criado especificamente para automatizar crimes virtuais.

LOGIN – Acesso a um sistema informático.

BITS – Menor unidade de informação que pode ser armazenada ou transmitida.

HASH – Sequência de bits gerados por um algoritmo de dispersão.

NEXT – Termo da língua inglesa que significa **próximo, seguinte, contíguo, logo em seguida, junto a, pregado.**

PEER-TO-PEER - É uma arquitetura de redes de computadores, onde cada um dos pontos da rede funciona tanto como cliente quanto como servidor, permitindo compartilhamentos de serviços e dados sem a necessidade de um servidor central.

OPEN CASE – Termo da língua inglesa que significa iniciar, abrir, destampar.

NEW CASE – Termo da língua inglesa que significa novo, recente.

HELP – Termo da língua inglesa que significa ajudar, apoiar, contribuir.

HOST - Qualquer máquina ou computador conectado a uma rede, podendo oferecer informações.

ADD – Termo da língua inglesa que significa somar, agregar, adicionar.

IMAGE – Termo da língua inglesa que significa imagem.

INTEGRITY - Termo da língua inglesa que significa integridade e honestidade.

CALCULATE - Termo da língua inglesa que significa somar, contar, extrair.

BIOS - Basic Integrated Operating System (Sistema Operacional Básico Integrado) é um programa de computador pré-gravado em memória permanente, executado por um computador quando ligado. Ele é responsável pelo suporte básico de acesso ao hardware, bem como por iniciar a carga do sistema operacional.

SUMÁRIO

1 – INTRODUÇÃO

Atualmente, a computação vem se tornando cada vez mais presente na vida da população mundial, apresentando aos usuários um grande número de informações processadas. Como em qualquer outro campo de estudo, a inovação tecnológica trouxe consigo uma série de benefícios para os indivíduos de um modo geral. Um bom exemplo a ser citado é comodidade e praticidade que esta inovação proporcionou, fazendo com que a necessidade de se estar presente para realização de determinadas tarefas do cotidiano se tornasse opcional ou até mesmo desnecessária, uma vez que tudo, ou quase tudo, pode ser resolvido através do uso de um simples celular, tablet, computador e etc.

Levando com consideração as inovações tecnológicas e avanço que o mundo vivencia, com tudo mudando a todo tempo, surgiu à necessidade de se criar mecanismos para auxiliar na resolução dos crimes digitais que começaram a surgir. E dessa forma, detectar os crimes, criminosos e também prevenir o acontecimento dos mesmos por meio de divulgação ampla das ameaças encontradas.

De acordo com Bustamante (2006) a Computação Forense realiza atividades e perícias relativas aos crimes de informática, tais como fraudes contra a administração pública, rastreamento de ameaças feitas via Internet, pedofilia, invasão de sistemas, quebra de privacidade de dados e outros. A grande diferença entre os crimes tradicionais e os crimes virtuais, é o modo de operação, uma vez que crimes virtuais utilizam dispositivos eletrônicos, computadores, redes e da Internet para a ação ou omissão do crime.

A tarefa de se identificar um criminoso tem se tornado cada vez mais complicada, devido ao anonimato exercido por eles, pela busca e coleta das evidências que podem estar distribuídas na web, dificultando a prática da perícia forense computacional. O presente trabalho aborda a utilização de ferramentas para apoio à investigação e perícia forenses dos chamados crimes digitais, de modo que tal ciência possa contribuir a fim de evitar e solucionar tais ocorrências.

1.1– OBJETIVOS DO TRABALHO

O objetivo principal deste trabalho é a abstração de conhecimento em torno da tecnologia e ferramentas de perícia forense na resolução dos casos de arquivos, mais especificamente em imagem. Demonstrando as vantagens da utilização dessa ciência, juntamente com um nível de segurança, evitando crimes digitais.

Depois de concluída a pesquisa, aplicar a mesma em algum segmento comercial ou forense onde será empregado todo conhecimento em forma de atividades práticas. A fim de apresentar as técnicas ensinadas para comprovação de que é possível obter um resultado satisfatório.

1.2 – JUSTIFICATIVA

Os números de crimes cibernéticos têm crescido anualmente, sendo assim a Computação sente falta de auxílio no combate e prevenção dos ataques cibernéticos. E paralelamente aos crimes, o crescimento tecnológico tem aumentado, principalmente com o uso de computadores, que atualmente é uma necessidade constante, visto que os seres humanos usufruem desta tecnologia para se comunicar com outras pessoas, do mesmo modo os criminosos também fazem uso desta tecnologia e estão sempre atentos para capturar informações importantes.

Adquirir conhecimento necessário para o uso correto e eficaz de todas as ferramentas e sistemas relacionados à perícia forense computacional, para auxilio ao processo de investigação e combate aos crimes.

1.3 – MOTIVAÇÃO

Atualmente, mais de 780 mil pessoas são vítimas de crimes realizados na Internet, o prejuízo mundial em 2012 já chegou a US$ 113 milhões, e no Brasil esse prejuízo é de R$ 18 milhões, sendo considerado o maior em todo o mundo. (LEPRE, 2013). Dessa forma, as empresas tem aumentado a busca por profissionais que atuam com a Computação Forense, buscando se prevenir contra os crimes virtuais e também proteger suas informações.

1.4 – PERSPECTIVA DE CONTRIBUIÇÃO

A perspectiva é que esse trabalho possa comprovar que tais técnicas e procedimentos utilizados podem auxiliar na resolução dos crimes virtuais. E, assim, despertar na sociedade e na comunidade acadêmica a ideia de prevenção, combate ao crime, identificação e julgamento de crimes virtuais. Este trabalho pretende disseminar aos alunos novas ideias em torno de boas práticas de uso de tecnologia da informação.

1.5 – METODOLOGIA DE PESQUISA

A metodologia aplicada neste trabalho é o estudo de caso, ou seja, aquela que desenvolve um estudo (técnicas e ferramentas utilizadas na Computação Forense) utilizando diversas fontes, entre elas: pesquisas bibliográficas em livros, internet, artigos e testes. Pretendendo responder questões do tipo: quais ferramentas e técnicas são utilizadas pelos peritos forenses e como prevenir um crime cibernético. Posteriormente será aplicado o conhecimento adquirido em forma de prática em algum segmento comercial ou forense, onde se possa comprovar tais técnicas e estudos.

1.6 – RECURSOS NECESSÁRIOS

Computador, máquina virtual, livros, ferramentas específicas e Internet.

1.7 - ESTRUTURA DO TRABALHO

Este trabalho foi dividido em capítulos que foram apresentados da seguinte maneira:

No primeiro capítulo apresentou-se a contextualização e a justificativa para o desenvolvimento da proposta de trabalho.

O Segundo capítulo abordou a importância da informação e a segurança da mesma para organizações e pessoas.

O Terceiro capítulo apresentou os crimes cibernéticos, também cita alguns exemplos de como os criminosos agem e alguns métodos de prevenção.

O Quarto capítulo mostrou o conceito da computação forense, quais são as técnicas, ferramentas e métodos utilizados pelos peritos para resolução dos casos.

Por fim, no último capítulo apresentada a conclusão do trabalho, e organograma atualizado.

2 – INFORMAÇÃO

Este capítulo explica de forma geral, sobre o que é a informação e segurança da informação, onde o mesmo dará uma visão geral sobre a importância da informação para as organizações e pessoas. E o porquê tais dados precisam ser íntegros, confiáveis e protegidos de pessoas não autorizadas ao acesso.

2.1 – O QUE É INFORMAÇÃO

Segundo o Dicionário de AURÉLIO BUARQUE DE HOLANDA FERREIRA, informação é um dado acerca de alguém ou algo, o conhecimento; e, segundo a Teoria da Informação, NBR ISSO/IEC 27002:2005, “é um ativo que, como qualquer outro, é importante para negócios, tem seu valor para organizações e consequentemente necessita ser protegido”.

No contexto de Tecnologia da Informação (TI), este conceito está relacionado a um conjunto de dados que constitui uma mensagem que possa ser interpretado a fim de solucionar problemas e colaborar para a tomada de decisões.

A informação é um elemento fundamental no processo da comunicação como um todo, que sofre processo de manipulação e organização dos dados, neste sentido, a informação é um conhecimento inscrito ou gravado sob uma forma escrita, oral ou audiovisual.

2.2 – SEGURANÇA DA INFORMAÇÃO

É a proteção da informação contra vários tipos de ameaças para garantir a continuidade, minimizar os riscos e maximizar o retorno dos investimentos e as oportunidades dos negócios. Levando em consideração três aspectos de extrema importância: confiabilidade, integridade e disponibilidade da informação. (Marcelo Sampaio, 2011).

1. Confiabilidade: garantia de que a informação é acessível somente por pessoas autorizadas a terem acessos;

2. Integridade: disponibilidade de informações confiáveis, corretas e íntegras;

3. Disponibilidade: garantia de que somente os usuários autorizados obtenham acesso à informação;

Diante dos tópicos apresentados, podemos concluir que para as organizações é imprescindível a proteção da informação, a fim de manter a ética da sua imagem, nome, competitividade e etc.

A imagem a seguir ilustra como a técnica de segurança de informação se baseia para realizar a proteção da informação. Os três aspectos que a tecnologia considera primordial para afirmar que um dado ou ativo precisa ter para ser considerável seguro.

Figura 1 – Aspectos necessários que envolvem a Segurança da Informação. (Dodt, Claudio, 2011).

3 – CRIMES CIBERNÉTICOS

Este capítulo apresenta uma visão geral sobre qual definição dos crimes cibernéticos, qual a forma que os mesmos ocorrem e qual a quantidade de crimes ocorridos anualmente. Também expõe quais os golpes mais realizados, quais os tipos de vírus e suas formas de envio, bem como, algumas dicas para prevenção dos mesmos.

3.1 – DEFINIÇÃO DE CRIMES CIBERNÉTICOS

Os Crimes Cibernéticos citados se referenciam aos crimes ocorridos em atividades criminosas contra dados ou informações privadas, ou até mesmo fraudes, pornografia e falsificação (Krone, 2005). Tal termo se refere aos famosos golpes, para tentar desviar dinheiro de contas, ter acessos a informações pessoais, como por exemplo: senhas, ou também a dados importantíssimos de organizações, a fim de se prejudicar a mesma.

Os crimes são divididos em duas categorias gerais, definidos para os efeitos desta pesquisa como crimes cibernéticos do tipo I e II.

Os crimes cibernéticos do tipo I apresentam as seguintes características:

• Do ponto de vista da vítima, é o evento que ocorre apenas uma vez. Por exemplo, a vítima baixa um Cavalo de Tróia sem saber, o mesmo instala um programa malicioso para registro de digitação no computador. Ou a vítima recebe um e-mail contendo o que parece ser um link para uma entidade conhecida, mas que na realidade é um link para um site malicioso.

• Em muitos casos, falhas ou vulnerabilidades no software fornecem um ponto de apoio para o criminoso. Por exemplo, criminosos que controlam um site podem aproveitar a vulnerabilidade de um navegador da Web para introduzir um Cavalo de Tróia no computador da vítima.

As características do crime cibernético do tipo II são:

• Geralmente de uma série contínua de eventos envolvendo interações repetidas com a vítima. Por exemplo, o criminoso faz contato com a vítima em uma sala de bate-papo para estabelecer uma relação ao longo do tempo. Com o tempo, o criminoso aproveita a relação para cometer um crime.

Geralmente, os criminosos usam programas que *não* estão incluídos na classificação de atividades ilegais. Por exemplo, as conversas podem acontecer usando clientes de mensagens instantâneas (IM) ou arquivos podem ser transferidos usando FTP.

Podem-se citar exemplos em que o criminoso consegue se apossar do equipamento para realizar tais crimes, ou quando ele tem acesso ao mesmo através de programa malicioso para conseguir furtar as senhas, informações importantes e etc.

O grande número de ocorrências desta natureza fez com que as instituições começassem a se especializar quanto ao combate e prevenção dos mesmos. Sendo assim, as organizações têm investido em aplicações inteligentes, daí a crescente busca pela perícia forense aplicada a informática. Os especialistas utilizam técnicas, métodos, ferramentas, normas e leis para comprovar tais crimes e rastrear o criminoso.

A imagem a seguir é um gráfico de incidentes reportados ao CERT. br (Centro de Estudos, Respostas e Tratamentos de Incidentes de Segurança no Brasil), que ilustra o crescimento de crimes digitais em nosso País.

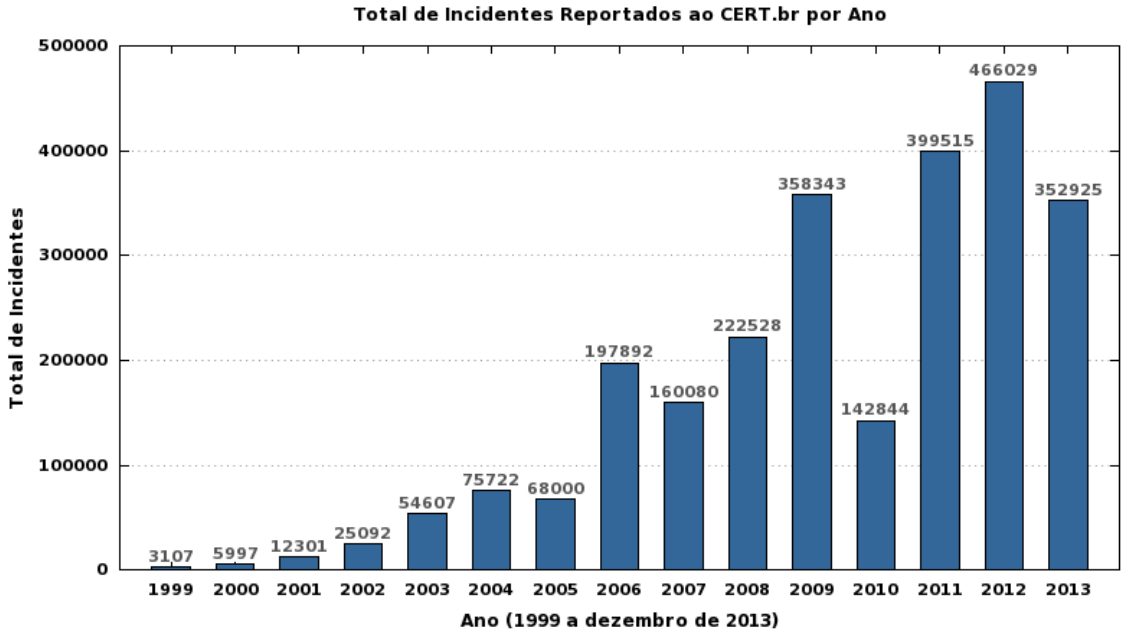


Figura 2 - Gráfico da evolução de ocorrências de Crimes Cibernéticos. (Estatísticas dos Incidentes Reportados ao CERT, 2013).

3.2 - PHISHING/PHARMING

Os dois temas tratados acima se referem aos famosos golpes on-line, onde os mandatários são ladrões de identidade especializados em tecnologia. E que se utilizam dos programas maliciosos ou através da *web,* por meio de sites para coletar informações sigilosas, contas bancárias e senhas de cartões de créditos das vítimas. Disponível em: <http://br.norton.com/cybercrime-phishing/promo> Acesso em: 25 fev. 2014.

Os eventos se iniciam geralmente com uma falha do sistema de segurança, onde são enviados os chamados “e-mails isca”, que direcionam o usuário para uma *web site* falso completamente igual ao site legítimo, onde o mesmo irá fornecer a senha e nome, e do mesmo modo conseguirá fazer o acesso normalmente. Posteriormente todas as informações pessoais do usuário serão enviadas ao mandatário por e-mail. Em alguns casos as informações ficam alocadas em algum servidor que o criminoso manipule.

Na maioria das vezes esses crimes duram em média alguns dias, onde as vítimas geralmente respondem em menos de 24 horas do início do caso.

3.3 - BOOTS

Referenciam-se a um sofisticado tipo de crime cibernético enfrentado pela internet, é semelhante ao Cavalo de Tróia, porém por ter uma variedade de tarefas recebeu esse nome. Suas principais tarefas são o envio de *spam*[1] e retiradas de sites da internet como negação de serviço. Fica a procura de computadores vulneráveis e desprotegidos onde possam infectar, depois de conseguir se alocar começa a responder as solicitações do seu mestre.

Os boots não funcionam sozinhos, fazem parte de uma rede de computadores infectados, chamada “bootnet”. As bootnets são criadas por invasores que infectam repetidamente os computadores-vítimas. Os computadores zumbis são controlados por um computador mestre chamado “servidor de comando de controle”. A partir deste, servidor, os criminosos

[1] Spam: é o termo usado para referir-se aos *e-mails* não solicitados, que geralmente são enviados para um grande número de pessoas, quando o conteúdo é exclusivamente comercial.

cibernéticos gerenciam suas *bootnets* e instruem um exército de computadores zumbis para trabalharem em seu nome.

3.4 - CAVALOS DE TRÓIA/SPYWARE

Um Cavalo de Tróia nada mais é que um programa que aparenta ser útil e interessante ao usuário, na qual só provocam danos ao computador. Cada vez mais são utilizados como primeiro passo de um ataque virtual onde ficam ocultos realizando downloads e instalação de ameaças mais robustas.

O cavalo de Troia é muito encontrado em computadores domésticos, onde sua principal atividade é capturar senhas para cometer os crimes. Já o *Spyware*[2] é um programa que espionam um computador, coletando informações pessoais, como nomes de usuários, senhas de bancos e etc.

Cavalos de Tróia e *Spyware* constituem os Crimes Cibernéticos: duas das principais ferramentas que um criminoso cibernético adota para obter acesso não autorizado e roubar informações de vítimas como parte de um ataque.

A figura 3 da página 23 ilustra no mapa o envio de Cavalos de Tróia mundialmente, expondo de onde foram enviados os vírus.

[2] Spyware: Programa automático de computador, que recolhe informações sobre o usuário.

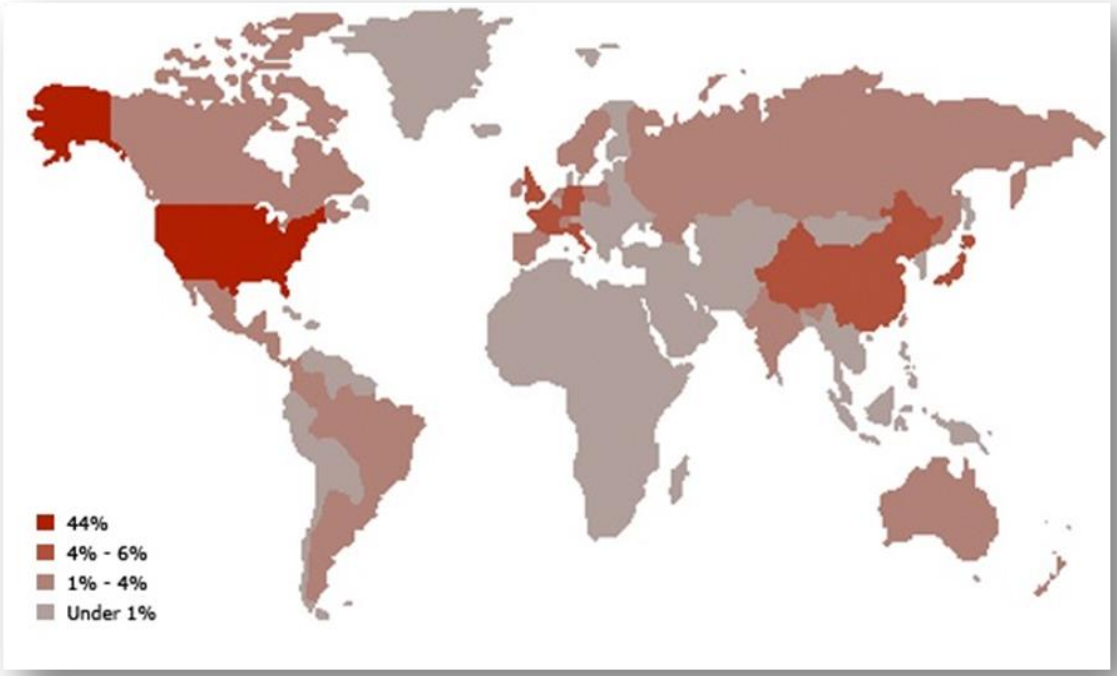


Figura 3 – Mapa dos Envios de Cavalos de Tróia no Mundo. (Symantec, 2012)

3.5 - PREVENÇÃO

Quanto à prevenção, a mesma pode ser simples, desde que o usuário esteja sempre atento a recomendações técnicas e sempre esteja desconfiado. Quanto mais difícil for o trabalho do criminoso, maior a chance dele desistir de realizar o ataque.

Algumas dicas que podem auxiliar:

- Mantenha seu computador atualizado com as atualizações mais recentes.
- Verifique se o computador está configurado com segurança.
- Escolha senhas complexas e não as divulgue.
- Proteja seu computador com softwares de segurança.
- Proteja suas informações pessoais

4 – PERÍCIA FORENSE COMPUTACIONAL

O capítulo a seguir apresenta a ciência que auxilia no combate aos crimes cibernéticos, como agem os peritos, quais suas técnicas e ferramentas de apoio. Consta nesse capítulo também onde pode ser aplicada a perícia, e qual é o objetivo principal desse trabalho.

4.1 – DEFINIÇÃO

É uma ciência que através de técnicas especializadas, trata da coleta, preservação e análise de dados eletrônicos em um incidente computacional ou que envolvam a computação como meio, apresentando a prova do fato através de laudo pericial para a Justiça (Marcelo Sampaio, 2011). No caso da Computação Forense o incidente computacional é tratado na esfera penal, buscando determinar causas, meios, autorias e consequências pós-crimes.

A perícia abrange todos os segmentos, e é considerada uma etapa de grande importância para as respostas a incidentes, onde buscará resolver de forma objetiva e clara o crime. Portanto, a Computação Forense tem como objetivo, determinar a dinâmica, materialidade e autoria de ilícitos à área da informática, tendo como questão principal a identificação e o processamento das evidências coletadas. A perícia forense utiliza-se de outros conceitos de subáreas, como: Banco de Dados, Redes de Computadores, Sistema Operacional e Algoritmos.

As principais ferramentas utilizadas para auxílio na resolução dos crimes são: Forensic Toolkit (FDTK), PERI-BR, Backtrack e Caine, entre outros utilitários de código aberto. Diversos equipamentos também foram desenvolvidos para auxiliar na obtenção de provas e preservação das provas, como bloqueadores de escrita de discos e duplicadores forenses, como o Forensic Recovery Evidence Device F.R.E.D.

4.2– CADEIA DE CUSTÓDIA

Procedimento utilizado para recolher e proteger as provas encontradas durante um caso de investigação, onde se irá documentar toda a história cronológica da evidência. Todos os processos relacionados à perícia, como: coleta, manuseio e análise com seus devidos cuidados tomados e sem nenhuma falha de integridade, poderão ser usados para a solução do incidente (Marcos Lopes, 2006).

A Cadeia de Custódia tem sido adotada para relatar todo o incidente, e tem sido muito utilizada para resolução dos casos, pressupõe-se que seja trabalhado em equipe, tanto o pessoal interno quanto o externo, desde a equipe responsável pelas análises toxicológicas forenses, englobando os responsáveis pela coleta, recebimento, analise e disposição final da amostra. Esta terminologia vem sendo legalmente utilizada para garantir a identidade e integridade da amostra, em todas as etapas do processo.

A figura abaixo ilustra dois modelos de etiquetas utilizadas pelos laboratórios de computação forense para identificação dos equipamentos coletados, entre eles computadores, celulares e tablet. Onde a mesma facilita na identificação e manuseio dos mesmos.

OCORRÊNCIA Nº		
LAUDO Nº:	EXPEDIENTE:	
CASO:	MARCA:	
MODELO:	CAPACIDADE:	NUM DE SÉRIE:

Exemplo de etiqueta para os dispositivos de armazenamentos.

OCORRÊNCIA Nº		
LAUDO Nº:	EXPEDIENTE:	
CASO:		
ORGÃO REQUISITANTE:		
AUTORIDADE REQUISITANTE:		
TIPO		
MARCA:	MODELO:	NUM DE SÉRIE:

Exemplo de etiqueta para equipamentos.

Figura 4 – Exemplo de Etiquetas preenchidas pelos laboratórios para exames de Máquinas e Dispositivos. (Sampaio, Marcelo). Computação Forense, 3ªEdição, 2011.

Todas as amostras são recebidas como evidências, as quais serão analisadas e o seu resultado, apresentado na forma de laudo que será utilizado no processo judicial. Estas devem ser manuseadas de forma cautelosa, para evitar futuras alegações de adulteração ou má conduta que possam comprometer as decisões relacionadas ao caso em questão. Disponível em: < http://jus.com.br/artigos/21391/a-cadeia-de-custodia-e-a-prova-pericial>
Acesso: 01 mar. 2014.

Na página seguinte, a figura 5 ilustra o modelo *e-Discovery,* o mesmo é utilizado como processo de coleta, tratamento, manuseio, classificação e revisão dos dados eletrônicos com a intenção de utiliza-los como evidências em um processo judicial.

Portanto, tal modelo tem o propósito de facilitar e mapear toda a análise realizada em meios eletrônicos que possam ser utilizados em processos. Sendo responsável pela coleta, preservação, documentação e, muitas vezes, pelo pré-processamento dos dados eletrônicos.

Em linhas gerais podemos observar as seguintes fases:

- Identificação e gestão das informações.
- Preservação e coleta.
- Pré-processamento e Processamento.
- Revisão e Classificação.
- Análise.
- Produção e Apresentação.

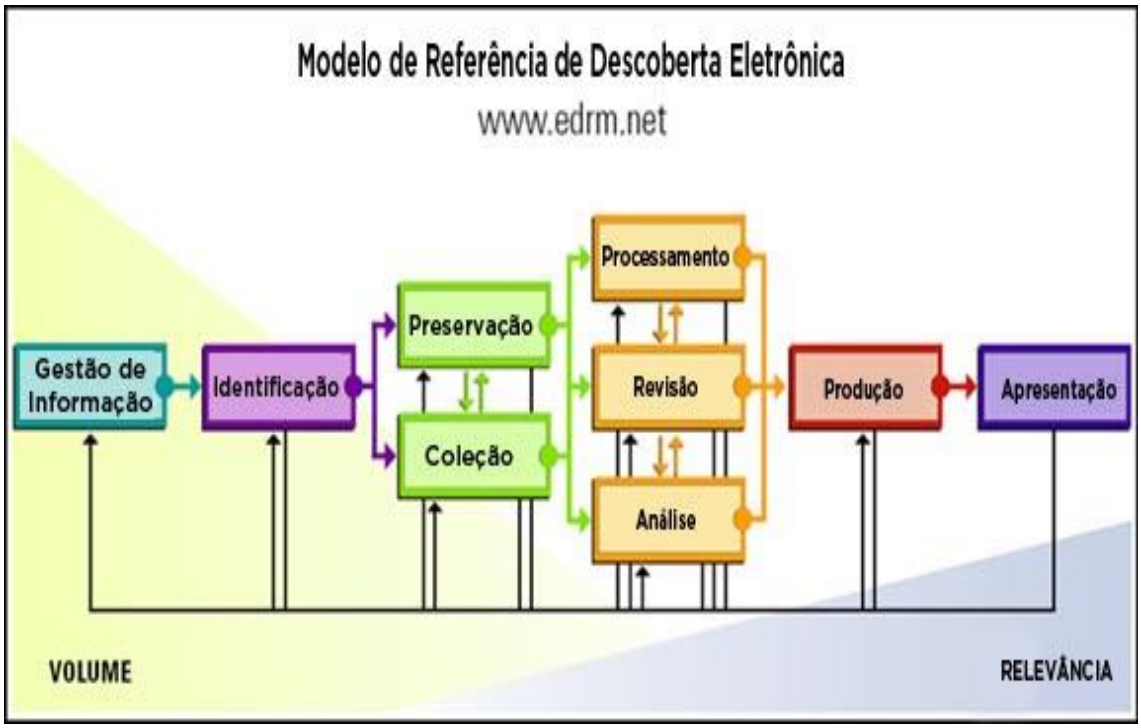


Figura 5 – Modelo de Referência de Descoberta Eletrônica (EDRM).
(http://www.edrm.net/resources/guides/edrm-framework-guides)

4.3 – PERÍCIA EM ARQUIVOS

A perícia pode ser aplicada a arquivos (áudio, vídeo e imagem) e também a rede. Tal trabalho tratará de periciar arquivos de um computador, como por exemplo: imagem. Onde se possam aplicar as técnicas pós-crimes, a fim de coletar evidências após o ataque, através da máquina que sofreu o incidente, buscando utilizar todo o conhecimento proporcionado para contribuir com a solução do caso.

4.3.1 – ÁUDIO

As gravações de áudio vêm se tornando cada vez mais populares no meio da comunicação, consequentemente também estão sendo utilizadas como provas de diversos crimes. Os peritos abordam três tipos básicos para se tirar uma conclusão: desgravação, autenticação e identificação. Além disso, realiza a transcrição mais exata possível do conteúdo registrado na gravação.

A prova baseada em gravação de áudio é considerada lícita quando um dos interlocutores realizou a gravação. Em outras palavras, é ilícita apenas a gravação de conversas de terceiros, seja por interceptação telefônica "grampo" ou gravação direta.

4.3.2 – VÍDEO

Outro arquivo que pode ser utilizado para coletar evidências são as gravações de vídeo, presente hoje em uma boa parte das residências, estabelecimentos comerciais, bancos e etc.

As gravações podem auxiliar em uma determinada investigação, por exemplo: melhorar a qualidade das gravações a fim de se identificar uma pessoa, que possa ter participado ou presenciado um crime. Também pode recuperar vídeos excluídos de sistemas de segurança interno, onde o mesmo foi apagado do sistema, para que não seja descoberta alguma atividade maliciosa de algum funcionário, cliente e prestador de serviços.

4.3.3 – IMAGEM

A imagem também é uma evidência que pode ser usada como prova de um crime cibernético. Chama-se tal atividade de processamento de imagens, que nada mais é que o aperfeiçoamento das imagens, visando melhorar a qualidade das mesmas, para fim de reconhecimento de pessoas. Este trabalho tem como foco esse tema, mostrar que é possível trabalhar com ferramentas específicas e comprovar que seus resultados são satisfatórios.

4.4– FERRAMENTAS PARA PERÍCIA EM ARQUIVOS

4.4.1. CAINE

O Software Caine[3] foi desenvolvido na Itália, baseado no GNU/Linux Ubuntu 10.04, como projeto da Digital Forensics. Oferece um ambiente computacional forense completo, organizado para integrar ferramentas de software existentes para fornecer uma interface gráfica bastante amigável.

Cria um ambiente gráfico que facilita o trabalho do investigador forense durante as fases da computação forense. Disponível em CD, máquina virtual e Caine-portable.

A Figura 8, da página 30 apresenta a interface do Software, onde a tela inicial traz consigo um menu de opções que contêm 80 ferramentas voltadas a área forense digital e outros aplicativos usados para tarefas comuns de computação de desktop.

[3] http://www.caine-live.net/

Figura 6 – Interface do Caine

4.4.2 – PERI-BR

O PERI_BR[4] é uma ferramenta LIVE-CD de perícia digital, desenvolvido como trabalho de pós-graduação em perícia digital da Universidade Católica de Brasília pelos alunos Marcel Carvalho e Jaqueline Carvalho, em 2009. É um sistema baseado no Ubuntu 9.04. Encontra-se nele uma ampla diversidade de ferramentas separadas por categorias de realização da perícia forense.

A referida ferramenta teve como base o FDTK para desenvolvimento, e tem como ponto negativo, a não atualização desde sua criação, a versão do software está no 1.0.

A Figura 7, da página 31 apresenta a interface do Software, onde a tela inicial traz consigo um menu de opções para realizar diversas atividades com foco forense computacional.

[4] https://sites.google.com/a/cristiantm.com.br/forense/home

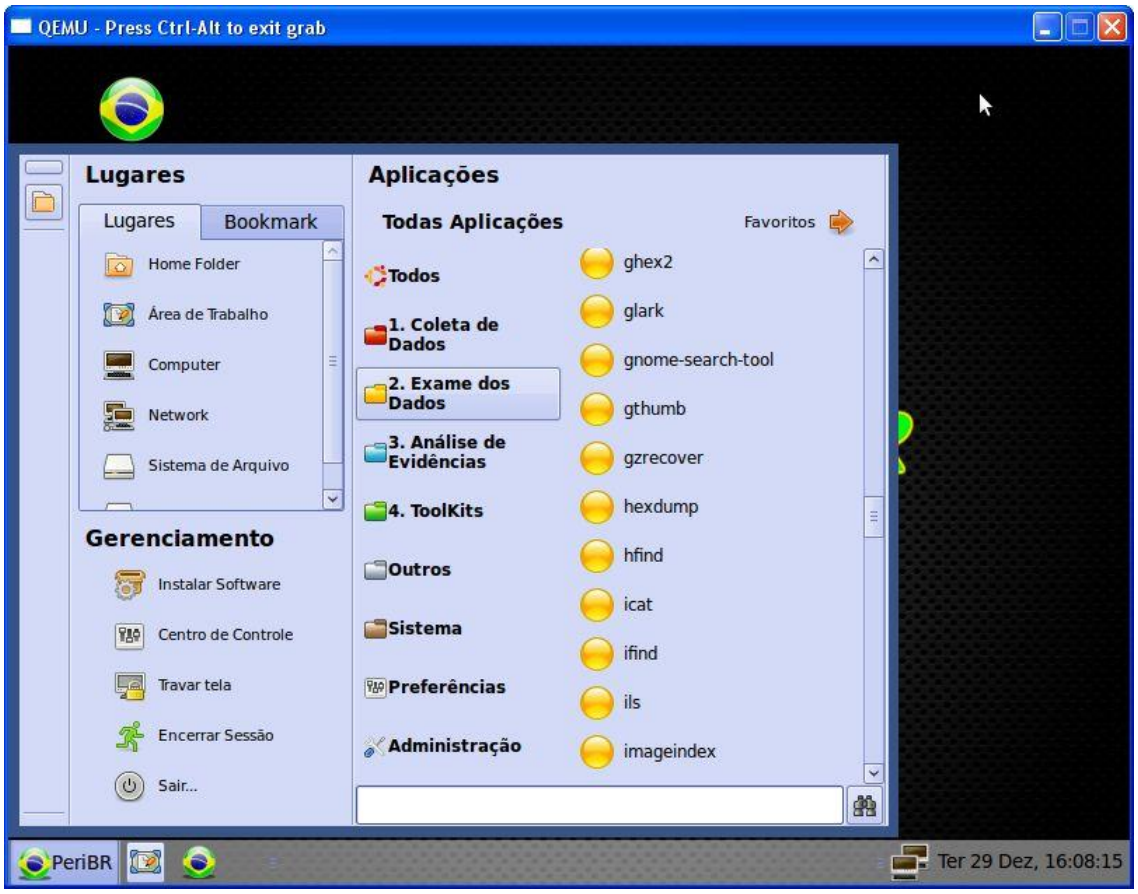


Figura 7 – Interface do PERI-BR

4.4.3 – BACKTRACK

Desenvolvido na Suíça, baseado no Linux, o Backtrack[5] teve como foco os testes em segurança e penetração, disponível também em Live CD/DVD ou instalação na máquina.

Em 2006 foi votado como o melhor software para distribuição de testes de segurança pela organização Insecure, além disso, apresenta testes de invasão em metodologias conhecidas e padronizadas, ajudando os profissionais em seu dia-a-dia.

A Figura 8, da página 32 apresenta a interface do Software que atualmente está na versão 5.0, e disponibiliza aos usuários um menu com 300 ferramentas para auxílio de testes de vulnerabilidades e análise de dados.

[5] http://www.backtrack-linux.org/

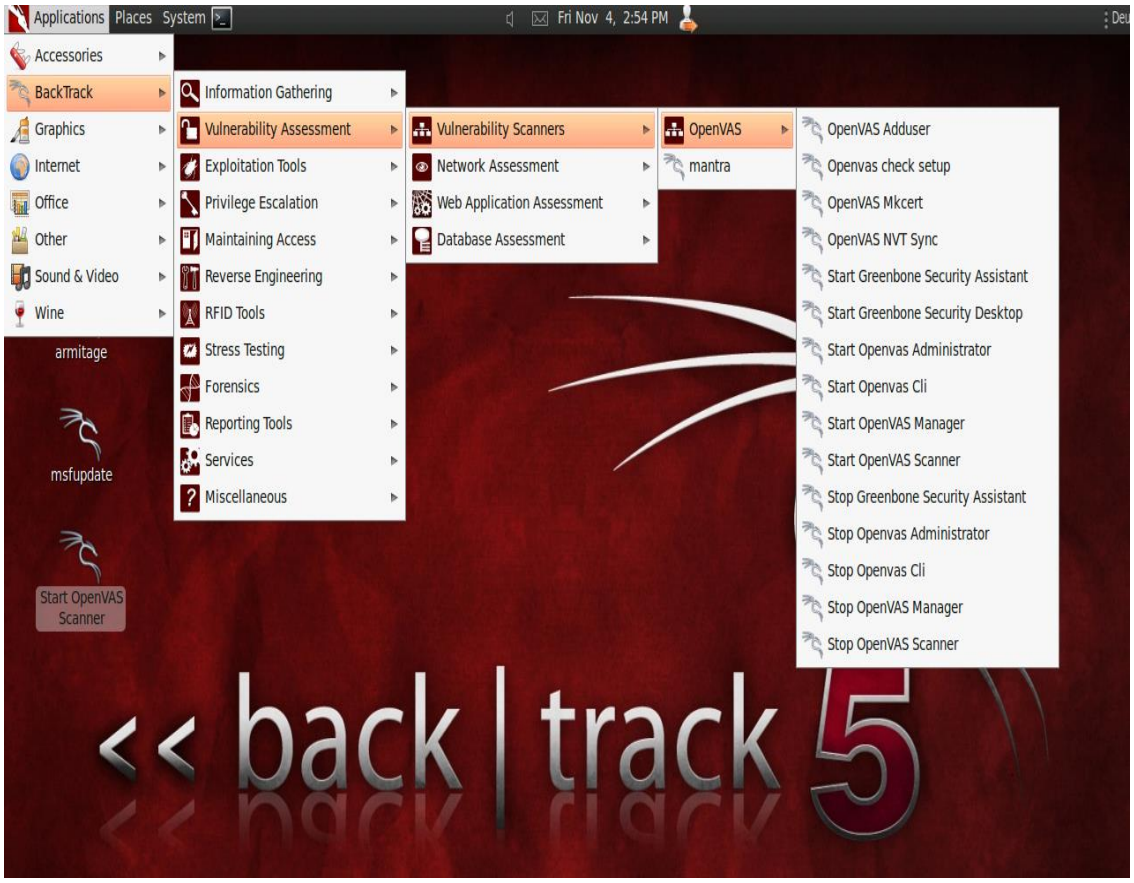


Figura 8 – Interface do Backtrack.

4.4.4 – FDTK

Criado por Paulo Neukamp, para trabalho de conclusão do curso de Segurança da Informação da Unisinos. O FDTK[6] foi baseado no Ubuntu e está focado a Forense Computacional.

Uma de suas ferramentas é capaz de revelar a senha de sistemas Windows, oferecendo a possibilidade de ser utilizado como LIVE-CD e também ser instalado em um equipamento transformando-o em uma estação Forense.

A ilustração da página 33 apresenta a interface do Software que está disponível na versão 3.0, possui mais de 100 ferramentas divididas em três etapas, sendo elas: coleta, exame e análise das evidências.

[6] http://fdtk.com.br/www/

Figura 9 – Interface do FDTK.

5 – INSTALAÇÃO E UTILIZAÇÃO DA FERRAMENTA CAINE

Neste capítulo será apresentando a ferramenta escolhida para estudo, juntamente com um breve tutorial de utilização da mesma para resolução de um caso de perícia forense em imagem. Onde serão aplicados os métodos que os peritos utilizam nos laboratórios forenses. A ferramenta que foi escolhida para esse trabalho é o Caine. A mesma possui diversas versões, porém faltam orientações para saber qual sua versão mais indicada, dessa maneira será utilizada a versão mais atualizada.

Sendo assim, esse estudo propõe auxiliar aos demais que tenham interesse em Perícia Forense Digital, a saber, quais ferramentas e os métodos de utilização das mesmas.

O processo está estruturado da seguinte forma:

1 – Processo de Download da Ferramenta;

2 – Processo de Gravação e Criação de Imagem em Mídia (DVD-R);

3 – Processo de Realização da Perícia Forense em Imagem (Original);

4 – Processo de Realização da Perícia Forense em Imagem (Contraprova);

5 – Processo de Realização da Perícia Forense em Imagem (Manipulada);

6 – Processo de Verificação de Autenticação;

5. 1 – PROCESSO DE DOWNLOAD DA FERRAMENTA

Para iniciar, será preciso realizar o *download* da ferramenta em seu site oficial. Digite em seu navegador o seguinte endereço: http://www.caine-live.net, selecione a opção “*downloads”* conforme ilustrada a figura a seguir.

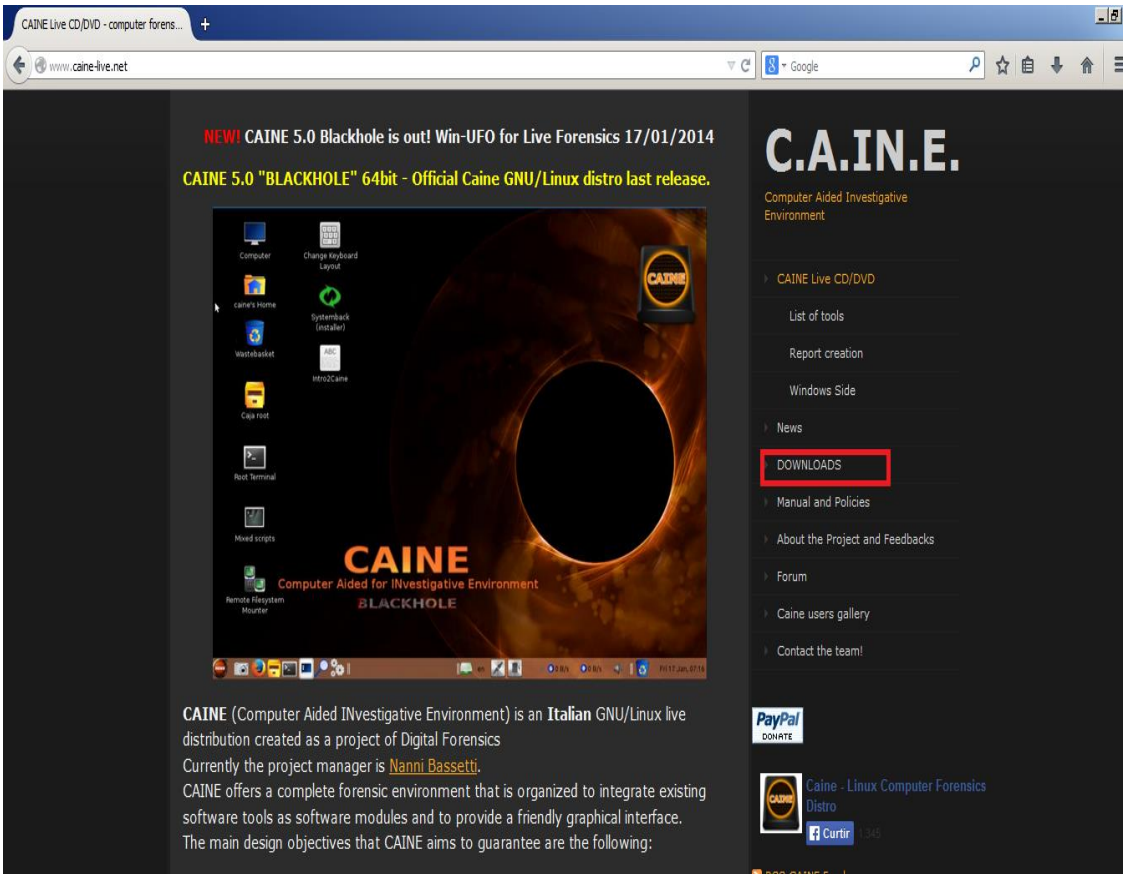


Figura 10 – Site para download do Caine.

Após selecionar a opção, irá abrir uma nova página com todas as versões das ferramentas disponíveis para utilização. Conforme citado no início desse capítulo, são diversas as versões, porém para realização desse trabalho, foi selecionada a versão 5.0.

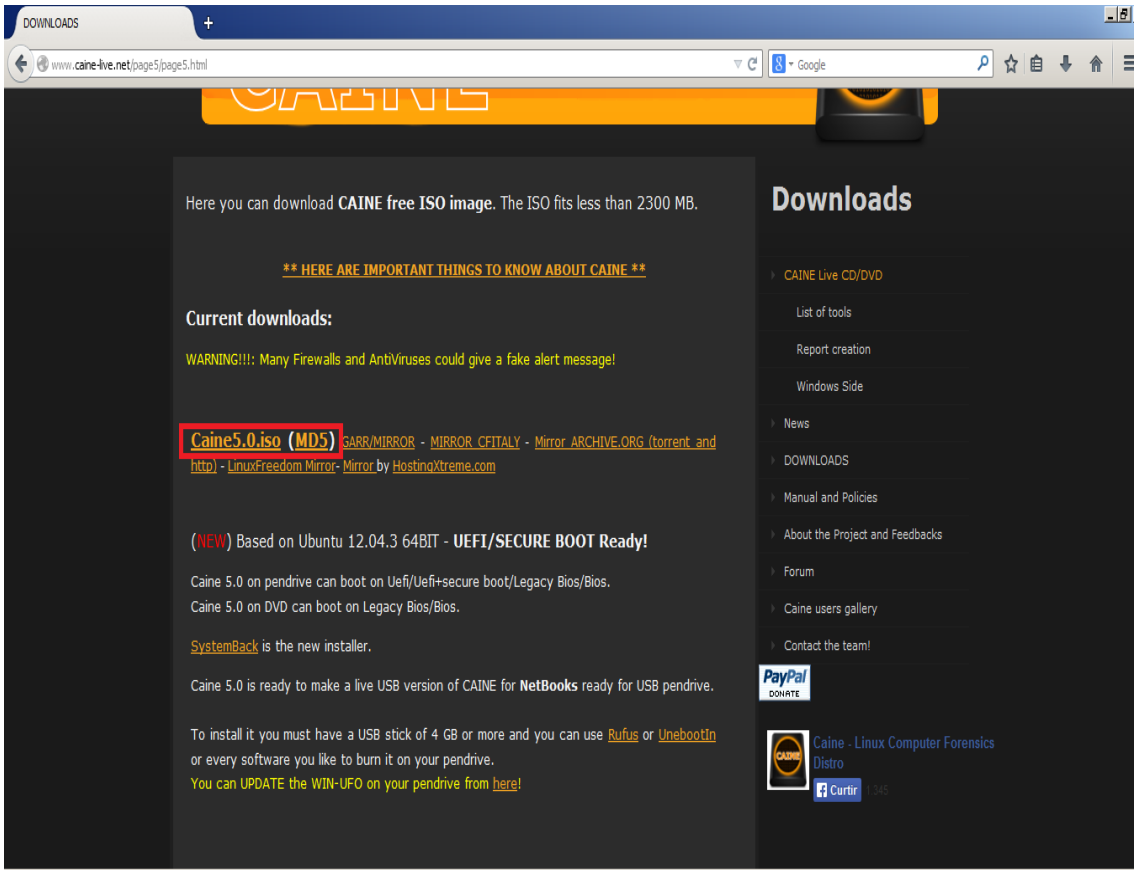


Figura 11 – Página de Download do Caine.

Após selecionar a versão desejada, a caixa de *download* será aberta pelo navegador, selecione a opção para realizar e aguarde a conclusão do mesmo.

5.2 – PROCESSO DE GRAVAÇÃO DA FERRAMENTA EM MÍDIA (DVD-R)

Após o término do *download* do arquivo, será preciso realizar a gravação do mesmo em uma mídia para execução da ferramenta. O processo de gravação é simples, apenas será preciso utilizar um *software* de gravação de mídias, como por exemplo, *Nero Burning ROM* que grava arquivos em CDs, DVDs e etc.

Encontre o arquivo que foi selecionado para salvar após concluir o *download* e pressione o botão direito do mouse em cima do mesmo. Selecione a opção

“Abri Com” e selecione o programa para gravar, no caso deste trabalho, como citado acima, será utilizado o Nero Burning ROM[7].

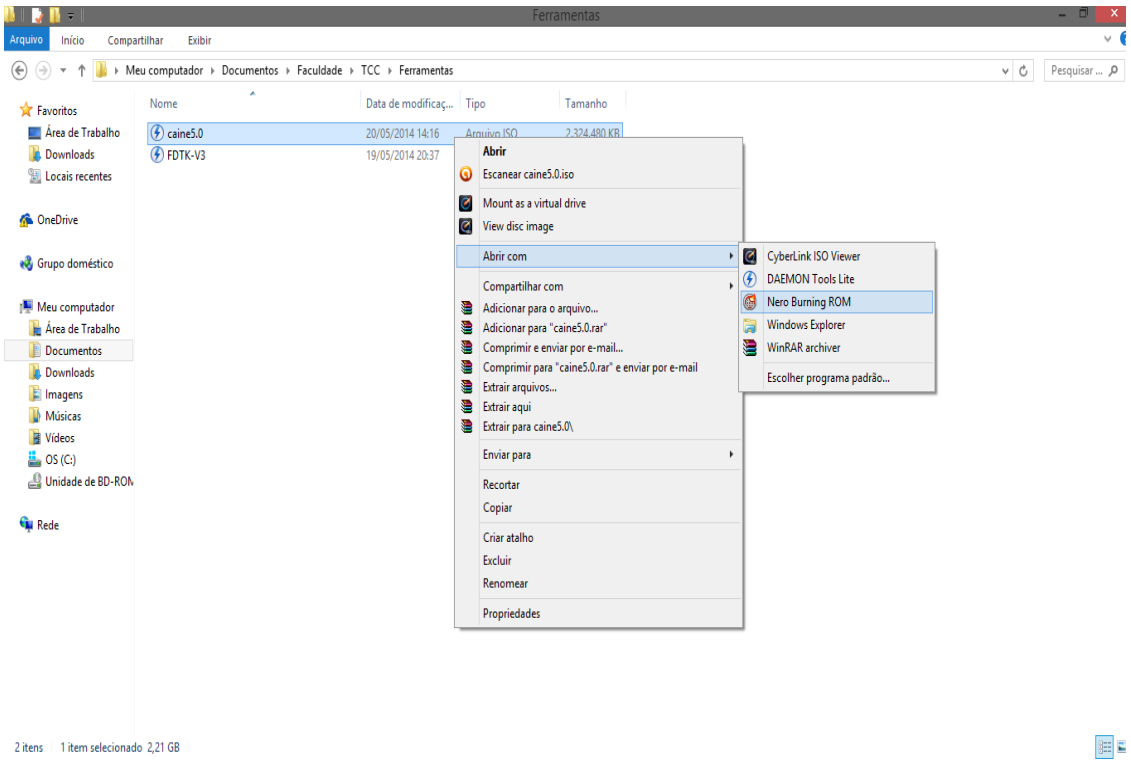


Figura 12 - Pasta onde está armazenado o arquivo após o download.

Logo após selecionar o programa, a interface do programa de pré-gravação do Nero será aberta com algumas opções de instalação já selecionados pelo software.

Apenas selecione a opção “Gravar” que o processo será inicializado.

[7] http://www.baixaki.com.br/download/nero-burning-rom-2014.htm.

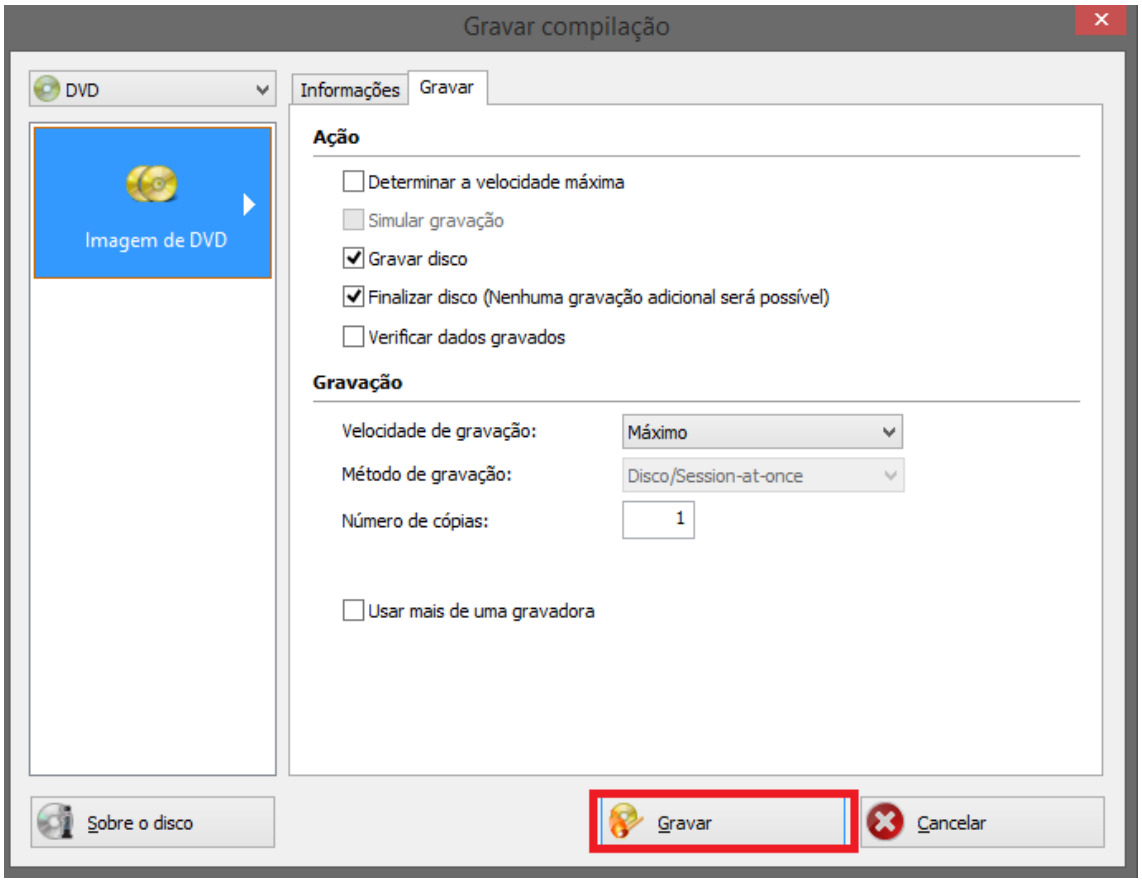


Figura 13 – Interface do Nero no processo Pré-gravação da mídia.

Selecione a opção “Gravar” conforme ilustração acima e aguarde a atualização de uma nova página. Depois de atualizar, o processo de gravação da mídia será iniciado e ao seu término uma mensagem de processo concluído aparecerá na tela, pressione “OK” e o processo será finalizado.

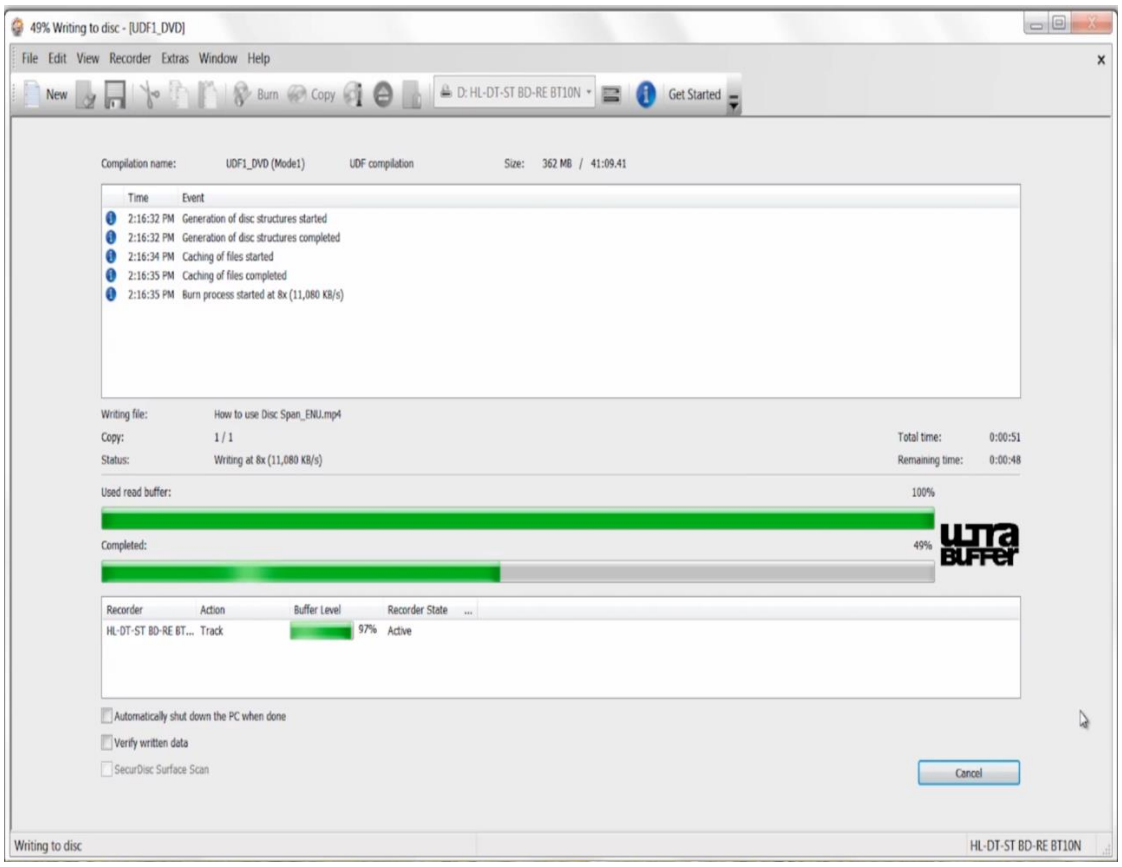


Figura 14 – Interface do Processo de Gravação da mídia.·.

5.3 – PROCESSOS DE REALIZAÇÃO DE PERÍCIA FORENSE EM IMAGEM

Depois de finalizar o processo de gravação da mídia, será iniciado o estudo de perícia forense em imagem, onde será aplicado todo o processo de estudo e prática em relação a suspeita de manipulação de um arquivo. Dessa maneira, primeiramente será feito a perícia em uma imagem.

Atualmente para poder chegar à conclusão de que um arquivo pode ter sofrido algum tipo de manipulação é preciso realizar o cálculo de integridade do mesmo. Esse método é realizando da seguinte forma, todo arquivo tem em sua propriedade uma sequência de 128 bits[8] pertencente ao mesmo, chamado de "*hash*" MD5.

[8] Bits: Menor unidade de informação que pode ser armazenada ou transmitida.

Esse *"hash"* é unidirecional e foi desenvolvido pela *RSA Data Security.* É muito utilizado por softwares com protocolo ponto-a-ponto (P2P, ou *Peer-to-Peer*[9], em inglês) na verificação de integridade de arquivos. O método de verificação é feito pela comparação de dois arquivos, um original e outro manipulado.

Após término de cada perícia, o *software* irá retornar o "*hash"* MD5, pertencente ao arquivo e depois de coletar os mesmos, será preciso validar a autenticação dos arquivos.

Para realizar esse trabalho e poder ter uma conclusão correta, serão realizados três testes. O primeiro será feito com a imagem original, depois o mesmo será repetido, a fim de se comprovar que o resultado obtido será o mesmo. E por fim será feito a manipulação na imagem e novamente o realizar o processo, visando obter o resultado diferente.

Após essa coleta de "*hash*", será desenvolvida uma aplicação que irá realizar a comparação das duas imagens e indicar qual é o arquivo manipulado e qual o original com base em seus "*hash*".

5.3.1 - PERÍCIA FORENSE EM IMAGEM (ORIGINAL)

Para iniciar o caso, é preciso ligar o computador, colocar a mídia (DVD-R) no leitor de CD/DVD-R do mesmo e acessar a BIOS[10]. Após acessar a BIOS, será preciso inicializar o *boot* da ferramenta e aguardar a inicialização da mesma iniciar.

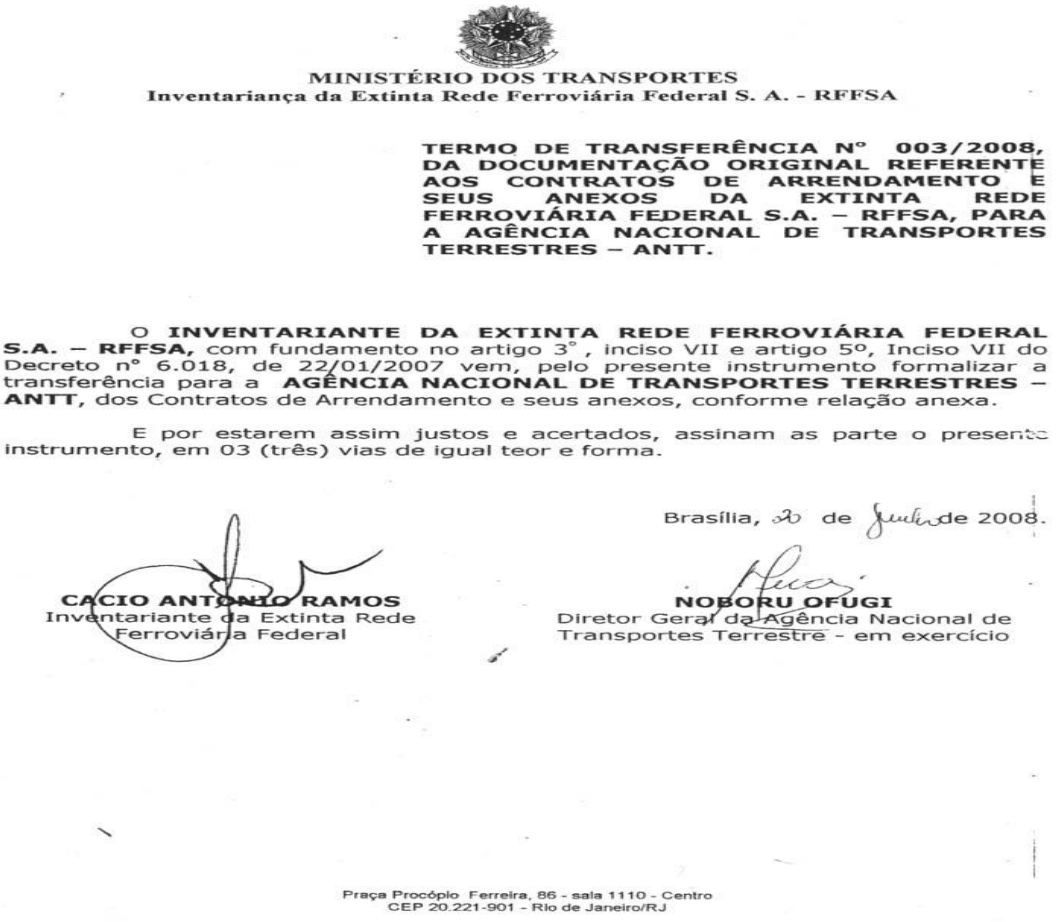
Depois de ligada, será preciso selecionar a imagem em que se deseja realizar a perícia, vários tipos de imagens são aceitos, desde imagem de disco, fotos e arquivo pdf.

Nesse exemplo, será utilizada a imagem de um contrato já assinado, onde um criminoso pode modificar o arquivo e escrever outras coisas que possam complicar a situação de quem assinou o contrato, conforme ilustração abaixo:

---

[9] Peer-to-Peer: É uma arquitetura de redes de computadores, onde cada um dos pontos da rede funciona tanto como cliente quanto como servidor, permitindo compartilhamentos de serviços e dados sem a necessidade de um servidor central.

[10] BIOS: programa de computador pré-gravado em memória permanente, executado por um computador quando ligado. Ele é responsável pelo suporte básico de acesso ao hardware, bem como por iniciar a carga do sistema operacional.



MINISTÉRIO DOS TRANSPORTES
Inventariança da Extinta Rede Ferroviária Federal S. A. - RFFSA

TERMO DE TRANSFERÊNCIA Nº 003/2008, DA DOCUMENTAÇÃO ORIGINAL REFERENTE AOS CONTRATOS DE ARRENDAMENTO E SEUS ANEXOS DA EXTINTA REDE FERROVIÁRIA FEDERAL S.A. – RFFSA, PARA A AGÊNCIA NACIONAL DE TRANSPORTES TERRESTRES – ANTT.

O **INVENTARIANTE DA EXTINTA REDE FERROVIÁRIA FEDERAL S.A. – RFFSA,** com fundamento no artigo 3°, inciso VII e artigo 5º, Inciso VII do Decreto nº 6.018, de 22/01/2007 vem, pelo presente instrumento formalizar a transferência para a **AGÊNCIA NACIONAL DE TRANSPORTES TERRESTRES – ANTT,** dos Contratos de Arrendamento e seus anexos, conforme relação anexa.

E por estarem assim justos e acertados, assinam as parte o presente instrumento, em 03 (três) vias de igual teor e forma.

Brasília, 20 de junho de 2008.

CACIO ANTONIO RAMOS
Inventariante da Extinta Rede Ferroviária Federal

NOBORU OFUGI
Diretor Geral da Agência Nacional de Transportes Terrestre - em exercício

Praça Procópio Ferreira, 86 - sala 1110 - Centro
CEP 20.221-901 - Rio de Janeiro/RJ

Figura 15 – Imagem escolhida para realizar a perícia forense. Disponível em: > http://www.jusbrasil.com.br/diarios/busca?q=EXTINTA+REDE+FERROVI%C3%81RIA+FEDERAL+S.A.+-+RFFSA< Acesso: 25 Mar. 2014

Após selecionar a mesma, acesse o “Menu Iniciar” do computador e selecione a opção *“Autopsy”.*

• Autopsy é uma interface gráfica para linha de comando digital, ferramenta de análise de investigação de arquivos. Pode analisar discos e sistemas de arquivos (NFTS, FAT, UFS1, Windows e Unix).

Após selecionar, será aberta uma janela semelhante ao “Prompt de Comando” do Windows, contendo algumas informações da ferramenta.

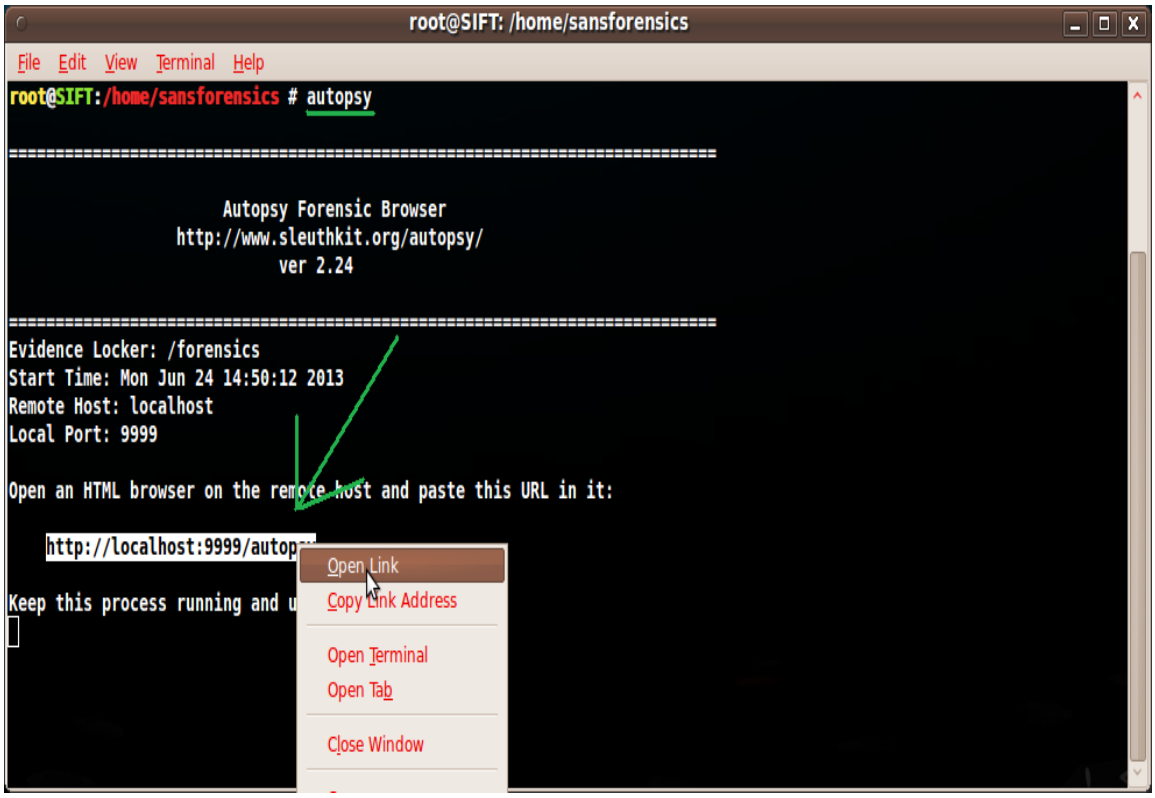


Figura 16 – Interface Gráfica do Caine.

Selecione o endereço em destaque conforme a ilustra a imagem, copie e cole no navegador. O mesmo irá se direcionar para a seguinte página, conforme Figura 17, na página seguinte.

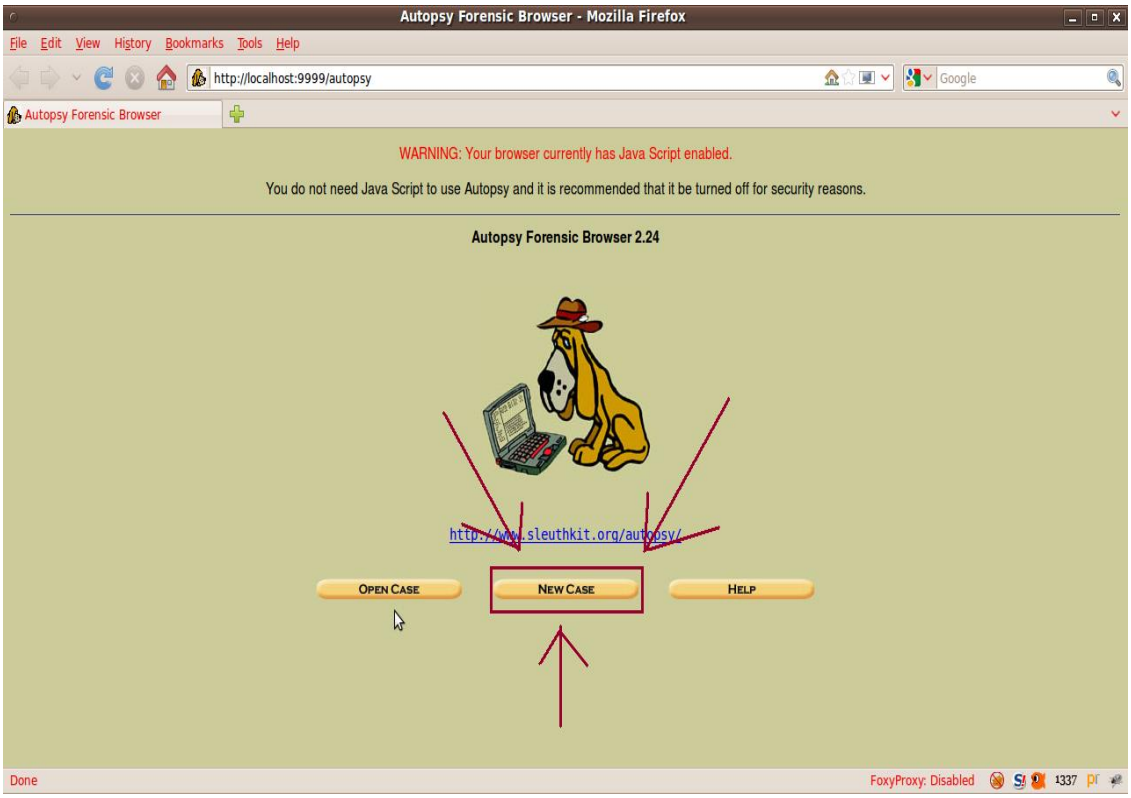


Figura 17 – Página Inicial do Caine – Menu de Opções.

A partir dessa página é que será iniciado o caso para perícia forense. A página inicial traz consigo três opções: "*Open Case*", para abrir um caso já existente. "*New Case*", para criação de um novo caso e "*Help*", onde se tira algumas dúvidas sobre a ferramenta.

Nesse exemplo, será criado um caso novo para que se possam acompanhar todas as etapas que devem ser seguidas para formulação de uma perícia digital.

Pressione o botão em "*New Case*", e aguarde a página ser atualizada e retornar da seguinte forma, conforme ilustra a figura 18, da página 43.

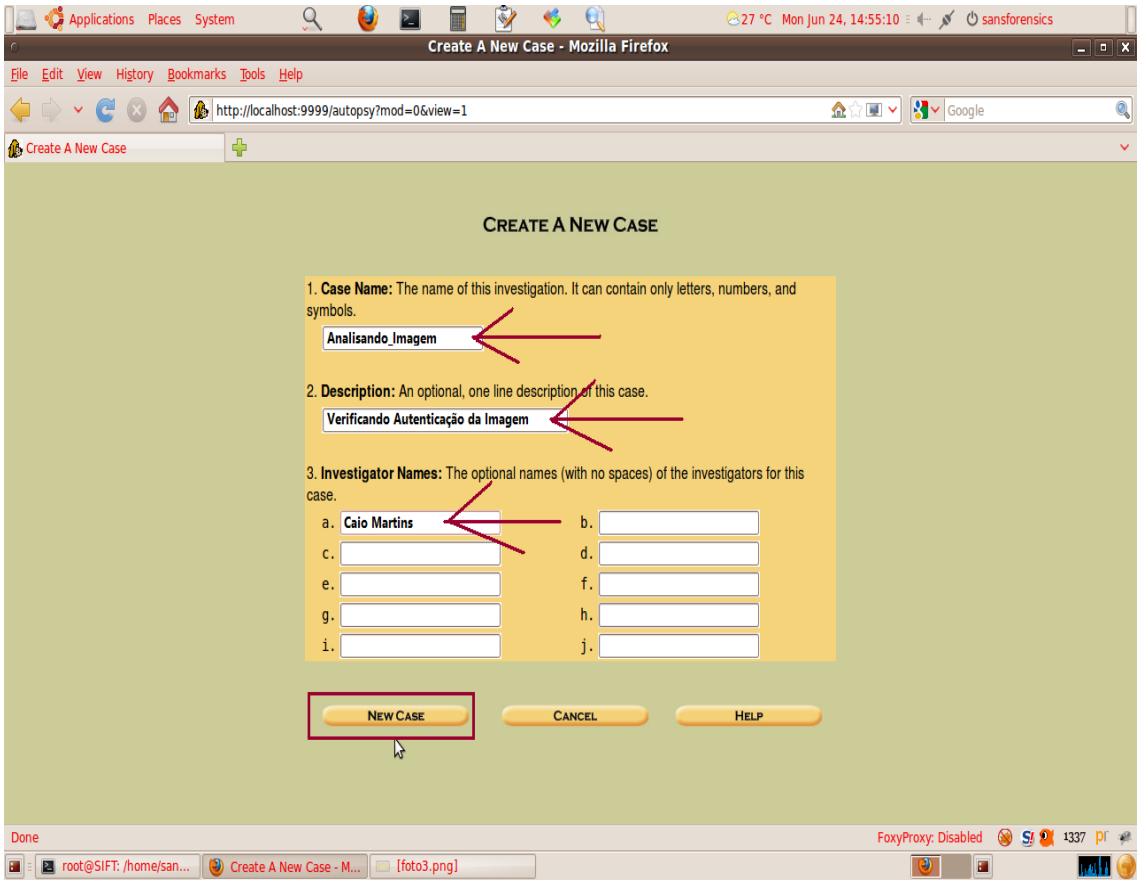


Figura 18 – Página para criação de um novo caso.

Primeiramente será preciso preencher alguns campos de identificação e descrição do caso, informe o nome que deseja, e também uma pequena descrição do que será realizada no caso e logo embaixo preencha o nome do usuário que examinará os arquivos.

Depois de preencher todos os campos, selecione a opção "*New Case*". A página será atualizada e retornará com alguns dados, informando que um novo caso foi criado com as informações fornecidas pelo usuário, conforme figura 19, da página 44.

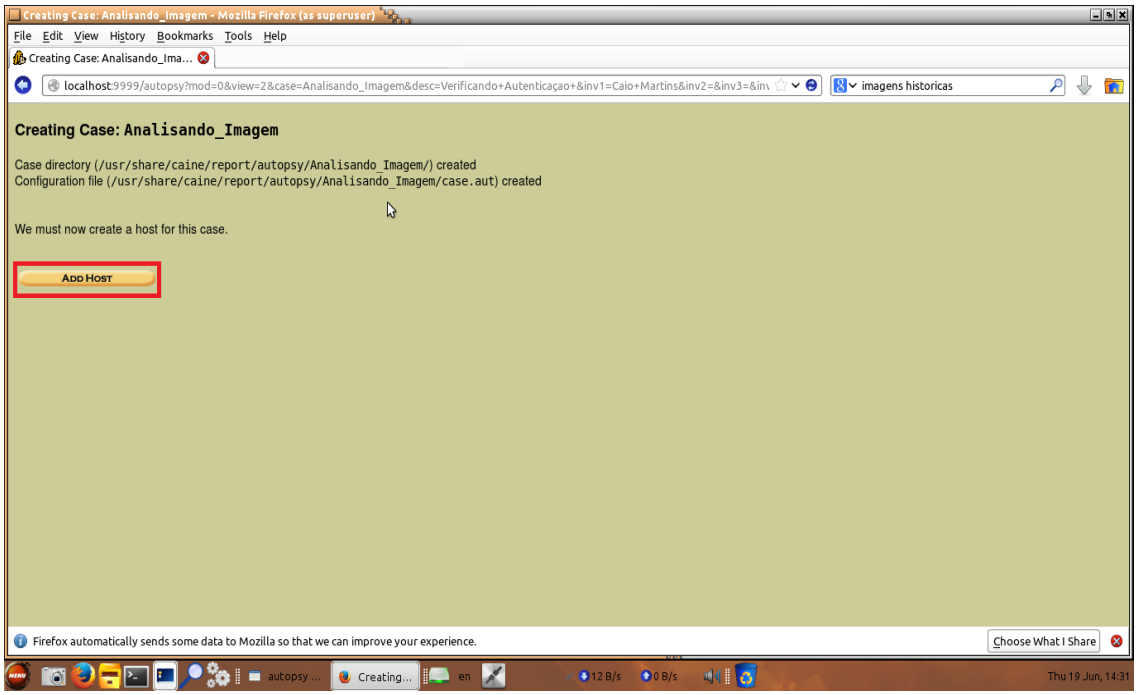


Figura 19 – Página que informa a criação de um novo caso.

Selecione a opção *"Add host"* e aguarde uma nova página carregar. Após carregar, pressione a opção "*Add Image*" para informar qual a imagem pertence ao caso criado.

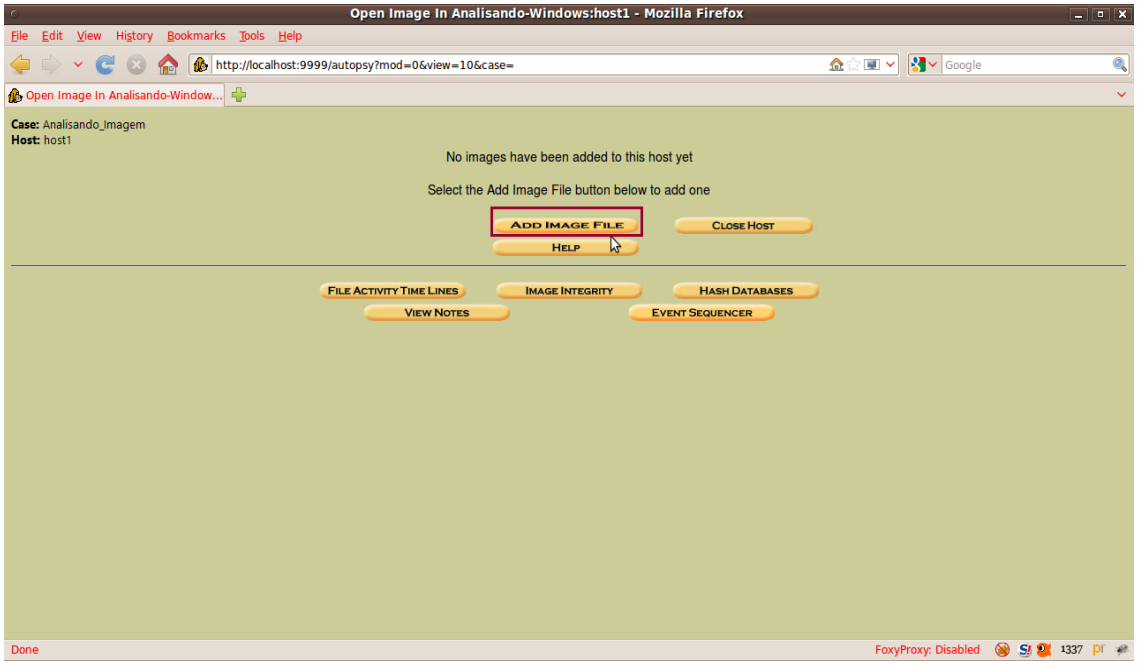


Figura 20 – Página onde o usuário seleciona qual será a imagem utilizada no caso.
Fonte: (Caio Martins, 2014).

Depois de atualizar a página, será solicitado ao perito que informe o diretório onde a imagem está armazenada e selecionar algumas opções conforme ilustração abaixo.

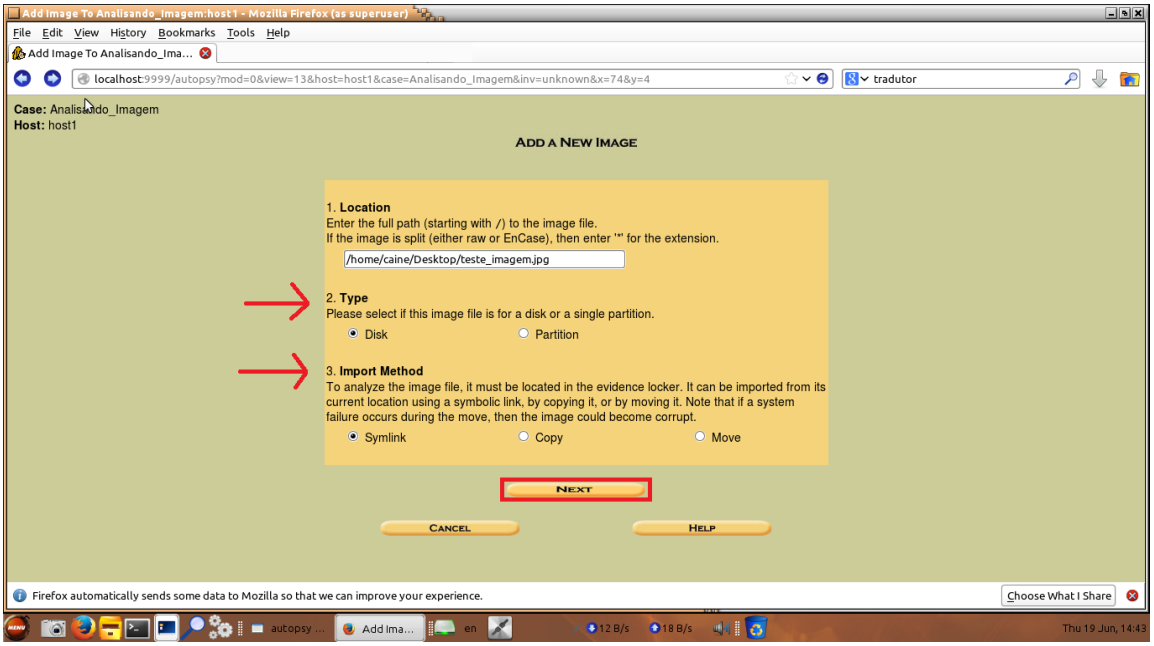


Figura 21 – Página que será informado o diretório que a imagem está armazenada.

A próxima página atualizada trazer algumas informações correspondentes à imagem selecionada.

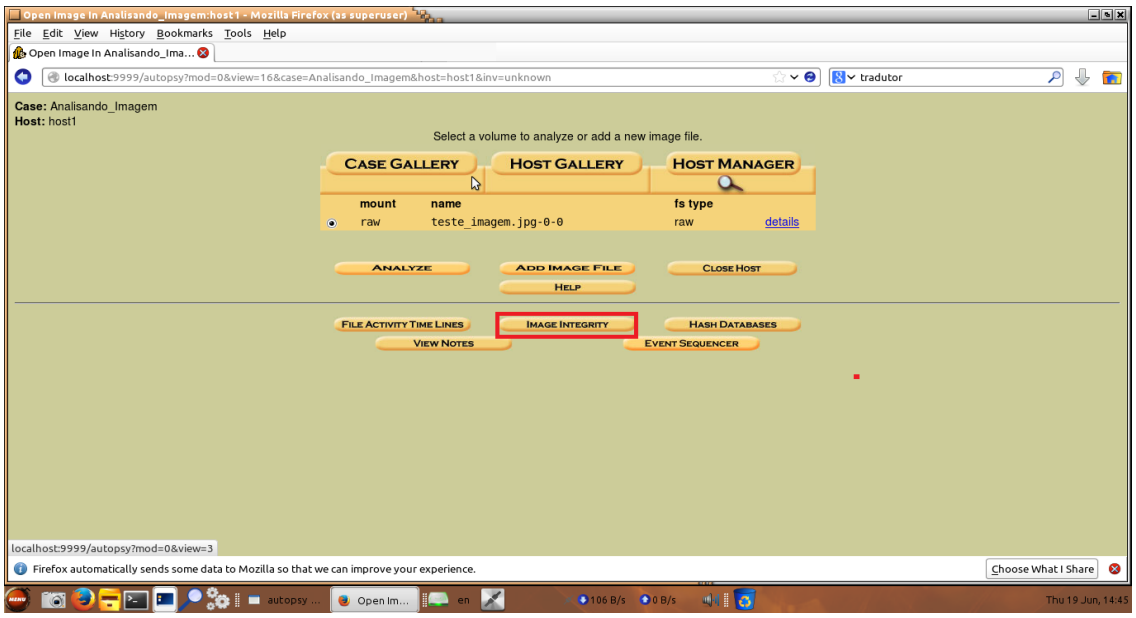


Figura 22 – Página para selecionar a opção para calcular a integridade da imagem.

Selecione a opção “*Image Integrity*”, esta é a opção que irá fazer o cálculo da integridade da imagem e então retornar o *“hash”* que pertence à mesma. Após selecionar, a página atualizará e retornará conforme a Figura 23.

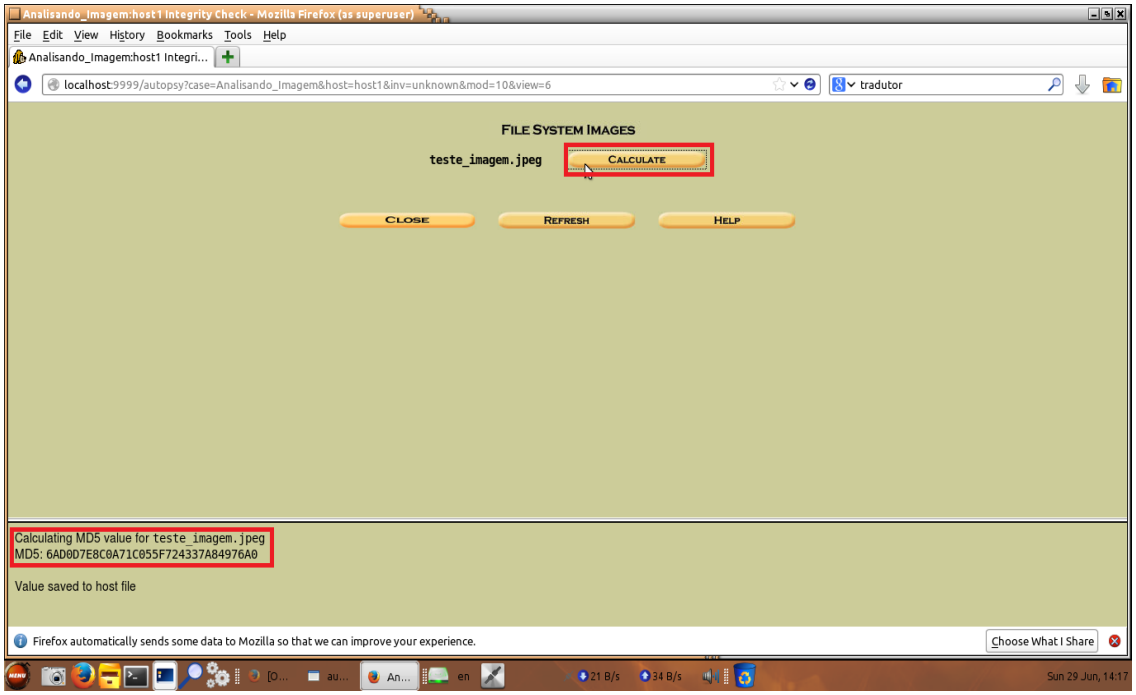


Figura 23 – Cálculo da integridade realizado e retorno do “hash” pertencente à imagem.

Selecione a opção “*Calculate*”. Após selecionar, a página será atualizada e no canto esquerdo da imagem será mostrado o valor do *“hash “ MD5* pertencente àquela imagem.

Pode-se observar que o valor retornado após a pericia da imagem é a seguinte sequência: **MD5: 6AD0D7E8C0A71C055F724337A84976A0.**

5.3.2 - PERÍCIA FORENSE EM IMAGEM (CONTRAPROVA)

Depois de se periciar a imagem original, o processo será repetido novamente com a mesma imagem, sem o arquivo ter sido manipulado. Sendo assim, o resultado obtido no fim da perícia, deverá ser semelhante ao coletado no capítulo anterior.

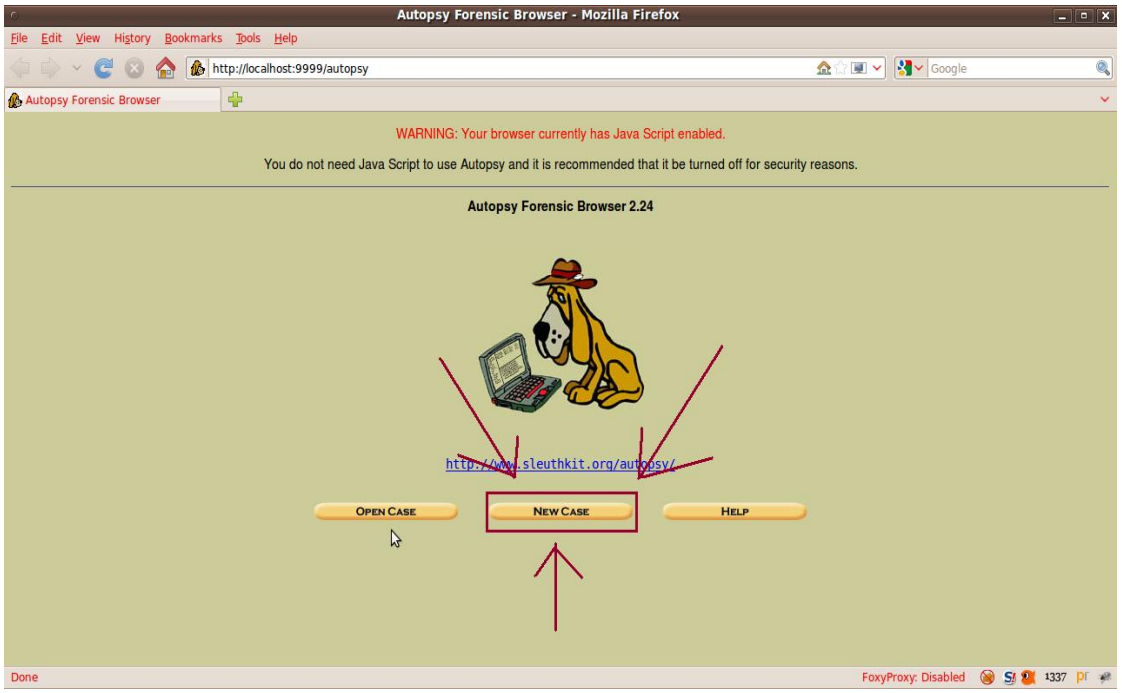


Figura 24 – Página Inicial do Caine – Menu de Opções (Contraprova).

Novamente será preciso criar um novo caso e posteriormente preencher os campos solicitados para criação de um caso. Note que o nome dado ao novo caso é “Analisando_Imagem1”, e o caso anterior tem o nome “Analisando_Imagem”, conforme ilustra as Figuras 24 e 25.

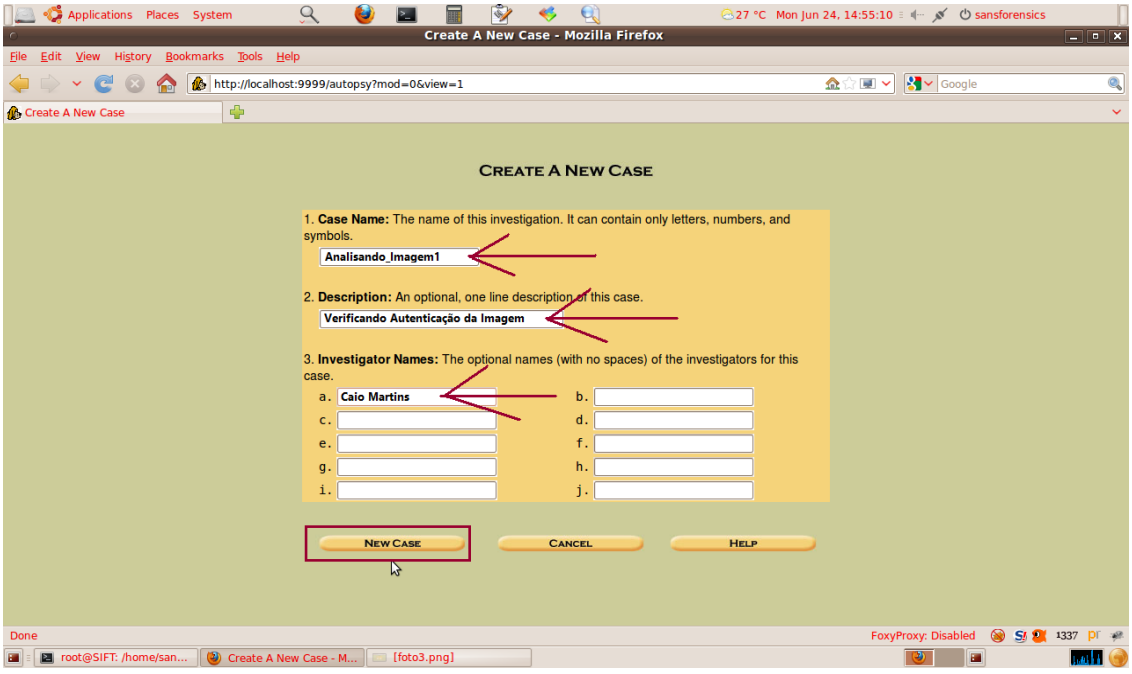


Figura 25 – Página para criação de um novo caso (Contraprova).

Após selecionar a opção *"New Case"*, a página será atualizada e será informado que um novo caso foi criado.

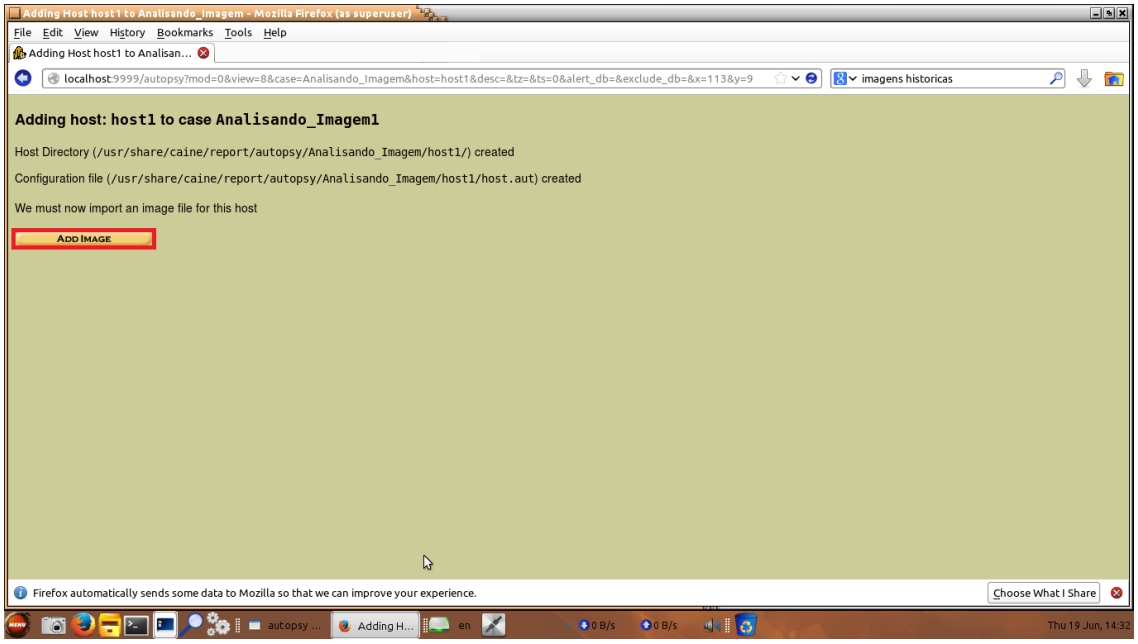


Figura 26 – Página que informa a criação de um novo caso (Contraprova).

Após adicionar o *host* à página novamente atualizará e será solicitado ao perito que novamente selecione a imagem que deseja adicionar ao caso.

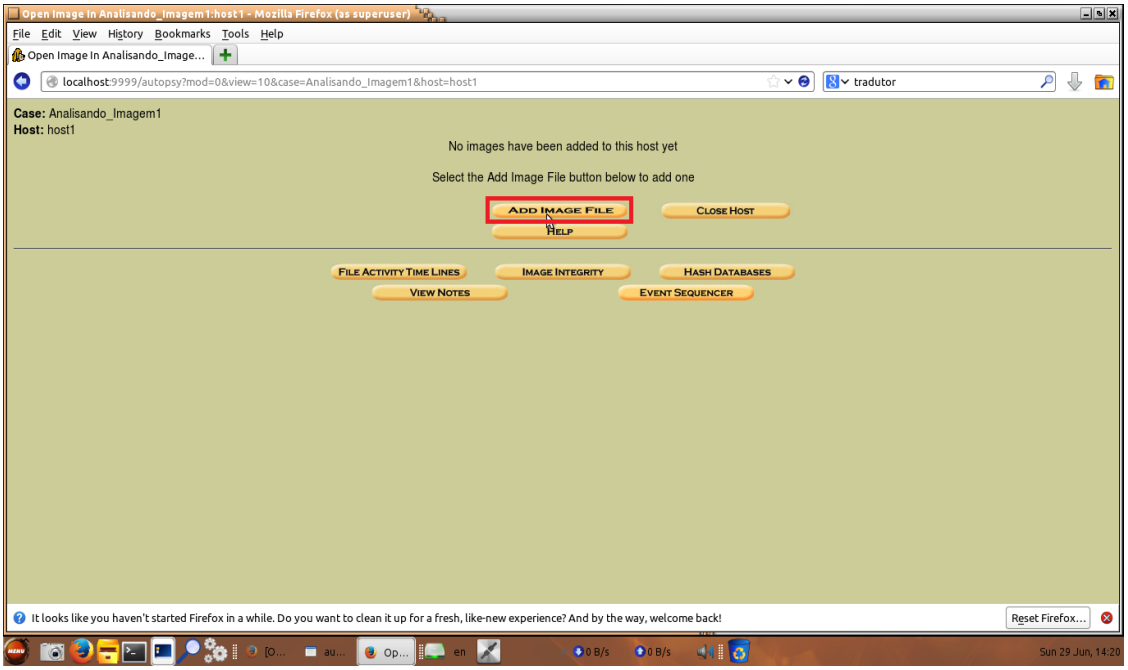


Figura 27 – Página onde o usuário seleciona qual será a imagem utilizada no caso (Contraprova)

Novamente, será preciso informar o diretório que a imagem está armazenada e selecionar algumas opções conforme Figura 28.

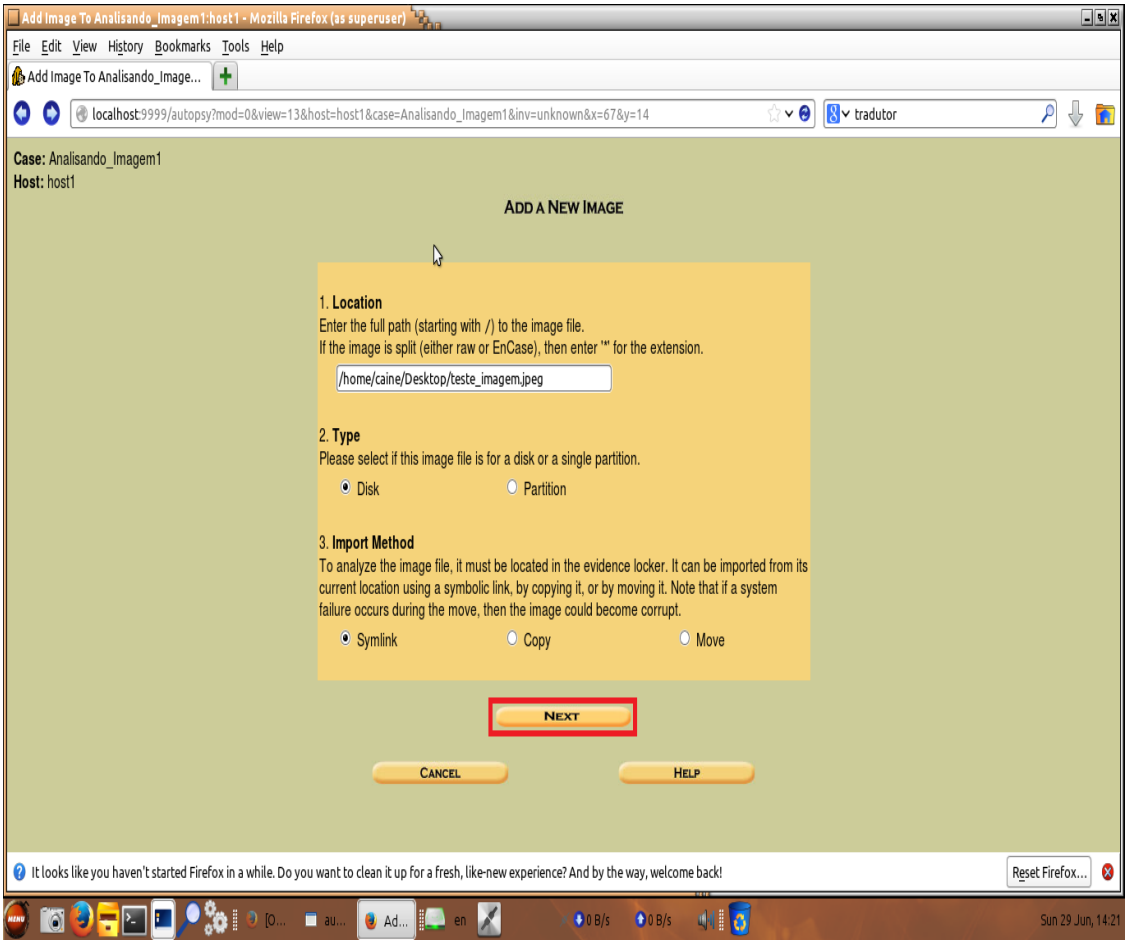


Figura 28 – Página que será informado o diretório que a imagem está armazenada (Contraprova).

Depois de preencher todos os campos, pressione o botão *"Next"*, a seguir a imagem será carregada ao caso e suas informações reaparecerão preenchidas na tela a seguir.

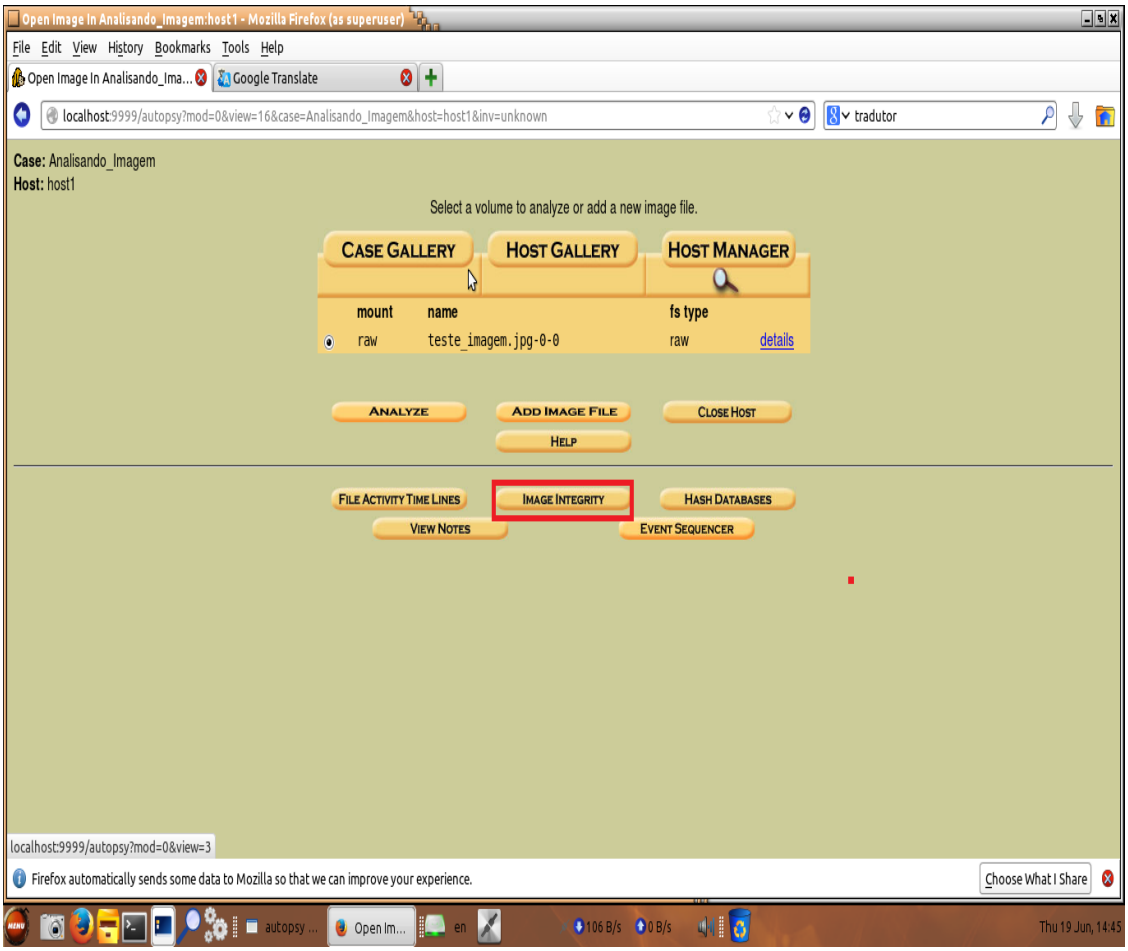


Figura 29 – Página para selecionar a opção para calcular a integridade da imagem (Contraprova)

Selecione a opção "*Image Integrity*" e aguarde a atualização da página. Depois de atualizada, selecione a opção "Calculate" e aguarde o processamento e o retorno do *"hash"* da mesma.

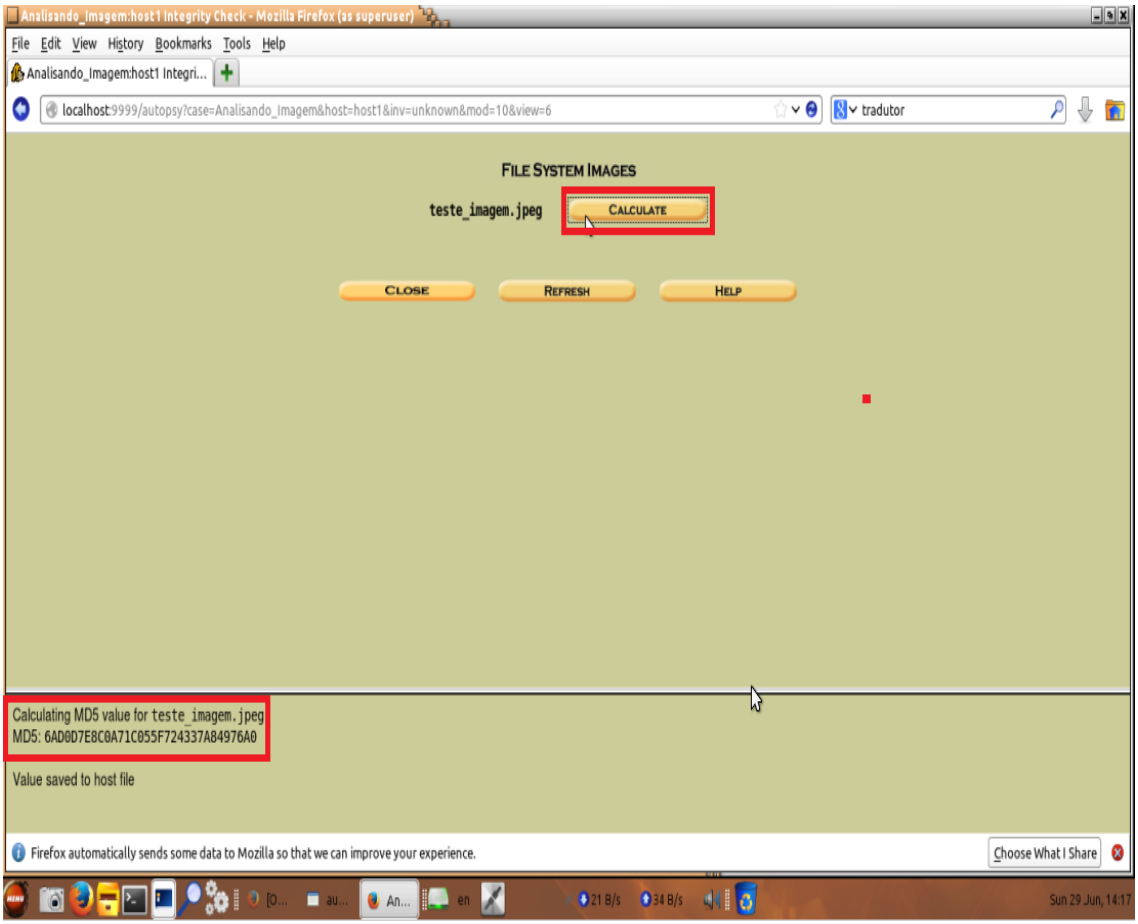


Figura 30 – Cálculo da integridade realizado e retorno do “hash” pertencente à imagem (Contraprova)

Como se pode observar, a sequência de *bits* retornados foi idêntica ao retornado na perícia original no capítulo 5.3.1, na página 48, na figura 23. Ou seja, podemos afirmar que para cada arquivo ou imagem há um “*hash*” pertence. E que se o processo for repetido por diversas vezes sem o arquivo sofrer alguma modificação, o resultado será sempre o mesmo.

MDS: 6AD0D7E8C0A71C055F724337A84976A0.

5.3.3 - PERÍCIA FORENSE EM IMAGEM (MANIPULAÇÃO)

Novamente, será iniciado novamente outro caso, só que diferentemente dos dois anteriores, nessa próxima perícia a imagem será manipulada. O que fará esse arquivo ser diferente do anterior, sendo assim as propriedades irá ser divergente da original e então um novo *"hash"* será pertencente ao mesmo.

Para iniciarmos, será novamente criado um novo caso.

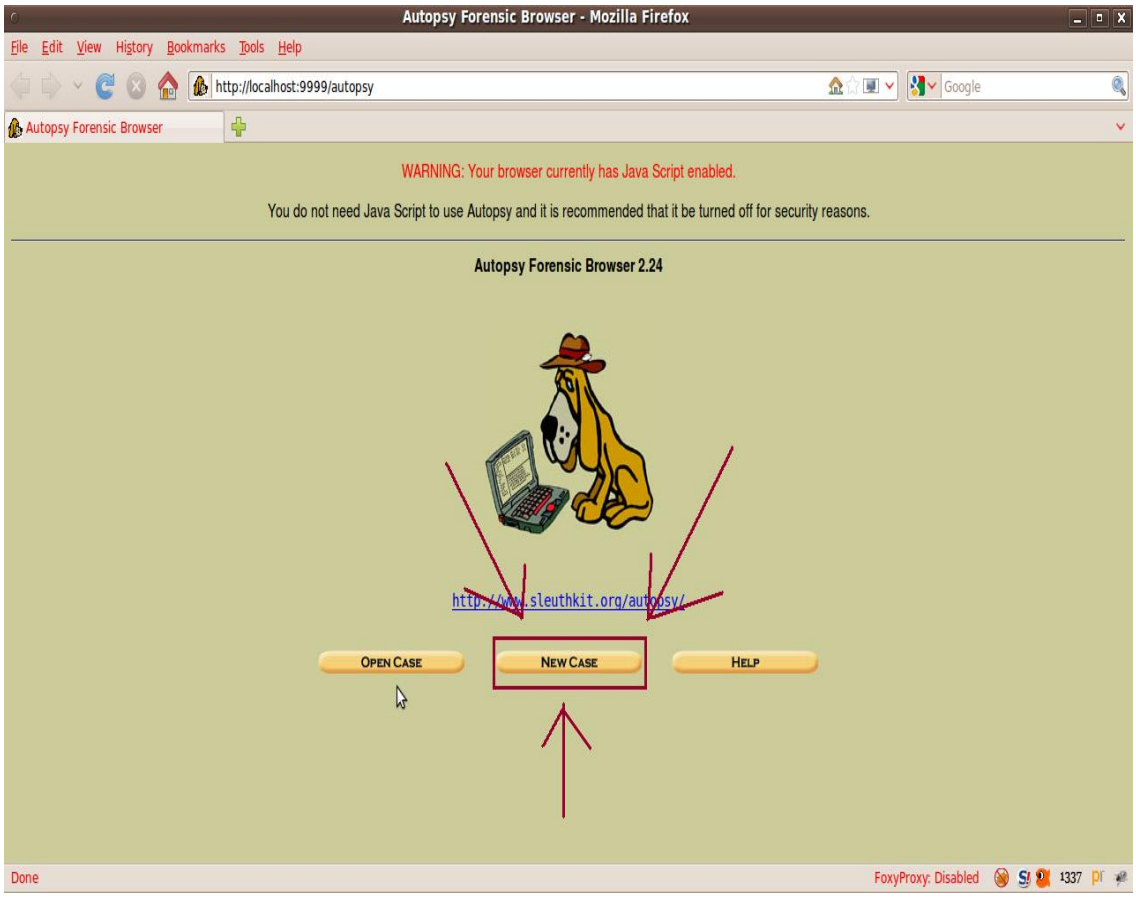


Figura 31 – Página Inicial do Caine – Menu de Opções (Manipulação)

Após a criação de um novo caso, será novamente preciso dar um nome ao caso e também fazer uma breve descrição do mesmo, conforme Figura 32.

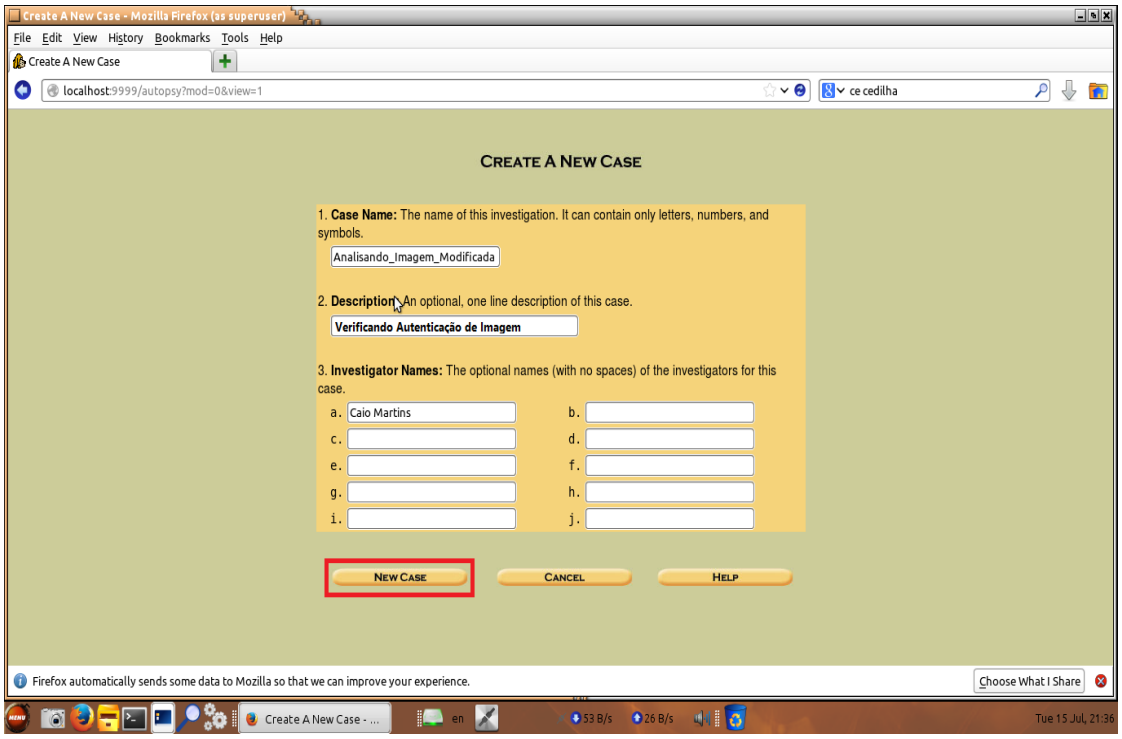


Figura 32 – Página para criação de um novo caso (Manipulação).

Depois de preencher os campos, selecione a opção *"New Case"* e aguarde a atualização da página. Depois de carregada, a página a seguir irá informar que um novo caso foi criado.

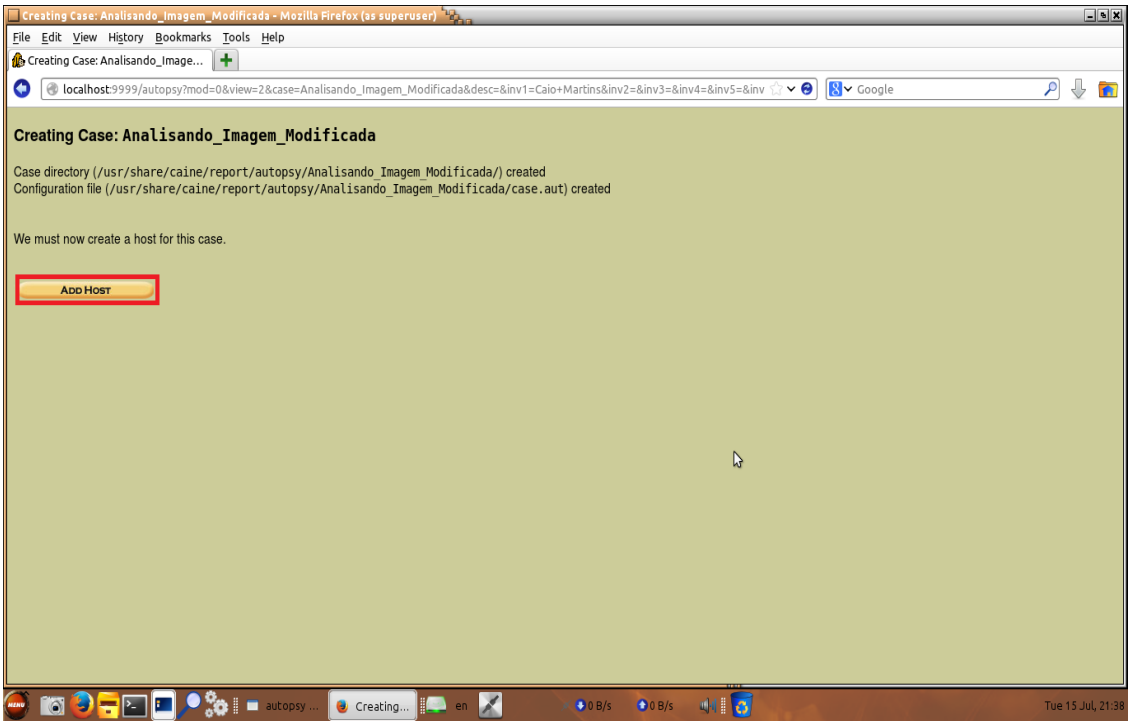


Figura 33 – Página que informa a criação de um novo caso (Manipulação).

Pressione o botão *“Add Host”* e a seguir será solicitado que o perito selecione a imagem a ser periciada.

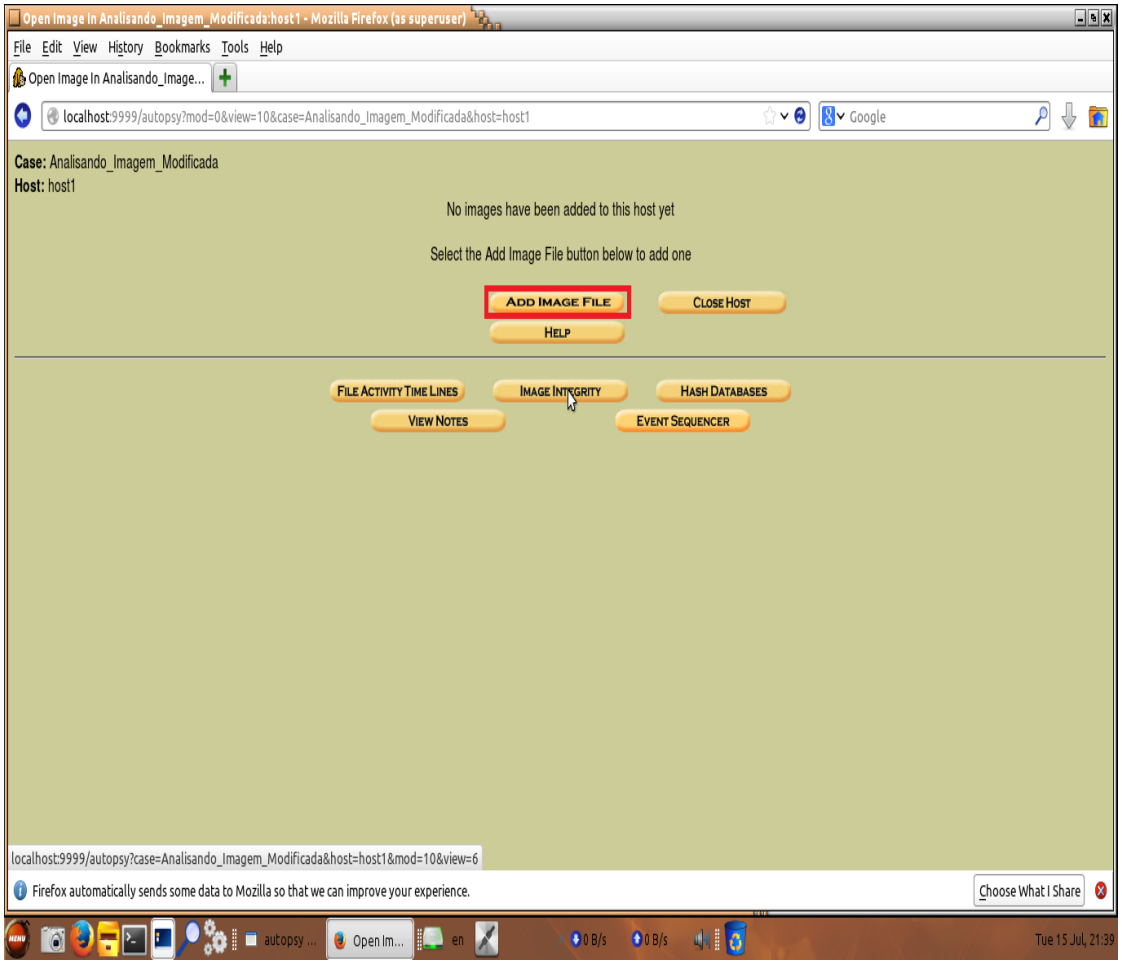
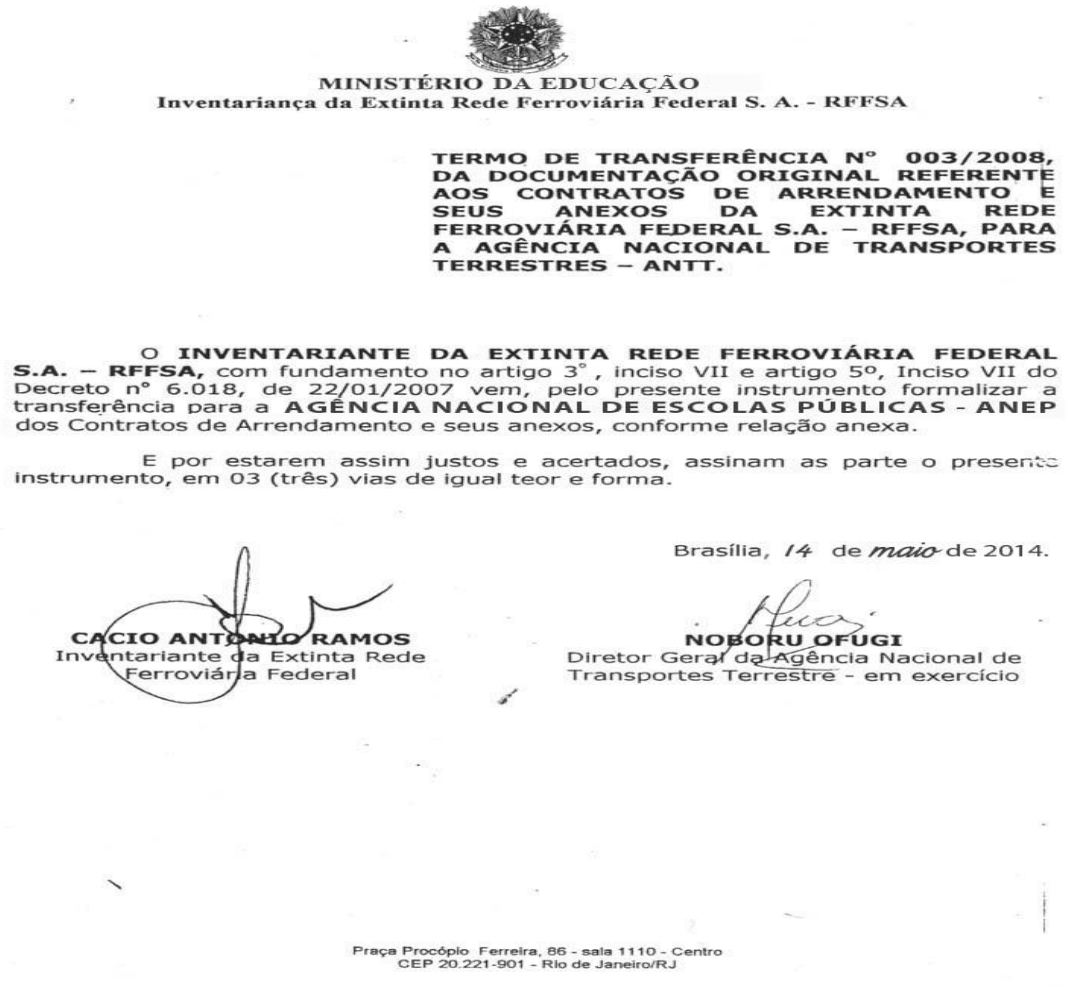


Figura 34 – Página onde o usuário seleciona qual será a imagem utilizada no caso (Manipulação)

Como nesse caso a imagem deverá ser modificada, foram feitas algumas modificações na escrita do contrato, como por exemplo, a data de assinatura e também o órgão judicial que o mesmo se refere. São exemplos de alterações que geralmente ocorrem e que passam ser ter sido notada.



MINISTÉRIO DA EDUCAÇÃO
Inventariança da Extinta Rede Ferroviária Federal S. A. - RFFSA

TERMO DE TRANSFERÊNCIA Nº 003/2008, DA DOCUMENTAÇÃO ORIGINAL REFERENTE AOS CONTRATOS DE ARRENDAMENTO E SEUS ANEXOS DA EXTINTA REDE FERROVIÁRIA FEDERAL S.A. – RFFSA, PARA A AGÊNCIA NACIONAL DE TRANSPORTES TERRESTRES – ANTT.

O **INVENTARIANTE DA EXTINTA REDE FERROVIÁRIA FEDERAL S.A. – RFFSA,** com fundamento no artigo 3°, inciso VII e artigo 5º, Inciso VII do Decreto nº 6.018, de 22/01/2007 vem, pelo presente instrumento formalizar a transferência para a **AGÊNCIA NACIONAL DE ESCOLAS PÚBLICAS - ANEP** dos Contratos de Arrendamento e seus anexos, conforme relação anexa.

E por estarem assim justos e acertados, assinam as parte o presente instrumento, em 03 (três) vias de igual teor e forma.

Brasília, 14 de maio de 2014.

CACIO ANTONIO RAMOS
Inventariante da Extinta Rede Ferroviária Federal

NOBORU OFUGI
Diretor Geral da Agência Nacional de Transportes Terrestre - em exercício

Praça Procópio Ferreira, 86 - sala 1110 - Centro
CEP 20.221-901 - Rio de Janeiro/RJ

Figura 35 – Imagem escolhida para realizar a perícia forense (Manipulação).

Depois de selecionar a imagem, será preciso informar qual o diretório que o arquivo está armazenado no computador e selecionar algumas opções, conforme Figura 36.

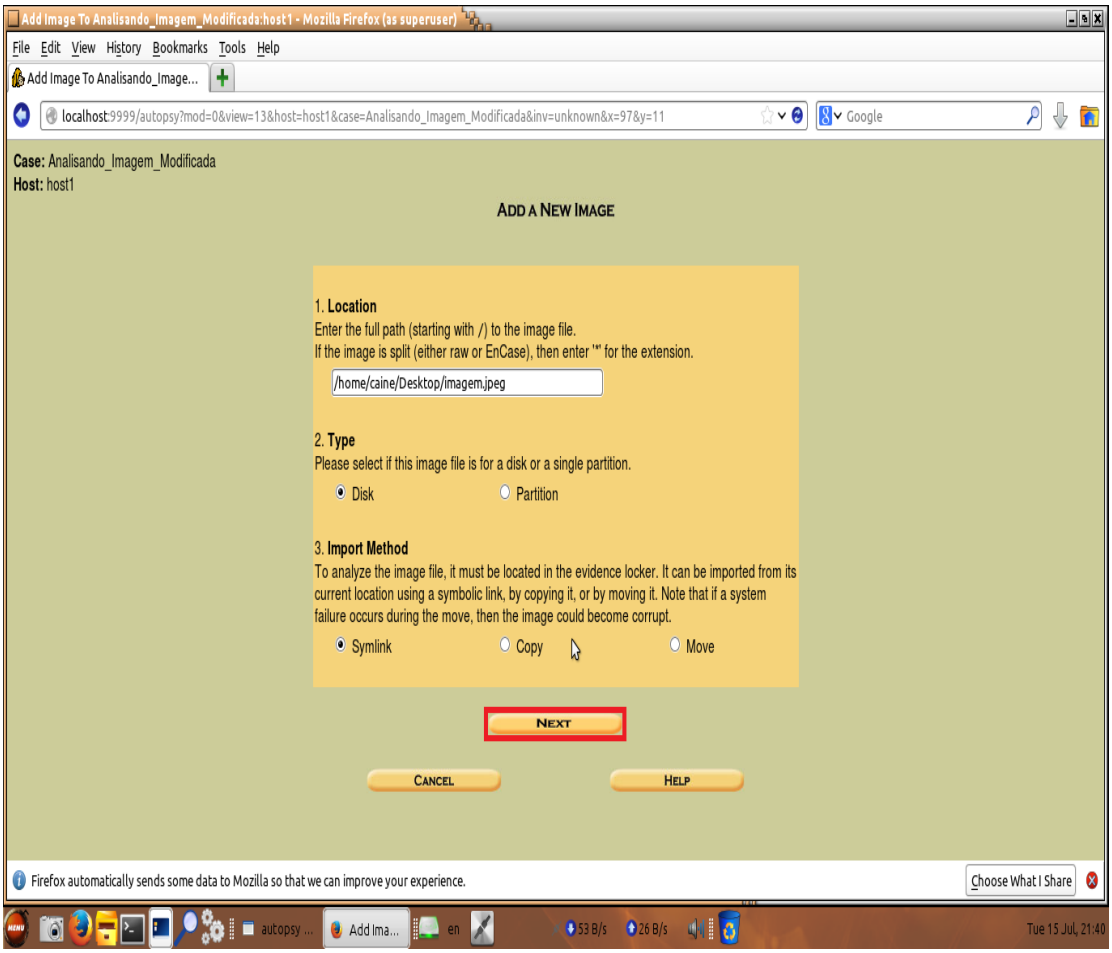


Figura 36 – Página que será informado o diretório que a imagem está armazenada (Manipulação)

Após informar o diretório, pressione o botão *"Next"* e aguarde a atualização da página. Depois de carregada, uma nova página retornará com as propriedades da imagem, como por exemplo, o tipo de arquivo e nome da mesma.

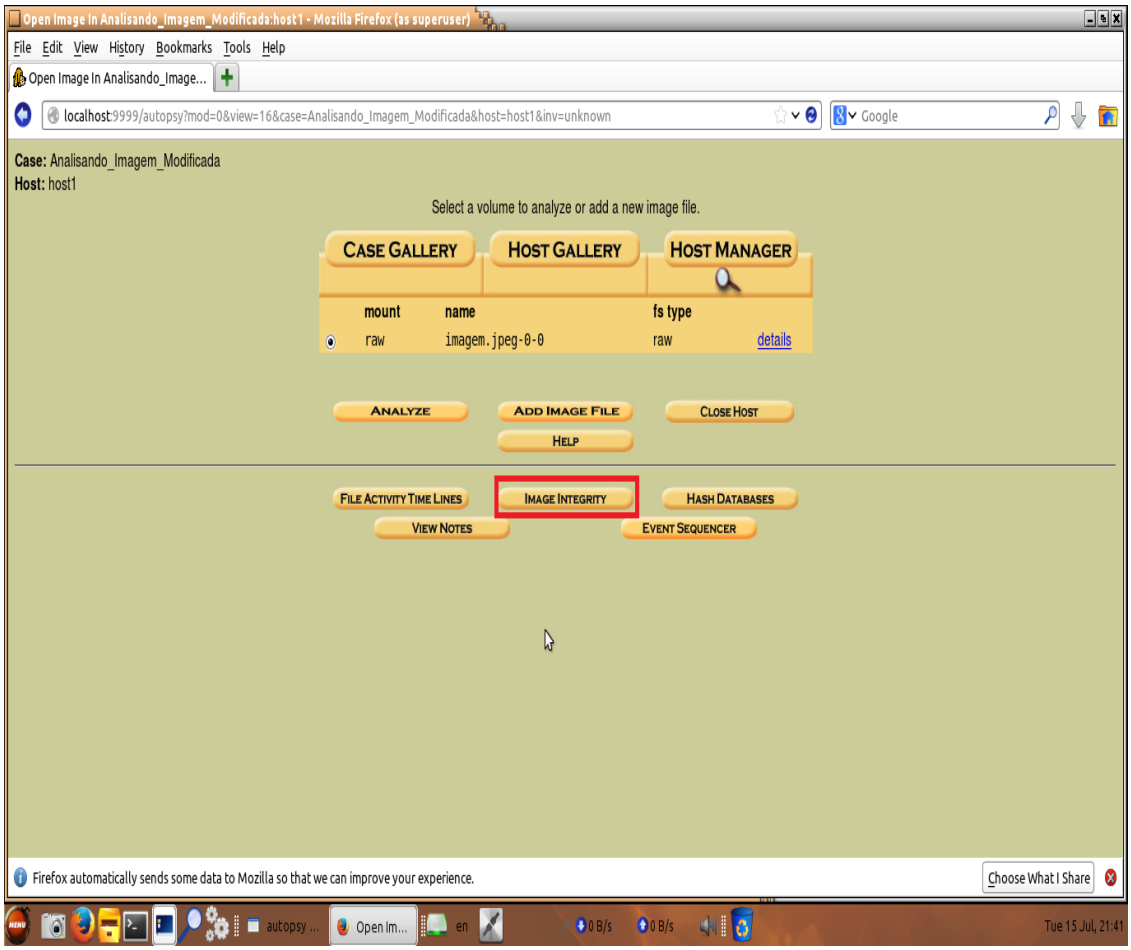


Figura 37 – Página para selecionar a opção para calcular a integridade da imagem (Manipulação)

Selecione a opção *"Image Integrity"* e aguarde a atualização da página. Após atualizar, pressione o botão *"Calculate"* e aguarde atualizar no canto esquerdo da tela a sequência de bits pertencente aquele arquivo, conforme Figura 37.

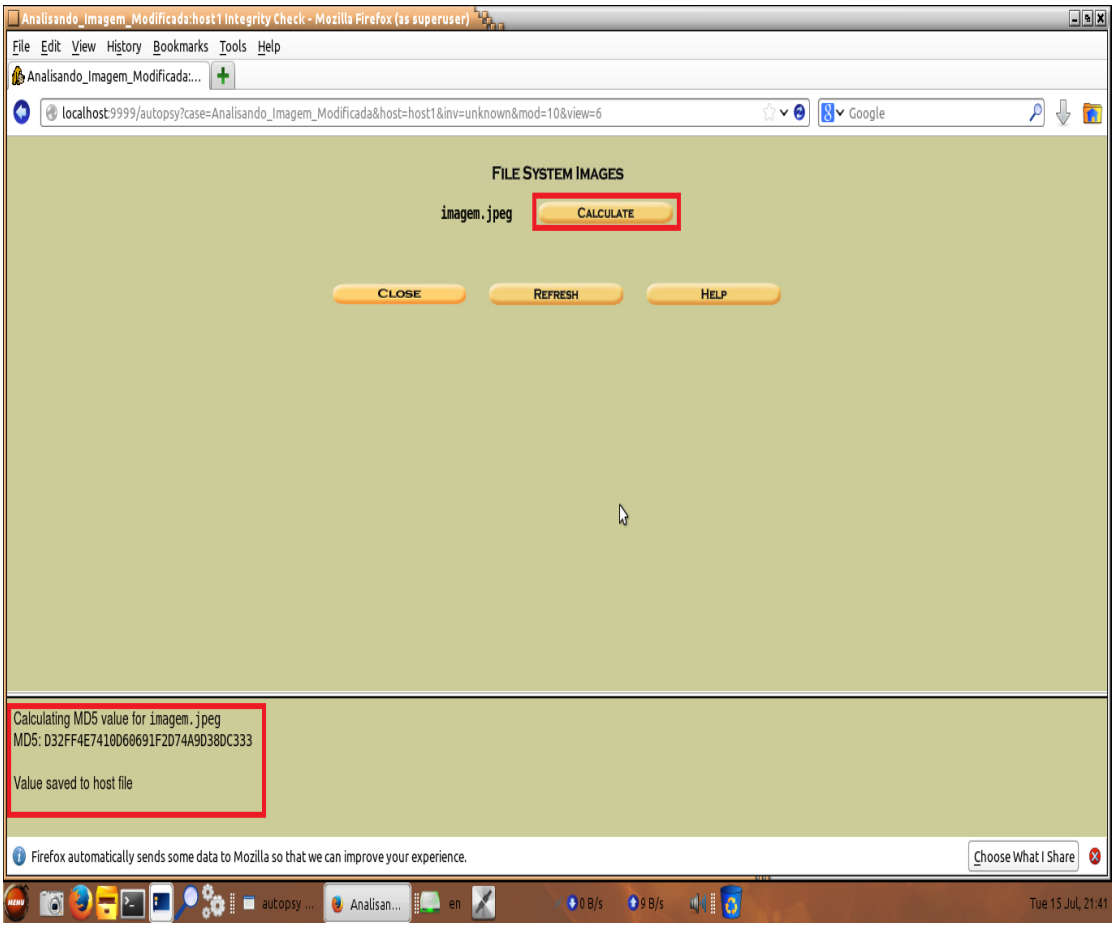


Figura 38 – Cálculo da integridade realizado e retorno do "hash" pertencente à imagem (Manipulação)

Depois de calculado, o *"hash"* retornado que pertence à imagem manipulada, tem a seguinte sequência de 128 *bits*.

MDS: D32FF4E7410D60691F2D74A9D38DC333.

Ou seja, após a modificação da imagem se obteve outro *"hash*[11]*"* totalmente diferente dos dois outros que haviam sido retornados nos capítulos anteriores, quando a imagem ainda era original.

Dessa forma, os peritos conseguem saber se um arquivo já foi modificado e se o mesmo é integro. Mas para poder chegar a essa conclusão é preciso validar os *"hash"* que foram retornados.

[11] Hash: Sequencia de bits gerados por um algoritmo de dispersão.

Sendo assim, após a coleta dos *"hash"*, será desenvolvida uma aplicação no Visual Studio que irá realizar a comparação entre as imagens. A fim de se comprovar, que com base nas sequências de 128 bits pertencentes a cada uma dos arquivos, é possível saber qual é o arquivo é original e também o modificado.

5.3.4 - APLICAÇÃO PARA COMPARAR AS IMAGENS

Para poder validar que as imagens são diferentes, será desenvolvido uma aplicação no Visual Studio, com base na linguagem de programação Visual Basic.

• Linguagem de programação desenvolvida pela empresa Microsoft, pertence ao pacote Visual Studio de desenvolvimento de aplicações. Em suas primeiras versões, o Visual Basic não permitia acesso a bancos de dados, sendo, portanto voltado apenas para iniciantes, mas devido ao sucesso entre as empresas, que faziam uso de componentes adicionais fabricados por terceiros para acesso a dados, a linguagem logo adotou tecnologias, também da Microsoft, permitindo fácil acesso a bases de dados.

Após explicar um pouco sobre a linguagem, será desenvolvida a aplicação. Abra o seu Visual Studio[12] e crie um novo projeto do tipo Windows Application usando a linguagem *VB.NET* e dê o nome do mesmo.

Será incluído no formulário padrão "*form1.vb"* os seguintes controles: dois *TextBox*, dois *Labels* e um *Button*. O formulário deverá ter a seguinte forma:

[12] http://www.microsoftstore.com/store?SiteID=msbr&Locale=pt_BR&Action=DisplayProductSearchResultsPage&result=&keywords=Visual%20Studio&tduid=a890d591e177c1656e3ea23068596588.

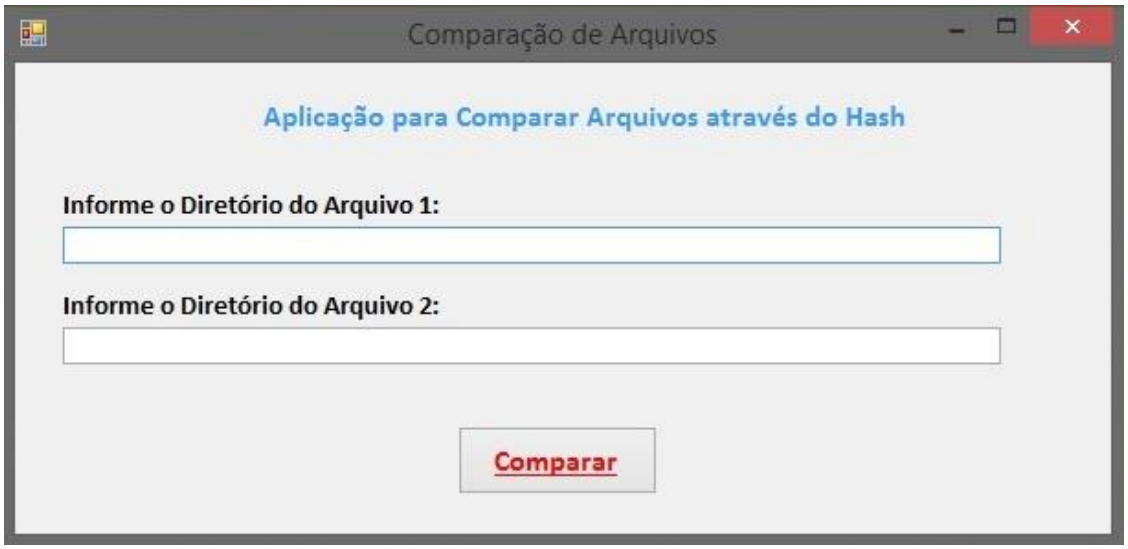


Figura 39 – Aplicação Desenvolvida para Comparar as Imagens com base no “hash” pertencente às mesmas.

A seguir será incluído todo o código de programação no botão “Comparar”. Sendo assim, a aplicação está pronta para ser executada e verificar a integridade das imagens.

Nos campos em branco será preciso informar qual o diretório que os arquivos estão localizados no computador, conforme ilustração abaixo:

Figura 40 – Aplicação Desenvolvida para Comparar as Imagens – Informando os Diretórios de cada arquivo.

Após informar os dois diretórios, selecione o botão “Comparar” e aguarde a aplicação retornar o resultado informando se os arquivos são iguais ou diferentes.

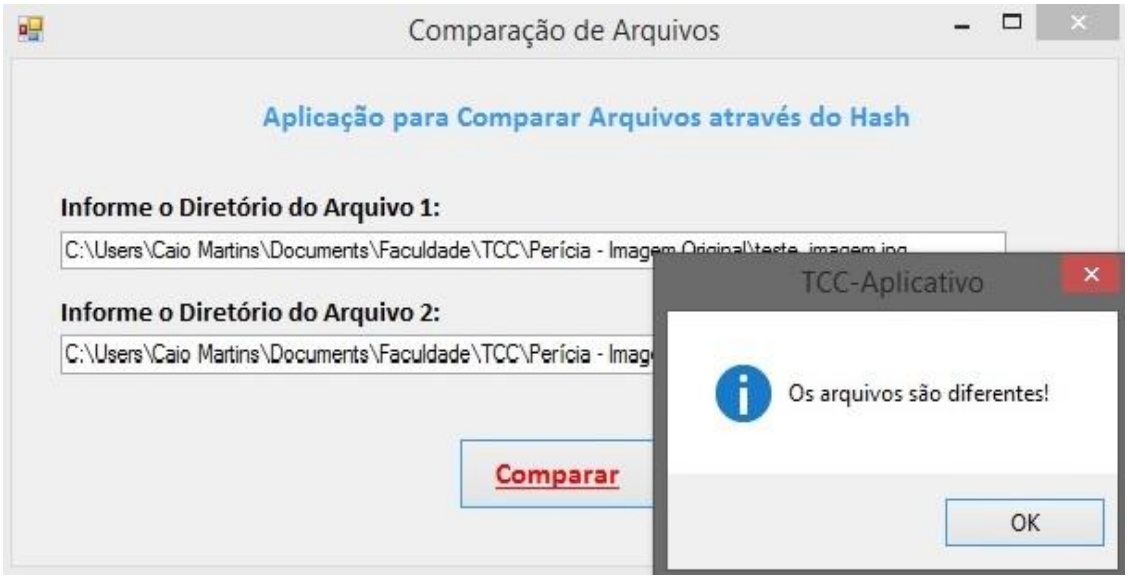


Figura 41 – Aplicação Desenvolvida para Comparar as Imagens – Resultado da comparação das imagens.

Ao selecionar o botão “Comparar”, a classe “ComparaArquivos.vb” é acionada, a mesma faz a verificação de existência dos arquivos no computador através dos diretórios informados e depois gera os “hash” de cada arquivo igual à ferramenta Caine. Por fim, a classe compara os arquivos, conforme ilustrado na Figura 42 da página 63.

```
'verifica se o arquivo1 existe
If Not File.Exists(caminhoArq1) Then

    Throw New Exception(caminhoArq1 & " não existe...")

End If


'verifica se o arquivo2 existe
If Not File.Exists(caminhoArq2) Then
    Throw New Exception(caminhoArq2 & " não existe...")
End If

Try

    'gera hash para o arquivo 1

    objFS = New FileStream(caminhoArq1, FileMode.Open)

    objReader = New StreamReader(objFS)

    aArquivo1 = objEncoding.GetBytes(objReader.ReadToEnd)

    strConteudo1 = objEncoding.GetString(objMD5.ComputeHash(aArquivo1))

    objReader.Close()

    objFS.Close()


    'gera hash para o arquivo 2

    objFS = New FileStream(caminhoArq2, FileMode.Open)

    objReader = New StreamReader(objFS)

    aArquivo2 = objEncoding.GetBytes(objReader.ReadToEnd)

    strConteudo2 = objEncoding.GetString(objMD5.ComputeHash(aArquivo2))


    'efetua a comparação dos arquivos

    bResposta = strConteudo1 = strConteudo2

    objReader.Close()
```

Figura 42 – Aplicação Desenvolvida para Comparar as Imagens – Código Fonte da Classe “ComparaArquivo.vbs”

Após a classe realizar a comparação dos arquivos, ela retorna a informação para outra classe chamada “Form1”, que irá informar o resultado da comparação ao usuário se o arquivo foi modificado ou não, conforme Figura 43 na página seguinte.

```
Imports System.Security.Cryptography

Public Class Form1

    Private Sub btnCompara_Click(sender As Object, e As EventArgs) Handles btnCompara.Click
        Try
            If comparaArquivos.comparador(txtArquivo1.Text, txtArquivo2.Text) Then
                MsgBox("O arquivo não sofreu modificação!", MsgBoxStyle.Information)

            Else
                MsgBox("O arquivo foi modificado!", MsgBoxStyle.Information)
            End If
        Catch ex As Exception
            MsgBox(ex.Message, MsgBoxStyle.Critical, "Erro!!")

        End Try
    End Sub

    Private Sub lblArq1_Click(sender As Object, e As EventArgs) Handles lblArq1.Click

    End Sub
End Class
```

Figura 43 – Aplicação Desenvolvida para Comparar as Imagens – Código Fonte da Classe “Form1.vb”

Como pode ser observado, o resultado informado revelou que as imagens são diferentes, ou seja, mesmo os arquivos contendo os nomes iguais e estando em diretórios diferentes, não foram suficientes para modificar o resultado. Uma pequena modificação no arquivo original irá modificar o “hash” pertencente ao mesmo, dessa forma, não serão encontrados “hash” igual em arquivos originais e modificados.

6 – CONCLUSÃO

Ao final do trabalho espera-se como resultado demostrar como é todo o processo de perícia forense digital com a ferramenta Caine, para que todos possam conhecer como agem os peritos em casos de manipulação de arquivos do tipo imagem.

Dessa forma, esse estudo propõe um processo de perícia digital, que poderá ser executado com sucesso por qualquer pessoa, físico ou jurídico. Pois o trabalho apresentado exibe todas as etapas de criação de um caso onde se tenha dúvidas quanto à autenticidade da imagem.

Cumprido este objetivo, considerado como principal neste trabalho, existe a expectativa de crescimento e desenvolvimento pessoal, obtida por intermédio do conhecimento da área de Segurança de Informação com base na Perícia Forense Digital, em um ambiente real, que certamente propiciará experiência e desafios úteis em minha trajetória profissional.

7 – REFERÊNCIAS.

BACKTRACK, Disponível em: > http://www.backtrack-linux.org/ < Acesso em: 25 fev. 2014.

CAINE, **Lista de Ferramentas**, Disponível em: >http://www.caine-live.net/< Acesso em: 25 fev. 2014.

BUSTAMANTE, Leonardo. **Introdução a Computação Forense**. Setembro. 2008.

BUSTAMANTE, Leonardo. **Computação Forense - Novo campo de atuação do profissional de informática**. Julho. 2006.

CARVALHO, Jaqueline Lima Soares. **PERI-BR: Geração de um LIVE-CD de perícia baseado no Ubuntu.** Disponível: https://sites.google.com/a/cristiantm.com.br/forense/ferramentas/livecd/peribr, Acesso em: 23 fev. 2014.

COSTA, Marcelo Antonio Sampaio Lemos, **Computação Forense,** Millenium Editora, Edição 3, 2011.

COSTA, Marcelo Antonio Sampaio Lemos. **Curso de Introdução às Perícias dos Crimes de Informática**. Millenium Editora. Julho. 2008.

ELEUTÉRIO, Pedro Monteiro da Silva; MACHADO, Marcio Pereira. **Desvendando a Computação Forense.** Novatec Editora, 2011.

FDTK**, Menu de ferramentas da Distro FDTK-UbuntuBr V 2.01**.

Disponível: > http://fdtk.com.br/www/ferramentas/ < Acesso em: 28 fev. 2014.

GIAVARATO, César Roxo & RAIMUNDO, Gerson dos Santos. **Backtrack Linux - Auditoria e Teste de Invasão em Redes de Computadores**, 2013, ISBN 9788539903740.

KRONE T, **High Technology Crime Brief**. Australian Institute of Criminology. Canberra, Australia. 2005.

LEPRE, Janaina. **Prejuízo Mundial com crimes pela Internet chega a US$ 113 milhões**. Outubro. 2013. Disponível em: > http://g1.globo.com/jornal-da-globo/noticia/2013/10/prejuizo-mundial-com-crimes-pela-internet-chega-us-113-bilhoes.html<. Acesso em: 24 fev. 2014

SYMANTEC, **Crimes Cibernéticos**, Disponível em: >http://br.norton.com/cybercrime-definition/promo< Acesso em: 10 mar. 2014.