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

DENIS MENDONÇA LADEIRA

UMA ABORDAGEM SOBRE FERRAMENTAS DA ANÁLISE FORENSE COMPUTACIONAL

Assis

2013

DENIS MENDONÇA LADEIRA

UMA ABORDAGEM SOBRE FERRAMENTAS DA ANÁLISE FORENSE COMPUTACIONAL

Trabalho de Conclusão de Curso apresentado ao Instituto Municipal de Ensino Superior de Assis, como Requisito do curso de Graduação.

Orientador: Prof° Dr. Luiz Ricardo Begosso

Área de Concentração: Forense Computacional

Assis

2013

FICHA CATALOGRÁFICA

LADEIRA, Denis Mendonça
Uma abordagem sobre ferramentas da Análise Forense Computacional / Denis Mendonça Ladeira. Fundação Educacional do Município de Assis – FEMA – Assis, 2013.

72 p.

Orientador: Luiz Ricardo Begosso.

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

1.Segurança. 2. Forense

CDD: 001.61
Biblioteca da FEMA

UMA ABORDAGEM SOBRE FERRAMENTAS DA ANÁLISE FORENSE COMPUTACIONAL

DENIS MENDONÇA LADEIRA

Trabalho de Conclusão de Curso apresentado ao Instituto Municipal de Ensino Superior de Assis, como Requisito do curso de Graduação, analisado pela seguinte comissão examinadora:

Orientador: Dr. Luiz Ricardo Begosso

Analisador (1): Esp. Diomara Martins Reigato Barros

Assis

2013

AGRADECIMENTOS

A Deus por mostrar-me os caminhos da vida, e sempre estar ao meu lado nas tomadas de decisões.

Aos professores, pelas instruções e amizade, em especial ao professor e amigo Dr. Luiz Ricardo Begosso, pela orientação neste presente trabalho e oportunidades que me foram oferecidas nas quais sou muito grato.

Aos amigos, pelo companheirismo e à todos os momentos em que compartilhamos juntos, desculpe-me caso faltei alguma vez. Lhes desejo toda a sorte do mundo, podem sempre contar com minha ajuda.

Aos meus familiares, pelo constante apoio e ajuda em todas as etapas da minha vida, um agradecimento especial aos meus pais, Luzia e Nelson pela educação e valores à mim repassados, tornando-me a pessoa na qual sou hoje.

E a todos que colaboraram direta ou indiretamente na execução deste trabalho.

RESUMO

O constante avanço da sociedade define-se pela necessidade das pessoas e organizações buscarem alternativas para facilitar e melhorar as atividades no qual elas são expostas diariamente. A tecnologia foi a maneira encontrada para suprir estas necessidades, possibilitando as organizações, por exemplo, maneiras para o melhor gerenciamento do negócio e consequentemente aumento no lucro. Já em termos pessoais as pessoas buscaram soluções em entretenimento e comunicação, aliando usabilidade e ao mesmo tempo funcionalidade, tomando como exemplo a Internet.

Consequentemente com este avanço, aumentou-se a cada ano o número de informações que são armazenadas nas mídias computacionais e que trafegam em redes de computadores todos os dias, resultando também, no aumento do número de incidentes na quebra de segurança destes meios, tornando a segurança de dados, um item imprescindível de qualidade em uma aplicação.

É com o objetivo de prevenir e solucionar tais incidentes referentes à segurança de dados, que surge a Computação Forense, ciência que prove de técnicas e ferramentas periciais afim de auxiliar no processo de produção de evidências digitais.

Palavras Chaves: segurança; dados; forense;

ABSTRACT

The constant advancement of society defined by the need for people and organizations find alternatives to facilitate and improve the activities in which they are exposed daily. Technology was the way found to meet these needs, enabling organizations, for example, ways to better manage the business and consequently increase in profit. Already in personal terms, people sought entertainment and communication solutions, combining usability and functionality at the same time, taking as an example the Internet.

Consequently with this breakthrough, was increased every year the number of information that are stored on computer media and traveling on computer networks, also resulting in increased number of security breach incidents in these media, making the security of these data an essential item of quality in an application.

It is aiming to prevent and resolve such incidents relating to data security, which arises Computer Forensics, science that proves forensic techniques and tools in order to assist in the production of digital evidence.

Keywords: security; data; forensic;

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1. INTRODUÇÃO

Nos últimos anos a Internet se tornou um dois meios de comunicação mais influente e utilizada em nosso cotidiano, atualmente com a entrada de novos dispositivos capazes de interagir em uma rede de computadores, é comum notar um envolvimento maior das pessoas nesse meio tecnológico, a segurança tem um papel preponderante dentro deste contexto seja de maneira geral ou particular. Entretanto, o discernimento dos armazenamentos digitais e fluxo de dados se tornam cada vez mais utilizados e maiores, as pessoas que utilizam tais meios digitais estão cada vez mais eminentes de furtos dos seus dados pessoais. (SANTOS, 2008)

Nos dias atuais, apesar da preocupação imposta pelas empresas em utilizar mecanismos para acrescer a segurança dos sistemas operacionais que fazem parte de uma rede de computadores, é incerto afirmar que estas empresas não serão mártir de um incidente de segurança, mesmo que assegurem todos os tipos de recomendações e implantem as mais modernas e exímias tecnologia. (OLIVEIRA, 2002).

Como nenhum tipo de tecnologia ou recurso garante 100% de segurança da informação, é importante a adoção de uma política de segurança, para que, no caso de uma ocorrência de invasão, a organização possa agir da melhor maneira possível para evitar que a situação se agrave, colocando em prática, por exemplo, o programa de resposta a incidentes. Segundo (SÊMOLA, 2003), este programa é composto por uma equipe multiespecializada, capaz de atuar de forma integrada e com velocidade para reduzir o tempo de exposição da empresa, minimizando os impactos da invasão. Essa equipe, em conjunto com as metodologias de análise forense, podem fazer surtir efeitos positivos para a empresa no que se refere à resolução de problemas causados pelas invasões e ações que visem desvendar as causas e os responsáveis pelos mesmos. Porém tais ferramentas e metodologias são muito pouco comuns na maioria das empresas.

A computação forense é um campo de pesquisa relativamente novo no mundo, porém, vem crescendo consideravelmente nos últimos anos, junto com o avanço das tecnologias, principalmente pela necessidade das instituições legais atuarem no

combate aos crimes eletrônicos. No Brasil, ainda conta-se com poucos pesquisadores na área e existem poucas normas estabelecidas o que gera um grande número de possibilidades de pesquisa. Nesta pesquisa, o objetivo é um estudo de ferramentas e técnicas que podem contribuir para uma boa resposta a incidentes nas organizações.

1.2. OBJETIVOS

Este trabalho tem como principal objetivo demonstrar técnicas e procedimentos que auxiliem no processo de análise forense de sistemas computacionais independentemente do Sistema Operacional ao qual o dispositivo é baseado; este estudo contribuirá para enriquecimento do material técnico sobre esta área, já que a mesma é tão pouco explorada didaticamente.

O trabalho tem como objetivo genérico debater sobre a importância da Segurança em redes de Computadores e apresentar os principais conceitos sobre a Perícia Forense através da realização de uma revisão bibliográfica sobre estes determinados termos.

1.3. JUSTIFICATIVAS

São levadas em consideração para o desenvolvimento da presente pesquisa o fato de que diversos peritos da área forense manifestam-se aos constantes acontecimentos referentes à furtos de dados digitais que envolvem empresas particulares e instituições públicas, com isto levante-se o fato em que a Computação Forense cresce diariamente com intuito de beneficiar e prevenir tais empresas e instituições.

A Computação Forense é uma área de pesquisa que cresce diariamente, é importante que aumente também o acumulo de material de apoio que se apresente de forma estruturada e organizada.

1.4. MOTIVAÇÃO

É importante que haja para assegurar a realização de uma investigação forense com eficácia, a composição de procedimentos e adoção de medidas e ferramentas para tal uso, isto garante uma rápida e eficaz resposta quando ocorre um incidente de segurança. Infelizmente, nos dias de hoje, existem poucos estudos e metodologias que abordam o assunto e auxiliam o estudo de pesquisadores e peritos na área, apesar da questão de segurança ser constantemente discutida em relação aos meios tecnológicos, principalmente quando se diz respeito à qualidade de sistemas.

Embora exista certo volume de documentação que pode ser encontrada em meios virtuais, ela se encontra em muitos casos desorganizada e confusa (SANTOS, 2008); e a maioria dos livros desta área está em língua estrangeira, o que muitas vezes dificulta o acesso de pessoas interessadas no assunto. A necessidade de aumentar o material em português e de forma organizada, serve de motivação para a realização deste trabalho.

1.5. REVISÃO DA LITERATURA

Conforme afirma (NOBLETT, 2000) a Computação Forense foi criada com o objetivo de atender a carestia das instituições legais no que diz respeito à manipulação das mais recentes formas de evidências eletrônicas. Ela é a ciência que estuda a aquisição, preservação, recuperação e análise de dados que foram processados eletronicamente e arquivados em algum tipo de mídia computacional.

A Computação Forense vem crescendo consideravelmente nos últimos anos, junto com o avanço das tecnologias, com isso novas formas de criar métodos de perícia computacional emergiram. Uma das principais aplicações nessa área é a busca por evidências forenses em computadores e periféricos. (FARMER, 2007).

1.6. PERPECTIVAS DE CONTRIBUIÇÃO

Este trabalho irá contribuir para futuras pesquisas de estudantes na área, que procuram adquirir conhecimento sobre o assunto, e buscam ferramentas e processos que auxiliem a perícia forense computacional.

O intuito é divulgar por meio deste trabalho, a importância de aplicações na busca pela prevenção de incidentes relacionado à segurança de dados, e a influência dos *Softwares* Livres perante as novas áreas de pesquisas.

1.7. METODOLOGIA DE PESQUISA

Será utilizado no estudo, informações contidas em artigos, teses, dissertações, revistas, Livros e internet; que servirão como fonte para assuntos como: Perícia Computacional Forense, Evidências Digitais, mídias de armazenamento digitais e segurança em Rede de Computadores.

Já em aspectos jurídicos e crimes digitais existe a possibilidade da realização de entrevistas com profissionais da área.

Para o estudo de caso de ferramentas que auxiliam a análise forense, a busca por conteúdo terá como base a Internet e descrições contidas em livros, e utilização de sistemas baseados no UNIX que tem como principais funcionalidades auxiliar o trabalho de professionais da área e pesquisadores.

1.8. ESTRUTURA DO TRABALHO

Este trabalho encontra-se dividido em duas partes relacionadas ao levantado de conceitos bibliográficos. Na primeira parte serão apresentados tópicos relacionados sobre os aspectos da segurança em redes de computadores e sistemas, enquanto que na segunda parte será realizado um levantamento bibliográfico teórico sobre a Computação Forense.

Na primeira parte serão discutidos, os fundamentos de segurança, evidenciando quais são as ameaças de uma rede, e quais os riscos para um todo, caso estas ameaças não sejam gerenciadas; do ponto de vista econômico foi discutido a importância de se pensar em segurança de informação apresentando fatos como o valor do patrimônio informacional da empresa e a vantagem competitiva no mercado caso à empresa adote esta filosofia.

Em seguida, será realizada uma conceituação de segurança, e levantado um questionamento sobre qual tipo de informação realmente é necessário proteger, visto que o mais importante é a proteção dos dados e não da rede em si tratando-se de hardware e software.

Ao final serão apresentados dois tópicos sobre as consequências de invasões e modelos para assegurar à segurança da informação.

Na segunda parte do trabalho, será desenvolvida uma conceituação teórica sobre Computação Forense, demonstrando a importância do tema, suas aplicações, as habilidades necessárias para os peritos forenses e suas responsabilidades.

Será levantada uma breve descrição a respeito de vulnerabilidades e de como rastreá-las; um texto sobre evidências digitais, dispondo suas principais características e fontes de dados. Por fim uma matéria sobre as etapas de uma investigação, apresentando um importante formulário para documentação da análise forense.

Ao fim destas duas partes, inicia-se o capítulo no qual é elaborado o principal objetivo deste trabalho, o estudo de caso sobre as ferramentas que auxiliam nos procedimentos e etapas de um pericia forense, quanto a extração, exame, e análise de dados.

Este estudo se fundamenta no comparativo entre duas distribuições Linux que se baseiam principalmente em prover uma estrutura de aplicações forenses para uso e estudo, são elas, o CAINE (*Computer Aided Investigative Environment*) e o FDTK (*Forense Digital ToolKit)*. O comparativo tem como objetivo evidenciar os pontos fortes e qual é o melhor ambiente para uso de tais aplicações.

Ao final do estudo, será destacado o uso de ferramentas forenses, que cooperem para o cotidiano das pessoas, apresentando um breve trecho descrevendo a Criptografia e sua importância na segurança de dados.

Ao final, apresenta-se a conclusão do trabalho, com uma discussão dos principais pontos da pesquisa, tendo como embasamento a segurança de informações, e a conclusão do estudo sobre o CAINE e FDTK.

2. SEGURANÇA EM REDES DE COMPUTADORES

A segurança tem seu papel importante para o funcionamento adequado de qualquer ação no contexto geral ou particular, seja para uma companhia ou para uma pessoa física. No contexto tecnológico, este termo é de grande importância, devido ao continuo desenvolvimento tecnológico e de situações de risco que o mundo real passou a estar submetido a partir das invasões e manipulações de dados particulares de pessoas e de empresas.

É imensurável o número de pacotes que trafegam todos os dias nas redes de computadores, o controle de todo este conteúdo deve ser feito de maneira segura e abrangente. Assim, a segurança da informação propõe que toda e qualquer informação, armazenada temporária ou permanentemente que trafegue por redes de computadores esteja protegida contra ameaças, isto é, a informação de maneira geral deve manter a sua confidencialidade, integridade e disponibilidade em situações diferenciadas de acesso devido aos riscos e ameaças de invasão em relação à segurança e privacidade do sistema em geral. Quanto a isso, a teoria mais aceita sobre esse assunto é a de que há um estágio de consciência da capacidade de resolução de problemas que diz respeito ao trafego de informações e das limitações na capacidade dessas resoluções quando o assunto é *hacketismo* e outros tipos de invasores e as novas formas de invasões a sistemas e redes de computadores.

Os riscos e ameaças intencionais e não-intencionais na segurança de maneira geral representam, para redes e sistemas, um fator de preocupação que tem sua importância quando se trata de vulnerabilidade a que estão expostas pessoas e empresas. Portanto, há que se pensar em mecanismos de defesa de maneira clara e objetiva. Dessa forma, os mecanismos de defesa para a proteção do ambiente computacional devem ser planejados e realizados com base no conhecimento das ameaças e dos riscos existentes e nos que possam vir a existir como forma de prevenção e proteção ao sistema. Isso permite que vulnerabilidades possam ser exploradas em ataques após as identificações preventivas terem sido aplicadas ao sistema especificado.

2.1. FUNDAMENTOS DE SEGURANÇA

A segurança de redes tem como principal objetivo proteger as informações que nela trafegam no sentido de garantir a sua confidencialidade, a sua integridade e a sua disponibilidade. De acordo com QUEIROZ aput Symantec (2006) define-se (1) confidencialidade como sendo uma propriedade cujo objetivo é o de responsabilizar-se por permitir acesso ao seu conteúdo somente a usuários que são autorizados; (2) a integridade define-se como sendo uma propriedade que garante a chegada de uma informação ao seu destino em toda a sua totalidade, isto é, sem restrições; (3) por último define-se disponibilidade como sendo uma propriedade que caracteriza-se por assegurar ao usuário do sistema acesso à informação quando esses necessitam. A Tabela 1 descreve cada uma das três propriedades situadas à esquerda e suas definições postas à direita de maneira resumida para melhor compreensão:

Propriedades	Definição
• Confidencialidade	É a propriedade que garante apenas aos usuários autorizados o acesso ao conteúdo
• Integridade	É a propriedade que garante a chegada da informação ao seu destino de uma forma integra, ou seja, sem que tenha sofrido nenhuma mudança em seu conteúdo em qualquer momento de sua existência.
• Disponibilidade	É a propriedade que garante a disponibilidade da informação para os usuários quando eles necessitam acessá-las.

Tabela 1 – Propriedade de segurança em Sistemas Computacionais (In: QUEIROZ, 2007, p. 5)

Os dados apresentados na Tabela 1 expõem que a segurança de redes e de sistemas devem assegurar a proteção contra ameaças que podem implicar na confidencialidade, integridade e disponibilidade de todas as informações armazenadas temporariamente ou permanentemente em um sistema. Assim acontece porque as ameaças e riscos intencionais e não-intencionais para a segurança de redes e sistemas, podem ser atingidos de forma comprometedora. Com isto, as ferramentas e mecanismos de defesa para a proteção em uma intranet ou de uma rede computacional pública, devem ser planejados e realizados com base no conhecimento das ameaças e dos riscos já existentes. É exatamente neste contexto que pode-se fazer a identificação das vulnerabilidades que por sua vez possam se apresentar no sistema intra-rede. A partir da realização de uma identificação, pode-se prover ações para que as vulnerabilidades sejam controladas e suspensas contra exceções de caráter prejudicial ao sistema.

Do ponto de vista econômico, a previsão dos riscos e ameaças pode significar para a segurança intra-rede uma questão, a grosso modo econômica, para que a organização interessada pondere os prejuízos causados por pacotes de informações infectados. Por outro lado, eliminar todos os perigos e ameaças conhecidas pode ser bastante caro. Sobre tudo não é justificável investimentos mais altos do que o valor da própria informação. Assim, o fundamental é que os riscos sejam gerenciados, ou seja, eles devem ser minimizados, sendo possível que os riscos restantes sejam tolerados pela empresa, ou mesmo transferidos para terceiros.

2.2. IMPORTÂNCIA DA SEGURANÇA EM COMPUTADORES E REDES

Pode parecer absurdo fazer a pergunta: “Porque é que a segurança do computador e da rede é tão importante?”, mas é crucial para a organização determinar como alcançar a segurança em fim tecnológico e quais os métodos irão utilizar para conseguir tal feito. É também uma ferramenta útil para usar quando se busca a autorização da gerência sênior para as despesas relacionadas com a segurança. A segurança em computadores e em redes de computadores é importante pelos seguintes fatos:

1. Para proteger o patrimônio da Empresa: Um dos principais objetivos da segurança do computador e da rede é a proteção do patrimônio da empresa. Por “patrimônio”, não significa dizer o hardware e software que constituem computadores e a rede da empresa. O patrimônio é composto de informações que estão armazenadas na rede e computadores de uma empresa. A informação é patrimônio organizacional vital. A segurança em redes computacionais estão relacionadas, acima de tudo, com a proteção, a integridade e a disponibilidade da informação. A informação pode ser definida como dados organizacionais que são organizados e acessíveis numa forma coerente e significativa.
2. Para ganhar uma vantagem competitiva: Desenvolver e manter medidas de segurança eficazes pode proporcionar a uma organização uma vantagem competitiva sobre seus concorrentes. A segurança de rede é particularmente importante na área de serviços financeiros da Internet e e-commerce. Pode significar a diferença entre a ampla aceitação de um serviço ou não. Por exemplo, quantas pessoas iriam usar o sistema de internet banking, se soubessem que o sistema havia sido invadido com sucesso no passado? Não seriam muitos. É importante garantir a informação também para as regularizações federais e governamentais que as empresas são submetidas.
3. Para manter seu emprego: Finalmente, para garantir sua posição dentro de uma organização e para assegurar a futura carreira, é importante colocar em pratica medidas que protegem o patrimônio organizacional. A segurança deve ser parte do trabalho de cada administrador de rede e sistema. A incapacidade de realizar adequadamente pode resultar em demissão. A rescisão não deve ser o resultado automático de uma falha de segurança, mas se, depois de uma avaliação completa, é determinado que o fracasso foi o resultado de políticas e procedimentos inadequados ou o não cumprimento com os procedimentos existentes, então é necessário que os gerentes realizem mudanças.

Precisa-se ter em mente que segurança em redes custa dinheiro: Custa dinheiro para contratar, treinar, e reter pessoal, para comprar hardware e software para proteger redes de uma empresa. Como resultado, a segurança da rede não é barato. No entanto, é provável que seja mais barato que os custos associados a ter a rede da empresa comprometida.

2.2.1 Segundo plano

Deve-se manter cautela em estatísticas utilizadas por várias organizações de quantificar ou medir os incidentes de segurança da informação, no entanto é útil rever alguns números apresentados. De acordo com (CANAVAN, 2001), em uma pesquisa realizada em 1999 em conjunto pela *American Society for Industrial Security and Pricewaterhouse-Coopers* (ASIS / PWC), informou que as empresas do *Fortune 1000*[1] perderam mais de US$ 45 bilhões de dólares em roubo de informações confidenciais. A pesquisa ASIS/ PWC também recebeu 97 respostas também do interesse, que relataram o seguinte:

- Quarenta e cinco por cento dos entrevistados disseram que tinham sofrido uma perda financeira como resultado de perda de informações, roubo ou apropriação indébita.
- Em média, as empresas respondentes relataram 2,45 incidentes com um custo estimado de US$ 500 mil dólares por incidente.
- O Número de incidentes relatados por mês haviam aumentado ao longo dos últimos 17 meses.

Em um levantamento anual realizado conjuntamente pelo FBI e o *Computer Security Institute* / CSI, (CANAVAN, 2001), também produziu alguns números interessantes. A pesquisa FBI/CSI recebeu 521 respostas de pessoas na área de segurança da informação de computadores. Os números variam para os vários tipos de incidentes:

- Trinta por cento dos entrevistados relataram uma invasão de uma fonte externa.
- Cinquenta e cinco por cento dos entrevistados relataram uma invasão não autorizada por uma fonte de dentro da organização.
- Desses entrevistados que relataram uma perda, a perda média de roubo de informações confidenciais aumentou de US$1,677,000 dólares em 1998 para $1,847,652 dólares em 1999.

[1] Lista mantida pela American Business Magazine Fortune, com as 1000 maiores empresas em relação à capital nos Estados Unidos.

- A perda média de fraudes financeiras subiu de US$ 388.000 em 1998 para mais de US$ 1.400.000 dólares em 1999.
- O total de prejuízos financeiros resultantes de crime de informática para os 521 entrevistados totalizaram mais de US$ 120 milhões.

É importante destacar que a maioria dos crimes informáticos não são relatados. Ao analisar os números que estão sendo relatados nessas pesquisas e extrapola-los a responder por todas as organizações, o número potencial de incidentes e perdas financeiras associadas é incompreensível. Algumas estimativas afirmam que mais de 90% dos crimes relacionados a computadores nem são comunicados às autoridades legais nem processado. As empresas podem deixar-se aberta a processos, acarretando na perda de confiança dos clientes por admitir uma perda de informações.

2.3. CONCEITUAÇÃO DE SEGURANÇA

A necessidade de segurança de rede é uma nova exigência das organizações. Antes da década de 1980 a maioria dos computadores não estavam em rede. Não foi devido à falta de vontade de estabelecer uma rede entre eles, era mais o resultado da falta de tecnologia. A maioria dos sistemas eram mainframes ou sistemas de médio porte que eram centralmente administrados e controlados. Os usuários interagiam com o sistema por meio de terminais “burros”. Os terminais tinham recursos limitados, e necessitavam de uma conexão física com uma porta dedicada. As portas frequentemente eram ligadas em série utilizando o protocolo RS-232. A IBM, Digital Equipment, e outros fabricantes de computadores, desenvolveram variações nesta arquitetura, utilizando servidores de terminal, mas o conceito básico foi o mesmo. Nada equivalente ao que existe hoje, onde milhares, de conexões podem chegar a um sistema em um único circuito de uma única rede.

Na década de 1980, a combinação do desenvolvimento do computador pessoal (PC), o desenvolvimento de padrões de protocolo de rede, a redução no custo do hardware, bem como o desenvolvimento de novas aplicações, fazendo a prática em

redes de computadores, um pouco mais aceitável. Como resultado, LANs, WANs, e a computação distribuída tiveram um enorme crescimento durante este período.

Quando implantado pela primeira vez, as redes LANs foram relativamente seguras, principalmente porque ficavam isoladas fisicamente. Não estando ligado a WANs, por isto a sua natureza independente protegia os recursos da rede.

Com o desenvolvimento de protocolos, tais como X25 e o (TCP / IP) reduziram o custo para implantar WANs, tornando-os mais atraentes para serem implementados. Estes protocolos permitiram que muitos sistemas compartilhassem circuitos. Muitas pessoas ou organizações poderiam ser interligados através da rede compartilhada. Não era mais necessário conectar sistemas em uma configuração ponto-a-ponto. Vulnerabilidades foram introduzidas com a implantação deste ambiente distribuído, utilizando redes de comutação de pacotes compartilhados empregando protocolos como o TCP / IP e o conceito de sistemas confiáveis.

A internet é o maior e mais conhecido deste tipo de rede. A internet utiliza o protocolo TCP/IP, e foi projetada principalmente para conectar computadores independentemente de seus sistemas operacionais em uma maneira fácil e eficiente. Segurança não fazia parte do projeto inicial do TCP/IP, uma série de ataques aconteceram divulgando que haviam muitos pontos fracos referentes ao seu design. Hoje, a segurança tem que ser mais importante do que a facilidade de acesso.

2.4. SEGURANÇA DA INFORMAÇÃO

A segurança de rede está relacionada, acima de tudo, com a segurança do patrimônio informacional da empresa. Muitas vezes perde-se de vista o fato de que esta informação é a informação que a empresa está tentando proteger, e não a segurança de redes e computadores. Uma definição simples para segurança da informação é que esta seria uma junção de alguns fatores tais como: confidencialidade, integridade, disponibilidade e autenticação.

Não pode haver segurança da informação, sem sigilo, o que garante que usuários não autorizados não interceptam, copiem ou reproduzam informações. Ao mesmo

tempo, a integridade é necessária para que as organizações tenham total confiança na informação para atuar sobre ela. Além disso, a segurança da informação exige que as organizações sejam capazes de recuperar dados, as medidas de segurança são inúteis se as organizações não podem ter acesso à informação vital que eles precisam para operar quando eles necessitam. Finalmente, a informação não é segura sem a autenticação que determina se o usuário final está autorizado a ter acesso.

Entre os muitos elementos da segurança da informação, estão garantidos a segurança física adequada, contratação de pessoal qualificado, o desenvolvimento e uso de procedimentos e políticas, fortalecimento e monitoramento de redes e sistemas, e o desenvolvimento de aplicações seguras. É importante lembrar que a segurança da informação não é apenas sobre a proteção do patrimônio de hackers externos. A maioria das ameaças são internas a uma organização.

A segurança da informação também trata sobre procedimentos e políticas que protegem as informações de acidentes, incompetência, e desastres naturais. Tais políticas e procedimentos devem abordar o seguinte:

• Backups, controles de configuração e controles de mídia;
• A recuperação de desastres e planos de contingência;
• A integridade dos dados.

Também é importante lembrar que a rede de segurança não é absoluta. Toda a segurança é relativa, ou seja, a segurança deve ser relacionada como um espectro que vai do muito inseguro para o muito seguro. O nível de segurança para um sistema ou rede é dependente de onde ele cair ao longo do espectro, em relação a outros sistemas. É tão seguro quanto aos outros sistemas relativos. Não existe um sistema ou rede absolutamente seguro.

A segurança de rede é um ato de equilíbrio que exige a implantação de “defesas proporcionais”. As defesas que são implantadas ou implementadas devem ser proporcionais à ameaça. Organizações determinam o que é apropriado em diversas maneiras, que seguem abaixo:

• Equilibrar o custo de garantia contra o valor do patrimônio que está sendo protegido;
• Equilibrar o provável contra o possível;
• Equilibrar as necessidades de negócios contra as necessidades de segurança.

As organizações devem determinar o quanto custaria para cada sistema ou rede comprometida, em outras palavras, quanto custaria perder informações em acesso ao sistema, ou experimentar o roubo de informações. Ao atribuir valor monetário para o custo de ter um sistema ou rede comprometida, as organizações podem determinar o limite que estão dispostos à gastar para proteger seus dados. Para muitas das organizações, este exercício não é necessário, porque os sistemas são a alma do negócio, sem eles, não há nenhuma organização.

Deve haver também, o equilíbrio com o custo de segurança. Geralmente, com o investimento em aumento de segurança, as perdas esperadas devem diminuir. As empresas não devem investir mais em segurança do que o valor do patrimônio informacional que estão protegendo. Este é o ponto onde a análise do custo benefício entra em jogo.

Também deve-se equilibrar as necessidades de negócio com a necessidade de segurança, avaliando o impacto operacional de implementação de medidas de segurança. Sempre que possível, as medidas de segurança devem complementar as necessidades operacionais e de negócios de uma organização.

2.5. AVALIAÇÃO DE RISCOS

O Conceito de avaliação de risco é fundamental para o desenvolvimento de defesas proporcionais. Para realizar uma análise de risco, as organizações precisam entender as possíveis ameaças e vulnerabilidades. Risco é a probabilidade de que uma vulnerabilidade seja explorada. Os passos básicos para a avaliação de risco são listados a seguir:

1. Identificação e priorização do patrimônio;
2. Identificação de vulnerabilidades;
3. Identificação de ameaças e suas probabilidades;
4. Identificar contramedidas;
5. O desenvolvimento de uma análise custo-benefício;
6. Desenvolvimento de políticas e procedimentos de segurança.

Para identificar e priorizar o patrimônio de informação e desenvolver uma análise custo-benefício, é útil realizar um questionamento simples, com as perguntas que seguem:

- O que você quer para proteger?
- Por que você quer protegê-lo?
- Qual é o seu valor?
- Quais são as ameaças?
- Quais são os riscos?
- Quais são as consequências de sua perda?
- Quais são os diferentes cenários?
- Qual será o custo da perda de informações ou do sistema?

Para priorizar o patrimônio e o sistema, é necessário atribuir valor. Levando em conta todos os custos possíveis que podem ser gastos com a segurança do patrimônio como, por exemplo, a perda de confiança do cliente. É preciso que o administrador de rede ou sistema, elimine as ameaças prováveis do possível, determine as ameaças que são mais prováveis, e desenvolva medidas para proteger contra essas ameaças.

2.6. CONSEQÜÊNCIAS DE INVASÕES

Quando os sistemas sofrem ações por intermédio de “hackers”, “crackers”, e outros elementos do tipo, haverá sempre uma consequência que deve atingir a rede de

computadores. Essas consequências podem ir desde uma simples queda de produtividade para restauração de um serviço, até a provação de reputação e consequente perda de mercado. É interessante notar que os prejuízos dependem do valor da informação, porém, devem ser considerados tanto os valores tangíveis, por exemplo, as horas de recuperação de informações, perdas de venda no período de interrupção ou contratação de consultorias para implementação de segurança; e os valores intangíveis, que por natureza são mais difíceis de serem quantificados e estão relacionados à perda de mercado ou de reputação, e até depredação na marca da empresa.

Dessa forma, as consequências de uma invasão bem-sucedida a uma empresa podem ser variadas, mas são sempre negativas. De acordo com QUEIROZ aput [HORTON & MUGGE, 2003], algumas delas são:

- Monitoramento não autorizado,
- Descoberta e vazamento de informações confidenciais.
- Modificações não autorizadas de servidores e da base de dados da organização.
- Fraude ou perdas financeiras.
- Imagem prejudicada, perda de confiança e reputação.
- Trabalho extra para a recuperação de dados.
- Perda de negócios, clientes e oportunidades.

Um ponto importante depois das invasões é que os invasores tentarão encobrir todos os procedimentos no qual realizaram. Algumas técnicas para isto são bastante conhecidas como (1) a substituição ou remoção de arquivos de logs, (2) troca de arquivos importantes do sistema para o mascaramento de suas atividades ou formatação completa do sistema. Esses procedimentos fazem com que tecnologias como sistemas de detecção de intrusão (Instrusion Detection System, IDS) sejam importantes, bem como planos de resposta a incidentes e a computação forense.

2.7. MODELOS DE SEGURANÇA

Há três abordagens básicas utilizadas para desenvolver um modelo de segurança de rede. Normalmente, as empresas empregam uma combinação das três abordagens para garantir a segurança. As três abordagens são a segurança por obscuridade, o modelo de defesa de perímetro, e a defesa do modelo de profundidade.

2.7.1. Segurança por Obscuridade

A segurança por obscuridade depende do disfarce da rede para a proteção. O conceito por detrás deste modelo é que ninguém saiba que uma rede ou sistema está em determinado lugar. A esperança do administrador de rede, é que quando se oculta uma rede ou pelo não anuncia à sua existência, isto sirva como garantia de segurança. O problema com esta abordagem é que nunca funciona, a longo prazo e uma vez detectada, uma rede é complemente vulnerável.

2.7.2. A Defesa por perímetro

O modelo de defesa por perímetro é análogo a um castelo cercado por um fosso. Ao utilizar este modelo em segurança de redes, as organizações fortalecem seus sistemas e roteadores periféricos, ou uma organização pode “esconder” a sua rede atrás de um firewall que separa a rede protegida por uma rede não confiável. Não é muito utilizado para proteger os outros sistemas da rede. O pressuposto é que as defesas de perímetro são suficientes para impedir intrusos de modo que os sistemas internos estão seguros.

Há várias falhas neste conceito. Em primeiro lugar, este modelo não faz nada para proteger os sistemas internos de um ataque de dentro da empresa. Como já foi discutido, a maioria dos ataques são lançados por alguém de dentro da empresa. Em segundo lugar, a defesa por perímetro eventualmente sempre falha, uma vez adotada, os sistemas internos ficam abertos para ataques.

2.7.3. A Defesa em profundidade

A abordagem mais robusta para uso é o modelo de defesa em profundidade. A defesa em profundidade tem como abordagem em segurança o endurecimento e monitoramento de cada sistema. Medidas adicionais ainda são tomadas em relação aos sistemas periféricos, mas a segurança da rede interna não repousa unicamente sobre os sistemas de perímetro. Esta abordagem é mais difícil de atingir e exige que todos os administradores de redes e sistemas façam a sua parte. Com este modelo, no entanto, há muito menos probabilidade da rede interna ser comprometida se um administrador comete algum erro, sendo assim, este sistema pode ser comprometido, mas os outros sistemas na rede serão capazes de se defender, podendo detectar tentativas de invasão do sistema comprometido.

Este conceito de defesa também proporciona muito mais proteção contra um invasor interno. As atividades deste intruso são mais propensas a serem detectadas.

3. COMPUTAÇÃO FORENSE

A Computação Forense foi criada tendo como objetivo a manipulação das novas formas de evidências eletrônicas, com o intuito de suprir as necessidades das instituições legais e organizações sobre este determinado tema. Segundo (SANTOS aput NOBLETT, 2008), ela é a ciência que estuda a aquisição, preservação, recuperação e análise de dados que estão em formato eletrônico e armazenados em algum tipo de mídia computacional.

Conforme citado por (NOBLETT, 2000), as informações produzidas pela computação forense podem ser decisivas e de sumo valor em um determinado caso.

É importante salientar que estar informações são passiveis de uma validação como em qualquer outro tipo de análise forense, pois é passível dependendo das circunstâncias, que estas informações coletadas tenham sido manipuladas a forma de induzir o perito a tirar conclusões errôneas sobre o caso, dificultando posteriormente uma nova análise de dados.

Como afirma (FARMER, 2000), para desvendar um mistério computacional nem sempre é fácil, fazendo-se uma analogia, deve-se analisar o sistema como um detetive examina a cena de um crime, e não como um usuário comum, ou como uma individuo comum. Muitas das habilidades necessárias para procurar um erro em um determinado código fonte, são também as mesmas habilidades necessárias para uma análise forense, tais como: raciocínio lógico, entendimento das relações de causa e efeitos em sistemas computacionais, ou seja, exemplificando é ter controle e experiência sobre as situações que envolvem a análise forense; e talvez a mais importante de todas, ter uma mente aberta.

Uma perícia em um computador suspeito envolve uma série de conhecimentos técnicos e a utilização de ferramentas coerentes para a análise, além de um alto censo de raciocínio e lógica que é justificado pela necessidade indiscutível de não alterar o sistema que está sendo analisado. Tais alterações, se efetuadas, podem ser traduzidas como alterações nos tempos de acesso aos arquivos, avariando assim uma das mais eficientes maneiras de se reconstituir o que aconteceu na

máquina em um passado não distante. Geralmente as ferramentas comuns não têm a preocupação de manter a integridade dos tempos de acesso.

Os peritos devem tomar o uso de alguns procedimentos para que as evidências de uma perícia não sejam comprometidas ou extraviadas, substituídas ou perdidas, pois assim, a legitimidade e veracidade dessas informações poderão ser contestadas pelos homens de direitos, prejudicando assim o caso.

Para (FREITAS, 2006, p.2):

> "Em muitos casos, as únicas evidências disponíveis são as existentes em formato digital. Isto poderia significar que a capacidade de punição a um invasor pode estar diretamente relacionada com a competência do perito em identificar, preservar, analisar e apresentar as evidências."

Para assegurar a legitimidade das informações diante do tribunal, é fundamental que o profissional em perícia adote uma postura levando como fatores disciplina, organização e sensatez, correspondendo assim às suas responsabilidades.

3.1. VULNERABILIDADES

Antes de discutir assuntos como as evidências digitais é importante dedicar este tópico sobre uma breve explicação sobre as vulnerabilidade presentes em sistemas e redes de computadores e as mais comuns fontes usadas para rastreá-las.

A vulnerabilidade é uma fraqueza inerente ao projeto, configuração e implementação de uma rede ou sistema que se torna suscetível a uma ameaça. A maioria das vulnerabilidades geralmente podem ser rastreadas por uma de três fontes:

- Mal planejamento: Os sistemas de Hardware e software que contém falhas de projeto que podem ser exploradas. Em essência, os sistemas são criados com furos de segurança. Um exemplo deste tipo de vulnerabilidade seriam as falhas no sistema de email padrão do UNIX "*sendmail*". As falhas do *sendmail* permitiam

que hackers obtivessem acesso privilegiado, ou seja, acesso ao *root* para os sistemas UNIX. Estas falhas foram exploradas em várias ocasiões.

- Fraca Implementação: Sistemas que estão configurados incorretamente e, portanto, são vulneráveis a ataques. Este tipo de vulnerabilidade, geralmente resulta da inexperiência, a formação insuficiente, ou mesmo de um trabalho mal feito. Um exemplo deste tipo de vulnerabilidade seria um sistema que não tem privilégios de acesso restrito em arquivos executáveis críticos, permitindo assim que estes arquivos sejam modificados por usuários não autorizados.
- Má Gestão: procedimentos inadequados, e insuficientes verificações e estimativas. As medidas de segurança não podem operar em um vácuo, pois deve-se haver a documentação e monitoramento dos mesmos. Mesmo algo tão simples como o backup diário de um sistema precisa ser verificado. Também precisa ser delimitado a reponsabilidade de algumas funções. Desta forma, uma organização pode garantir que os procedimentos estão sendo seguidos e que nenhuma pessoa tem o controle total de um sistema.

3.2. EVIDÊNCIAS DIGITAIS

Segundo o dicionário Aurélio, uma evidência é tudo aquilo que pode ser utilizado para provar que determinada afirmação é verdadeira ou falsa. Existem vários tipos de evidências, como por exemplo a evidência científica, que unindo os conceitos das palavras pode-se dizer que é o conjunto de elementos capazes de suportar a confirmação ou negação de uma determinada teoria ou hipótese científica. Porém neste item será discutido a Evidência Digital, que tem como conceito, segundo FREITAS (2006), toda a informação armazenada ou transmitida em formatos ou meios digitais, sendo que essa evidência, na maioria dos casos, é frágil e volátil, o que requer a atenção de um especialista com certificação ou bastante experiente, a fim de assegurar que os materiais com valor comprovatório possam ser efetivamente isolados e extraídos de forma correta e licitamente. Estes materiais podem ser expostos em um tribunal de justiça como prova de materialidade de um crime, por exemplo; ou mesmo como parte de um laudo pericial.

Existem vários fatores que auxiliam na busca por uma evidência digital, mas para isso é necessário identificar em qual dispositivo digital está ocorrendo a procura por uma evidência. Com isso, é importante ressaltar o horário, o dia, o local, o nome do responsável pelo computador e outros.

“Diferentes crimes resultam em diferentes tipos de evidências, e, por este motivo, cada caso deve ser tratado de forma especifica” (SANTOS, 2008, p.21 apud FREITAS, 2006).

A evidência digital abrange os periféricos e dispositivos ligados à cena do crime, onde pode-se coletar e averiguar os dados ali contidos seja em um computador ou em um dispositivo móvel. Entretanto, na busca de uma evidência é importante respeitar a autenticidade dos dados, tentando deixá-los exatamente igual ao momento em que foi coletado na cena do crime. Tais fatores auxiliam na documentação da análise forense e geram novas informações na conclusão de uma perícia computacional (LISITA; MOURA; PINTO, 2009).

REIS e GEUS (2002) explicam que o termo evidência digital é associado a toda e qualquer informação digital capaz de determinar que houve uma intrusão ou que forneça alguma ligação entre o delito e as vítimas ou entre o delito e o atacante.

Ainda referenciando o mesmo autor do parágrafo anterior, a evidência digital também é considerada uma grandeza física, composta de campos magnéticos, campos elétricos e pulsos eletrônicos que podem ser coletados e analisados através do uso de ferramentas apropriadas. Entretanto, a evidência digital possui algumas características próprias, como lista REIS e GEUS (2002):

- Ela pode ser duplicada com exatidão, permitindo a preservação dos dados originais durante o processo de análise;
- Valendo-se do uso de métodos e ferramentas apropriadas é relativamente fácil determinar se uma evidência digital foi modificada;
- A evidência digital é extremamente volátil, podendo ser facilmente alterada durante o processo de análise.

Em um sistema computacional pode-se observar alguns dispositivos que são considerados fontes de informações importantes em um processo de busca por evidências. Abaixo encontra-se uma lista com as principais fontes de dados de um sistema computacional e um breve comentário sobre cada uma delas.

- Dispositivos de Armazenamento da Unidade Central de Processamento (CPU)

As informações contidas nas memórias da CPU são impossíveis de serem capturadas, porém são de mínima utilidade. As memórias caches até podem conter informações que ainda não foram utilizadas pela memória principal do sistema, porém essas informações não possuem nenhum valor como prova pericial pelo fato de conter apenas cálculos em linguagem de máquina, que são impossíveis de serem traduzidas em informações com garantia legal perante a justiça.

- Memória de Periféricos

Alguns dispositivos periféricos como, por exemplo, modems, placas de vídeo, aparelhos de fax e impressoras possuem algum dispositivo para armazenamento de suas atividades capazes de serem acessados e salvos, muitas das vezes esses dados consistem em informações que não estão mais presentes no sistema analisado como gravações de voz, documentos e mensagens de texto ou números de telefone e fax.

- Memória Principal do Sistema

Na memória RAM está contido todo tipo de informação volátil como informações de processos que estão em execução, dados que estão sendo manipulados e ainda não foram salvos em disco e informações do sistema operacional, neste último estão inclusos textos plenos que no disco estão codificados.

Outra fonte de evidências dentro da memória principal do sistema pode ser os chamados *crash dump*, que guardam uma imagem da memória enquanto o mesmo

está em execução, servido como uma espécie de “caixa preta” do sistema, para que se houver uma falha, tudo que estava em execução no momento da falha seja recuperado. Os *crash dump* também contém outras informações como o motivo no qual causou a falha, além de outros dados, como senhas, por exemplo.

- Tráfego de Rede

É possível reconstruir a comunicação entre o atacante e a máquina alvo, de modo que uma sequência de eventos pode ser estabelecida e comparada com as outras evidências encontradas na máquina comprometida, este fato torna-se verídico a partir de datagramas[2] de tráfego capturados. Existem várias ferramentas capazes de capturar o tráfego de rede, denominados de *sniffers*, que além de capturar os datagramas que trafegam na rede, podem decodifica-los e exibi-los em um formato mais legível, ou até realizar operações consideradas mais complexas como por exemplo a recuperação de arquivos transferidos pela rede.

- Estado do Sistema Operacional

O estado do sistema operacional e informações relacionadas a ele podem fornecer pistas importantes quanto à existência, tipo e origem de uma ataque em andamento. Tais informações representam uma imagem do sistema operacional em um determinado instante como processos em execução, conexões de rede estabelecidas, usuários autenticados, tabelas e caches[3] mantidas pelo sistema e geralmente são perdidas quando o sistema é desligado.

- Módulos do Kernel

Os módulos do kernel foram criados para que se permitisse adicionar e retirar recursos do sistema no ar, não mais sendo necessário a instalação de um novo kernel e a reinicialização do sistema para tal. Esses módulos podem servir para

[2] **Datagrama**: é uma unidade de transferência básica, associada a uma rede de comutação de pacotes em que a entrega, hora de chegada e a ordem não são garantidos. (KUROSE, 2007).
[3] **Cache**: é um dispositivo de acesso rápido, interno a um sistema, que serve de intermediário entre um gerenciador de processos (processador) e o dispositivo de armazenamento ao qual esse operador acede.

vários propósitos como por exemplo, fornecer recursos para um novo dispositivo, incorporar uma linguagem ao sistema, permitir tratamento de novos tipos de sistemas de arquivos e reescrever as chamadas do sistema operacional, esta última é considerada a principal vantagem promovida pelos módulos do kernel. Porém também pode ser considerada como um problema, pois um sistema uma vez invadido, o invasor pode carregar facilmente um novo módulo do kernel, desta vez malicioso, com o propósito de esconder atividades das ferramentas de prevenção e auditoria do sistema, interceptar comandos do sistema e produzir resultados falsos.

- Dispositivos de Armazenagem Secundária

O disco representa a maior fonte de informações e cada porção dele, por menor que seja, onde possa ler ou escrever um conjunto de bits representa uma possível fonte de informações para análise forense. Algumas áreas do disco não podem ser acessadas por um sistema de arquivos e podem conter informações que um invasor pode manter escondida ou, ainda, vestígios que o mesmo tentou apagá-la. Com esta informação pode-se classificar as informações armazenadas no disco em duas classes: as acessíveis pelo sistema de arquivos (os arquivos propriamente ditos e seus atributos) e as informações armazenadas em áreas não acessíveis através do sistema de arquivos (espaços não alocados ou marcados como danificados, por exemplo).

Além disso, algumas áreas do disco podem conter informações deletadas, pois quando um arquivo é deletado, sua referência é removida, porém os dados contidos no arquivo não são apagados do disco. Tais dados permanecem alocados no disco aguardando serem sobre escritos, por este motivo podem ser recuperados e utilizados em um processo de análise forense.

É importante efetuar uma cópia *bit* a *bit* do disco. Este tipo de cópia é diferente de uma cópia normal de arquivos, pois todo o conteúdo do disco será copiado, inclusive os espaços não utilizados.

3.3. ETAPAS DE UMA INVESTIGAÇÃO

REIS e GEUS (2002) afirmam que para se transformar dados extraídos de dispositivos de armazenamentos computacionais em provas concretas e utilizáveis em um processo de investigação, é necessário que o perito tenha muito cuidado na manipulação dos dados e haja num nível máximo de sistematização possível. Por isso é extremamente recomendado seguir alguns procedimentos antes de começar a investigação para que este processo se inicie mantendo a integridade, tanto dos dados como do local da investigação.

- O perito deve limpar todas as suas mídias para garantir que estas sejam executadas sem qualquer limitação.
- Certificar-se de todas as ferramentas (*Softwares*) que serão utilizadas estão devidamente licenciados e pontos para uso.
- Verificar se todos os equipamentos e materiais necessários estão à disposição.
- Ao chegar ao local da investigação, o perito deve providenciar que nada seja tocado sem seu consentimento, com o objetivo de preservar a integridade dos dados e do local da investigação. Este processo chama-se manter a idoneidade do local.

- Os investigadores devem filmar ou fotografar o ambiente e registrar todos os detalhes sobre o equipamento investigado, como marca, modelo, números de série, componentes internos e externos, periféricos, etc.
- Manter a cadeia de custódia.

NEUKAMP (2007) diz que após o seguimento rigoroso dos procedimentos descritos acima, pode-se então dar andamento à investigação criminal, que por sua vez, é dividida em algumas etapas primordiais para o sucesso da investigação. A Figura 1 reflete muito claramente quais são essas etapas, a ordem que elas seguem e o propósito sugerido por ela.

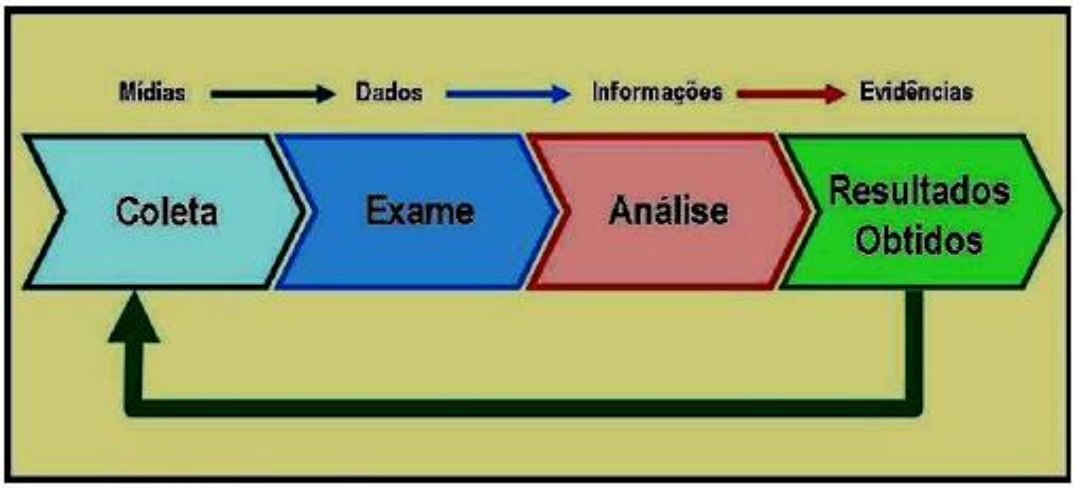

Figura 1. Fases de uma investigação Criminal.
Fonte: RAMOS, SATUNINO e FERREIRA (2007, p.18)

Vale ressaltar que as fases ilustradas na Figura 1 não são apenas de investigações de crimes computacionais, mas também de qualquer outro tipo de investigação, elas apenas foram adaptadas à Computação Forense.

3.4. CADEIA DE CUSTÓDIA

Antes de implementar qualquer processo em meio computacional, é importante pensar sobre documentação. Quando ocorre a realização de uma análise forense não é diferente. Torna-se importante antes de toda análise manter um registro de caso, documentando a história cronológica da evidência, a fim de rastrear a posse e o manuseio da amostra a partir da coleta, do transporte, do recebimento, da análise e do armazenamento, descrevendo assim toda a sequência de posse.

Utiliza-se no processo de investigação forense um documento em forma de formulário e bem semelhante à um laudo pericial denominado “Cadeia de Custódia” que exerce como função tal qual como o laudo, detalhando todos os procedimentos da análise, afim de produzir um documento técnico com teor irrefutável, que se torne prova real para garantir a idoneidade do caminho no qual a amostra percorreu.

Segundo (CHASIN 2001), a “Cadeia de Custódia” se divide em externa e interna: a fase externa seria o transporte do local de coleta até a chegada ao laboratório. A interna, refere-se ao procedimento interno no laboratório, até o descarte das amostras.

Como a “Cadeia de custódia” é usada para registrar as informações do local de coleta, de laboratório e das pessoas que manusearam as evidências, pressupõe-se um trabalho de equipe que envolva todos os profissionais internos e externos do laboratório de análises forenses, englobando os responsáveis pela coleta, recebimento, análise e disposição final da amostra que deverão desenvolver suas atividades conforme um programa previamente estabelecido e acordado pela instituição, com conscientização e treinamento sobre as suas respectivas responsabilidades.

A Figura 2 apresenta um exemplo de formulário preenchido, usando dados aleatórios e irrisórios.

EVIDÊNCIA ELETRÔNICA

FORMULÁRIO DE CADEIA DE CUSTÓDIA

Caso Num.: 144 **Pag.: 1** **De: 2**

MÍDIA ELETRÔNICA/DETALHES EQUIPAMENTO

Item:	Descrição:		
1	Hard Disk 500 GB		
Fabricante:	Modelo:	Num. de serie:	
WESTERN DIGITAL	HTR-500	1	

DETALHES SOBRE A IMAGEM DOS DADOS

Data/Hora:	Criada por:	Método usado:	Nome da Imagem:	Partes:
13/4/13 13:00	Denis M. Ladeira	AIR 2.0.0	image_hd.dd	1
Drive:	HASH:			
Disco Completo	4e3w1g5e5427953d7yda3ddc90213of2vg			

CADEIA DE CUSTÓDIA

Destino:	Data/Hora:	Origem:	Destino	Motivo:
001 - Encaminhado para coleta de Dados	Data: 13/04/2013 Hora: 12:00	Nome/Org.: SIGILO Assinatura:	Nome/Org.: LAB. PERICIAL Assinatura:	Denuncia de Estelionato
	Data: Hora:	Nome/Org.: Assinatura:	Nome/Org.: Assinatura:	
	Data: Hora:	Nome/Org.: Assinatura:	Nome/Org.: Assinatura:	
	Data: Hora:	Nome/Org.: Assinatura:	Nome/Org.: Assinatura:	

Figura 2. Cadeia de Custódia.

4. ESTUDO DE CASO: FERRAMENTAS FORENSES

Este capitulo tem como intuito realizar uma pesquisa e demonstração de ferramentas que auxiliam no trabalho do professional perito na área de análise forense. A utilização de ferramentas é fundamental para a realização de qualquer fase do processo de análise forense, desde a coleta dos dados, até o exame e análise das informações coletadas.

É de suma importância que estas ferramentas apresentem um alto nível de qualidade, oferecendo primeiramente atributos funcionais e de segurança, que cooperem para o decorrer da análise e dos resultados obtidos com a mesma.

Para este estudo de caso, serão utilizadas duas principais plataformas, o FDTK (*Forense Digital ToolKit*) e o CAINE (*Computer Aided Investigative Environment*), que são baseadas no ambiente operacional Linux e são utilizadas primordialmente em caráter de peritos forense, pois possuem uma gama de ferramentas forenses, apresentadas de maneira organizada para auxiliar o usuário.

A finalidade deste estudo é a realização de uma comparação entre estas duas plataformas, afim de determinar em qual meio a plataforma melhor se adequa, por exemplo, uso profissional ou para estudo. Apesar das duas apresentarem características semelhantes, cada uma possui um perfil especifico, que condiz a qual fim cada plataforma foi construída, sendo assim, não é de interesse no estudo determinar qual a melhor entre as duas.

Além deste estudo, este capítulo oferece um tópico relacionado sobre ferramentas específicas voltadas para o uso de usuários comuns de computadores, mantendo o foco em criptografia de dados, objeto de estudo importante para a segurança de dados computacionais.

4.2. FDTK

O FDTK (*Forense Digital Toolkit*) é uma distribuição do Sistema Linux, criada a partir da já consagrada distribuição Ubuntu, reunindo mais de 100 ferramentas capazes de atender à todas as fases do processo de uma investigação em Forense Computacional, oferecendo a oportunidade de ser utilizada como Live CD, ou seja, não é necessário ser instalado no disco rígido, basta usar o driver de CD e executar com o auxílio da memória RAM; ou também pode ser instalado em um equipamento, transformando-o em uma estação forense. Essa distribuição está em contínuo desenvolvimento e caracteriza-se não apenas pelo número de ferramentas, mas também por uma interface amigável e organizada, estruturada conforme as etapas do processo de perícia, contando ainda como sendo uma distribuição no idioma português.

O FDTK é uma distribuição brasileira do Linux, criada à partir de um trabalho de conclusão na Universidade do Vale do Rio dos Sinos (Unisinos), pelo pesquisador Paulo Alberto Neukamp no ano de 2007 em sua primeira versão de número 1.0, apresentado no canal Linux, obteve um expressivo sucesso tendo 7.000 (sete mil) *downloads* efetuados em apenas quinze dias.

Atualmente o projeto do FDTK encontra-se na versão 3.0, tendo como pretensões para a próxima versão aumentar o número de ferramentas forenses, determinando como foco o surgimento de ferramentas para auditoria de redes, forense mobile e ferramentas compatíveis com a plataforma Windows.

4.2.1. Lista de Ferramentas – FDTK

O FDTK oferece uma série de ferramentas para os processos de análise forense, tais como coleta e exame de dados e análise de evidências obtidas, além de um modelo para preenchimento da Cadeia de Custódia.

As ferramentas de são organizadas no FDTK de maneira estruturada, separando-se as ferramentas conforme a etapa de análise na qual a mesma melhor se adeque, e suas respectivas funções no processo.

A Figura 3 ilustra a tela inicial do FDTK, evidenciando o menu de aplicativos composto por ferramentas forense:

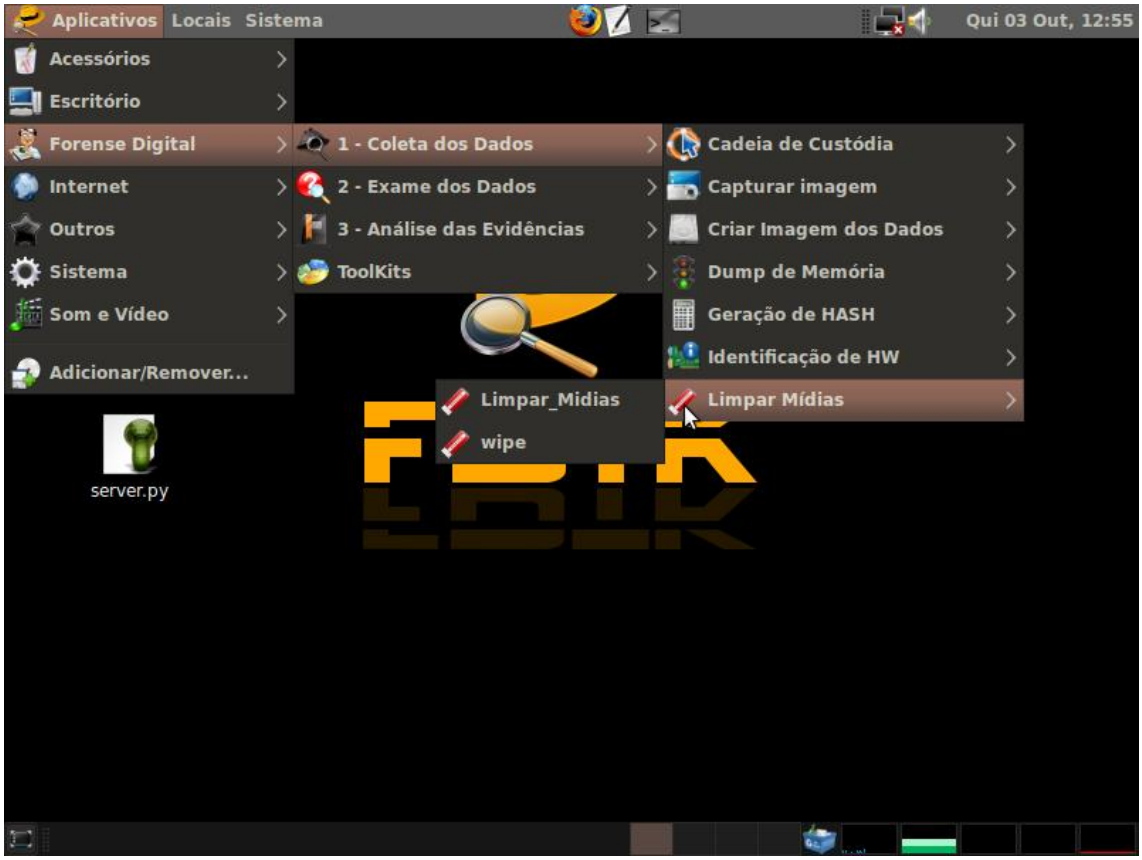

Figura 3. Tela Inicial FDTK.

Todas as aplicações que compõem o FDTK são de origem *Open-Source*, compartilhando o mesmo conceito de Software Livre da mesma maneira que a distribuição. Estas ferramentas são relacionadas adiante contendo uma breve descrição sobre sua função.

- Coleta de Dados:

- Formulário : Formulário de Cadeia de Custódia
- gnome-screenshot: Salvar imagens da àrea de trabalho ou de janelas individuais

- aimage: Geração de imagem dos dados das mídias utilizando o padrão aff
- air: Interface gráfica para dd/dcfldd, para criar facilmente imagens forense
- dc3ddgui: Interface gráfica para O DC3DD, para criar imagens forense
- dcfldd: Versão aprimorada pelo DOD-Departament of Defense do dd
- dd: Ferramenta para geração de imagem dos dados
- ddrescue: Recuperar dados de hds com setores defeituosos (bad blocks)
- mondoarquive: Copiar dados de fitas, cd's, nsf ou hd's
- mondorestore: Restaurar dados de fitas, cd's, nsf ou hd's
- rdd: Versão mais robusta do dd
- rddi: Prompt interativo do rdd
- sdd: Versão da ferramenta dd para Fitas (DAT, DLT...)
- memdump: Dumper de memória para sistemas UNIX-like
- md5sum: Gerar hash md5
- sha1sum: Gera hash sha 160bits
- discover: Informações sobre Hardware
- hardinfo: Informações e Testes do Sistema
- lshw-gráfico: Lista os dispositivos de hardware em formato HTML
- sysinfo: Mostra informações do computador e do sistema
- wipe: Remover totalmente os dados das Mídias

- Exame dos Dados

- cabextract: Acessar conteúdo de arquivos .cab
- orange: Ferramenta para manipular arquivos .cab
- p7zip: Acessar arquivos zip
- unace: Ferramenta para descompactar extensões .ace
- unrar-free: Ferramenta para descompactar arquivos rar
- unshield: Ferramenta para descompactar arquivos CAB da MS
- xarchiver: Criar, modificar e visualizar arquivos compactados
- zoo: Acessar arquivos compactados .zoo
- dcraw: Acessar imagens cruas de câmeras digitais
- exif: Ler informações EXIF de arquivos jpeg

- exifprobe: Exame do conteúdo e da estrutura dos arquivos de imagens JPEG e TIFF
- 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: Visualizar arquivos em formato HEX
- hexcat: Visualizar 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: Ferramenta para 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

- ToolKits

- autopsy: Ferramenta browser para realizar Perícias Forenses.

4.2.2. Procedimento FDTK

Demonstrar alguns procedimentos da análise forense computacional utilizando ferramentas contidas no FDTK, trará de forma prática como um perito deve se portar quanto à posse de dados computacionais coletados à partir de uma determinada cena.

Primeiramente o perito deve ter em mente, a necessidade de manter as propriedades e o estado original dos matérias coletados, não alterando-o em qualquer hipótese, mantendo assim a legitimidade e posteriormente a veracidade das evidências extraídas à partir dos dados.

O FDTK, permite que seja feita a extração da imagem, ou seja, a cópia de um dispositivo para o exame os dados sem ao menos montar o dispositivo, e após todo o procedimento comparar por meio do conceito de *Hash*, se a imagem do dispositivo original é idêntica a imagem gerada com base no mesmo.

Primeiramente, deve ser executado o Editor de configuração, ou tela de preferências, pressionando as teclas Alt+F2, e digitando o texto contido na Figura 4:

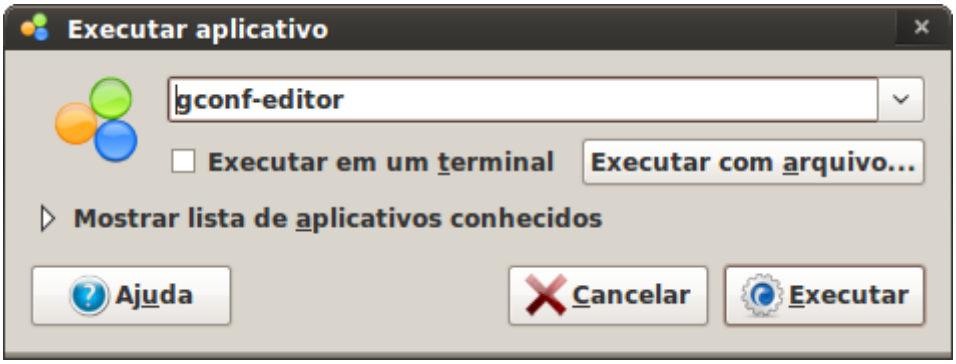

Figura 4: Executar aplicativo Linux.

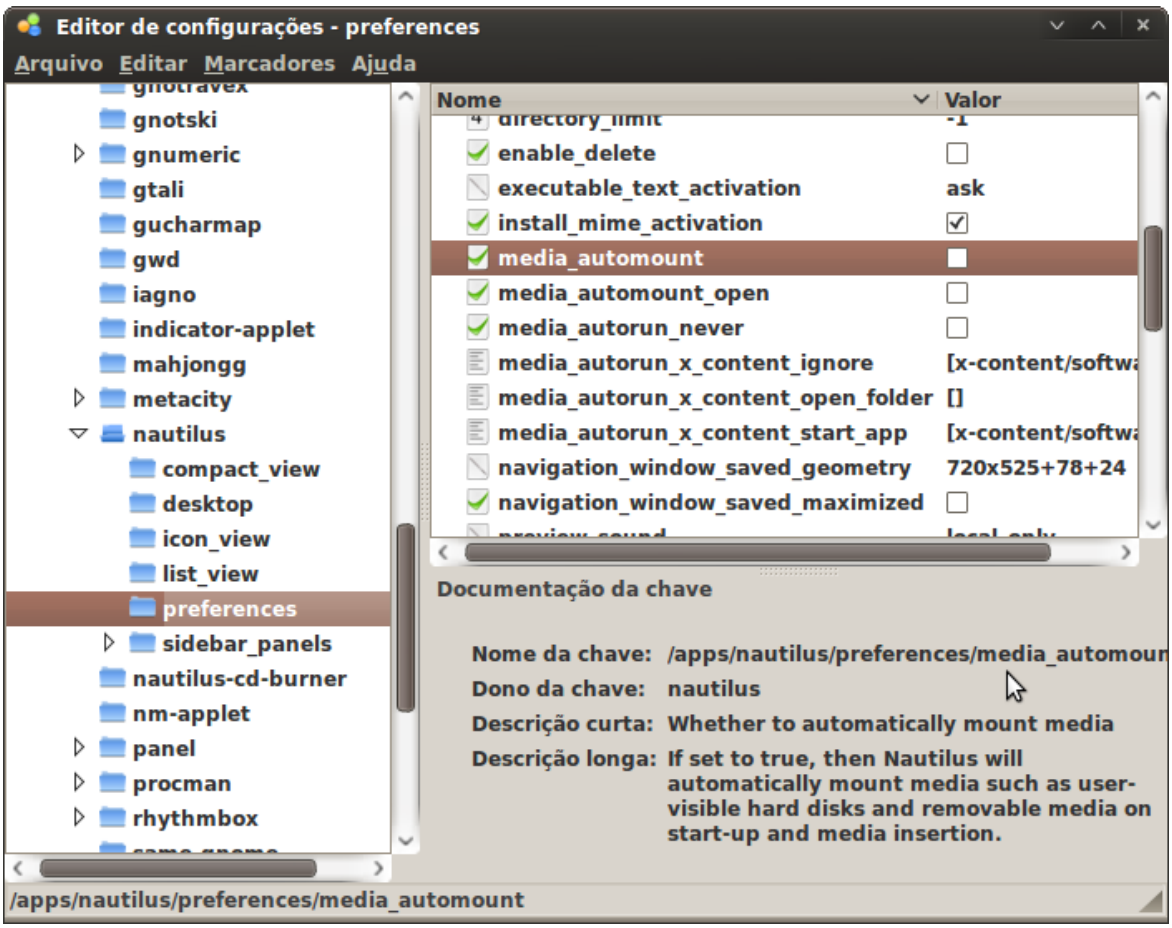

Figura 5: Editor de Configurações FDTK.

Para desativar a opção da montagem automática de dispositivos, deve-se acessar o seguinte caminho ilustrado na figura 5.

- apps → nautilus → preferences

A desmarcação das opções *media_automount* e *media_automount_open*, faz com que todos os dispositivos conectados a partir deste momento, não serão montados, sendo assim, não será possível ter acesso aos dados diretamente pelo dispositivo original.

Agora, será demonstrado uma maneira de extrair a imagem do dispositivo, e apresentar uma maneira de demonstrar as suas similaridades, ou seja, que ambos são idênticos.

Primeiramente, é necessário identificar o tamanho do bloco para os dispositivos no qual a imagem será coletada e copiada. Segue os comandos utilizados para a demonstração abaixo.

- Origem: fdisk -l /dev/sda
- Destino: fdisk -l /dev/sdb1

É utilizado para a geração da imagem de dados, o comando *dd*.

- dd id=/dev/sdb1 of=/media/disk-1/image/imagem_pendrive/image/image_pendrive.dd bs=512k

Onde:
if - é o caminho de origem;
of - o caminho de destino, acrescido do nome e extensão *dd* para a imagem gerada;
bs - o tamanho do bloco de ambos.

As figuras 6 e 7, ilustram a utilização dos comandos, por meio do terminal do FDTK:

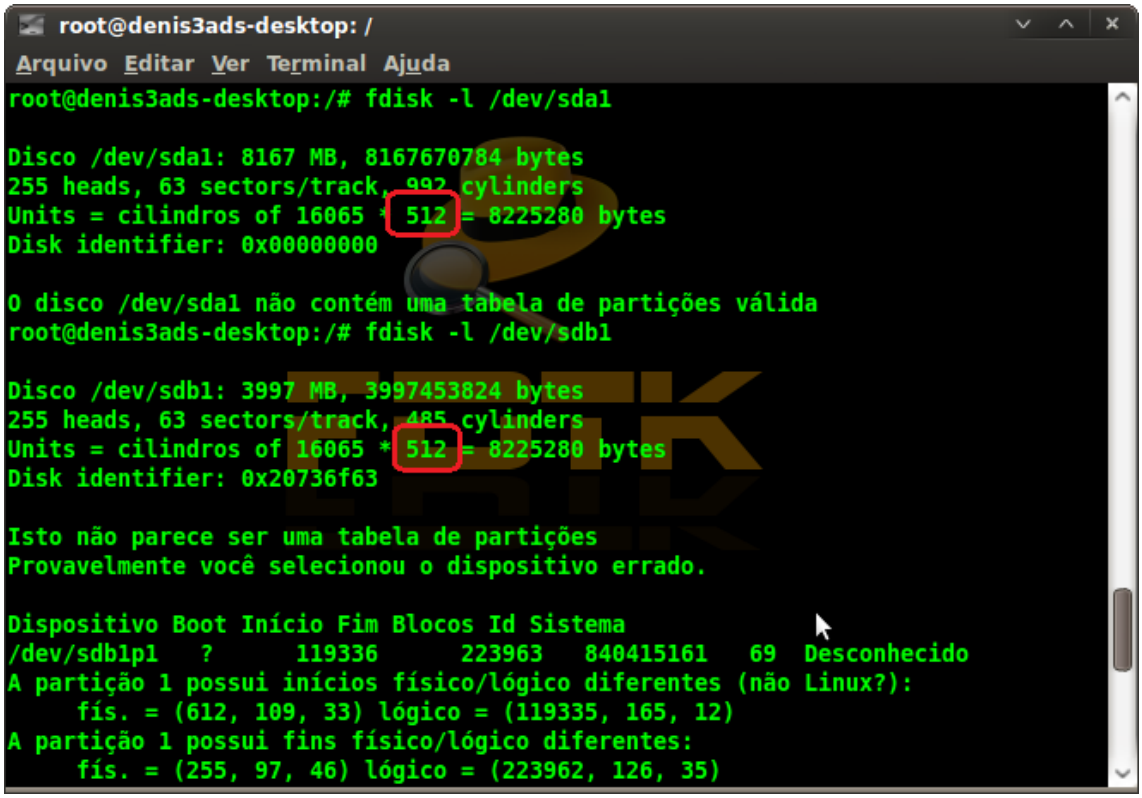

Figura 6: Verificando o tamanho do bloco.

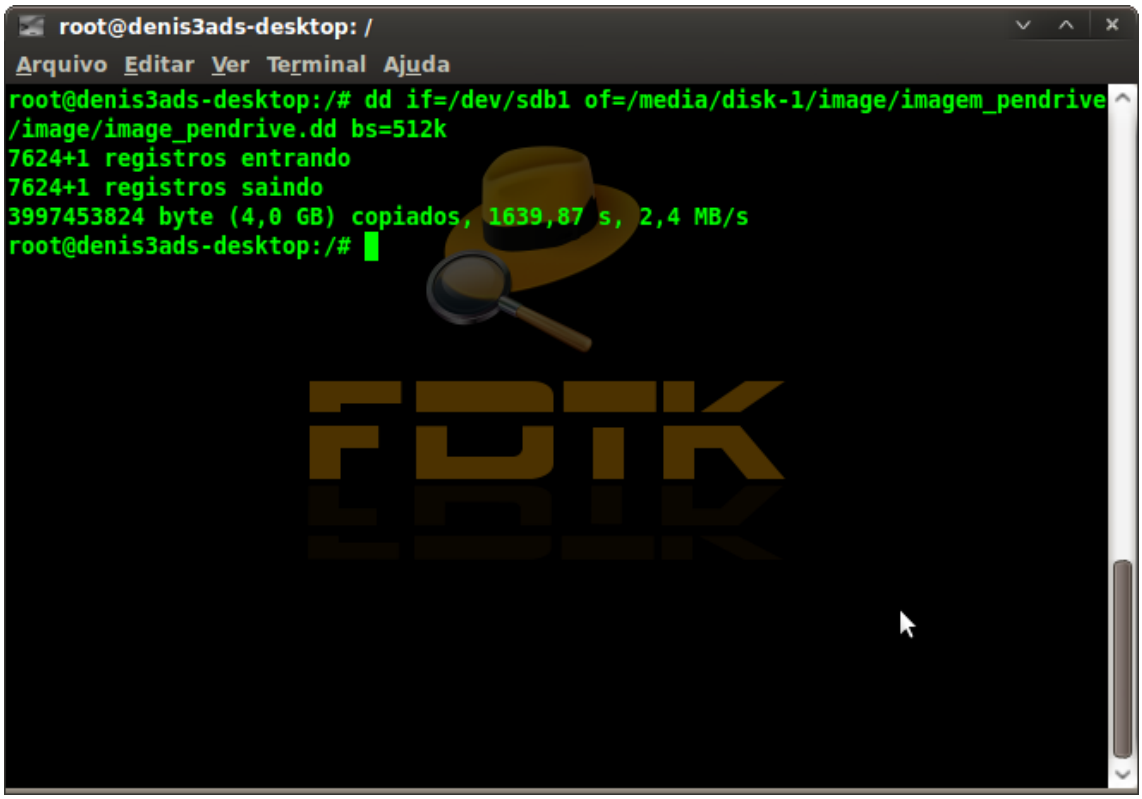

Figura 7: Geração da Imagem.

Também pode ser utilizado a ferramenta AIR para geração de imagem, esta no caso provê uma interface gráfica, possuindo uma maior praticidade para novos estudantes, porém, com uma performance menor que o próprio comando dd.

Além de sua principal função, o AIR oferece a verificação das imagens por meio da verificação por *hash*, utilizando dois métodos para tal tarefa, o md5sum e/ou sha1sum. A Figura 8 serve para exemplificar o AIR.

Hash nada mais é que uma sequência em bits gerada por um algoritmo de dispersão, geralmente representada em base hexadecimal, utilizada para identificar um arquivo ou informação unicamente. (SANTOS, 2008)

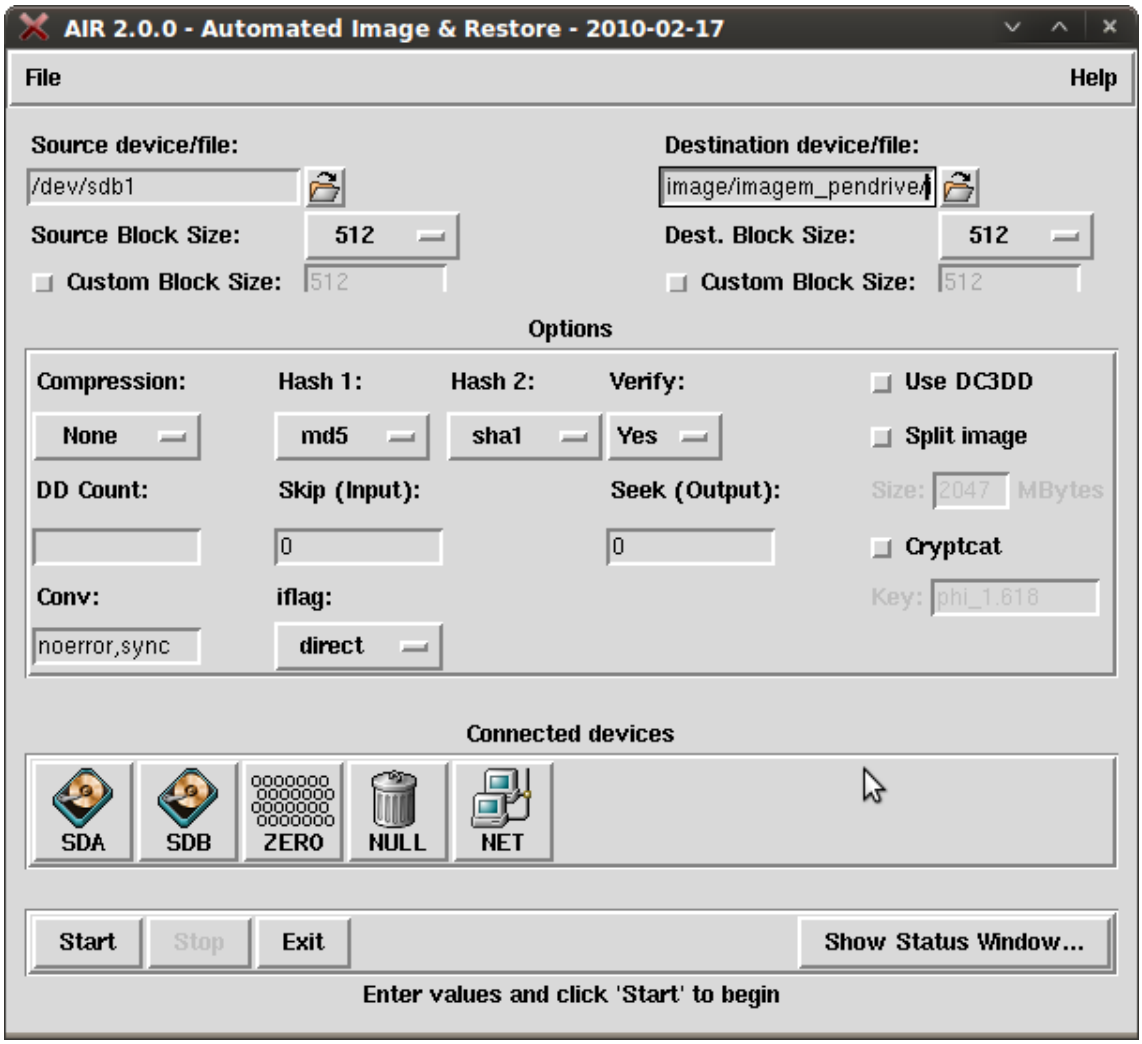

Figura 8: AIR - Geração de dados.

Após realização do procedimento acima, é utilizado o Hash para verificar que os dois arquivos são estritamente iguais, ou seja possuem o mesmo conteúdo e tamanho.

Abaixo encontra-se o comando md5sum, utilizado para realização da tarefa:

- md5sum /dev/sdb1
- md5sum /media/disk-1/image/imagem_pendrive/image/image_pendrive.dd

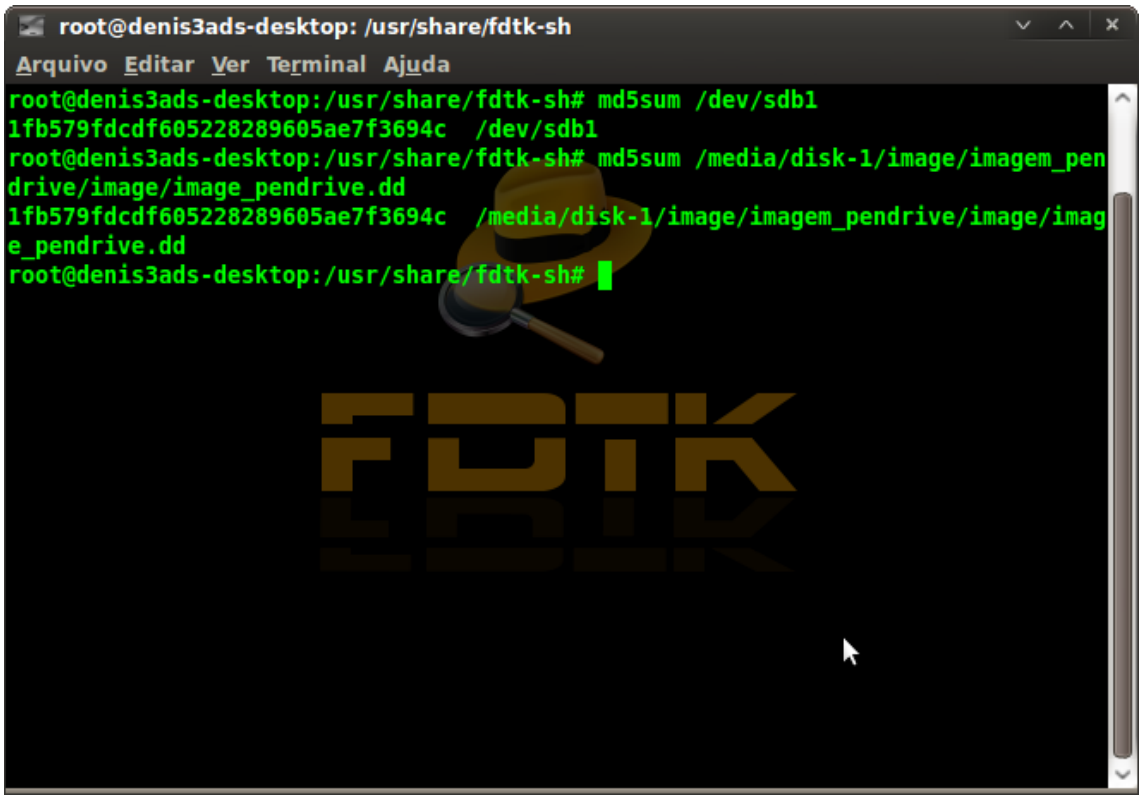

Figura 9: Utilização do Hash.

Analisando a Figura 9, verifica-se que o dispositivo e imagem possuem exatamente o mesmo número de *hash*, caracterizando-se similaridade em ambos, servindo assim, de instrumento importante para garantir que em nenhum momento os dados originais foram modificados.

Para montar a imagem, simplesmente utiliza-se o comando:

- mount -o loop /media/disk-1/image/imagem_pendrive/image/image_pendrive.dd /mnt/pendrive

Onde:

-o loop: caracteriza-se à utilização de *loopback*, um meio que torna possível montar um arquivo como se fosse um dispositivo, seguido do caminho no qual a imagem está armazenada, e o caminho no qual será montada, como apresenta a Figura 10:

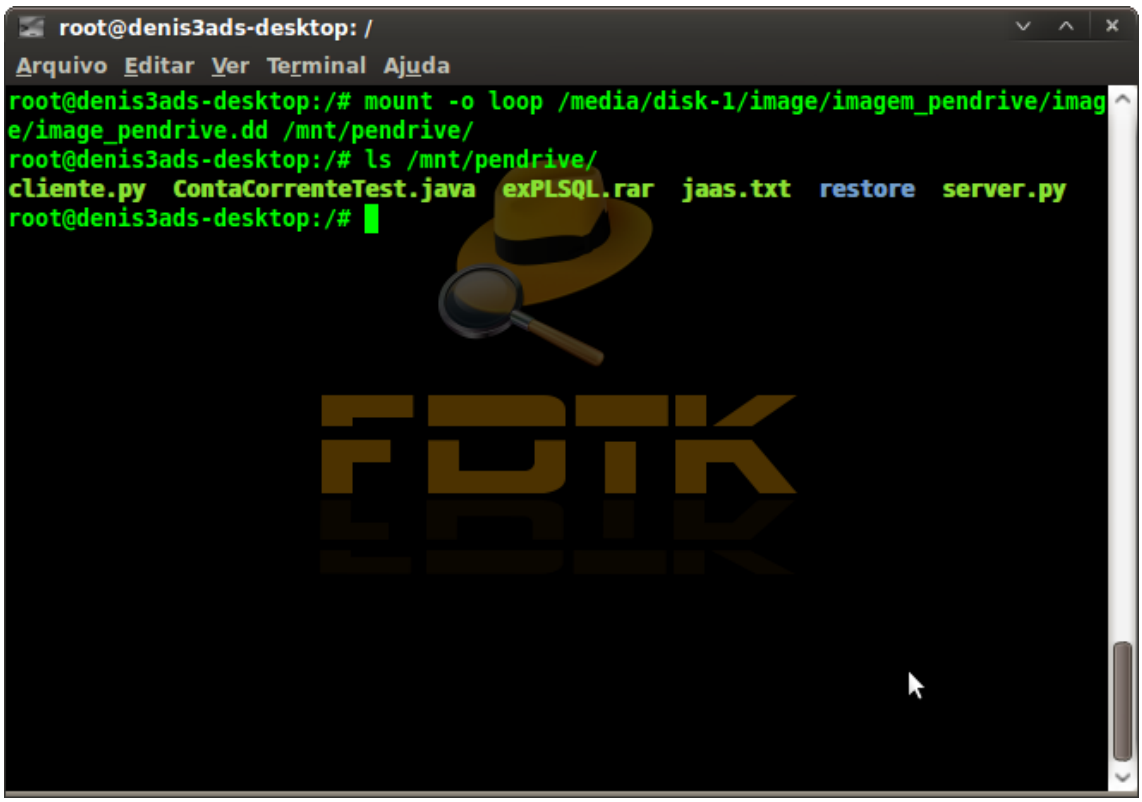

Figura 10: Montagem de Imagem no Linux.

Realizado o procedimento de coleta de dados, pode-se realizar o exame dos dados e evidências. As ferramentas se expandem exponencialmente na análises de dados, por exemplo, vamos supor que exista um arquivo protegido com senha, e necessita-se o acesso ao seu conteúdo. Abaixo conta uma demonstração do comando fcrackzip, destinado à quebra de senha de arquivos zipados (.zip), assim como a Figura 11 ilustra sua utilização.

- fcrackzip -b -l 2-3 -c 1 -u /home/denis3ads/Desktop/hereIAm.zip

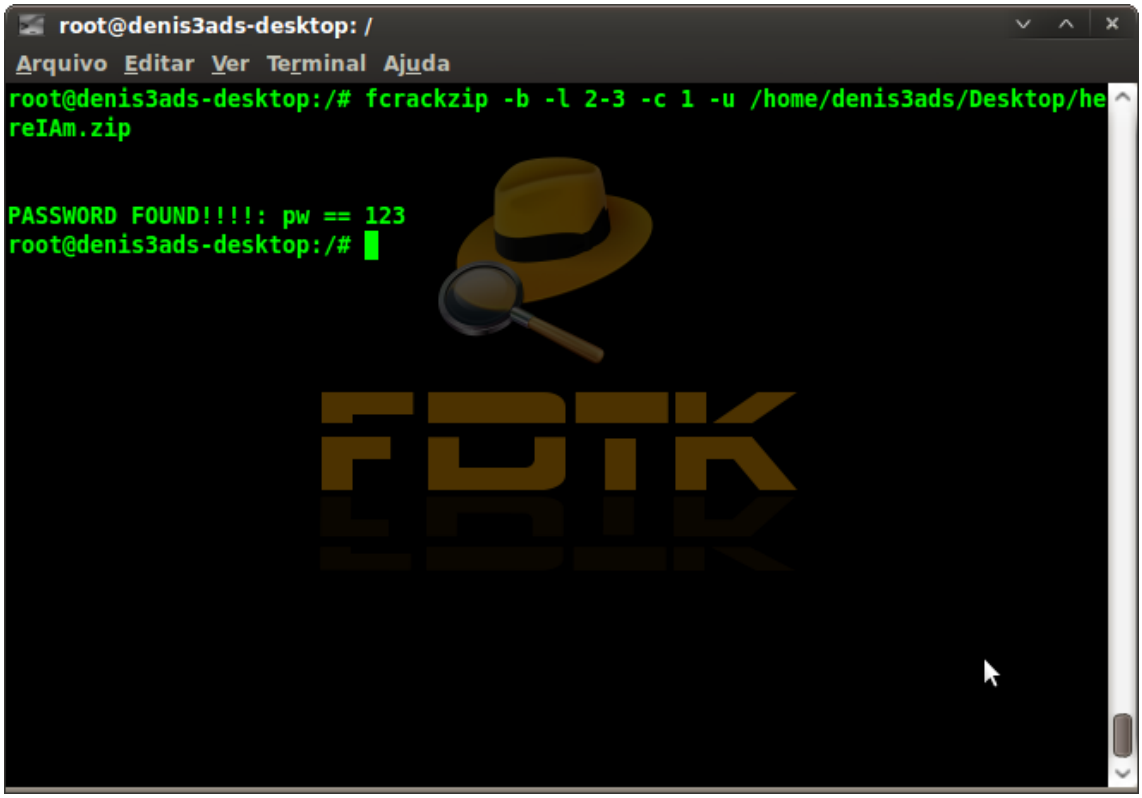

Figura 11: Comando fcrackzip.

Onde:

-l: É o tamanho estimado da senha. (Entre 2 e 3)

-c: Caracteres que serão utilizados, por exemplo -c aA1, neste caso serão utilizados caracteres alfanuméricos minúsculos e maiúsculos de A à Z, e caracteres numéricos.

-b: Usar força bruta para quebra de dados.

-u: Orienta ao comando testar a senha antes de afirmar que a mesma é a correta.

A melhor forma de adquirir conhecimento é fazer uso das ferramentas como forma de praticar, tendo em mente que o mais importante é obter maturidade no processo de perícia forense, torna-se importante tal conhecimento quando almeja-se ser um profissional da área.

4.3. CAINE

O CAINE (*Computer Aided Investigative Environment*) da mesma forma que o FDTK, foi baseado na plataforma Ubuntu, criado basicamente para atender a demanda na área da perícia forense. O projeto inicial do CAINE foi concebido na Itália no ano de 2008, pelo italiano Giancarlo Giustinipara, no qual foi apresentado na Universidade de Modena, região norte da Itália, o projeto encontra-se atualmente em sua versão 4.0, e até hoje é apoiado pela própria Universidade. A figura 12 apresenta a tela de boas-vindas do sistema. Atualmente o líder do projeto é Nanni Bassetti.

O CAINE tem uma interface bastante intuitiva para o usuário, pois oferece um menu de suas principais ferramentas para o ambiente forense. Inicialmente, em versões anteriores, o CAINE vinha com o teclado no padrão italiano porém nessa nova versão existe um aplicativo somente para configuração do layout do teclado, podendo o usuário por exemplo, escolher a configuração em português do Brasil (pt). As ferramentas Windows do CAINE, assim como as outras ferramentas contidas no *LiveCD*, são *Open Source* fazendo com que o usuário possa verificar seu código e alterá-lo se necessário.

De acordo com informações retiradas do página oficial do CAINE, seus principais objetivos são os seguintes:

- Um ambiente operacional no qual auxilia o investigador digital durante as quatro fases da investigação digital;
- Uma interface gráfica amigável;
- Uma compilação semiautomática do relatório final.

Desta forma, interpretando os objetivos acima, obtém-se de forma bem simples, o resultado de várias investigações de uma forma organizada.

O CAINE possui cerca de 80 (oitenta) ferramentas voltadas à Forense Computacional, e também ferramentas do pacote Libre Office, trazidas do Ubuntu, o que era uma deficiência na versão anterior. O CAINE é um dos únicos *LiveCD* que

pode ser instalado no computador caso o usuário queira tê-lo como Sistema Operacional em seu computador.

O suporte em português para o CAINE, surgiu de um trabalho idealizado pelo pesquisador brasileiro Tony Rodrigues, conhecido perito e pesquisador da área de Forense Computacional.

Figura 12: Tela Inicial CAINE

A configuração para o Layout do teclado, é efetuada como consta na Figura 13. Na área de trabalho do sistema, contamos com o aplicativo *ChangeKeybordLayout*, usado para tal tarefa, seu parâmetro de execução é o código de configuração para à localização.

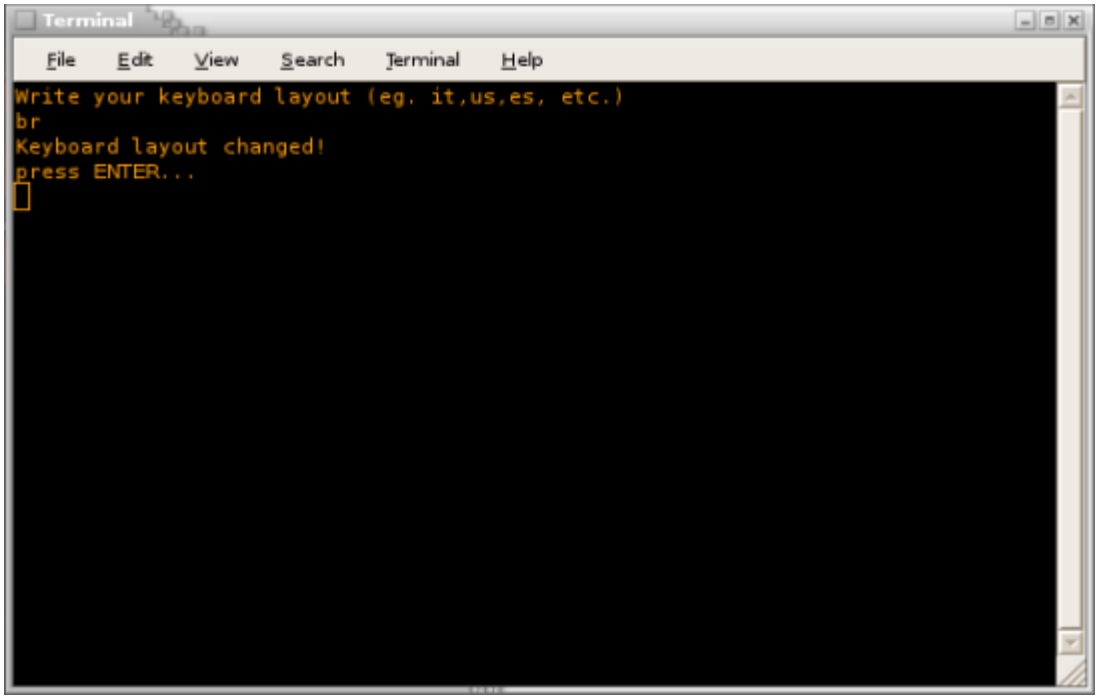

Figura 13: Configurar teclado - CAINE

4.3.1. Ferramentas CAINE

Assim como no FDTK, todas as ferramentas do CAINE são Open Source, inclusive as voltadas para Windows e dispositivos móveis.

As primeiras versões do CAINE apresentam muitas ferramentas também contidas no FDTK, como é o caso do AIR, gerador de imagem com opção de Hash provido de uma interface gráfica, e tantas outras ferramentas na qual são executadas no próprio terminal Linux.

Assim esclarecido, abaixo consta as ferramentas adicionadas ao CAINE a partir de sua terceira versão, descritas com um breve trecho explicando sua principal função. Qualquer ferramentas não listada abaixo utilizada na demonstração, será documentada no próprio procedimento.

- Adicionadas ao CAINE 4.0

- LibreOffice 4.0.1: Pacote office das distribuições Ubuntu
- sqliteman: Administrador de Banco de dados SQL Lite3

- sdparm: Utilidade para o acesso dos parâmetros de dispositivos SCSI
- remote Filesystem Mounter: Montador de imagens para dispositivos remotos
- netdiscover: Scanner de redes *wireless*.

- Adicionadas ao Caine 3.0

- iphonebackupanalyzer: Analisador e recuperador de dados para iOS
- exiftool phil Harvey: Ferramenta para leitura e edição de metadados, informações que complementam e resumem arquivos
- tcpflow: programa que captura dados transmitidos como parte de conexões TCP (fluxos)
- tshark: Analisador de protocolo de rede
- john: Auditor de senhas
- wireshark: Analisador de tráfego de rede
- Firefox: Browser de Internet
- vinetto: Examinador de arquivos Thumbs.db
- mdbtool: Documentador de arquivos MDB, formato usado pela Microsoft para o pacote do banco Access
- gdisk: Criação e manipulação de tabelas de partições
- LVM2: Gerenciador de volumes lógicos
- tcpdump: Administrador de rede, verificador de pacotes (*sniffer*)
- Mobius: Script em Python para gerenciar *Cases*.
- QuickHash: Ferramenta para extração de Hash
- SQLiteBrowser: Gerenciador com interface gráfica para SQL Databases
- FRED: Editor de registros do Windows.
- knowmetanalyzer: Analisador de metadados
- PEFrame: Script para análise estática de Malware
- grokEVT: Scripts para leitura de Logs do Windows
- zenmap (nmap): Scanner de portas lógicas
- blackberry tools: Ferramentas para dispositivos Blackberry
- IDevice tools: Ferramentas para Iphone

4.3.1. Procedimento CAINE

Nesta seção será demostrado algumas aplicações do CAINE, como os procedimentos de coletas de dados foram apresentados no FDTK, no CAINE focaremos na utilização de aplicações voltadas para a análise de dados e tráfego de rede.

- **Wire Shark**

O Wireshark (conhecido anteriormente no Brasil como Ethereal) é um aplicativo que analisa o tráfego de rede, e o organiza por protocolos. As funcionalidades do Wireshark são semelhantes com o tcpdump mas com uma interface GUI (interface gráfica voltada para o Linux), com mais informações e com a possibilidade do uso de filtro para a análise. A Figura 14 apresenta a tela principal do aplicativo

É então possível gerenciar o tráfego de uma rede e saber todos os pacotes de redes que são enviados e recebidos pela mesma em tempo real, para diversos protocolos e redes no qual o computador está conectado.

Também é possível gerenciar o tráfego de um determinado dispositivo de rede num computador que pode ter um ou mais desses dispositivos. Caso esteja numa rede local, com máquinas ligadas através de um *hub* ou *switch,* aparelhos utilizados na distribuição e comunicação de rede, outro usuário pode usar o Wireshark para capturar todas as suas transmissões.

Poder gerenciar o tráfego de uma rede é muito importante quando se deseja prover de uma política para evitar as vulnerabilidades na qual a rede está exposta, conseguir enxergar os pacotes endereçados torna-se bastante útil para proteger-se rapidamente de um ataque ou invasão.

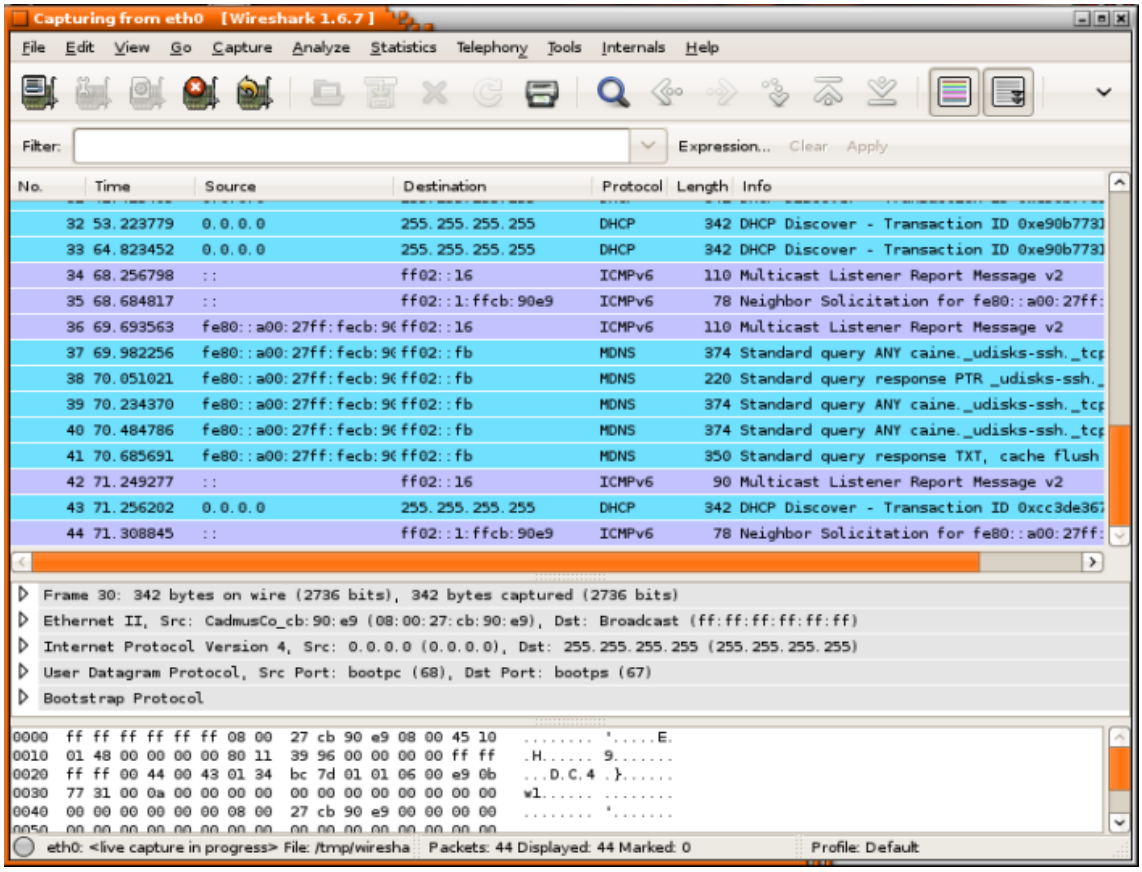

Figura 14: WireShark

- **QuickHash**

Como pode-se demostrar com o FDTK, a utilização do *Hash* é de suma de importância quando se trabalho com a coleta de dados. O QuickHash prove da utilização do GUI para realizações de coleta da sequência de *Hash*, de forma à apenas um arquivo ou dispositivo, ou de vários arquivos contidos em um só dispositivo, podendo salvar as sequências em um arquivo texto, servindo de documentação para o exame. A ferramenta é ilustrada na Figura 15.

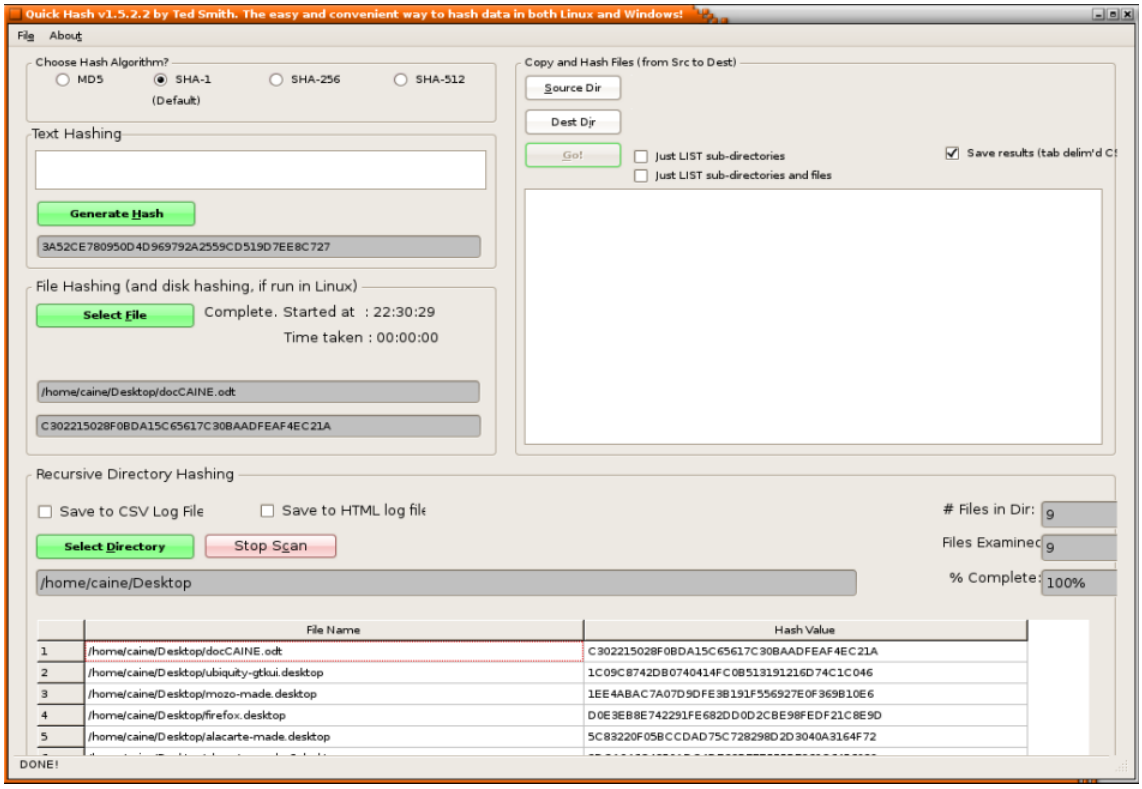

Figura 15: QuickHash.

5. FERRAMENTAS PESSOAIS

Embora a maioria das ferramentas forenses sirva exclusivamente para a área, muitas delas podem ser extremamente úteis quando é necessário realizar simples tarefas, como por exemplo, a recuperação de dados apagados de um determinado dispositivo de forma acidental, ou mesmo aplicativos que auxiliam na proteção do acesso ao conteúdo de dados e informação que sejam importantes.

O Recuva é um software utilizado para recuperação de dados em partições. A ferramenta provê de uma simples interface com suporte ao português. Seu procedimento é simples, primeiramente determina-se a partição a ser escaneada, assim feito, é apresentado uma lista com os dados que podem ou não ser recuperados, seguido de informações como nome, e data de criação do arquivo. A Figura 16 torna está definição clara. Além da versão gratuita, o Recuva possui sua versão *Pro* de distribuição paga, provida de mais recursos que a versão padrão.

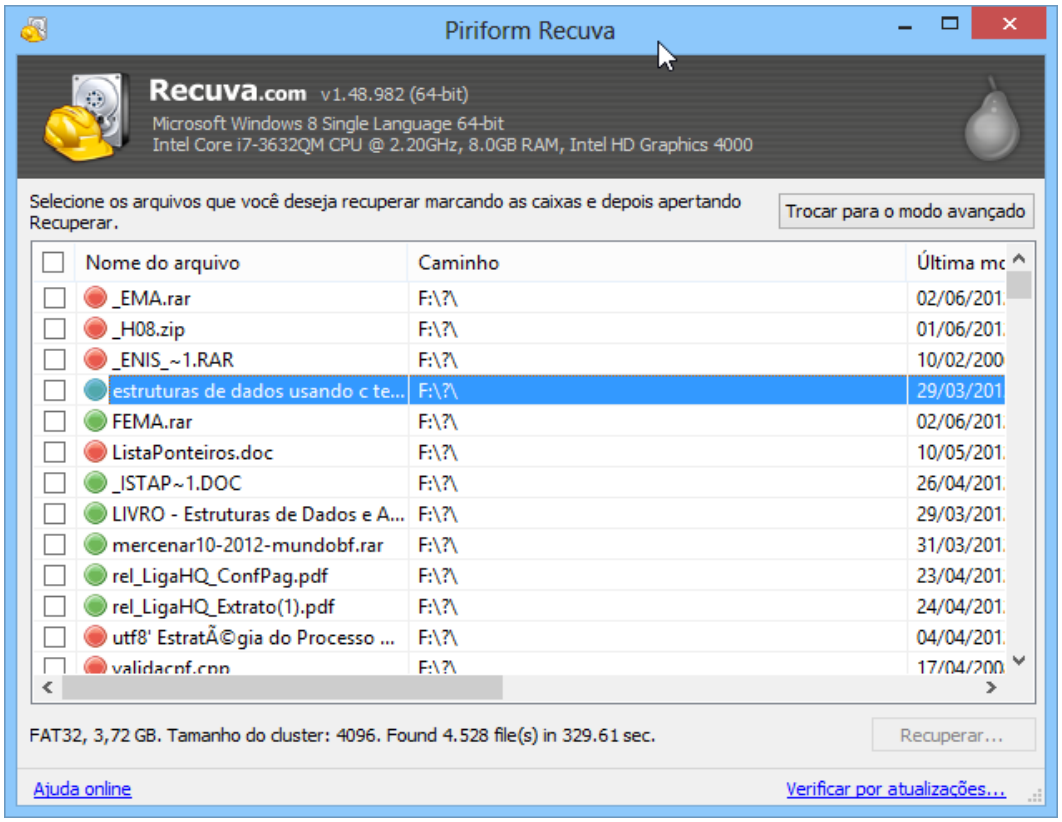

Figura 16: Recuperação de dados – Recuva.

5.1. CRIPTOGRAFIA

Um dos paradigmas da segurança está relacionado sobre o que deve-se proteger, isto é, qual propriedade seja ela física ou intelectual deve ser mantida segura, longe de qualquer fator que possa comprometer seu valor e causar transtornos posteriores a seus proprietários.

Como já foi discutido neste trabalho, o princípio da segurança de dados e informações armazenadas em mídias digitais, não é manter seguro os dispositivos que armazenam, e sim as informações em si. Partindo do princípio que a informação não está inteiramente segura, deve-se buscar mecanismos caso em determinado momento ocorra seu extravio.

Com fim de resguardar todo o patrimônio pessoal e intelectual é que surge a Criptografia, ciência formada por um conjunto de técnicas para ocultar uma informação do acesso não autorizado (PIZA, 2012). O objetivo da criptografia é transformar um conjunto de informações legíveis em um texto preenchido por caracteres impossível de ser compreendido, utilizando-se de recursos matemáticos para cifrar e decifrar as mensagens.

Criptografar partições e volumes de dados, é uma excelente alternativa para manter os dados seguros. As duas ferramentas abaixo como função montar volumes (partições falsas) e utilizar algoritmos para criptografar suas senhas de acesso.

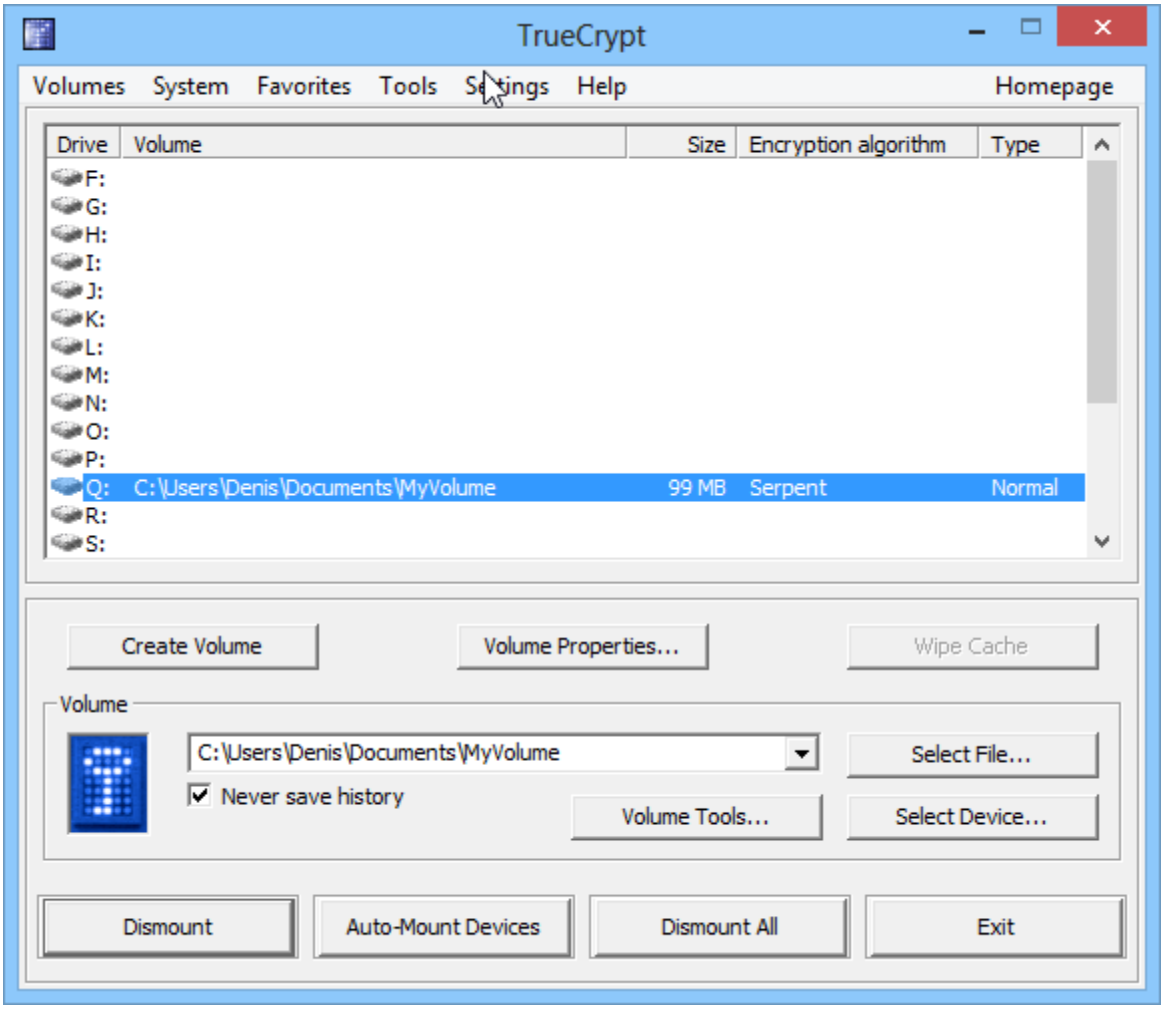

Figura 17: TrueCrypt

O *TrueCrypt*, apresentado na Figura 17 e o *SafeHouse Explorer* na Figura 18 utilizam o seguinte procedimento, primeiramente define as opções de criptografia e após monta o volume de dados. As duas ferramentas possuem interface simples e de fácil uso. O *TrueCrypt* contém oito diferente algoritmos de criptografia (*AES, Serpert, Twofish, AES-Twofish, AES-Trofish-Serpert, Serpent-AES, Serpert-Twofish-AES, Twofish-Serpert*), todos utilizando chaves de 256 Bits, há o *SafeHouse Explorer* apenas um de 256 Bits.

Os volumes criados são tratados de modo que apenas a própria ferramenta tenha acesso ao arquivo, podendo montá-lo como partição mediante à digitação da senha configurada pelo próprio usuário.

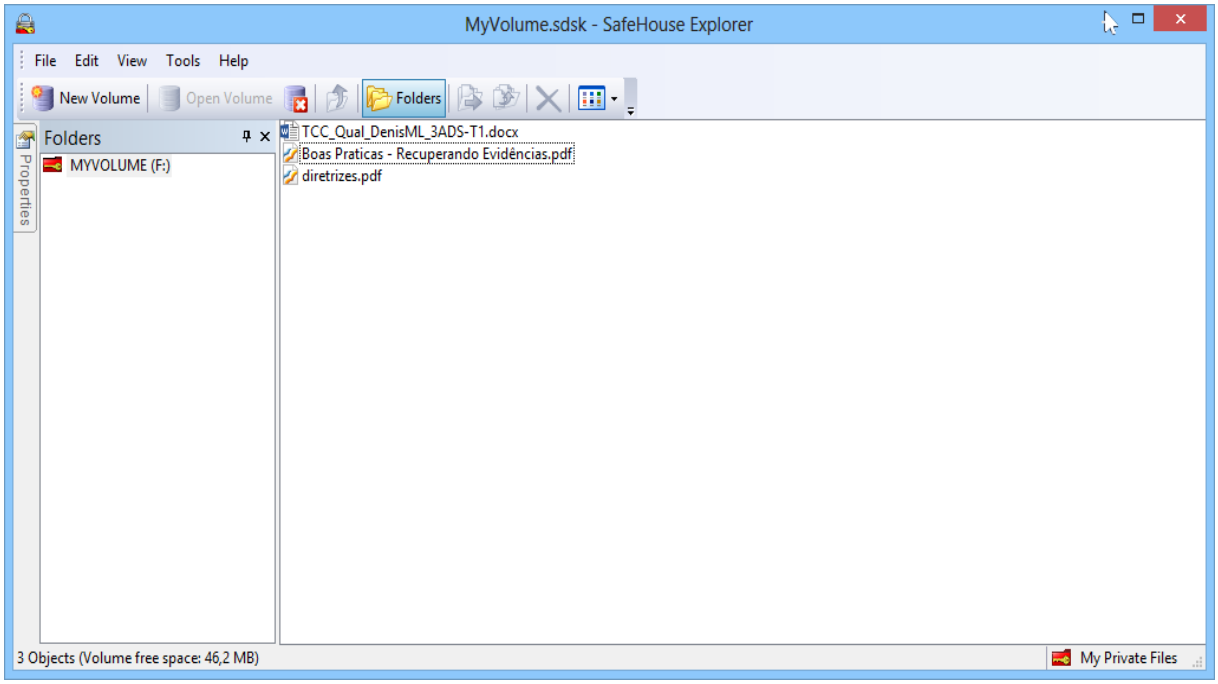

Figura 18: SafeHouse Explorer

6. CONCLUSÃO

Pode se concluir diante do material apresentado neste trabalho, a importância da segurança da informação na sociedade moderna em que vivemos, através da observação do número de informações que circulam diariamente nas redes de computadores e o valor que possuem. O roubo de informações pessoais e organizacionais caracteriza como um roubo comum diante das circunstâncias causadas por tal ação.

De acordo com a pesquisa realizada pela (SYMANTEC, 2012), empresa que concentra suas atividades na segurança de redes e computadores, as informações digitais armazenadas pelas empresas em todo o mundo, estão avaliadas em um valor de 1.1 trilhão de dólares. Outro dado apresentado, diz que as informações determinam aproximadamente metade do valor total de uma empresa. Refinando esta pesquisa somente na América Latina, temos os seguintes dados:

Quanto aos gastos com segurança:

- US$ 38 milhões para empresas de grande porte
- US$ 332 mil para empresas de pequeno porte

As consequências da perda de informações pelas empresas são apresentadas graficamente em forma percentual na Figura 19:

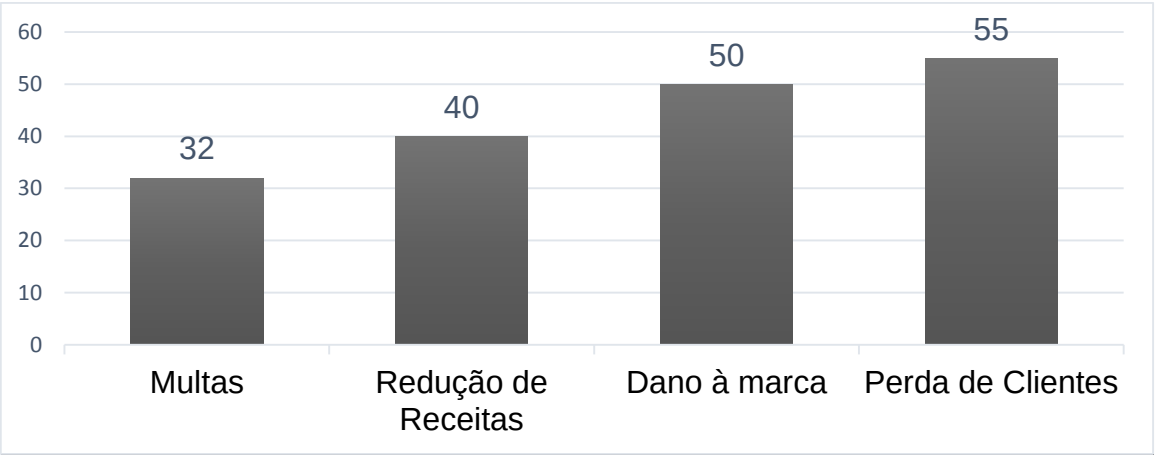

Figura 19: Gráfico - Consequências da perda de informações

Para finalizar a pesquisa, determinou que nos últimos 12 meses, 80% das empresas sofreram perda de informações de negócios importantes e 71% tiveram suas informações confidenciais expostas.

Diante dos dados apresentados e o decorrer do trabalho, percebe-se o valor do trabalho do perito na análise forense computacional quanto à busca e manipulação de evidências digitais afim de utiliza-las como forma de solucionar um determinado incidente cometido em meio virtual.

As ferramentas tem um papel fundamental na realização das etapas contidas no processo de investigação, em tese, sem a utilização de ferramentas torna-se impossível proceder com uma perícia forense. Vale ressaltar a qualidade das ferramentas, fator elementar para se atingir o resultado final.

Além do conhecimento técnico envolvendo o processo e uso das ferramentas, o perito deve prover de equipamentos que também o auxiliem. Não menos importante, deve sempre se respeitar o ordem de volatilidade das informações e os padrões de documentação.

Com uma análise forense bem documentada, cria-se uma oportunidade de disseminar a informação e deixar todos os envolvidos cientes das causas e efeitos das falha de segurança que culminaram no incidente; sendo assim de grande valia para a organização, por deixá-la imune a tais erros no futuro. (SANTOS, 2008)

Antes que necessitem da ajuda de um perito, os envolvidos quando dispõem do conhecimento sofre as vulnerabilidades que estão expostos, podem simplesmente aplicar procedimentos dos quais dificultem a atividade de terceiros ao acesso de dados privados. Ao final do trabalho, foi capaz de se concluir, que a Criptografia é a melhor solução para proteção de dados. Sendo uma ciência que possui um conceito chave simples sobre segurança, são inúmeras as aplicações que fazem seu uso.

6.1. CAINE E FDTK

Durante o procedimento realizado pode-se avaliar algumas peculiaridades de cada ferramenta. Ambas possuem características qualitativas para o uso no estudo da área de perícia forense, possibilitando uma compreensão definida sobre as etapas que englobam todo o processo. Para o uso profissional recomenda-se preferencialmente o uso do FDKT, por tratar-se de uma distribuição brasileira que possui um certo nível de documentação e prospectivas maiores de melhoria diante do próprio CAINE, tendo como plano para a próxima versão, exatamente oferecer ferramentas para suprir seus pontos negativos.

Na Tabela 2, é apresentado um comparativo de forma resumida sobre as distribuições, destacando os pontos positivos, negativos, o destaque e o número de ferramentas.

Características	CAINE	FDTK
Pontos positivos	• Não utiliza swap (partição para otimizar transferência de arquivos) e não monta dispositivos automaticamente. • Geração de relatórios semiautomática	• Tem praticamente todas suas ferramentas organizadas no menu. • Atualizações frequentes com prospectivas para melhoramento
Pontos negativos	• Pouca documentação • Poucas ferramentas • Teclado com layout Italiano como *default*	• Falta de ferramentas forenses para redes. • Falta de ferramentas para dispositivos móveis
Destaque	• Ferramentas voltadas ao Windows	• Suporte em português.
Número de ferramentas	• Cerca de 80 (oitenta) ferramentas.	• Mais de 100 (cem) ferramentas

Tabela 2: Comparativo entre as distribuições CAINE e FDTK

7. REFERÊNCIAS

BASSETTI, Nanni. **CAINE**. Disponível em <http://www.caine-live.net/index.html>. Acesso em 17 out.2013.

CANAVAN, John E. **Fundamentals of Network Security.** United States: Artech House telecommunications Publisher, 2001.

CHASIN, Alice Aparecida da Matta. **Parâmetros de confiança analítica e irrefutabilidade do laudo pericial em toxicologia Forense**. Revista Brasileira de Toxicologia, v. 14, n. 1, p. 40-46, 2001.

FARMER, Dan. **Perícia forense computacional.** São Paulo-SP. Editora Pearson. Prentice Hall, 2007.

FARMER, Dan. **What are MACTimes?** Outubro de 2000. Disponível em:< http://www.drdobbs.com/what-are-mactimes/184404275> Acesso em: 01 Jun. 2013.

FREITAS, Andrey Rodrigues de; **Perícia Forense aplicada à informática: Ambiente Microsoft**. p.55. Rio de Janeiro, 2006.

KUROSE, James. Redes de Computadores e a Internet: Uma Abordagem Top-Down. 5ª Edição. Editora Pearson, 2010.

LISITA, Bruno Lopes; MOURA, Thiago Silva Machado de; PINTO, Tiago Jorge. **Forense Computacional Em Memória Principal.** 2009. Trabalho de Conclusão de Curso. (Pós Graduação em Segurança em Redes de Computadores) – SENAI – FATESG. Goiânia.

NEUKAMP, Paulo A. **Forense Computacional: Fundamentos E Desafios Atuais.** 11 Junho de 2007. Universidade do Vale do Rio dos Sinos (UNISINOS). 06 Nov. 2007.

NEUKAMP, Paulo A. **FDTK.** Universidade do Vale do Rio dos Sinos (UNISINOS). Disponível em < http://www.caine-live.net/index.html>. Acesso em 12 set. 2013.

NOBLETT, Michael G.; POLLITT, Mark M.; PRESLEY, Lawrence A. **Recovering and Examining Computer Forensic Evidence**. Forense Science Communications.outubro 2000, Vol. 2 N. 4; Federal Bureau of Investigation.

OLIVEIRA, Flávio de Souza. **Respostas a incidentes e análise forense para redes baseadas em Windows 2000**. Campinas: 2002, 19p. Universidade Estadual de Campinas, 2002

PIZA, Pedro. **O Que é Criptografia?** Jun. de 2012. Disponível em: <http://www.techtudo.com.br/artigos/noticia/2012/06/o-que-e-criptografia.html> Acesso em: 25 Out. 2013.

QUEIROZ, Claudemir da Costa. **Segurança Digital: Um Estudo de Caso.** Fortaleza: FLF, 2007, 71p. Monografia (Graduação), Bacharelado em Ciência da Computação, Faculdade Lourenço Filho, Fortaleza, 2007.

RAMOS, Allder Ramos, Andre Teixeira Saturnino e TEIXEIRA, Pedro H. Amorim. **Um novo conceito de Live CD para Forense Computacional.** FATESG, 2009. 73p. Monografia (Graduação). Tecnologia em Redes de Computadores, Goiânia, 2009.

REIS, Marcelo Abdalla Dos e GEUS, Paulo Lício de. **Análise Forense De Instruções Em Sistemas Computacionais**, Campinas, 2002.

RODRIGUES, Tony. **Computação Forense 0800**. Disponível em <http://www.slideshare.net/tonyrodrigues/> Acesso em 20 Nov. 2013.

SANTOS, Laudelino Azeredo. **Computação Forense em Sistemas GNU/LINUX.** Lavras: UFLA, 2008. 54 p. Dissertação(Pós-Graduação), Administração em Redes Linux, Universidade Federal de Lavras, Lavras, 2008.

SÊMOLA, Marcos. **Gestões da segurança da informação: visão executiva da segurança da informação: aplicada ao Security Officer.** Rio de Janeiro. Editora Campus, 2003.

STALLINGS, William. **Network Security Essentials: Applications and Standards.** 4°Edição. United States, Pearson Education, 2011.

SYMANTEC**. Pesquisa sobre custo e gestão da informação**. 2012. Disponível em: <http://www.symantec.com/pt/br/about/page.jsp?id=infosurvey> Acesso em: 28 de Out. 2013.

ANEXO A

EVIDÊNCIA ELETRÔNICA

FORMULÁRIO DE CADEIA DE CUSTÓDIA

Caso Num.: 144 Pag.: 1 De: 2

MÍDIA ELETRÔNICA/DETALHES EQUIPAMENTO

Item:	Descrição:	
Fabricante:	Modelo:	Num. de serie:

DETALHES SOBRE A IMAGEM DOS DADOS

Data/Hora:	Criada por:	Método usado:	Nome da Imagem:	Partes:
Drive:	HASH:			

CADEIA DE CUSTÓDIA

Destino:	Data/Hora:	Origem:	Destino	Motivo:
	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 20: Formulário para Cadeia de Custódia

Disponível em: http://fdtk.com.br/files/formulario.xls