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

ANDRÉ LUIZ FERNANDES

PERÍCIA DIGITAL COMO FERRAMENTA AUXILIAR NA SOLUÇÃO DE CIBERCRIMES

Assis - SP
2014

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

ANDRÉ LUIZ FERNANDES

PERÍCIA DIGITAL COMO FERRAMENTA AUXILIAR NA SOLUÇÃO DE CIBERCRIMES

Projeto de Iniciação Científica apresentado ao Instituto Municipal de Ensino Superior de Assis – IMESA/FEMA, como requisito à participação do Programa de Iniciação Científica.

Orientando: André Luiz Fernandes
Orientador: Prof. Me. Fábio Eder Cardoso
Linha de Pesquisa: Segurança da Informação

Assis - SP
2014

Sumário

1. Introdução/Contextualização 02
2. Problematização 03
3. Formulação de Hipótese 03
4. Objetivos 04
    - Objetivo Geral 04
    - Objetivos Específicos 04
5. Relevância ou Justificativa 04
6. Revisão da Literatura 05
7. Metodologia 07
8. Cronograma Físico 07
9. Orçamento 08
10. Resultados 08
11. Referência Bibliográfica 10

1. Introdução/Contextualização

Os crimes virtuais já superaram os crimes reais e, por conta desta demanda, muitos crimes não são solucionados, quer pela ineficácia da polícia no tocante ao levantamento de provas, quer pelo criminoso que, por meio de técnicas especiais, não deixa vestígios do crime cometido.

Desta forma, surgiu a necessidade de técnicas e ferramentas para identificação de tais crimes, criminosos e, com isso, a redução de riscos de ocorrência de *cibercrimes* que podem ser definidos como ações que consistem em fraudar a segurança de sistemas computacionais.(Albuquerque, 2006)

Neste contexto a perícia digital apresenta-se como uma das ferramentas de auxílio na detecção, rastreio e solução de crimes cibernéticos. O uso da perícia digital coligada com os procedimentos judiciários formam o conceito de perícia forense computacional.

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

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

2. Problematização

Com a crescente demanda de crimes digitais onde o foco dos criminosos são os segmentos públicos e privados, há a necessidade de se criar mecanismos que auxiliem os órgão competentes no combate a esses crimes. Sabe-se que a prevenção ainda é o método mais seguro e que no mundo cibernético a questão segurança da informação e prevenção de incidentes não tem o devido foco.

Investir em ferramentas que detectam fraudes digitais que já ocorreram, por meio de vulnerabilidades de sistema, tem um custo muito alto e as técnicas de perícia digital ainda são conceitos pouco conhecidos.

Outro fator de extrema importância é o rastreamento de criminosos que praticam o *cibercrime* por meio de sistemas computacionais, uma vez que o crime já ocorreu e que torna-se difícil o levantamento de provas para a condenação destes criminosos.

3. Formulação de Hipótese

As técnicas e ferramentas para o estudo de perícia digital podem ser obtidos por meio de um pequeno investimento. Atualmente, existem sistemas operacionais abertos que possuem diversas ferramentas de perícia digital.

Outra vantagem que viabiliza a implementação do projeto é que toda os conceitos que permeiam a tecnologia, como ferramentas de análise de imagens, vídeos, *logs* de acesso à *Internet* podem ser encontradas na *web* sem nenhum custo, uma vez que este projeto vislumbra o uso de ferramentas totalmente livres.

Importante salientar que o estudo e pesquisa a respeito de perícia digital resultará em um profundo conhecimento sobre segurança da informação, redes de computadores, sistemas operacionais e banco de dados.

4. Objetivos

4.1. Objetivo Geral

Abordar os conceitos sobre perícia digital na investigação e esclarecimento de ocorrências no mundo cibernético, apresentando as ferramentas para este fim.

Apresentar os métodos de análise forense que resultará em um estudo comparativo entre estes métodos, viabilizando as melhores técnicas que permeiam as mais variadas formas de análise digital.

4.2. Objetivos Específicos

Os objetivos específicos vislumbrados por esta pesquisa são:

- Aprofundar os conhecimentos sobre perícia digital;
- Entender, aprender e disseminar os conceitos sobre cibercrimes, suas consequências e, principalmente, os métodos de proteção;
- Utilizar as técnicas e ferramentas que envolvam perícia digital;
- Gerar manuais e tutoriais *online* contextualizando o uso de sistemas para o trabalho com as ferramentas de perícia digital;
- Publicar o trabalho em congressos de iniciação científica como forma de divulgação da tecnologia e da Instituição;
- Criar parcerias com órgãos públicos e privados para auxiliar nas tarefas de detecção de crimes digitais.

5. Relevância ou Justificativa

Com a realização desta pesquisa pretende-se desenvolver um estudo introdutório que resultará no conhecimento dos conceitos sobre perícia digital, segurança da informação, *cibercrimes* e forense computacional.

O fruto deste estudo servirá de base para estimular a comunidade acadêmica na pesquisa a respeito deste contexto, tornando a Instituição um

centro de pesquisa a fim de auxiliar os órgãos competentes que necessitem desta mão-de-obra.

A necessidade de combater e prevenir os crescentes ataques cibernéticos, levantamento de informações que permitirão a recuperação de dados perdidos de forma acidental ou maliciosa como, por exemplo, identificar o furto de informações por terceiros ou funcionários da própria empresa.

. Como as ferramentas que serão utilizadas são totalmente livres e não apresentam custo algum, este projeto justifica-se, uma vez que esta pesquisa resultará em informações extremamente relevantes à comunidade e, principalmente, com a divulgação da Instituição FEMA como centro de pesquisa em perícia digital.

6. Revisão da Literatura

Atualmente, a computação automatiza a maioria de nossas tarefas, essas tarefas podem ser desde o processamento de sistemas governamentais complexos ao simples controle de batimentos cardíacos. De modo geral, tudo que possui componentes eletrônicos está relacionado com a atividade computacional.

Segundo (Freitas, 2006), a computação é a organização e execução de rotinas e métodos de caráter repetitivo.

O termo perícia pode ser entendido como relatório, laudo, documento ou outra forma de expressão, emitido por profissional que detém conhecimento específico. (Freitas, 2006)

Quando se une os termos computação e perícia obtém-se a perícia digital. Este contexto é extremamente importante em relação à procedimentos que podem ser executados após o cometimento de crime digital, pois, por meio da perícia digital é que pode-se detectar o possível autor do crime.

Com o uso massivo de sistemas computacionais por milhares de usuários, o cometimento de *cibercrimes* ocorrem diariamente. O combate a esta modalidade de crime deve ser realizado por profissionais especializados e com profundo conhecimento sobre legislação a respeito. Neste contexto surge a perícia forense computacional que, segundo (Albuquerque, 2006) a

computação forense realiza procedimentos e perícias digitais relativa aos crimes de informática, tais como fraudes contra a administração pública, rastreamento de ameaças feitas via *Internet*, pedofilia, invasão de sistemas, quebra de privacidade de dados entre outros.

A forense computacional tem como característica básica a cadeia de custódia que se refere à documentação cronológica das atividades, apresentando a apreensão, custódia, controle, transferência, análise e eliminação de provas, sendo elas físicas ou eletrônicas.(Queiroz, 2010)

A cadeia de custódia, como fase de perícia digital, ocorre para ser utilizadas em um tribunal como provas para condenar pessoas por crimes cometidos e, por conta destes processos, toda a fase de cadeia de custódia deve ser tratada com o maior rigor possível para evitar posteriores alegações, por parte dos criminosos, de adulterações ou má conduta na perícia.

Toda a fase, desde coleta de material até a apresentação das evidências em um tribunal, deve ser rigorosamente documentada incluindo todas as condições sob as quais as provas foram recolhidas, contendo a identificação dos peritos, o tempo de duração da custódia as condições de segurança no manuseio das provas e com essas etapas a assinatura dos profissionais envolvidos.

A *Internet* é um serviço sobre as redes de computadores em que os criminosos mais utiliza para a realização de ataques e cometimento de furtos de senhas. O conhecimento de protocolos de redes, dispositivos e meios físico é de suma importância por parte dos peritos.(Kurose, 2010)

A perícia em redes de computadores é uma das modalidades mais desafiadoras, pois, por meio da rede, a tarefa rastreamento de criminosos é mais crítica uma vez que os mesmos utilizam computadores de usuários comuns para realização dos ataques.

Este trabalho pretende expor alguns métodos de perícia digital forense em conjunto com a fase de cadeia de custódia e, principalmente, com foco em perícia digital sob redes de computadores.

7. Metodologia

Para a realização da pesquisa serão utilizados materiais didáticos como apostilas, livros, artigos e consultas eletrônicas com o intuito de gerar conhecimento que servirá de base para a implementação do projeto.

A pesquisa segue em conformidade com o cronograma e como método haverá a instalação, configuração e aplicação de ferramentas e técnicas pertinentes à perícia digital, a fim de fundamentar a metodologia.

Como fase final do projeto e com os conhecimentos adquiridos, será gerado um manual contendo todos os detalhes sobre as referidas técnicas e ferramentas estudadas onde toda a comunidade poderá utilizá-lo como forma de pesquisa.

8. Cronograma Físico

Mês	Atividade
Fevereiro/Março	Levantamento bibliográfico sobre os conceitos gerais que envolvem Perícia Digital. Criação de parcerias público/privadas
Março/Abril	Levantamento bibliográfico sobre *Cibercrimes*.
Maio/Junho	Período para elaboração do Relatório Parcial.
Julho/Agosto	Instalação e Testes de implementação e levantamento das informações relevantes sobre resultados parciais.
Setembro	Avaliação e impressões sobre o trabalho após o uso de técnicas e ferramentas sobre pericia digital.

Outubro	Participação na apresentação de Seminários do PIC e na Semana de Ciência e Tecnologia de 2012.
Novembro/Dezembro	Etapa de fechamento do projeto e elaboração do Relatório Final.

OBS: o cronograma apresentado poderá sofrer alterações por conta do estudo de novas tecnologias que envolvem perícia digital.

9. Orçamento

A pesquisa será realizada, basicamente, em livros, artigos e sites da *Internet*. Para a realização da prática, haverá necessidade do uso apenas de computadores presentes no laboratório de redes de computadores e sistemas operacionais.

Será necessária, apenas, a impressão de cópias de artigos, capítulos de livros e tutoriais encontrados na *Internet* para enriquecer o conteúdo teórico da pesquisa.

10 . Resultados

Mediante as pesquisas realizadas durante todo o ano, onde o aluno se empenhou na busca de conhecimento sobre perícia digital, pode-se classificar o trabalho, bem como o desempenho do aluno como satisfatório, uma vez que o presente trabalho resultou em publicação nos anais do VII fórum científico ocorrido nesta instituição.

Como descrito nos objetivos específicos, a grande maioria deles foram cumpridos. Entretanto, a parceria com órgãos públicos ligados à secretaria da Segurança Pública não foi efetivada, visto a preservação da integridade do aluno bem como a da Instituição, uma vez que esta parceria poderia infirngir em crime, pois, em casos de crimes virtuais, somente peritos do Instituto de Criminalística da Polícia Civil e Peritos delegados pelo Fórum de Justiça podem

ter acesso aos processos e aos dispositivos em que estão envolvidos os criminosos.

Contudo, a pesquisa realizada pelo aluno foi de extrema importância para seu conhecimento científico, uma vez que o mesmo se deteve em assuntos pertinenetes à perícia digital, conteúdo este, não aplicado nas ementas do curso de Análise e Desenvolvimento de Sistemas.

11. Referências Bibliográficas

ALBUQUERQUE, Roberto Chacon. **Criminalidade informática**. São Paulo: Editora Juarez de Oliveira, 2006.

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

KUROSE, James; ROSS, Keith. **Redes de computadores e a Internet: uma abordagem top-down**. 5ª ed. Tradução Opportunity translations. São Paulo: Editora Addison Wesley, 2010.

QUEIROZ, Claudemir. **Investigação e Perícia Forense Computacional: certificações, leis processuais e estudo de caso**. Rio de Janeiro: Editora Brasport, 2010.