Forense Computacional: pesquisa sobre peritos na cidade de Catalão (GO)

Fábio Justiniano Ribeiro[1], **Leandro Fernandes Cardoso**[1], **Tiago Batista Lúcio**[1]

[1]Departamento de Ciência da Computação Universidade Federal de Goiás (UFG)
Caixa Postal 15.064 – 91.501-970 – Catalão – GO – Brasil

fabio_justiniano@hotmail.com, leandrofc514@gmail.com, tiagocomp.ufg@hotmail.com

Abstract. *With the growing use of Internet computing and the advent of cybercrime increase gradually. With this it is necessary to the existence of professionals and companies dedicated to this idea. In this report we discuss a detailed analysis of the forensic experts in the city of Catalão (GO). Also addressed will be important concepts that the pros use to uncover crimes, such as tools, findings, among others. Use will be for this, the methodology of analysis to literature works.*

Resumo. *Com o crescente uso da internet e o advento da computação os crimes virtuais aumentam gradativamente. Com isso é necessário à existência de profissionais e empresas voltadas a essa idéia. Neste trabalho é abordada uma analise minuciosa sobre os peritos forenses na cidade de Catalão (GO). Também abordar-se-á conceitos importantes que os profissionais usam para descobrir delitos, como ferramentas, laudos, entre outros. Utilizar-se-á, para tanto, a metodologia de análise a obras bibliográficas.*

1. Introdução

Com o crescente avanço do uso do computador na sociedade atual há também o aumento dos chamados crimes de informática. Hoje, o homem utiliza o computador para vários procedimentos, desde trabalhos mais tranquilos aos mais complexos. Este mundo é realidade e os crimes que passam a ser cometidos com o uso desses meios também. A forense computacional é um campo de pesquisa recente e está desenvolvendo-se principalmente pela necessidade das instituições legais atuarem no combate aos crimes eletrônicos. No Brasil conta-se ainda com poucos pesquisadores na área e existem poucas normas estabelecidas, o que gera um grande número de possibilidades de pesquisa.

A cidade de Catalão é considerada de porte médio e possui várias empresas que dependem da tecnologia para gerar seus lucros. A necessidade de informatização dos meios para aumentar os ganhos é alta. Acompanhando essa idéia, os crimes relacionados a computação também aumentam. Este trabalho vai apresentar uma pesquisa feita na cidade de Catalão (GO) sobre os profissionais que atuam na área de computação forense. Também verificar-se-á a existência de empresas na cidade que tratam do assunto tratado neste trabalho a Forense Computacional. Também apresentaremos uma analise de qual é o perfil do profissional na cidade, entre outros. Também vamos apresentar analises de mercado para os profissionais interessados em atuar nesta área. Como vamos observar no decorrer do trabalho, não existem muitos profissionais preparados para este tipo de requisição. Para quem tiver interesse em atuar nesta área, será uma boa forma de analise para sua escolha.

2. Forense computacional

Hoje as pessoas utilizam os computadores para tudo em suas vidas. Compras pela internet estão se tornando uma ação habitual dos mesmos. Antigamente isso era um processo pouco praticado. Acesso à conta de bancos via computador também era outra ação não muito utilizada e agora está sendo usada em larga escala. As formas de segurança na internet como antivírus garantem, pelo menos minimamente, uma proteção ao usuário. Sistemas mais concisos também garantem uma proteção maior ao mesmo. Isso é um dos motivos pelos quais as pessoas aderiram o uso do computador para facilitar suas vidas. Essas formas somente não garantem por completo a integridade de informações. Empresas que trabalham com softwares (desenvolvimento, venda) e com comercio pela internet são as que mais sofrem invasões maliciosas. Já que existe esse tipo de crime, também devem existir formas para se descobrir quem comete tais delitos. Uma forma é a computação forense, que é um meio pelo qual podemos empregar para a tentativa de descoberta de fraudes na informática.

A forense computacional é voltada para a obtenção, preservação e documentação de evidências, a partir de dispositivos de armazenagem eletrônicos digitais, todos os procedimentos, sejam feita de forma local ou remota, ou seja, via rede, são feitos a fim de preservar o valor comprobatório das evidências e para assegurar que isto possa ser utilizado em procedimentos legais. Tais ações, na maioria das vezes estão relacionadas a roubo de informações, fraudes, casos de pedofilia, espionagem, ou seja, crimes cibernéticos em geral.

3. Laudo da Perícia

Não há um modelo específico para o laudo ou relatório da perícia do profissional forense. Nas subseções são colocados alguns dados que são importantes para a composição do laudo.

a) Período da realização da análise forense: compreende o intervalo de tempo em que é feita a perícia, com a data, e se possível, horário de início, e as mesmas informações para o fim;

b) Breve relato do ocorrido (notícias iniciais): Basta um resumo descrevendo os motivos da necessidade da perícia sobre o ocorrido;

c) Dados gerais: sobre a máquina e/ou sistema atacado (nome da máquina, portas abertas, partições existentes, etc.);

d) Detalhamento dos procedimentos realizados: especificação de cada procedimento de forma minuciosa e organizada;

e) Dados e fatos relevantes encontrados: relato das evidencias encontradas na análise pericial, que leva a descrever alguma ação suspeita, esta fase será a pesquisa propriamente dita, em que praticamente todos os filtros de informação já foram executados. A partir deste ponto o perito poderá focalizar se nos itens realmente relevantes ao caso em questão;

f) Conclusão e recomendações: conclui-se a pesquisa, ressalta pontos que sejam mais importantes, indicando possíveis falhas e fazem-se recomendações do que deverá ser feito para correção, e para preservar a segurança;

g) Apêndices e anexos: para fim de complemento sobre a informação coletada na pericia.

4. Implicação Legal

Para ser perito criminal, o profissional tem que ter curso superior e prestar concurso público específico, podendo existir peritos contratados sem concurso para alguma eventual necessidade (estes também devem possuir curso superior). Logo quando se descobre algum delito como cópia de software, pedofilia na internet, invasão na rede de uma empresa, por exemplo, deve-se imediatamente entrar em contato com as organizações de resposta a incidente de segurança e tomar todas as medidas legais cabíveis. No Brasil não existem regras específicas que determinam a forense computacional, contudo existem normas gerais que abrangem todos os tipos de perícia (ditadas nos Códigos de Processo Penal) e processo cível, podendo ser adotadas no âmbito computacional, salvo algumas peculiaridades. No caso de uma perícia criminal existe a figura do Perito Oficial (dois para cada exame), onde o seu trabalho deve servir para todas as partes interessadas (Polícia, Justiça, Ministério Público, Advogados, etc.).

5. Ferramentas computacionais forenses

A tecnologia evolui cada dia mais rapidamente, assim como as formas de ataques aos sistemas hoje em atividade. Sendo assim, os peritos forenses computacionais necessitam de uma metodologia de padronização para seus laudos e ferramentas sofisticadas para a busca e identificação desses infratores. Além disso, é necessário se padronizar esta busca e apresentar evidências mais consistentes possíveis, para que sejam entregues às devidas autoridades. Abaixo, estão listadas algumas ferramentas comuns utilizada no dia-a-dia desses profissionais que são compatíveis com o sistema operacional Windows que contribuem para este propósito:

a) Caller IP: esta ferramenta monitora a entrada, saída e invasão de IPs, ela ajuda na indicação de entradas, saídas e possíveis invasões de IP na maquina investigada. Ela age informando qual IP está conectado ou tentando se conectar a, apresentação em um mapa mundi a localização com endereço, telefone e responsável pelo proprietário daquele IP. Na figura 1 é mostrado o Caller IP em execução, ela mostra a localização do IP que está tentando ter acesso ilegal que é mostrada em um mapa-mundi;

b) RecoverMyFiles: recupera dados deletados ou formatados em discos rígidos, ela nos permite recuperar esses arquivos que foram apagados em uma determinada partição do sistema operacional Windows. Ela não necessita instalação, sendo executa diretamente em um disco flexível, evitando a escrita no disco durante a perícia em uma maquina. Ela oferece a opção para selecionar quais extensões de arquivos serão buscadas;

c) Smartwhois: auxilia na verificação de IPs e de domínios na Internet, sendo indicado o IP ou domínio, é apresentando na tela a localização destes, gerando endereço, telefone, responsável pelo IP ou pelo domínio em questão;

d) EmailTracker: ela fornece através de uma entrada de um e-mail ou uma lista de e-mails o local de origem, onde foi criado, a rota entre empresas filiadas, ou não, a organização em questão e a mesma responsável pelo e-mail, sendo identificada com a apresentação de seu endereço, telefone, dentre outros dados;

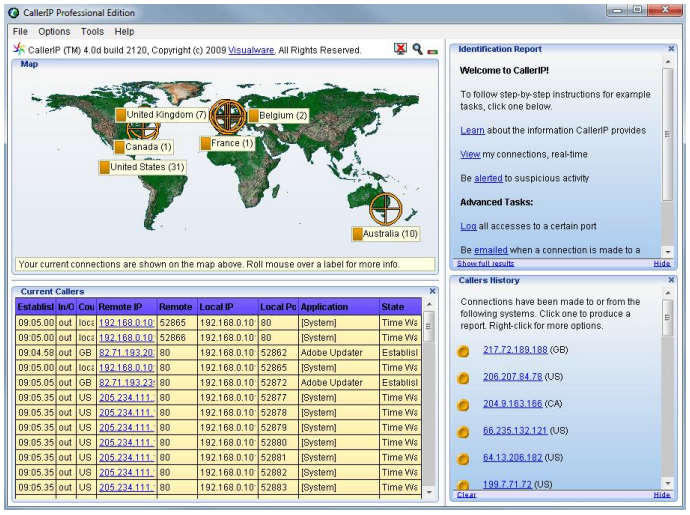

Figure 1. Janela principal do Caller IP

e) EnCase: é uma das ferramentas mais completas da área forense, além de auxiliar recuperação de arquivos deletados, padroniza laudos periciais, organiza um Banco de Dados com as evidências, fornece senhas e quebra as senhas dos arquivos, analisa hardwares, analisa logs, analisa formatos e tipos de e-mails e fornece uma opção de se manusear a evidência sem danificá-la. Das ferramentas faladas acima, a mais utilizada é a EnCase,pois como foi falado é uma das mais completas e utilizadas na área de padronização de laudos, armazenamento de evidencias, recuperação de dados, e uma infinidade de outras unidades para o auxilio no manuseio da evidencia. Na figura 2 é mostrada a execução do EnCase.

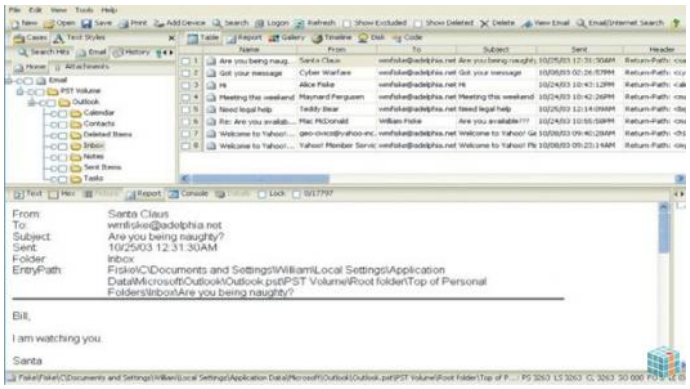

Figure 2. Janela de execução do EnCase

6. Computação Florense aplicada na cidade de Catalão (GO)

Na cidade de Catalão não existe nenhum perito na área de informática cadastrado no fórum de acordo com informações obtidas no próprio fórum. De acordo com um funcionário, somente uma vez foi contatado um profissional de TI (Tecnologia da Informação) para uma perícia. E mesmo assim não existe nenhum cadastro. Talvez a inexistência desse cadastro e de pessoas interessadas a prestar esse serviço seja pela falta de procura da pericia na área da informática, e falta de informação da área de atuação para

os profissionais de TI e da existência do serviço para a população. Se um profissional de TI quiser dispor os seus serviços para o fórum, ele deverá levar seu currículo, que será analisado por um juiz quando for necessária a pericia na área , e de acordo com a necessidade de habilidades e com o apresentado no currículo, é escolhido o profissional para fazer a pericia. Não informaram se é necessário que o profissional seja graduado, apenas é necessária a apresentação do currículo do profissional.

7. Conclusão

Este trabalho mostrou a definição, atividades e ferramentas do profissional da computação florense, área que vem se desenvolvendo cada vez mais na nova era digital, pois a grande disseminação de sistemas computacionais que trabalham interligadas a rede de internet os torna o alvo de muitos ataques. Foi realizado um estudo no município de Catalão (GO) na tentativa de se identificar tais profissionais. Verificando que a profissão de computação florense está carente nessa cidade, abrindo as portas para aqueles que se interessam em trabalhar nessa área.

8. Referências

A Função Pericial do Estado; Perícia Criminal - DF http://www.apcf.org.br

FILHO, J.E. (2009) Forense computacional em Linux for dummies: uma rápida visão introdutória http://www.softwarelivre.gov.br/clientes/softwarelivre/softwarelivre/palestras-tecnicas-cisl/forense.pdf

FREITAS, A. R. (2003) Perícia Forense Aplicada à Informática http://www.linuxsecurity.com.br/info/general/andrey-freitas.pdf

ICoFCS/ABEAT ed.,Natal, Brazil, 122 pp. - ISSN 1980-1114, (2009) Proceedings of The Fourth International Conference of Forensis Computer Science http://www.icofcs.org/2009/ICoFCS2009-FULL.pdf

Perícia Forense Computacional - Ferramentas Periciais http://imasters.uol.com.br/artigo/6485/forense/pericia_forense_computacional_ferramentas_periciais

REIS, M.A. e GEUS,P.L. (2001) Forense Computacional: Procedimentos e Padrões http://www.las.ic.unicamp.br/~paulo/papers/2001-SSI-marcelo.reis-forense.padroes.pdf

Caller IP-Pró (2010) Caller IP http://www.callerippro.com

Recovermyfiles (2010) Recovermyfiles http://www.recovermyfiles.com/pt

Smartwhois (2010) Smartwhois http://www.tamos.com/products/smartwhois

Emailtracker (2010) Emailtracker http://www.emailtrackerpro.com