ATUAÇÃO DO PERITO FOSENSE COMPUTACIONAL NO BRASIL[1]

Moacir Ferreira Rocha

Resumo:

Com a inovação de crimes cometidos por criminosos que estão utilizando, cada vez mais da tecnologia, faz-se necessário usar novos métodos para investigar quem, como e porque esses crimes são cometidos. Diante deste cenário, é imprescindível um profissional altamente qualificado, para apurar os mais variados tipos de crimes virtuais, buscando através de pequenos detalhes, descobrir provas que levam à um julgamento justo os reais culpados. Para a realização deste trabalho, há o Perito Forense Computacional, que deverá analisar os dados contidos nos equipamentos coletados no local do crime, bem como a preservação e integridade desses equipamentos. Logo após esse profissional deverá formalizar um laudo, que ateste as evidências do ocorrido do crime virtual.

Palavras-chave: Perito. Forense. Computacional.

1 INTRODUÇÃO

É bem verdade que estamos vivenciando uma utilização grande de recursos digitais/tecnológicos, seu uso diário nos últimos anos, cresce a todo instante. Podemos perceber a utilização destes recursos não só em atividades de cunho profissional, pessoal

[1] Artigo apresentado como Trabalho de Conclusão do Curso de Especialização em Gestão da Segurança da Informação, da Universidade do Sul de Santa Catarina, como requisito parcial para a obtenção do título de Especialista em Segurança da Informação.

e entretenimento, mas também amoralmente num novo jeito de praticar crimes. Os chamados Crimes Digitais.

Neste contexto, antiético e amoral surge a necessidade de uma segurança para os órgãos públicos e privados, precisando buscar novas técnicas de investigação e apuração de evidências que comprovem de forma eficaz, crimes efetuados por pessoas usando dessas novas tecnologias digitais.

É nesse contexto que surge no Brasil o Perito Forense Computacional. Esse profissional deverá ser criterioso com a forma de lidar no ambiente a ser investigado. Sua atenção deverá estar voltada para os equipamentos ligados (em uso) na cena de um crime, deve desliga-los ou não. Atenção também, na verificação, se durante a retirada de equipamentos de um ambiente, estará ou não apagando evidencias de dispositivos por eletromagnetismo. E orientar a forma correta de guardar esses equipamentos.

Como objetivos específicos, foram explanados tópicos em que o Perito Forense Computacional deverá estar atento quanto aos aspectos técnicos e teóricos, para que não tenha dificuldades em desenvolver o seu trabalho.

Foram verificados os seguintes tópicos:

- Formações profissionais e qualificações específicas do perito.
- Áreas de atuação do perito.
- Ferramentas de trabalho.
- Erros comuns cometidos durante uma investigação.
- As dificuldades encontradas pelo Perito na Análise Forense Computacional.

Através de pesquisa teórica, identificamos quais os principais entraves encontrados pelo Perito Forense Computacional, com base em relatos de diversos autores, através de artigos, palestras e webcast na web.

2 ATUAÇÃO DO PERITO FORENSE COMPUTACIONAL

A evolução tecnológica vem acontecendo em ritmo frenético, onde uma tecnologia levava anos nas décadas de 1980 e 1990 para ser distribuída pelo mundo, hoje pode levar dias ou somente horas.

Na mesma velocidade que estas tecnologias são disseminadas, os crimes digitais também evoluem e são aprendidas e reinventadas por indivíduos, no intuito de utilizá-las de forma ilícita.

A sofisticação desses crimes, superam as técnicas aprendidas em cursos técnicos e de graduação, fazendo que, a cada dia o profissional de segurança da informação, fique atendo as novas técnicas e tecnologias que podem ser utilizadas por estes criminosos, com intuito de acessar, modificar, roubar e vender informações sigilosas de pessoas e instituições privadas e/ou públicas, para obter algum tipo de vantagem social e/ou econômica/financeira.

Neste interim, este trabalho tem a intenção de divulgar as dificuldades que o profissional Perito Forense Computacional, encontra para desvendar como, onde e porque um crime digital foi praticado.

2.1 FORMAÇÕES PROFISSIONAIS E QUALIFICAÇÕES ESPECÍFICAS DO PERITO

2.1.1 FORMAÇÃO PROFISSIONAL

O profissional em perícia forense computacional deverá ter no mínimo um curso a nível superior, com especialização na matéria, conforme alteração do Código de Processo Civil datado de 1984 (Lei 7.270/84).

O ideal é que ele tenha uma formação superior em computação e outra em direito[2], já que o no seu trabalho deverá, além do entendimento técnico em computação, precisa coordenar os trabalhos periciais como qualquer outro tipo de investigação, dentro dos parâmetros estipulados em lei. Que neste caso, podemos citar o Código Civil, Código Penal e os procedimentos e normas processuais na apuração de provas.

Infelizmente, como em várias outras profissões, existem pessoas que se autoqualificam para desempenhar as atribuições de perito forense computacional. Pior ainda, aquelas que são designadas sem ao menos ter um curso superior.

> Ainda temos casos no Brasil onde o dono da loja de informática da cidade é o perito, ou economistas e contadores nomeados como peritos digitais, e isto é um risco para a efetividade da tutela jurisdicional, considerando que é comum os juízes confiarem na palavra do especialista (MILAGRE 2007).

[2] Esta é a formação ideal para a maioria das funções executadas pelo Perito Forense Computacional, mas deverá ser observados em vagas de emprego, editais de concurso, etc, as exigências prevista para a ocupação do cargo.

2.1.1.1 QUALIFICAÇÕES ESPECÍFICAS

Além das formações profissionais, o perito forense computacional, deverá ter inúmeras habilidades para desenvolver o seu trabalho.

Podemos enumerar que deverá ter:

- Conhecimento sobre sistemas operacionais em geral e seus sistemas de arquivos, redes de computadores e conhecimentos básicos sobre programação.
- Domínio sobre as ferramentas, metodologia e embasamento técnico na busca de evidências, preservando ao máximo o material a ser analisado.
- Demonstrar experiências em frameworks, compliance e melhores práticas previstas na tecnologia da informação como SOX, COBIT, ITIL, PCI, ISO 27001. (FRANCO, 2016)
- Utilização de técnicas hackers na busca de entendimento e rastreio das prováveis evidências. Pensar como um hacker, é a melhor forma de descobrir como foi o procedimento utilizado para que o mesmo tenha sucesso em sua incursão.
- Intuição, saber onde procurar, ter faro investigativo na busca de evidências onde outros deixariam passar.

2.2 ÁREAS DE ATUAÇÃO DO PERITO

2.2.1 ÁREA PÚBLICA

O aspirante a perito pode optar por seguir carreira pública, prestando concurso tanto na esfera Federal ou Estadual como perito criminal, ou atuando junto a Delegacias e auxiliando o Ministério Público não especializadas, através de petição junto ao juiz sua habilitação que poderá ser aceita ou não.

Neste último, sempre que há a necessidade de um perito onde o Estado não possui mão de obra especializada, é nomeado através de um juiz, um perito qualificado para investigar o caso.

2.2.2 ÁREA PRIVADA

Os peritos que atuam na área privada, poderá compor uma equipe multidisciplinar de profissionais da área jurídica e técnica (MILAGRE, 2007).

Estes ajudaram a planejar e gerenciar estrategicamente o Time de Resposta a Incidentes da Empresa ou prestar serviço como consultor.

2.2.3 EXEMPLOS DE ATUAÇÃO DO PERITO

2.2.3.1 EXAME DE LOCAL DE INFORMÁTICA

O perito é chamado para descobrir de onde partiu um e-mail que contém texto de calúnia e difamação, e o mesmo deverá responder se o serviço de acesso à internet no local examinado é compartilhado entre os demais clientes. Se é possível descobrir o titular do e-mail que foi enviado, em caso negativo quais fatores que contribuíram para tal impossibilidade (ELEUTÉRIO E MACHADO, 2010, p. 141).

Chegando ao provedor de serviços foi identificado que o endereço IP, naquela data e hora, pertencia a um cyber-café. Além de identificar que no estabelecimento haviam 13 computadores contando com o servidor que era utilizado pelo funcionário, havia um switch da marca Encore modelo ENH916P-NWY, responsável pela distribuição do link da Internet aos treze computadores e o próprio roteador ADSL DSLink 260E.

No computador do funcionário, existia um programa de controle dos computadores do cyber-café, com cadastro dos clientes, onde foi analisado os computadores que foram utilizados na data e hora em que o e-mail foi enviado.

Com o objetivo de encontrar qual dos computadores foi utilizado, foram feitas buscas por palavras-chave, mas sem sucesso.

Foi verificado que alguns programas estavam sendo executados em todas as máquinas do cyber-café, e que um deles é utilizado para limpar arquivos temporários, cache, cookies, arquivos de lixeira, swap e outros arquivos do computador.

Então, constatou-se que esse programa era o responsável por executar a limpeza de disco, todas as vezes em que o computador for desligado.

Ainda no programa de controle dos computadores, os peritos levantaram informações sobre dados de todos os usuários cadastrados e todas as visitas cadastradas naquela data.

Como respostas aos quesitos elaborados pela justiça, foram divulgados pelos peritos que:

- Os treze computadores partilhavam de uma mesma conexão e um único endereço IP externo. Sendo que, qualquer dos 13 computadores poderiam ter sido utilizados para o envio do e-mail.
- Não foi possível determinar qual computador foi utilizado pelo titular do e-mail, pois não foram encontrados vestígios. No local, é utilizado um programa que faz a limpeza de dados temporários, históricos, cache e outros dados importantes para a realização de buscas por evidências digitais.
- No local havia um programa de controle de acesso aos computadores e usuários e os dados foram coletados pelos peritos e apresentados em anexo ao laudo pericial.

2.2.3.2 EXAME EM DISPOSITIVO DE ARMAZENAMENTO COMPUTACIONAL

A investigação corre em torno de uma empresa de cartuchos para impressoras, e o perito tem em mãos, um disco rígido de 20GB contendo supostos arquivos relativos a contabilidade, lista de preços, fornecedores, compradores, folhetos de propaganda de cartuchos de impressoras, além de arquivos de administração e controle, faturamento,

compras, propriedade e transações de bens, direitos e valores de alguma pessoa física ou jurídica da empresa (ELEUTÉRIO E MACHADO, 2010, p. 153).

A primeira providência realizada pelo perito, foi o espelhamento do disco rígido, para que se possa trabalhar com segurança com uma cópia das informações contidas no mesmo, preservando assim, os dados do original.

Para a realização da recuperação dos dados foi utilizado softwares próprios, onde foram encontrados diversos arquivos previamente apagados e inspecionados os conteúdos desses arquivos quantos aos que já estavam acessíveis no disco rígido.

Diversos arquivos foram encontrados, conforme os quesitos, que foram extraídos e relacionados conforme as seguintes categorias:

- Access: diversos arquivos de banco de dados do programa Microsoft Access.
- Administração e controle: arquivo com relação a administração e controle da empresa.
- Clientes: arquivo contendo possíveis clientes.
- Contabilidade e finanças: arquivos que tem relação a contabilidade finanças.
- Lista de preços: lista de preços de cartuchos.
- Outros: outros arquivos separados pelo perito.
- Propaganda: propagandas, folhetos e descrição da empresa.
- Propriedade e transação de bens: relação de propriedade e/ou transação de bens entre pessoas físicas e/ou jurídicas.

Em alguns arquivos relacionados, foi detectado pelo perito a presença de senhas, que foram recuperadas e listadas juntamente com os arquivos.

Todos arquivos foram copiados para um CD, onde um arquivo “hashes.txt”, contendo a saída de tamanho fixo de 512 bits através do algoritmo SHA-512, dos arquivos de evidências encontrados no disco rígido, e no laudo escrito, também foi relacionado o código de integridade do arquivo “hashes.txt”.

2.3 FERRAMENTAS DE TRABALHO

O perito forense computacional dispõe no mercado uma variedade de ferramentas tanto proprietária quanto opensource.

Durante uma investigação ele deve estar atento quanto as licenças de software e hardware utilizadas na obtenção de provas.

Estas provas poderão ser invalidadas caso o perito tenha utilizado em seu laboratório software pirata, ou que tenha sido alterado sem a devida autorização do autor, podendo o seu laudo ser invalidado diante do juiz.

Como dito antes, várias ferramentas estão à disposição do perito, e este deverá escolher aquelas que melhor ajudam na obtenção de evidências. Mas ao mesmo tempo deverá estar atento aos diversos ambientes operacionais existentes, onde muitos profissionais se especialização em somente um sistema operacional, deixando outros de lado.

> Muitas ferramentas opensource já homologadas pela comunidade estão em plataforma Unix, logo, um perito que opere somente e plataforma Windows, não trará o grau de profundidade necessária para que uma perícia seja considerada correta, verdadeira, ou melhor, para que não seja questionada por advogados do direito digital (MILAGRE, 2007).

Pode-se observar a importância dos conhecimentos aprofundados na apuração de evidências, pois um descuido, falta de conhecimento e análise de dados, poderá confirmar ou não um autor de um crime, deixando que um indivíduo inocente pague por um ilícito que não cometeu, colocando um culpado à solta na sociedade.

2.4 - ERROS COMUNS COMETIDOS DURANTE UMA INVESTIGAÇÃO

A falta de habilidade ao tratar um incidente ou local de investigação poderá desqualificar as informações coletadas para posterior julgamento.

Diversos cuidados devem ser tomados, para garantir a integridade e não repúdios dos dados investigados durante as fases de preparação, extração, análise e formalização do laudo. Os seguintes erros devem ser evitados segundo BOCCARDO, 2015:

- Não documentar o processo de captura de dados e das evidências
- Não documentar a máquina alvo
- Desligar ou reiniciar a máquina
- Utilizar comandos da própria máquina, pois o invasor pode ter alterado aqueles comandos. Onde os comandos não retornaram as informações verdadeiras.
- Sem metodologia, sem conhecimento, sem embasamento este tipo de atividade não pode de forma alguma ser exercida.

A responsabilidade do perito forense computacional é grande, pois um deslize durante qualquer uma das etapas da investigação, colocará em dúvida os trabalhos por ele desenvolvido. E neste meio, um deslize, poderá acabar com a carreira do perito com anos de experiência.

2.5 AS DIFICULDADES ENCONTRADAS PELO PERITO NA ANÁLISE FORENSE COMPUTACIONAL

Nos locais de crime, o perito é o responsável por orientar a equipe, quanto a apreensão dos equipamentos.

Segundo ELEUTÉRIO E MACHADO (2010), imediatamente devem ser tomadas providências para a preservação dos dados digitais, que incluem:

- impedir que pessoas estranhas à equipe utilizem os equipamentos de informática existentes sem a anuência/supervisão do perito;
- não ligar equipamentos computacionais que estejam desligados.

Durante a busca por equipamentos computacionais para apreensão, o perito deverá ter em mente o que deve apreender, de forma a diminuir o tempo de busca de evidências. Não adianta sair recolhendo impressoras e/ou scanners, se na verdade estamos procurando por vídeos que possam provar que naquele local está sendo utilizado para praticar crimes envolvendo pornografia infanto-juvenil.

Depois que se define o que deve ser apreendido, todos os equipamentos que forem apreendidos, deverão ser descritos com todas as suas especificações técnicas, para que seja garantido a cadeia de custódia.

O perito deverá ter o máximo de cuidado com os equipamentos que serão apreendidos, pois cada dispositivo requer uma forma diferente de ser acondicionado e transportado.

Mídias como CDs, DVDs, e Blu-Ray são sensíveis a poeira e eles podem riscar, dificultando a leitura dos dados. Discos rígidos devem ficar longe de campos

eletromagnéticos e não podem sofrer grandes impactos. Pen drives, cartões de memória, equipamentos de rede, impressoras e outros, devem ficar longe, da água, calor, poeira e vibrações excessivas.

Durante a fase de preservação dos dados, deve-se tomar cuidados especiais, pois simplesmente ligar um computador que tenha instalado um sistema operacional da família Microsoft Windows, os dados contidos são alterados, mesmo que o usuário não execute nenhuma operação (ELEUTÉRIO E MACHADO, 2010, p. 54).

Na extração de dados, o perito deverá ter um conhecimento e faro investigativo, pois além do grande número de arquivos a serem verificados, muitas informações referentes ao crime poderão estar oculto em arquivos através da esteganografia, juntamente com uma criptografia, o que dificulta ainda mais durante a análise dos dados.

O uso de ferramentas na extração e análise de dados são fundamentais para o perito quanto a facilidade e agilidade, mas que ainda dependem do bom preparo, técnicas e metodologias que o mesmo possui.

Em alguns casos, há a necessidade do perito, utilizar a técnica de quebra de senhas de dispositivos e arquivos, o que demanda tempo e grande potência do equipamento para tentar quebra-la.

A procura de um criminoso através da internet, torna-se um trabalho árduo, pois o indivíduo poderá estar em outro país, camuflando o seu endereço IP através de diversos servidores. O que pode ser frustrante quando não há cooperação com outros países, pois os dados mantidos pelas operadoras, poderão não estar mais acessiveis no momento da investigação.

> Outro empecilho é a legislação que se diferencia para cada nação, o que é considerado crime em outros países pode não gerar penalidade alguma aqui no Brasil e vice e versa, portanto, o julgamento de um criminoso de outro país vai depender principalmente da colaboração mútua entre os países. (TOLENTINO, SILVA, MELO, 2011, p. 35).

A elaboração do laudo, deverá ser o mais claro possível, evitando o máximo possível da utilização de termos técnicos, trazendo com objetividade os métodos e exames realizados e para a transparência do processo forense como um todo (ELEUTÉRIO E MACHADO, 2010).

Trabalhar com perícia computacional forense exige muita atenção e ética, pois em muitos casos, são encontrados outros tipos de evidência que provam outros crimes, mas o perito deverá manter o escopo da investigação e não divulgá-lo em seu laudo.

> Não sou eu quem diz isso, mas o próprio FBI, ou seja, pela boa prática, tenho de ter uma autorização para relatar novos fatos no meu laudo. (MILAGRE, 2007)

3 CONCLUSÕES

Diante das várias atividades que o Perito Forense Computacional terá que desempenhar, concluímos que esse profissional sempre deverá estar um passo à frente quanto as inovações tecnológicas, tendo uma visão aprofundada dos diversos sistemas computacionais, além de estar atento às legislações vigentes ao que diz respeito na apuração de evidências.

Vale ressaltar, que o Perito deverá estar continuamente buscando novos conhecimentos quanto as técnicas e ferramentas que possam ajudá-lo na busca de evidências e vestígios de crimes virtuais, no trabalho de “escovação” de bits.

Um bom procedimento é tentar saber como o criminoso virtual pensa, ou melhor, se colocar no lugar dele, assim o Perito terá uma chance maior de saber quais passos dar

durante um ataque, uma fraude. Como por exemplo em um crime de pornografia infanto-juvenil e nos diversos outros ilícitos que podem ser feitos através da tecnologia.

Enfim, são vários desafios e dificuldades que o Perito Forense Computacional deverá transpor, para que seu trabalho seja realizado de forma correta e ética. Onde os detalhes é que fazem a diferença, através de trabalho árduo e conhecimento de técnicas, metodologias e procedimentos capazes de definir as provas necessárias para uma investigação eficiente e eficaz.

REFERÊNCIAS

BOCCARDO, Davidson. SegInfocast #23 – Análise Forense Computacional II, 2015. Disponível em: <https://seginfo.com.br/2015/09/14/seginfocast-23-analise-forense-computacional-ii-2/>. Acessado em 18/07/2017.

ELEUTÉRIO, Pedro Monteiro da Silva; MACHADO, Marcio Pereira. Desvendando a Computação Forense. São Paulo: Novatec, 2010.

FRANCO, Deivison, A Atuação do Perito Forense Computacional na Investigação de Crimes Cibernéticos, 2016. Disponível em: <https://cryptoid.com.br/banco-de-noticias/atuacao-do-perito-forense-computacional-na-investigacao-de-crimes-ciberneticos/>. Acessado em 10/07/2017.

KLÉBER, Ricardo. Quanto ganha um Perito Forense Computacional? Disponível em: <http://segurancaderedes.com.br/artigo-quanto-ganha-um-perito-forense-computacional/>. Acessado em 17/07/2017.

MELO, Gilberto. A profissão do futuro: Como ser um perito digital, 2011. Disponível em: <http://gilbertomelo.com.br/a-profissao-do-futuro-como-ser-um-perito-digital/>. Acessado em 31/08/2017.

PEREIRA, Evandro Della Vecchia; FAGUNDES, Leonardo Lemes; NEUKAMP, Paulo; LUDWIG, Glauco; KONRATH, Marlom. Forense Computacional: fundamentos,

tecnologias e desafios atuais, 2007. Disponível em: <http://www.sbseg2007.nce.ufrj.br/documentos/Minicursos/minicurso_forense.pdf>. Acessado em 31/07/2017.

TOLENTINO, Luciano Cordova; SILVA, Wanessa; MELLO, Paulo Augusto M. S. Perícia Forense Computacional, 2011. Disponível em: <http://revista.faculdadeprojecao.edu.br/index.php/Projecao4/article/download/168/149>. Acessado em 20/07/2017.