ISSN 2447-1097

Direito & TI – Porto Alegre / RS www.direitoeti.com.br

A FRONTEIRA ENTRE A INVESTIGAÇÃO E A PERÍCIA DIGITAL

Evandro Della Vecchia[1]

RESUMO

O presente artigo tem por objetivo, dentro do contexto da investigação digital, abordar as diferenças entre a investigação criminal e a perícia digital, procurando deixar claro onde termina uma e onde começa a outra, com breves e objetivas definições. Assim, tem por finalidade evitar a confusão entre o que realmente é investigação e o que é perícia.

Palavras-chave: computação forense; forense digital; investigação digital; perícia digital.

INTRODUÇÃO

Há aproximadamente duas décadas as pessoas registravam compromissos, contatos e outras informações em agendas de papel, blocos de anotações, cadernos, e, raramente, em computadores. Na atualidade o contrário é verdadeiro, sendo comum que sejam utilizados *smartphones*, *tablets* e outros dispositivos eletrônicos compactos para registrar tais informações.

Desta forma, quando há a necessidade de investigação (tanto criminal, quanto cível), o conhecimento necessário passa a ser aquele que apenas profissionais da área de informática costumavam ter no passado. Isso é verdade não apenas para investigadores, mas também para os operadores do Direito.

O principal objetivo deste artigo é mostrar as diferenças entre "investigação" e "perícia digital". Desta forma, o leitor terá condições de saber em que situações a "investigação" consegue resolver um caso e em que momento a "perícia" é necessária.

De outra parte, não serão mostrados conceitos avançados ou muito técnicos. Tais conceitos e técnicas mais avançadas serão exploradas em análises (artigos) futuras.

1 A INVESTIGAÇÃO DIGITAL

O principal conceito a ser aprendido (na investigação digital) deve ser o endereçamento IP, o identificador único na rede mundial de computadores. Quando um usuário se conecta à Internet, ele recebe um endereço IP e este será o mesmo enquanto tal conexão existir. Ao se desconectar e conectar-se novamente, o endereço pode mudar. Os registros de conexão de cada cliente (endereço IP

[1] Autor do Livro **Perícia Digital:** Da investigação à análise forense; Perito Criminal no IGP/RS; Professor na PUCRS e em diversos cursos de pós-graduação na área de perícia criminal. evandrodvp@gmail.com.

recebido, a data e horário de início e fim de tal conexão) são de responsabilidade do provedor de acesso, e o tempo que tais registros devem permanecer armazenados (um ano) está regulado pelo Marco Civil da Internet[i].

Depois de conectado à Internet, o usuário pode utilizar diversos serviços, tais como redes sociais, e-mails, *blogs* etc. Tais serviços geralmente registram o endereço IP do visitante ou de quem enviou alguma mensagem, e-mail ou outro tipo de dado. O tempo de armazenamento do registro do endereço IP, data e horário de utilização do serviço também é regulado pelo Marco Civil da Internet (seis meses).

Por exemplo, se uma mensagem caluniosa for enviada através de uma rede social, através de um perfil falso, o investigador tem condições de solicitar (via ordem judicial) à empresa que provê o serviço, o endereço IP que o usuário possuía quando enviou a mensagem. Se for uma investigação cível, é extremamente recomendável que uma Ata Notarial seja realizada, mostrando ao tabelião, ou oficial escrevente, a mensagem caluniosa, o nome do perfil que enviou a mensagem e outras informações consideradas importantes. Desta forma, mesmo que a mensagem seja excluída, a Ata Notarial comprova que ela existiu e quando foi enviada, ou seja, foi dada fé pública àquele dado/informação encontrado na web.

Diante do endereço IP informado pela empresa fornecedora do serviço, é possível identificar o responsável, através de uma consulta às bases de dados públicas[ii]. Porém, na grande maioria das vezes, consegue-se identificar que o endereço IP pertence a um provedor de conexão à Internet. Isso ocorre porque, com exceção de poucas empresas (ou até mesmo usuários domésticos), a maioria dos consumidores de Internet recebem um endereço IP dinâmico, como já foi explicado anteriormente, e este endereço pertence a uma faixa que o provedor disponibiliza. Logo, somente o provedor poderia informar qual cliente possuía tal endereço IP em determinada data e horário.

Então, é necessária uma nova solicitação judicial, agora destinada ao provedor de conexão à Internet, solicitando os dados do cliente (nome e endereço, por exemplo). Após receber tais informações, o investigador tem condições de analisar se é necessário solicitar a realização de perícia de aparelhos de telefone celular, computadores, ou qualquer outro dispositivo que tenha conexão com a Internet (para o caso do exemplo mostrado).

Há situações em que é solicitado ao juiz um mandado de busca e apreensão e realizada uma análise no próprio local. Por exemplo, se houver a suspeita de uso de um aparelho de telefone celular ou de um *notebook* de alguém para o envio da mensagem pela rede social, o investigador pode ir até a casa do suspeito, com o mandado judicial. Se o suspeito admitir a culpa, entrar na rede social, mostrar que foi ele mesmo, pode evitar a busca e apreensão dos equipamentos. Caso contrário, a apreensão pode ser realizada para posterior envio à perícia.

2 PERÍCIA DIGITAL

A perícia digital, também conhecida como *computação forense*, entre outros nomes, pode ser realizada, basicamente: ao vivo (*live forensics*), com o equipamento ligado, em um flagrante; ou, após o desligamento do equipamento (*post mortem forensics*). Quando for ao vivo, deve haver um profissional qualificado (perito) para tal, pois o investigador pode não ter o conhecimento suficiente e pode inclusive contaminar a prova[iii].

Na perícia também podem ser realizadas tarefas como rastreamento de origem de e-mail, ou outras que podem ser realizadas na investigação[iv]. Mas como já foi mostrado na seção anterior, não teria o porquê enviar para perícia uma tarefa que poderia ser realizada na própria investigação, tornando o resultado mais rápido[v].

Diante dos equipamentos (no local da busca ou apreendidos), o perito tem condições de realizar os procedimentos, de acordo com as melhores práticas. Tais práticas recomendam, resumidamente: (1) identificação do material questionado; (2) proteção da mídia de armazenamento questionada contra gravação; (3) duplicação forense (espelhamento) dos dados para uma outra mídia; (4) análise dos dados espelhados; (5) elaboração do Laudo Pericial[vi].

A duplicação forense realiza a cópia até mesmo dos dados já excluídos. Desta forma, o perito pode realizar recuperação de arquivos ou fragmentos de arquivos excluídos, sem o perigo de danificar a mídia questionada. Somente se houver algum problema físico durante a duplicação dos dados, a análise pode ficar comprometida.

Além da recuperação de dados excluídos, outras atividades importantes na perícia incluem:

(1) Filtros de arquivos: busca por arquivos através da extensão, tipo, tamanho, nome, entre outros atributos;

(2) Busca por palavras-chave: busca por arquivos ou trechos de arquivos em toda a cópia dos dados, incluindo a possibilidade de expressões regulares (ex.: ####-#### significa um telefone com oito dígitos separado por hífen);

(3) Quebra de senhas: arquivos, partições de disco ou o disco inteiro podem estar criptografados. Peritos utilizam técnicas de quebra de senha através de diversas tentativas automatizadas, de palavras conhecidas de um dicionário ou dos dados pessoais, entre outras;

Para facilitar a realização de tais atividades periciais são utilizados *softwares* forenses. Quando o sistema de arquivos da mídia questionada é conhecido (utilizados em Windows, Linux etc.), existem diversos *softwares*, incluindo alguns gratuitos. Quando um sistema proprietário é analisado, como por exemplo um sistema utilizado em um *Digital Video Recorder* (DVR) de um fabricante específico, a

análise fica mais complexa, pois geralmente não há softwares que auxiliam. Desta forma, o perito deve estudar o sistema para verificar como analisar, ou tentar contato com o fabricante para solicitar ajuda.

CONCLUSÃO

O foco deste artigo foi mostrar a diferença básica entre a investigação (criminal) e a perícia digital, ou seja, onde termina uma e começa a outra (quando for necessária a segunda). Não foram mostrados conceitos ou atividades muito complexos, pois detalhes de técnicas de investigação e de perícia em meios digitais serão explorados em artigos futuros.

REFERÊNCIAS

BRASIL. Lei nº 12.965 de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. In: **Diário Oficial da República Federativa do Brasil**, Brasília, DF, 24 abr. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 07 set. 2015.

DELLA VECCHIA, Evandro. **Perícia Digital**: da investigação à análise forense. Campinas: Millenium Ed., 2014.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos: ameaças e procedimentos de investigação**. 2ª ed. Rio de Janeiro: Brasport, 2013.

WENDT, Valquiria Palmira Cirolini. A prova penal e a cadeia de custódia. In: Emerson Wendt; Fábio Motta Lopes. (Org.). Investigação Criminal: Provas. 1ed. Porto Alegre: Livraria do Advogado, 2015, v. 1, p. 51-64.

[i] BRASIL. Lei nº 12.965 de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. In: **Diário Oficial da República Federativa do Brasil**, Brasília, DF, 24 abr. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 07 set. 2015.

[ii] Uma consulta inicial pode ser realizada em <https://www.arin.net/>.

[iii] Sobre cadeia de custódia e prova penal ver mais em WENDT, Valquiria Palmira Cirolini. A prova penal e a cadeia de custódia. In: Emerson Wendt; Fábio Motta Lopes. (Org.). **Investigação Criminal**: Provas. 1ed.Porto Alegre: Livraria do Advogado, 2015, v. 1, p. 51-64.

[iv] Sobre a investigação de origem de e-mail, ver mais em WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos: ameaças e procedimentos de investigação**. 2ª ed. Rio de Janeiro: Brasport, 2013. Págs. 107-128.

[v] Sobre rastreamento de e-mail ver mais em DELLA VECCHIA, Evandro. **Perícia Digital**: da investigação à análise forense. Campinas: Millenium Ed., 2014. Págs. 08-15.

[vi] Sobre aprofundamento das etapas da perícia digital, ver em DELLA VECCHIA, Evandro. **Perícia Digital**: da investigação à análise forense. Campinas: Millenium Ed., 2014. Págs. 77-90.