ISSN: 2175-1897

Modelo de Laudo Forense Pericial Considerando Dispositivos de Redes de Computadores

Ricardo Oliveira Marques

Pontifícia Universidade Católica de Campinas – São Paulo – Brasil

ricardoemarques@gmail.com

Alexandre de Assis Mota

Pontifícia Universidade Católica de Campinas – São Paulo – Brasil

amota@puc-campinas.edu.br

Lia Toledo Moreira Mota

Pontifícia Universidade Católica de Campinas – São Paulo – Brasil

lia.mota@puc-campinas.edu.br

Resumo - A crescente evolução da tecnologia tem gerado preocupações de segurança das informações nas organizações. O ambiente de negócios corporativos está cada vez mais restritivo quanto à confidencialidade dos dados e sigilo das informações, sem necessariamente seguir uma padronização reconhecida internacionalmente. este trabalho objetiva propor modelo de laudo de perícia forense em ambientes cooperativos de redes de computadores, analisando uma situação de ambiente de perícia e tratando os elementos envolvidos em um processo de investigação. Espera-se que os resultados deste trabalho possam contribuir para reduzir as eliminações judiciais de laudos tecnicamente corretos por violação de questões formais de direito.

Palavras-chave: Gerência de Redes de Computadores, Perícia Forense, Laudo Pericial, Planejamento e Gestão de Redes, Segurança da Informação.

Abstract - The growing evolution of technology has created security concerns of information in organizations. The corporate business environment is becoming increasingly restrictive about data confidentiality, without necessarily following a internationally recognized standard. The objective of this work is to propose a forensic report model to assess computer networks cooperative environments, analyzing and treating the elements involved in a situation of expert investigation.

ISSN: 2175-1897

It is expected that the results of this study may reduce technically correct reports judicial eliminations by violations of formal questions of law.

Keywords: Computer Network Management, Forensic Expertise, Expert Report, Planning and Network Management, Information Security.

1. Introdução

Nos últimos anos o crescimento da utilização de computadores pela sociedade em geral aumentou de forma significativa, da mesma forma que a utilização desses computadores como meio para prática de crimes de tecnologia e o aumento dos riscos operacionais em empresas. A internet, com todas as suas ferramentas e possibilidades de integração, possibilita além de tudo a inclusão digital. Neste sentido, novos desafios se apresentam em relação às práticas forenses, cujo propósito é o de encontrar evidências que possam servir para apurar crimes ocasionados em empresas, de ordem pessoal ou judicial.

A importância da perícia é cada vez mais patente, pois diversas empresas têm avaliado que manter em segurança os segredos industriais têm se tornado um desafio cada vez mais difícil. Eventos cada vez mais freqüentes como, fraudes, invasão de *crackers*, avarias em rede, distribuição de vírus e abusos de uso de credenciais administrativas em sistemas, têm objetivos de subtração de algo alheio ou ainda de causar prejuízos operacionais. Por outro lado, existem diversas razões que levam a não investigação, como o alto custo associado e a ausência de recursos de infraestrutura. Na maioria das vezes pode ser mais fácil e rápido reconstruir o sistema do que investigar as causas que levaram à sua queda ou então ao roubo de alguma informação (COSTA, 2014; TANG & DANIELS, 2010). Para reduzir estes problemas, se faz necessário a alocação de equipes especializadas em analises forenses com conhecimentos técnicos e científicos para conduzir a investigação das suspeitas que envolvem o ambiente de tecnologia. Apesar da massificação do uso de computadores, as leis brasileiras não estão preparadas para tipificar os delitos envolvendo os computadores e redes; praticar um crime com uso da internet está cada vez mais fácil para quem detém um mínimo de conhecimento técnico, pois para adentrar ao espaço cibernético o criminoso, atualmente, precisa apenas de uma máquina conectada à Internet.

A investigação forense computacional surge neste contexto com o intuito de garantir que as evidências de crimes envolvendo computadores e rede sejam adequadamente preservadas, para serem apresentadas em juízo e para ser a parte de convencimento na materialidade de um delito. A dificuldade de manter a integridade das provas digitais surge como grande desafio, pois dependem de uma série de conhecimentos técnicos apropriados e a utilização de ferramentas específicas para análise e apuração de todos os rastros eventualmente deixados pelo criminoso nos dispositivos e redes (COSTA, 2014; TANG & DANIELS, 2010; MACHADO, et. al, 2014).

ISSN: 2175-1897

Embora seja de competência direta de profissionais da área tecnológica, o assunto da perícia forense ainda é difundido de forma incipiente em relação à formação profissional. Esse contexto incentiva e cria, então, oportunidades para a definição de um modelo de laudo forense pericial, de forma que sejam cobertos os itens necessários em uma análise pericial. Contudo, cabe salientar que a riqueza e caracterização das informações apresentadas dependem de uma série de fatores e de pessoas, denominadas equipe de perícia, preferencialmente de natureza interdisciplinar quanto à formação, que adicionalmente podem se beneficiar também com essa definição de um modelo de laudo, favorecendo o diálogo entre as diferentes áreas na medida em que estabelece um denominador comum para a coleta e formalização das informações.

2. Elaboração de Laudo Forense Pericial: Referencial Teórico e Métodos

Como responsável pelo laudo o perito deve envolver todas as pessoas que achar conveniente em sua investigação, de acordo com (REINALDO, 2007), para os casos onde a perícia é fundamentada para empresas, é importante considerar pessoal de (a) auditoria de sistemas, para certificar que as informações coletadas são coerentes e precisas; (b) segurança da informação, que tem atuação direta na investigação como um elo dos processos de segurança e tecnologias; e (c) setor jurídico, tem papel fundamental, pois tem conhecimentos das leis e também no auxílio para preparação do encadeamento de evidencias. Os itens que seguem, explicitados ao longo do trabalho, definem os capítulos do modelo proposto apresentado em formato de laudo, que poderá ser usado para laudos e pareceres técnicos de perito.

.

2. 1. Capítulo: Capa

A capa do laudo deve conter informações relevantes a respeito do número do laudo, data do laudo, tipo do documento, caso seja um laudo pericial ou caso seja um parecer técnico, dados do perito, como nome completo, algum organismo de classe que ateste sua formação (por exemplo, o registro no CREA, para profissionais liberais especialistas engenheiros), telefones de contato e e-mail, dentre outras informações que possam atestar positivamente o conhecimento técnico do perito perante a um juiz.

2.2. Capítulo: Contratantes

Devem ser detalhadas as informações dos contratantes ou requerentes do laudo, bem como os requeridos, cabe informar dados, como nomes, documentos de identificação, endereços residenciais e endereços do local investigado ou dispositivo. Cabe salientar, caso laudo tenha sido requisitado por um juiz, deve-se informar os dados do foro, bem como o nome do requisitante; caso o laudo tenha sido solicitado em formato de segredo de justiça, sugere-se informar apenas o foro responsável pela solicitação.

ISSN: 2175-1897

2.3. Capítulo: Localização

Neste capitulo, a intenção é apresentar um relato a respeito do local, ou os locais envolvidos com os elementos que compõe o objetivo do laudo. Cabe salientar que em casos que compõe mais de um local de analise em um mesmo laudo, recomenda-se que exista um mapa, ilustrando as distancias dos locais e tempo de locomoção, por veículo ou a pé. Como exemplo, na figura 1, item (a), ilustra-se uma imagem de um possível endereço onde será feita a analise pericial; o local marcado por um retângulo preto esconde o nome real do local, por questões de sigilo. Ainda na figura 1, item (b), exemplifica-se como ilustrar a imagem interna onde a mídia digital foi encontrada, bem como sua situação de uso no instante do início da perícia.

Figura 1 - (a) Local da análise; (b) Foto da mídia.

2.4. Capítulo: Preliminares ou Histórico

Para elucidar o histórico ou preliminares do trabalho, é necessário entender o que levou o pedido da perícia ou laudo. Ainda neste tópico, cabe registrar as informações a respeito da aquisição dos produtos periciados, tais como: notas fiscais, garantias, estado de conservação dos produtos e as atividades que foram feitas pelos donos do produto antes do incidente.

2.5. Capítulo: Metodologia Utilizada, Normas, Referências, leis e decretos

Neste capitulo deve ser descrito como foram executados os métodos da perícia, além das ferramentas utilizadas. De acordo com (VECHIA, 2014) os itens pertinentes que devem ser citados na metodologia utilizada são:

- Tipo de análise: usualmente descrita como *post mortem forensics* - forense após morte, que trata a forense nos equipamentos ou ambiente após ter ocorrido algo.
- Tipo de cópia: preferencialmente bit a bit, ou seja, cópia de todos os dados armazenados em uma mídia.

ISSN: 2175-1897

- Tipos de filtros utilizados: item que tipifica a busca por documentos eletrônicos tipificados por extensões (*.doc, *.docx, *.pdf) e arquivos de armazenamento de e-mails em lote do tipo (*.pst e *.ost).
- Ferramentas de softwares utilizadas: item que descreve as mesmas, como, por exemplo: "... *utilizou-se a ferramenta DEFT LINUX, trata-se de uma ferramenta de software e adquirida pelo perito...*".
- Garantias de integridade: item que descreve as mesmas, como, por exemplo: *"... antes do início do procedimento de cópia, garantiu-se através do ferramental utilizado que não houvesse alteração nos dispositivos de armazenamento de forma que não gere alterações nas mídias. Para que fosse possível ter esta garantia, um hash de assinatura digital foi gerado, conforme segue: 1aabac6d068eef6a7bad3fdf50a05cc8*".
- Mídias analisadas: item que descreve as mesmas, como, por exemplo: *"... foram analisadas as mídias indicadas através da figura 1-b, onde constam a mídia do computador e a mídia de armazenamento externa, denominadas discos rígidos...*"
- Conversão de formato: descreve as ações tomadas, como, por exemplo "*... formatos de arquivos não descritos nos tipos de filtros utilizados neste capitulo, não foram identificados e/ou convertidos para análise...* ".

2.6. Capítulo: Objeto do Laudo Pericial ou Parecer Técnico

Deve-se considerar neste tópico, as questões que necessitem provar, os motivadores para a investigação e elaboração do laudo ou parecer técnico, bem como o que foi observado de forma resumida, cabe informar ainda, se ocorreram visitas ao local, horário e até testemunhas que presenciaram o fato ou cena do crime em conjunto com o perito. A figura 2 demonstra um modelo de como pode ser registrado o objeto do laudo pericial em um caso de perícia de danos causados por deleção e subtração de dados eletrônicos.

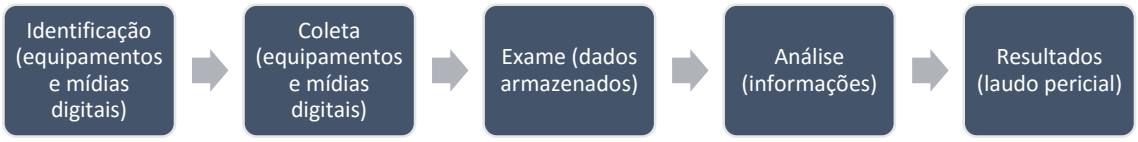
Para elencar os aspectos do objeto envolvido no laudo pericial, foram tratados cinco passos para elaboração e coleta das evidencias. De acordo com (VECHIA, 2014) estes passos ou etapas tratam uma cadeia seqüencial para obtenção das provas digitais, e preservação da cadeia de custodia, conforme a figura 3. Os resultados de cada objetivo citados nessa figura, serão discutidos nos próximos capítulos, cabe salientar que estes passos são amplamente reconhecidos por peritos e sendo um modelo para levantamento, coleta e preservação das evidencias.

Figura 2 - Descritivo do objeto ou parecer.

ISSN: 2175-1897

Elaboração e execução de serviços de perícia em dispositivos de armazenamento de dados (PenDrive), estavam localizados no momento da perícia no endereço Av: Estados Unidos 1301, apartamento 22, Campinas, SP, CEP 13099-000, destacado através desta **PERICIA DE DANOS CAUSADOS POR DELEÇÃO E SUBTRAÇÃO DE DADOS ELETRONICOS.** Observou-se que o dispositivo estava com lacres elaborados pelo fabricante intactos, constatou-se, que o dispositivo estava armazenado no veículo Volkswagen GOL de placas DDD-0000, no endereço supra citado. Eu, Ricardo Oliveira Marques, especialista em redes de computadores, designado pelo contratante para execução do laudo pericial, com objetivo de antecipação de provas, "Ad Perpetuam Rei Memorian" em observância a fase de subtração dos dados, tendo procedido aos estudos e diligencias que se fizeram necessárias, transcrevo o respectivo trabalho.

Figura 3 - Processo de perícia forense adaptado.



2.7. Capítulo: Identificação ou Tipologia

A tipologia cobrirá as informações sobre a descrição detalhada do que está sendo analisado, que devem incluir, data de aquisição, o fornecedor ou onde foi adquirido o item, informações sobre o número da nota fiscal, o descritivo do material e a situação que o equipamento estava no momento da perícia, para este último cabe informar se o equipamento estava com embalagens e lacres do fabricante, ou ainda sem embalagens e lacres. Na figura 4, adotou-se como modelo a análise de apenas dois itens no ambiente de perícia, contudo, pode-se ainda incluir uma coluna adicional informando e tipificando cada equipamento, isto é importante para casos de muitos equipamentos para análise.

Cabe aqui também informar os detalhes pertinentes a localização do equipamento, bem como relatório fotográfico da situação onde se encontrava o item no momento da perícia. Sugere-se também que cada passo representado do escopo de coleta seja tipificado com uma imagem representando o inicio do da execução e o resultado da ação de um comando submetido ao sistema.

Figura 4 - Informações sobre o dispositivo

Data de aquisição	Fornecedor	Nota fiscal	Descritivo	Situação do equipamento
01/01/2015	Submarino.com	10090	HD Externo, Seagate freagent goflex, Capacidade 1TB	Sem Embalagem
01/02/2015	Submarino.com	10091	HD Externo, Seagate freagent goflex, Capacidade 3TB	Lacrado pelo fabricante, sem uso

2.8. Capítulo: Coleta

Deve-se descrever, neste capitulo, como ocorreu a coleta das mídias digitais e computadores, dentre outros. Cabe ao perito neste instante, definir a melhor estratégia para não corromper as provas digitais, preservar o ambiente além de garantir que as informações coletadas não sofram qualquer alteração. Ocorre de forma similar à praticada em locais de crimes convencionais, onde as evidencias e provas ali existentes devem ser preservadas e nos meios digitais este procedimento não é diferente. O exame está relacionado com a coleta física

ISSN: 2175-1897

e coleta lógica dos dados, que foram feitas no mesmo local citado na figura 2; contudo, o processo de trabalho técnico para coleta lógica dos dados deve seguir conforme o exemplo descritivo dado pelos itens (1) a (5) que seguem, e devem considerar os horários pontuais de cada operação e o que tecnicamente foi efetuado pelo perito responsável.

1) As 9:40hs foram ligados em ato continuo o monitor e CPU sobre a mesa.

2) As 9:42hs foi inserido uma mídia digital CD no respectivo drive do equipamento.

3) As 9:43hs foi conectado um cabo ligando a CPU a um HD externo.

4) As 9:45hs o sistema identificado por DEFT LINUX, encontrava-se iniciado.

5) As 9:47hs buscou-se um “LX terminal”, escrevendo os seguintes comandos na tela:

a) df –kh, em seguida ENTER (objetivo é mostrar os dispositivos conectados ao equipamento).

b) fdisk /dev/sda, em seguida ENTER (mostra configurações do dispositivo /dev/sda)

c) fdisk /dev/sdb, em seguida ENTER (mostra configurações do dispositivo /dev/sdb)

d) mkdir –p /mnt/sda /mnt/sdb, em seguida ENTER (objetivo é criar diretórios para cópia da imagem dos discos)

e) mount –o ro /dev/sda2 /mnt/sda2, em seguida ENTER, (objetivo é acessar o disco que necessita de imagem pericial)

f) cyclone, em seguida ENTER, (aciona a aplicação do sistema que efetua a imagem pericial.

g) /dev/sda2, em seguida ENTER, (indica o disco rígido que necessita da imagem pericial)

h) /mnt/sdb1/caso-joao-modelo-silva.img, em seguida ENTER, (objetivo de indicar onde será copiada a imagem do disco rigido).

i) 1, em seguida ENTER (com objetivo de indicar o tipo de cópia que será feita).

j) Y, em seguida ENTER (com objetivo de confirmar as opções escolhidas e iniciar o processo de cópia forense).

k) As 12:45hs a cópia forense terminou com assinatura digital com o numeral:

MD5: ede1cf2904a163f7df28c27358d113d6

SHA1: fb3b51278f3be658ec5a8d822b5c40285750a450

Respeitados todos os quesitos da coleta, cabe registrar a importância de registro fotográfico no laudo, que elucida e complementa cada uma das ações descritas neste capítulo. Estas imagens não estão expostas neste artigo. Em seguida, deve ser efetuado o exame das cópias das mídias.

2.9. Capítulo: Exame

Esta etapa trata o exame das informações coletadas e geradas através do passo anterior, consiste em garantir que o material coletado esteja preservado para aplicação das técnicas de busca e pesquisa e descobertas de dados ocultos. O foco principal é identificar a integridade da cópia da imagem digital gerada, para que possa dar início ao processo de análise. Para validar a

ISSN: 2175-1897

integridade da imagem, os itens (1) a (4) que seguem apresentam uma proposta de procedimento e registro de ações correspondentes.

1) Utilizar-se de um novo computador com o mesmo sistema identificado por DEFT LINUX.
2) As 16:40hs este computador foi ligado.
3) As 16:45hs buscou-se um “LX terminal”, com objetivo da validação das assinaturas e em um ato continuo foi escrito os seguintes comandos na tela:
   a) md5sum/mnt/sdb1/caso-joao-modelo-silva.img (com objetivo de validar a assinatura digital, de acordo com o padrão de algoritmo de md5sum).
   b) sha1sum/mnt/sdb1/caso-joao-modelo-silva.img (com objetivo de validar a assinatura digital, de acordo com o padrão de algoritmo de sha1).
4) Os resultados dos comandos anteriores das assinaturas digitais devem coincidir com o citado na etapa de coleta item (5, k), pode-se afirmar que a cópia forense foi executada com sucesso.

Com o exame dos insumos coletados e a validação da sua integridade deve-se proceder com a análise e busca dos insumos dentro da imagem forense efetuada.

2.10. Capítulo: Análise

Diante do exame, o perito neste capitulo deve apontar como foi feita a análise e especificar o que foi buscado na imagem forense, existe um número muito grande de arquivos que são utilizados pelos sistemas operacionais e não cabe ao objeto da análise identificar para este laudo pericial estas informações. Contudo, salienta-se que em casos de infecção ou propagação de vírus, a análise deve percorrer todos os arquivos do sistema operacional. A análise desta pericia é feita com a aplicação de filtros de busca por documentos eletrônicos tipificados por extensões (*.doc, *.docx, *.pdf) e arquivos de armazenamento de e-mails em lote do tipo (*.pst e *.ost). Os itens (1) a (7) que seguem apresentam uma proposta de procedimento e registro de ações correspondentes à citada análise.

1) As 18:35hs, utilizando o mesmo recurso de computador e sistema operacional identificados no item de coleta, os seguintes comandos na tela.
2) mkdir/discopericia(com objetivo de criar uma área para tornar acessível a imagem forense para análise).
3) mount –o loop /mnt/sdb1/caso-joao-modelo-silva.img /discopericia (com objetivo de tornar acessível a imagem forense para análise).
4) mkdir /pendrive-recuperacao(com objetivo de criar uma área temporária para cópia dos arquivos recuperados).
5) mount /dev/sdc1 /pendrive-recuperacao(com objetivo de inserir um pendrive para colocar todos os arquivos para recuperação).
6) find /discopericia -iname '*.doc' -o -name '*.docx' -o -name '*.pdf' -o -name '*.pst' -o -name '*.ost' -execcp '{}' /pendrive-recuperacao \; (com objetivo de buscar todos os arquivos existentes na imagem periciada, sem diferenciar maiúsculas e minúsculas, considerando os dados excluídos do sistema, lixeiras e copia-los para o diretório de um pendrive externo montado sob o nome de /pendrive-recuperacao).

ISSN: 2175-1897

7) ls -la /pendrive-recuperacao(com objetivo de listar tudo o que foi copiado para o pendrive).

Todos os documentos que apareceram no diretório citado no item 2.6, figuram a recuperação pericial. O próximo capitulo deve abordar os resultados desta investigação limitando-se ao escopo que foi tipificado.

2.11. Capítulo: Resultados

Neste item, as evidencias da existência dos dados digitais, devem ser exploradas e informadas, cabe ao perito dizer o que encontrou, além de indícios de dados para os casos onde as informações estiverem visíveis, porém corrompidas e claro para os casos íntegros. Se forem encontrados arquivos tipificados por extensões (*.doc, *.docx, *.pdf, *.pst, e *.ost), tais arquivos devem ser listados com assinaturas digitais, utilizando o mecanismo citado no item de exame (3), criadas pelo perito que assina o laudo. Cabe salientar que todos estes arquivos devem estar íntegros, acessíveis de forma a garantir e validar as evidências.

2.12. Capítulo: Garantias Envolvidas

Este capítulo descreve as garantias dos trabalhos de forense digital, que permeiam a integridade dos arquivos e dados encontrados nas buscas. Essa garantia deve ter um mecanismo que permita checar que os arquivos encontrados são os mesmos e que, em hipótese alguma, sofreram qualquer tipo de alteração, seja por parte do perito ou das pessoas que tiveram ou poderão ter acesso às mídias digitais. Para isto, justifica-se o uso da atribuição de assinaturas digitais a todos arquivos relevantes à perícia. As assinaturas digitais para cada arquivo são importantes para proteger a integridade dos dados periciados. Isso porque caso ocorra qualquer tipo de alteração ou violação, a assinatura digital é alterada, como uma espécie de marca, única para cada tipo e características de arquivo.

2.13. Capítulo: Conclusão ou Resposta aos Quesitos e Apontamentos

Este capítulo conclui as ações descritas no laudo em pauta tratando as manifestações dos requerentes; deve-se informar se existiam arquivos que foram deletados de forma sumaria e recuperados no procedimento de perícia. Deve ser também informado se é possível ou não afirmar a autoria de uma eventual a remoção, verificando se o equipamento em questão utiliza (ou não) padrões de usuário e senha para identificação. Como parte do escopo de recuperação de dados, uma cópia de toda mídia digital deve ser efetuada e ser devidamente identificada através de assinatura digital, como, por exemplo: SHA1-da39a3ee5e6b4b0d3255bfef95601890afd80709. Devem ainda ser informadas as possibilidades de existência de patologias provenientes de intrusos, como vírus, salientado que as cópias da imagem digital são ainda

ISSN: 2175-1897

submetidas a um processo de busca por vírus e também analisada por ferramentas que identificam o comprometimento da integridade dos arquivos, concluindo explicitamente se nada foi encontrado. Finalmente, devem necessariamente ser identificadas as formas de deleção dos arquivos (manualmente, por exemplo).

2.14. Capítulo: Bibliografia

Este capítulo apresentará, de acordo com as normas em vigência, as referências que especificam as fontes consultadas como base para a elaboração do laudo, e que constituem o arcabouço técnico-profissional de embasamento legal do profissional que assina o Laudo.

2.15. Capítulo: Anexos

Este capítulo deverá apresentar os elementos necessários para o completo entendimento do conteúdo do laudo, mas que não precisam constar no corpo principal do documento, tais como: imagens adicionais, listagens, assinaturas digitais, lista de equipamentos, lista de domínios e usuários, etc.

3. Considerações Finais

Espera-se, com base no modelo proposto, apresentar uma contribuição para que os profissionais de Tecnologia da Informação e Comunicação e Engenharias afins possam obter maior eficiência nas condições de pericia de dispositivos eletrônicos, que permeiam questões legais e de direto, além dos conteúdos técnicos e, portanto, devem ser observadas de forma criteriosa. Este modelo apresenta também os aspectos relevantes da perícia pontual em discos rígidos e busca por elementos armazenados e excluídos propositalmente. Tratou-se também da garantia da integridade das provas digitais, além de seguir um processo através de uma linha do tempo (apresentada na figura 3), de modo que em juízo o laudo não sofra questionamentos quanto a sua validade e formas de trabalho do perito ou da equipe de perícia.

Referências

REINALDO, N.G. (2007). *Forense Computacional Corporativa*, ed. Brasport, 1ª Ed.

VECHIA, Evandro Della (2014). *Pericia Digital da Investigação à Análise Forense*, ed. Millennium.

COSTA, Roberto Costa (2012). *Metodologia e Arquitetura para Sistematização do Processo Investigatório de Análise da Informação Digital*. Dissertação (Mestrado), UNIVERSIDADE DE BRASILIA.

MACHADO, T. G. ; MARQUES, R. O. ; MACHADO, L. F. ; MOTA, Alexandre de Assis ; MOTA, Lia Toledo Moreira (2014). *Simulação de ataques em uma rede sem fio IEEE*

ISSN: 2175-1897

802.11 em ambiente urbano. In: Anais do I Simpósio do Programa de Pós-Graduação Stricto Sensu em Sistemas de Infraestrutura Urbana - SPInfra 2014, Campinas (SP).

TANG, Y; DANIELS, T.E. (2010). *A research configuration for a Digital Netwotk Forensic Lab*. In. Proceedings of IEEE Third International Workshop on Systematic Approaches to Digital Forensic Engineering.