DESAFIOS DA COLETA DE DADOS E EM EVIDÊNCIAS DIGITAIS

LILIAN NORONHA NASSIF
Doutora em Ciência da computação. Especialista em Engenharia de Telecomunicações, Segurança da Informação e *Crime Scene Investigation*. Professora do programa de Mestrado em Segurança Pública e Cidadania da Universidade do Estado de Minas Gerais (UEMG).

Resumo: A investigação de crimes que utilizam dispositivos eletrônicos exige um mecanismo adequado de coleta e extração dessas evidências. Se o investigador ou policial não apreende provas digitais de forma a serem usadas em um processo forense, algumas informações importantes podem ser perdidas, e os juízes podem descartar provas do caso porque a apreensão ou a extração foram inadequadas. A correta apreensão de forense digital envolve a preparação de profissionais das áreas de direito, de segurança policial e de informática. O artigo apresenta importantes desafios enfrentados durante a coleta e extração de dados de evidências em diferentes perspectivas de lugares. A pesquisa abrange os principais ambientes virtuais e presenciais, objetivando elencar obstáculos técnicos e preocupações com privacidade e integridade. Os resultados aqui obtidos podem ser incluídos em Procedimentos Operacionais Padrão (POP) das equipes de forense digital, estimulando a padronização e a definição de melhores

práticas neste campo da criminalística moderna.
Palavras-chave: Evidência digital. Forense. Apreensão. Extração de dados.

Abstract: Crime investigation involving electronic devices demands an appropriated mechanism of evidence acquisition and data extracion. If the investigator or police officer does not acquire digital evidence to use in a forensic process, some important information can be lost and judges can discard the case because seizure was inadequate. A correct seizing of digital evidences englobes preparation of professionals of law, police, and information technology. This paper presents important challenges faced during evidence collection and data extraction in different perspectives of places. The research covers the main virtual and presencial environments, aiming to list technical obstacles and concerns with privacy and integrity. The results obtained here can be included in the standard operational procedures (SOPs) of digital forensic teams, stimulating best practices standardization in this modern criminology field.
Keywords: Digital evidence. Forensic. Seizing. Data extraction.

1 INTRODUÇÃO

Uma evidência digital pode ser aceita em um tribunal desde que permaneça confiável desde a sua apreensão. O primeiro interventor da evidência digital e o especialista em evidência digital[1] precisam estar preparados antes mesmo do crime existir. Os promotores e delegados devem entender como os aspectos técnicos podem influenciar no processo legal, por exemplo que tipo de evidência digital coletar e quanto tempo a evidência requer preparação e análise. Os dispositivos smartphones e notebooks são amplamente usados e frequentemente revelam conversas, fotos e vídeos particulares. O momento da coleta de evidências é crucial e as ferramentas forenses devem ser cuidadosamente selecionadas com antecedência.

A área forense digital é um dos novos campos da criminalística moderna e vários juízes ainda possuem dúvidas sobre o entendimento da preservação das evidências. Os Procedimentos Operacionais Padrões (POP) devem ser definidos e seguidos durante a fase de coleta de evidências digitais, incluindo o uso de materiais específicos, como bolsas antiestáticas, luvas para retirada de discos rígidos (HDs) e bolsas Faraday para armazenar telefones celulares, para bloqueio de sinais eletromagnéticos e impedimento de acesso remoto ao celular.

A análise forense digital carece de uma reflexão atualizada sobre os desafios da coleta de evidências digitais. Sem uma clara compreensão dos principais obstáculos, vários erros podem ser cometidos, desde a cena do crime até o laboratório forense.

Este artigo apresenta uma lista detalhada de problemas na coleta

[1] Especialista em Evidência Digital (DES): indivíduo que pode executar tarefas de um DEFR e possui um conhecimento especializado, aptidão e habilidade para lidar com uma ampla gama de questões técnicas.

de evidências digitais, definindo referências para inclusão em procedimentos de melhores práticas, visando a integridade dos dados. Os promotores, policiais e técnicos em informática devem ter uma visão semelhante dos problemas relativos à coleta de evidências digitais, pois formam elos de atuação complementar nos procedimentos de apreensão, exame e investigação. Esta interatividade contribui para a melhoria contínua de cada operação deflagrada.

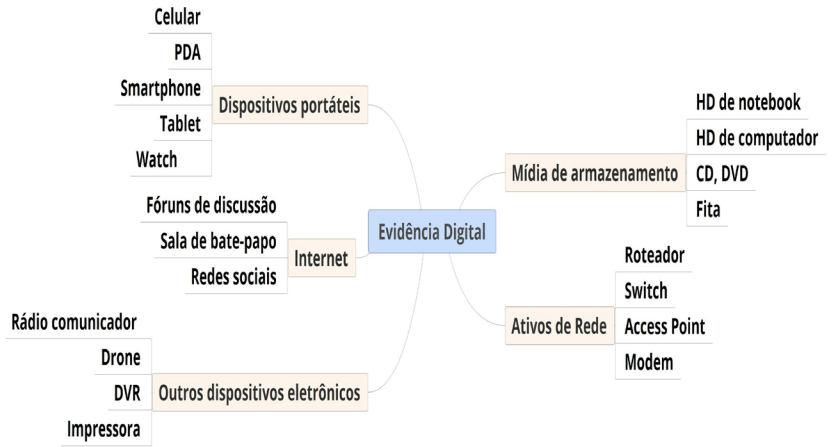
Este artigo está organizado da seguinte forma: a Seção 2 apresenta algumas particularidades das evidências digitais. A Seção 3 apresenta locais onde as evidências digitais podem ser coletadas, considerando sites reais e virtuais. A Seção 4 relaciona desafios na coleta de evidências e a Seção 5 conclui o artigo.

2 Evidência Digital

Evidência digital é qualquer informação de valor probatório que seja armazenada ou transmitida em formato digital. Os tipos de evidências digitais aumentam continuamente. Uma lista não exaustiva de evidências digitais é apresentada pelo National Institute of Justice (2007). A Figura 1 organiza-as em grupos, de acordo com a similaridade dos exames necessários.

As evidências agrupadas como mídia de armazenamento e dispositivos portáteis merecem uma atenção especial, considerando-se que frequentemente são o foco de investigação devido à sua ampla utilização.

Figura 1: Evidências digitais em agrupamentos por similaridade



Fonte: Elaboração própria, 2018

O smartphone é um acessório inseparável hoje em dia para todos. É equipado com todos os tipos de tecnologia para registrar fotos, conversas, navegações de internet, notas, chamadas e localizações, dentre outros, conforme detalhado pelo *International Data Corporation* **(**2018). Todo o tipo de interação e movimento pode ser recolhido a partir de um smartphone pessoal. Isso pode explicar o quão valiosa é essa evidência digital e os cuidados necessários para coletá-la. Se o smartphone não estiver devidamente desligado e todos os tipos de redes não estiverem desconectados, é possível que todas as informações possam ser apagadas antes mesmo de chegar ao laboratório forense (NIJ, 2008).

A mensagem instantânea (IM) é uma das aplicações mais importantes usadas para organizar crimes hoje em dia. Devido à possibilidade de comunicação com privacidade implementada por algoritmos de criptografia, as mensagens instantâneas, como o WhatsApp, podem fornecer excelentes oportunidades

para a sociedade, mas também podem ser usadas para a prática de delitos (ZHANG *et al.*, 2015).

O HD é outra importante evidência digital que pode ser removida fisicamente do desktop ou notebook para análise posterior no laboratório forense. No entanto, os investigadores geralmente não obtêm informações voláteis durante um procedimento de apreensão. Informações voláteis contêm hora do sistema, usuários conectados, arquivos abertos, informações de rede, histórico de comandos e memória de processo, por exemplo. Essas informações podem ser obtidas se o computador for encontrado ligado (NIJ, 2008). Evidências digitais geralmente são apreendidas após outras fases de investigação, como escutas telefônicas.

Após a obtenção de provas digitais, todos os envolvidos estão alarmados. A apreensão de evidências digitais é importante para validar algumas investigações e deve ser tratada com extremo cuidado. Após essa fase, os investigados tendem a eliminar todos os tipos de provas, e a evidência digital pode ser a última chance para um caso de sucesso.

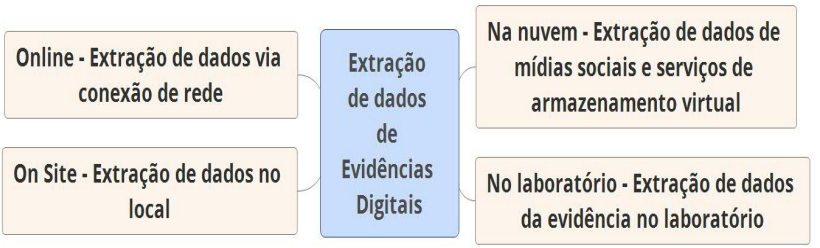
3 Lugares para apreensão e extração de dados e evidências digitais

Investigadores e policiais podem coletar evidências *on site* e *on-line* e podem enviar provas para o laboratório forense. Quando um investigador coleta evidências no local (*on site*), o investigador está fisicamente presente na cena do crime. Quando um investigador coleta evidências *on-line*, o investigador está adquirindo dados usando uma rede ou extraindo dados da nuvem. No laboratório, mais precisamente no laboratório forense, os investigadores podem extrair todo tipo de informação de uma evidência digital previamente apreendida.

A Seção 4 apresenta os desafios envolvidos para cada local.

Ao capturar computadores *on site*, eles podem estar ligados e, nesse caso, é possível obter dados voláteis da RAM (*Random Access Memory*). Também é recomendado fotografar a tela. A Figura 2 resume onde a coleta de evidências ocorre.

Figura 2: Extração de dados de evidências digitais



Fonte: Elaboração própria, 2018

Em alguns casos, é possível adquirir a imagem da evidência *on site*. Esse procedimento não remove a evidência do local original e uma cópia *bitstream* da evidência e sua função *hash* são enviadas para o laboratório forense para posterior análise.

4 Desafios para apreender e extrair dados de evidências digitais

Esta seção apresenta desafios de acordo com os diferentes locais onde a evidência digital está sendo coletada, considerando sua apreensão e extração de dados, conforme apresentado na Figura 2.

4.1 Desafios na coleta de evidências on site

Quando os investigadores chegam à cena do crime ou em um ambiente onde os dispositivos eletrônicos utilizados pelos investigados estão disponíveis, é necessário tomar decisões

sobre como coletar evidências. Alguns desafios são abaixo referenciados:

Impossibilidade de remoção física: Se o *hardware* for de alta plataforma, provavelmente é impossível remover a evidência do site. Nesse caso, o espelhamento da evidência ou alguma seleção de dados deve ser feita no site.

Tamanho do disco: Uma cópia de evidência exige um disco de pelo menos o mesmo tamanho, se nenhuma compactação for usada. Em algumas situações é difícil calcular previamente a quantidade de discos necessária para espelhar uma evidência.

Quantidade de evidências: Se a quantidade de evidências disponíveis na cena do crime for numerosa, o investigador deve ter vários equipamentos do mesmo tipo, por exemplo várias ferramentas de clonagem de disco.

Tempo de coleta: O tempo de coleta de evidências pode ser restrito. Este desafio é aumentado pelas dificuldades já apresentadas acima, por exemplo o tempo é curto, o tamanho das evidências é grande e é impossível remover as evidências do local original.

Conectividade: O investigador precisa interagir com a evidência usando uma conexão cabeada ou *wireless*. Uma grande variedade de cabos deve estar disponível para integrar o equipamento forense à evidência digital. Isso é particularmente difícil para os telefones celulares por causa da falta de padrão de interoperabilidade.

Esses desafios devem ser combinados para cada caso. Além disso, a plataforma de *hardware* deve ser considerada, por exemplo: plataformas de computador alta e média (*mainframe, blade* e virtualização), plataforma baixa de computador (desktop, laptop e tablet) e celular.

4.2 Desafios em coletar evidências on-line

A coleta de evidências *on-line* apresenta vários desafios, como descritos a seguir:

Taxa de transferência: Na aquisição de evidências *on-line*, o investigador copia todas as informações do equipamento suspeito usando uma rede. No entanto, o *throughput* da rede é inferior à aquisição de dados local, tornando o processo mais lento do que a aquisição *on site*.

Alteração de dados: Durante a aquisição de dados *on-line*, o usuário local pode modificar os dados. Tal situação pode resultar em problemas de imagem de disco, porque os arquivos podem estar em uso durante a cópia.

Desconexão da máquina: A aquisição de dados *on-line* pode ser interrompida a qualquer momento se a máquina suspeita estiver desconectada da rede por qualquer motivo. Este incidente resulta em um cancelamento abrupto do processo.

Reconhecimento de coleta de dados: Durante a aquisição de dados, o usuário local pode perceber que uma cópia remota está ocorrendo e, consequentemente, ele pode modificar seu comportamento. Ele pode excluir ou modificar arquivos, bloquear

o acesso remoto ou desativar a evidência, por exemplo. Isso pode impedir uma aquisição de dados confiável.

Problemas de rede: Quando a aquisição *on-line* ocorre em uma rede local, a transferência maciça de dados entre o equipamento do investigador e a máquina suspeita pode degradar o desempenho da rede. Outros usuários da mesma rede podem enfrentar problemas em atividades comuns, como baixa latência para acessar a Internet, abrir um documento remoto ou imprimir um arquivo.

4.3 Desafios em coletar evidências na nuvem

A coleta de dados na nuvem é mais difícil do que a aquisição de dados no local e a aquisição de dados *on-line*. A computação em nuvem é definida como um modelo para acesso conveniente a recursos compartilhados remotos (MELL; GRANCE, 2011).

A análise forense da nuvem é definida como um subconjunto da análise forense da rede, pois é baseada em acesso extensivo à rede. A aquisição de dados de evidência na nuvem pode ser aplicada em serviços de nuvem e em mídias sociais. Os desafios na coleta de evidências de cada um deles são descritos a seguir.

O modelo de negócios disponível para nuvens oferece serviços com diferentes controles de recursos. Os principais tipos de nuvem são agrupados em três categorias: *Software* como serviço (SaaS), plataforma como serviço (PaaS) e infraestrutura como serviço (IaaS) (ZHANG; CHENG., 2010). O SaaS fornece aplicativos sob demanda pela Internet. Alguns exemplos de SaaS incluem o

Google Drive (QUICK; CHOO, 2014) e o Rackspace. A PaaS oferece recursos de camada de plataforma, incluindo suporte a sistemas operacionais e estruturas de desenvolvimento de *software*. Alguns exemplos de PaaS incluem o Windows Azure (AZURE, 2015) e o Google App Engine (GOOGLE, 2018). IaaS refere-se ao provisionamento sob demanda de recursos de infraestrutura, geralmente máquinas virtuais. Alguns exemplos de IaaS incluem o Amazon EC2 (AMAZON, 2015) e o GoGrid (GOGRID, 2018).

A seguir, são apresentados importantes desafios enfrentados durante a coleta de evidências nos serviços de nuvem e discutidos em mais detalhes em Zawoad e Hasan (2013):

Dados voláteis: No IaaS, o usuário pode desligar a Máquina Virtual e, como consequência, todos os dados voláteis são perdidos. Embora os dados possam ser sincronizados em um armazenamento persistente, geralmente os usuários não contratam esse serviço, principalmente quando desejam explorar essa vulnerabilidade.

Confiança no provedor de serviços: Quando a investigação emite uma intimação para um provedor de serviços para reunir informações sobre um usuário, ocorrem alguns problemas de confiança. O técnico que trabalha no provedor de serviços de Internet (ISP), SaaS, PaaS e IaaS será o responsável por coletar as informações. No entanto, geralmente não é um investigador forense e nem sempre é possível garantir a integridade dos dados coletados para apresentação em um tribunal.

Privacidade: Em uma estrutura de nuvem, muitos usuários

podem compartilhar os mesmos recursos físicos. A imagem de um HD na nuvem pode violar a privacidade de outros usuários. É necessário provar que os dados suspeitos não estão misturados com dados de outros usuários.

Problemas de registro: Logs diferentes em um ambiente de computador podem ajudar na reconstrução de um crime cibernético. No entanto, reunir logs diferentes na nuvem às vezes pode ser impossível. Os problemas de log estão relacionados à volatilidade dos logs em máquinas virtuais, várias camadas de log (banco de dados, sistema operacional, rede), várias pessoas acessando logs (desenvolvimento, administradores de rede) e a falta de um formato de log padrão.

Cadeia de custódia: A cadeia de custódia na nuvem é questionável porque várias pessoas podem ter acesso às evidências e o processo depende do provedor de serviços.

Legislação sobre dados além das fronteiras: O armazenamento de dados de um provedor de serviços pode ser distribuído em todo o mundo. O invasor pode acessar o serviço de computação em nuvem de um país e os dados podem ser armazenados em um data center em outro país. Diferentes leis podem ser aplicadas a esta situação, e o investigador deve obter os dados considerando todos esses aspectos.

4.4 Mídia Social

A coleta de dados nas mídias sociais pode ser uma fonte valiosa de informações durante uma investigação. No entanto, sem

ferramentas forenses adequadas, é difícil reunir provas de maneira a serem aceitas em juízo. Alguns estudos e casos reais estão ajudando a definir as melhores práticas para essa situação.

Segundo Gogrid (2018), os principais tipos de mídias sociais são classificados nos seguintes grupos:

1) Redes sociais: este serviço consiste em um perfil de usuário que interage privada e publicamente com outras pessoas (por exemplo, Facebook e LinkedIn);

2) Compartilhamento de mídia: este serviço permite que um usuário envie vídeos e fotos e compartilhe com outras pessoas (por exemplo, Youtube, Instagram);

3) Acompanhamento de atividades: este serviço permite que um usuário registre determinadas atividades, como visitar um determinado local (por exemplo, FourSquare);

4) Blogs e microblogs: Um blog funciona como um diário e um microblog funciona como atualizações curtas para qualquer pessoa inscrita para recebê-lo (por exemplo, Twitter);

5) Notícias sociais: este serviço permite que um usuário compartilhe itens ou links para artigos de notícias (por exemplo, Digg);

6) Fóruns de discussão: Fóruns são criados sobre um tópico específico de interesse comum para um grupo e os participantes podem discutir abertamente;

7) Revisões: este serviço permite que um usuário participe da seção de comentários (por exemplo, o TripAdvisor).

Embora as informações nas mídias sociais sejam públicas, o usuário pode configurar seu perfil para restringir o acesso de pessoas desconhecidas. A maioria dos usuários permite que amigos acessem suas postagens. Em algumas situações judiciais, pode-se rejeitar a evidência se um investigador fingir ser um amigo para obter informações do suspeito, podendo esse comportamento ser interpretado como desonestidade, fraude, engano ou deturpação.

A seguir, apresentamos importantes desafios de coletar evidências de mídia social, discutidas em Zawoad e Hasan (2013), Bosack *et al.* (2014), Murphy e Fontecilla (2013) e I-Sight (2014):

Preocupações com a privacidade: Um empregador não pode solicitar a senha do funcionário nas mídias sociais mesmo que o funcionário esteja sob investigação de má conduta profissional. Apenas as informações relevantes para a investigação devem ser acessadas.

Privacidade e políticas de mídia social: Os empregadores devem definir uma política explícita de mídia social para seus funcionários que descreva qual conteúdo pertence ao empregador. Isso pode evitar uma expectativa razoável na privacidade para diferentes interações do funcionário, como, por exemplo, um e-mail pessoal enviado de computadores do trabalho ou o estabelecimento de conexões profissionais no LinkedIn.

Alteração e manipulação de dados: Os usuários podem facilmente excluir informações de seu perfil de mídia social. Infelizmente, os usuários também podem ser vítimas de manipulação de dados

em seu próprio espaço de mídia social. Em Murphy e Fontecilla (2013), os investigadores são orientados a registrar o que estão vendo nas mídias sociais usando ferramentas como Camtasia (CAMTASIA, 2017) e Screencast-O-Matic (SCREENCAST-O-MATIC, 2018). Também é importante garantir que os dados não sejam manipulados após essa gravação. Portanto, o investigador deve identificar-se, registrar dia e horário, explicar o objetivo da investigação e enviar a gravação para várias pessoas, incluindo seu chefe, o advogado e uma empresa terceirizada com capacidade de auditar atividades (MURPHY; FONTECILLA, 2013).

4.5 Desafios em coletar evidências no laboratório

O laboratório forense é o local mais fácil e controlado dentre os que aqui foram apresentados para a extração de dados. No entanto, se procedimentos inadequados foram tomados durante a aquisição, os investigadores provavelmente não terão sucesso na extração de dados.

Desafios importantes enfrentados durante a extração de dados de evidências no laboratório são apresentados a seguir:

Dispositivos bloqueados: A cada dia é mais frequente o número de pessoas que bloqueiam seus smartphones. Se o smartphone for uma nova versão do iPhone, a probabilidade de desbloquear o dispositivo no laboratório é muito baixa. Nesses casos, a abordagem policial para aproveitar esse tipo de evidência no local é muito importante. Uma possibilidade é obter o iPhone diretamente desbloqueado do proprietário e continuar com o mecanismo de desbloqueio no dispositivo.

Erro de Entrada e Saída (E/S) do HD: O HD é um dispositivo sensível e, se sofrer algum tipo de choque, pode culminar em um erro de E/S. Esse tipo de erro não permite que o investigador faça uma imagem adequada do HD original. Esse tipo de problema pode ser evitado se o HD for adequadamente transportado do local para o laboratório forense.

Smartphone ligado: Alguns smartphones têm um botão sensível para ligá-lo e desligá-lo. Normalmente, vários smartphones são apreendidos em um mesmo caso e são enviados para o laboratório forense em uma mesma bolsa. Se o smartphone for ligado involuntariamente durante o transporte e tiver sido previamente configurado para ser apagado remotamente, o alvo poderá executar esse comando e o investigador não poderá extrair os dados quando as evidências chegarem ao laboratório.

5 Conclusão

A análise forense digital ainda enfrenta diversos desafios relacionados à fase de coleta de evidências digitais. Diferentes locais virtuais e reais podem ser considerados como cena do crime. Os obstáculos técnicos e as fronteiras legais devem ser considerados para preservar e aceitar a prova digital em um tribunal.

Este artigo apresentou vários desafios associados a cada local onde as evidências digitais podem ser apreendidas e a extração de dados pode ser realizada. A mesma dificuldade deve ser compartilhada entre promotores, investigadores e policiais envolvidos na apreensão de evidências digitais.

Os processos forenses devem seguir padrões que devem ser otimizados continuamente. A primeira fase para entender o problema é caracterizá-lo adequadamente.

Este trabalho contribui para essa elucidação e descreve sistematicamente vários desafios na crucial fase forense de coleta de evidências, aumentando assim os procedimentos de preparação e o sucesso na preservação das evidências digitais.

Embora o trabalho tenha apresentado as situações de desafios mais populares, a lista não é exaustiva, tendo em vista a permanente evolução das tecnologias. Novos ambientes de armazenamento de dados e novas barreiras de acesso a dados dificultam consideravelmente a correta e bem sucedida coleta forense.

Como trabalhos futuros, a pesquisa identificará e tabulará os principais problemas de coleta de dados sob a perspectiva de dispositivos com barreiras de acesso, tais como dispositivos com criptografia ou técnicas antiforenses habilitadas.

REFERÊNCIAS

AMAZON. **Amazon Elastic Computing Cloud**. Disponível em: http://aws.amazon.com/ec2. Acesso em: 10 jan. 2015.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **ABNT NBR ISO/IEC 27037. T**ecnologia da informação – Técnicas de segurança – Diretrizes para identificação, coleta, aquisição e preservação de evidência digital. 2013.

AZURE. **Windows azure**. Disponível em:http://www.windowsazure.com. Acesso em: 10 jan. 2015.

BOSACK et al. **Social Media Evidence:** Ethical and Practical

Considerations for Collecting and Using Social Media Evidence in Litigation. Corporate Conseul CLE Seminar. 2014.

CAMTASIA. **The best all-in-one Screen Recorder and Video Editor.** Disponível em: http://www.techsmith.com/camtasia.html. Acesso em: 03 jan. 2017.

GOGRID. **Cloud Hosting, Cloud Computing and Hybrid Infrastructure from GoGrid**. Disponível em: http://www.gogrid.com. Acesso em: 09 mar. 2018.

GOOGLE. **Google App Engine**. Disponível em: https://cloud.google.com/appengine . Acesso em: 10 jan. 2015.

INTERNATIONAL DATA CORPORATION (IDC). **Smartphone OS**. Disponível em: <http://www.idc.com/prodserv/smartphone-os-market-share.jsp>. Acesso em: 30 abr. 2018.

I-SIGHT. **How to Gather Social Media Evidence. Avoid Legal Disasters and Win More Cases**. Disponível em: <http://i-sight.com/how-to-gather-social-media-evidence>. Acesso em: 10 nov. 2014.

MELL, P.; GRANCE, T. **The NIST Definition of Cloud Computing.** NIST Specional Publication 800-145. 2011.

MURPHY, J., FONTECILLA, A. **Social Media Evidence in Criminal Proceedings:** An Uncertain Frontier.Richmond Journal of Law & Technology. Volume XIX, Issue 3. 2013.

NATIONAL INSTITUTE OF JUSTICE (NIJ). **Electronic Crime Scene Investigations:** A Guide for First Responders. 2nd Edition. NCJ 219941. Washington, DC. 2008.

NATIONAL INSTITUTE OF JUSTICE (NIJ). **Investigative uses of technology:** devices, tools, and techniques. NIJ Special Report NCJ213030. Washington, DC. 2007.

QUICK, D.; CHOO, K. **Google Drive:** Forensic analysis of data remnants. Journal of Network and Computer Applications 40 pp.

179-193. 2014.

RACKSPACE. **Focus on your business**. Available at http://www.rackspace.com. Acesso em: 03 jan. 2015.

SCREENCAST-O-MATIC. **Video creation for everyone.** Disponível em: http://screencast-o-matic.com/. Acesso em: 05 jan. 2018.

ZAWOAD, S.; HASAN R. **Cloud Forensics:** A meta-Study of Challenges, Approaces, And Open Problems. arXiv preprint arXiv:1302.63.12, pp 1-15, 2013.

ZHANG, L.; Xu, C.; PATHAK, P.; MOHAPATRA, P.. **Characterizing Instant Messaging on Smartphones**. Volume 8995. Lecture Notes in Computer Science pp. 83-95. 2015.

ZHANG, Q.; CHENG, L. **Cloud computing:** state-of-the-art and research challenges. Journal of Internet Services and Application. 1(1), 7-18. 2010.