DESAFIOS DA FORENSE EM DISPOSITIVOS MÓVEIS[1]

Pablo Lopes Mesquita

Resumo: Cada vez mais as empresas estão consolidadas com a TI, seja em uso de computadores ou smartphones, onde há acesso as informações corporativas a qualquer momento. Entretanto o uso destes dispositivos, seja ele equipamento pessoal ou corporativo, podem gerar um comprometimento na segurança das informações ocasionando prejuízos para a organização. A segurança da informação hoje é um dos desafios da tecnologia pois buscam-se soluções de como tratar as ameaças e ataques ao sistema computacional, sendo assim, a forense computacional tem como objetivo investigar esses crimes cibernéticos, coletando vestígios, examinando-os e analisando com o intuito de buscar evidências do crime cometido e se possível, montar o cenário criminoso.

Palavras-chave: computação na nuvem; investigação digital; forense computacional.

1 INTRODUÇÃO

Atualmente empresas e governos têm se tornado alvos de ataques virtuais e de pessoas mal-intencionadas devido às vulnerabilidades dos seus sistemas informatizados, pois cada vez mais as empresas estão consolidadas com a TI (Tecnologia da Informação), seja em uso de computadores ou smartphones, onde se tem acesso as informações corporativas a qualquer momento. Mesmo já fazendo parte das nossas vidas há algum tempo e nos mantendo em comunicação constante, estes dispositivos estão atuando, entre outras funções, como escritório portátil, ferramenta social de entretenimento.

Entretanto (HYPPOLITO, 2017) cita que nos últimos anos, inúmeros dos ataques foram da categoria “engenharia social” que tem por objetivo persuadir um

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

indivíduo a realizar uma ação onde disponibilize o acesso ao atacante ou a divulgação de informações de seu interesse.

Durante o ataque a vítima não tem o discernimento de que suas ações são perigosas e com isto o criminoso explora a ingenuidade do alvo para a aquisição de informações que lhe são interessantes criando assim, um comprometimento na segurança, visto que o elo mais fraco de uma gestão de segurança sempre será o usuário.

Com possíveis ataques que podem ocorrer a qualquer momento, torna-se necessário que os profissionais de TI possuam criteriosas rotinas de mitigação dos riscos do ambiente computacional. Nota-se, no entanto, que o preparo de muitas empresas e seus profissionais não é suficientes por questões diversas, tais quais: custos, tempo hábil para qualificação dos profissionais e planejamento.

Sempre que recursos computacionais são utilizados para o tratamento de informações, correm-se riscos de segurança. Este fato torna-se evidente com o acompanhamento do crescimento de ataques aos sistemas computacionais.

A segurança da informação hoje é um dos desafios da atualidade, pois se buscam soluções de como tratar as ameaças sendo assim, a forense computacional tem como objetivo investigar esses crimes cibernéticos, coletando vestígios, examinando-os e analisando com o intuito de buscar evidências do crime cometido e, se possível, montar o cenário criminoso.

Segundo BATISTA, na atualidade os smartphones estão incorporando recursos cada vez mais sofisticados e a comodidade oferecida através da massificação da internet, contribui para a disseminação dos crimes virtuais que ocorrem através destes aparelhos. Para combater esse tipo de crime, não basta apenas usar meios convencionais de investigação, mas também é necessário o conhecimento das tecnologias existentes.

Devido ao aumento de ações ilícitas, a importância do papel do “especialista em computação forense” ou “perito forense computacional”, vem ganhando grande relevância e destaque. Entretanto se faz necessário aprimorar cada vez mais os conhecimentos, métodos e ferramentas na área, pois há um grande desafio na busca de

arquivos e informações do proprietário que podem, assim, materializar um delito ou simplesmente comprovar o seu envolvimento em atos que estão em investigação policial ou empresarial.

A partir dessa situação, surge a necessidade de profissionais capazes de elaborar laudos a fim de determinar a dinâmica, a materialidade e a autoria de ilícitos eletrônicos, para que viabilize e possibilite a punição para determinado caso que envolva esses tipos de crimes (FRANCO, 2017).

Diante destes problemas, formula-se a seguinte pergunta: como será a evolução dos métodos e técnicas que a perícia forense pode adotar para a auditoria dos dados em um ambiente de computação nas nuvens e smartphones?

Com a integração de serviços tais como e-mail, redes sociais e armazenamento na nuvem, muitos equipamentos não se resumem apenas em armazenar seus dados em mídias locais, surgindo assim à necessidade de analisar também o conteúdo em outros armazenamentos e na Cloud-Computing.

Há a necessidade de novas ferramentas e processos capazes de localizar e recuperar provas suficientes de conjuntos de dados maiores de forma rápida, eficiente e completa. As ferramentas forenses são, muitas vezes, produtos comerciais, de modo lucrativo e não baseado em ciência, e não atendendo as verdadeiras necessidades forenses.

Este artigo demonstra a evolução da forense computacional diante das novas tecnologias desenvolvidas, apresentando conceitos relevantes bem como a sua evolução diante das novas tecnologias existentes para automatização e cruzamento de informações e problemas encontrados no universo computacional.

2 EVOLUÇÃO DO CRIME CIBERNÉTICO

Com o passar dos anos, o avanço tecnológico impôs facilidades e dependências de empresas e pessoas em relação aos equipamentos e seus sistemas informatizados, sejam eles computadores, celulares, GPS’s e afins. A tecnologia está cada vez mais

presente nas interações sociais, assim como na esfera criminal, onde sistemas computacionais são utilizados para cometer ou mediar crimes.

É empiricamente comprovado que uma grande parte das atividades ocorre inteiramente de maneira local, em computadores conectados à internet e controlados pelos usuários, porém há uma forte tendência de mudança de uso com a massificação da internet (DIDONÉ, 2011).

Segundo Fragola (2015), esta nova modalidade de crime já emprega tecnologias complexas, como a engenharia social aplicada às redes sociais e o uso de "clusterização" de milhares de máquinas escravas para o processamento colaborativo de grandes massas de dados, sendo estas apenas algumas das inúmeras ferramentas que os criminosos possuem para praticar os crimes cibernéticos.

A partir disto, surgiu uma nova classe de crime que tem se tornado mais prevalente com a evolução da tecnologia, sendo esta realizada, parcialmente ou completamente, através da internet com o uso de dispositivos eletrônicos, sendo denominada de “Crime Cibernético” e consecutivamente ocasionando o surgimento da “Perícia Forense Computacional”.

3 O QUE É FORENSE?

Forense é o conjunto de conhecimentos científicos e técnicas que, em conjunto, são utilizadas para desvendar crimes sejam eles tecnológicos ou não. Ela é considerada uma área interdisciplinar, pois envolve física, química, biologia, entre outras.

A Perícia Forense Computacional é definida como uma ciência multidisciplinar, que por sua vez aplica técnicas investigativas para determinar e analisar evidências, diferentemente dos outros tipos de perícias forense conhecida (LOPES, 2016).

Segundo Eleutério e Machado (2011), a computação forense é a ciência que usa técnicas especializadas, para coletar, preservar e analisar os dados digitais de um equipamento utilizado em um crime virtual.

Podemos resumir então que a Perícia Forense Computacional ou Computação Forense como a ciência, em contínua evolução, que envolve técnicas para a coleta e qualificação de informações a fim de determinar a ocorrência de um evento ilícito.

3.1 ETAPAS DA INVESTIGAÇÃO

O processo de investigação na Perícia Computacional Forense é divido em quatro etapas: Coleta, Preservação, Análise e Relatório, constituindo o propósito que é a extração de evidências relacionadas a um caso investigado, para que propicie conclusões sobre o desfecho do delito.

Na primeira etapa o objetivo é registrar e coletar todas as evidências físicas e digitais relacionadas ao incidente que está sendo investigado. É fundamental que os dados voláteis (aqueles que constam na memória RAM ou trafegando em rede de computadores) e outras possíveis fontes de evidências, sejam coletados de forma idêntica a sua origem, de modo a que seja possível aos peritos executarem a analise sem apagar qualquer vestígio nos equipamentos apreendidos.

Após a coleta das informações deverá a haver o processo de preservação das evidencias havendo um foco maior na integridade física deles, esta fase tem o objetivo de garantir que as informações armazenadas no material questionado jamais sejam alteradas durante toda a investigação e processo.

A análise dos dados consiste no exame das informações extraídas do material questionado durante a fase anterior, a fim de identificar evidências digitais que tenham relação com o delito investigado. Após a identificação e avaliação das evidências encontradas no material questionado, é possível responder as perguntas feitas pela autoridade solicitante.

Dessa forma, é importante que o a autoridade solicitante busque sempre detalhar o que procura, descrevendo no máximo de detalhes possíveis, ou seja, que mostre para a equipe pericial exatamente o quê deve ser buscado, para dessa forma, evitar desperdício de trabalho dos peritos.

A última etapa do processo constitui na construção do relatório, apresentando os resultados relevantes para o caso. Nessa etapa também é redigido o laudo pericial, o qual deve ter conclusão imparcial, clara e concisa; devendo ser exposto os métodos utilizados na perícia e possuindo uma interpretação fácil de modo que pessoas com pouco ou nenhum conhecimento técnicos possam compreender as informações escritas.

Os processos acima descritos podem exemplificados na figura 1 de forma sucinta e autoexplicativa.

Figura 1 – Ilustração dos Processos de Investigação

Fonte: Pág. 1 pt.slideshare.net (2011)

Como podemos ver, uma simples investigação forense se trata uma ordem de procedimentos que devem ser realizados minuciosamente para que a execução da tarefa não se torne falha comprometendo a investigação.

4 DESAFIOS DA FORENSE

A comunidade forense digital enfrenta um desafio constante para se manter a par das últimas tecnologias que podem ser usadas para expor indícios relevantes em uma

investigação. Um dos maiores desafios forenses quando se trata da plataforma móvel é o fato de que os dados podem ser acessados, armazenados e sincronizados em vários dispositivos. Como os dados são voláteis e podem ser rapidamente transformados ou excluídos remotamente, é necessário mais esforço para a coleta destes dados.

Segundo Heather (2016), o rápido aumento no número de diferentes tipos de telefones móveis torna difícil desenvolver um único processo ou ferramenta para examinar todos os tipos de dispositivos. Os telefones móveis estão evoluindo continuamente à medida que as tecnologias existentes avançam e outras são desenvolvidas.

Nesta situação quando um dispositivo móvel é encontrado durante um inquérito, muitas questões surgem: Qual é o melhor método para coletar a evidência? Como o dispositivo deve ser tratado? Como provar, em uma determinada situação, que a ação criminosa não foi realizada pelo dispositivo?

Devido a estas perguntas o perito forense possui um ambiente desafiador para trabalhar com inúmeros equipamentos, situações e técnicas de coletas de informações, pois cada equipamento possue suas peculiaridades.

Um dos maiores problemas é o aumento da capacidade de armazenamento e complexidade das novas tecnologias dos dispositivos, pois cada fabricante possui sua tecnologia proprietária e isso sugere que o analista forense possua equipamentos com a mesma capacidade e ainda tenha um tempo maior para coleta e análise.

Os profissionais da área têm um conjunto cada vez maior e complexo de informações para examinar, desde ferramentas de comunicação, redes sociais até imagens de vídeo e um curto espaço de tempo e orçamento para lidar com essas demandas crescentes.

"A forense digital é uma área que está se tornando cada vez mais importante na computação e muitas vezes requer a análise inteligente de grandes quantidades de dados complexos", concluiu um estudo publicado pela Digital Evidence&Electronic Signature Law Review (Coatne, 2017).

5 FORENSE EM SMARTPHONES

A forense em dispositivos móveis é um ramo de forense digital relacionado à recuperação de evidências digitais ou dados de dispositivos móveis. O termo “dispositivo móvel” geralmente se refere a telefones smartphones, entretanto, ele também pode se relacionar com qualquer dispositivo digital com capacidade de comunicação, por exemplo, smartwatchs, dispositivos GPS e tablets.

Um dos maiores desafios forenses quando se trata da plataforma móvel é o fato de que os dados podem ser acessados, armazenados e sincronizados em vários dispositivos. Como os dados são voláteis e podem ser rapidamente transformados ou excluídos remotamente, é necessário mais esforço para a coleta dos mesmos.

Todos os celulares exigem conhecimentos e habilidades especiais de especialistas forenses, entretanto não é necessário ser experiente em informática para entender todas as peculiaridades e dificuldades a se enfrentar neste ramo de investigação (EFORENSICSMAG, 2017).

Os sistemas operacionais dos dispositivos móveis são dividido entre 2 grandes fornecedores: Android da Google Inc e IOS da Apple Inc. Em intervalos de tempo os desenvolvedores criam tecnologias novas de modo a se destacar em relação aos concorrentes.

Para estarem competitivos, os fabricantes dos smartphones que hoje existem no mercado, alteram as estruturas de arquivos do sistema operacional, armazenamento de dados, serviços, periféricos e até mesmo conectores e cabos.

Apesar de que todos os sistemas operacionais apresentam aproximadamente as mesmas funções e opções, eles diferem consideravelmente na forma como armazenam dados e direitos de acesso, bem como a segurança e outras características. E com todas estas peculiaridades de cada fabricante tornam a forense uma área de atuação complexa e diversificada onde o perito e os desenvolvedores de ferramentas devem estar em constante evolução.

Como resultados desta constante evolução tecnológica são desenvolvidos inúmeros tipos de ferramentas para a extração evidências de dispositivos móveis; Nenhuma ferramenta ou método possui a capacidade de adquirir todas as evidências de todos os dispositivos.

5.1 SEGURANÇA

Um aspecto básico da segurança em smartphones modernos é a aplicação de senhas criadas pelo usuário para acessar o dispositivo. Existem vários mecanismos de bloqueio diferentes, incluindo códigos simples de 4 ou 5 dígitos, scanners de impressões digitais, entre outros gerando uma das maiores barreiras para a realização de trabalhos forenses em um smartphone.

5.2 RECUPERAÇÕES DE DADOS

Os smartphones armazenam os seus dados na memória flash NAND ou no cartão de memória, caso exista, e há situações em que os dados foram excluídos, porém estão teoricamente presentes na memória e simplesmente foram marcados como espaço não alocado pelo controlador.

Neste caso o perito através de ferramentas especializadas consegue acessar estas informações e extrair uma possível evidencia, porém há situações onde não é possível realizar esta recuperação sendo necessário realizar pesquisas de arquivos de backups.

5.3 APLICAÇÕES

Um dos aspectos deste dispositivo é a possibilidade de execução de aplicações ocultas. “No mundo do forense, só porque você não vê algo inicialmente, não significa que nada esteja lá" (GILLWARE, 2017).

Embora a compreensão de como usar ferramentas forenses é útil de várias maneiras, algumas aplicações podem ocultar ou até mesmo mascarar informações com outras do sistema de modo que passem despercebidos pelo perito.

6 FORENSE NA IOT

O termo IoT ou Internet das Coisas é o conjunto de dispositivos inteligentes que possuem diversas aplicações, dentre elas: coletar dados de sensores remotos em plataformas; coleta de dados climáticos e o controle de termostatos inteligentes (HP, 2017).

Estes dispositivos abrem para empresas, agências governamentais e consumidores individuais um leque de possibilidades de aplicações úteis tornando rotinas cotidianas mais convenientes e dinâmicas. Entretanto há grandes problemas de segurança e privacidade devido a recursos não implementados.

Hoje, as discussões se concentram em benefícios ao invés de respostas a incidentes e pesquisas caso haja a utilização indevida destes equipamentos. Há uma necessidade de metodologias inteligentes e adaptáveis para investigar os crimes relacionados à IoT, no entanto, está se tornando pertinente.

A todo instante a forense neste tipo de dispositivo necessita de ferramentas novas, atualizadas e técnicas especializadas e uma das razões é que os dispositivos IoT estão sendo amplamento implantados e os consumidores desta tecnologia estão focados nos recursos que a mesma pode trazer ao invés de protegê-la (SCAR, 2017).

Mas a falta de segurança nestes dispositivos pode levar a uma catástrofe em cenários futuristas como projetos recentes da Samsung Electronics em conjunto SK Telecom que ambas pretendem desenvolver cidades inteligentes na Coréia do Sul utilizando-se destes equipamentos (RICKER, 2016).

A IoT Forensics tem mais áreas de interesse do que a forense tradicional, além do tipo tradicional de redes - com fio, sem fio(Wi-Fi) e móvel há também os IoTware que nada mais são do que eletrodomésticos e dispositivos médicos conectados a internet, devendo assim serem considerados fontes de evidência durante as investigações.

O principal desafio na investigação de um crime é a combinação de muitas áreas das tecnologias principais, que incluem computação em nuvem, dispositivos móveis

(computadores, tablets, etc..), sensores e também os protocolos e interfaces físicas proprietárias.

Os padrões pelos quais as evidências são análisadas e coletadas em investigações devem ser alteradas para acomodar a natureza variável da evidência digital a partir de um ambiente de computação em nuvem ou o dispositivo auditado (Taylor, Haggerty, Gresty e Hegarty, 2010).

A preservação das informações é um desafio e aconselham-se os peritos que não desliguem os dispositivos em investigação de modo que preservem os horários de arquivos modificados, criados, acessados e outras informações relevantes (Hegarty, R.C, Lamb, D.J, Attwood, 2016).

Pode-se dizer que a afirmação deles é embasada nos principios das investigações forenses digitais convencionais; no entanto, a situação é muito mais complexa nas investigações IoT, devendo haver um critério avaliativo do perito que determine se os dispositivos devem ser desligados ou deixados em funcionamento.

De acordo com DAVID, BRETT, TADHG e MARK (2016), o problema da investigação nestes ambientes é a complexidade dos dados adquiridos onde o seu volume de informações é grande e a falta de automação para análise dos mesmos torna a investigação demorada e trabalhosa de modo que é executada manualmente.

Outro ponto destacado pelos autores é a possibilidade de não haver um sincronismo de horários das múltiplas fontes gerando um cruzamento de informações mais criticas podendo levar a informações inconsistentes.

Entretanto dos aspectos citados, o que mais se destaca como um grande empecilho para os investigadores na resolução do evento é a falta de padronização de informações e protocolos de comunicação, pois dependendo do fabricante pode haver técnicas diferentes para as coletas de informações pertinentes, aumentando a probabilidade de perca de informações cruciais.

7 DISPOSITIVOS MÓVEIS E COMPUTAÇÃO NA NUVEM

Uma das inúmeras tendências quando se fala em tecnologia é a computação em nuvem ou cloud-computing, proporcionando poderes de armazenamento e processamento “ilimitados” para organizações, sendo possível a implantação de soluções escaláveis por meio da internet.

Os principais benefícios desta arquitetura são as reduções das despesas com servidores e outros equipamentos para manter uma infraestrutura capaz de processar o grande volume de dados da organização, sendo assim, a computação em nuvem para dispositivos móveis é uma tendência muito atraente e potencialmente lucrativa.

7.1 SMARTPHONES E CLOUD-COMPUTING

Entrentanto a integração com esta plataforma gera um benefício adicional, pois muitos dos dispositivos móveis que as organizações possuem, têm capacidades de processamento e hardware inferiores ao que necessita-se para a execução de, por exemplo, um aplicativo corporativo de envio de arquivos e com isto restringindo, muitas vezes, o desenvolvimento de software para esses dispositivos.

A computação em nuvem permite que os desenvolvedores e/ou organizações evitem essas restrições, permitindo que as tarefas que exigem processamento mais intenso sejam realizadas em infraestrutura de alta capacidade e somente enviando os resultados serão enviados para o dispositivo via internet.

Este serviço é capaz de melhorar a experiência do uso do dispositivo reduzindo a necessidade de que os usuários transportem os seus dados e dispositivos de armazenamento externos adicionais mantendo assim os seus dados seguros, evitando perda de dados e acidentes indesejados através de aplicativos de sincronização automatica.

7.2 INTERNET DAS COISAS (IOT) NA COMPUTAÇÃO NA NUVEM

A Internet das coisas (IoT) esta gradativamente transformando a forma como vivemos nossas vidas, mas toda a conveniência adicional e o aumento da eficiência têm um custo.

O IoT está gerando uma quantidade sem precedentes de dados, o que, por sua vez, coloca uma enorme pressão sobre a infra-estrutura da internet. Como resultado, as empresas estão trabalhando para encontrar maneiras de aliviar essa pressão e solucionar o problema do volume de tráfego.

Segundo (Digital, 2017), durante a 6° edição anual do Cisco Global Cloud Index foi apresentada que o tráfego da nuvem deverá sofrer um aumento de 3,7 vezes de trafego de informações indo de 3,9 zetabytes ($10^{(21)}$) (ZB) em 2015 para 14,1 ZB até 2020.

Esse rápido crescimento é atribuído ao aumento da migração para arquiteturas de nuvens por conta da capacidade de se expandir rápida e eficientemente e suportar mais cargas de trabalho do que os datacenters tradicionais.

À medida que os serviços em nuvem crescem, o mesmo acontece com a probabilidade de seu uso em atividades criminosas. Os provedores devem se preparar para aumentar a ênfase na forense da nuvem.

Os serviços em nuvens estão sendo usados para os mais diversos fins, sejam eles para hospedagem de arquivos pessoais ou corporativos, envio de informações pelos dispositivos IoT, mas um fato é veridico – “Ao longo do tempo, espera-se que as nuvens contenham cada vez mais evidências de atividades criminosas”.

Nos últimos anos, pesquisadores em forense digital tentaram abordar os problemas encontrados no Cloud Forensics em questão a “coleta evidências digitais de um servidor remoto” o qual muitas vezes são armazenados em outra jurisdição tornando-se, assim, um trabalho complexo devido a questões legais.

As dificuldades encontradas na realização de uma investigação forense podem ser listadas em processos simples de um caso típico de crime digital. A determinação de que a forense na nuvem só poderá ser investigada se dará diante de aquisição das credenciais de login armazenadas de um dispositivo digital físico, como um laptop ou smartphone.

Na procura de evidências no datacenter, os problemas tendem a aumentar devido à impossibilidade de aprensão dos servidores e as leis digitais vigentes no local onde estão os servidores.

Ao longo do tempo, o uso de evidências digitais em assuntos criminais e civis continuará a se expandir sendo assim os provedores de nuvem e os clientes precisam configurar suas infraestruturas para atender a esses pedidos legais ou enfrentar multas e outras repercussões legais. Além disso, eles precisam fazê-lo sem violar as leis locais de privacidade ou fornecer acidentalmente segredos competitivos.

Outro problema enfrentado pelo perito é a dificuldade de sincronização e técnicas para a segregação dos logs, pois no momento, as maiorias dos provedores de serviços em nuvem não estão abertas para falar sobre isso porque não conhecem o problema e também não possuem normas para tratar tais situações.

8 ESTRATÉGIAS DE FORENSE NA CLOUD-COMPUTING

A computação em nuvem vai de oposição à computação padrão, pois possui inúmeros problemas que podem causar relutância ao utilizar este serviço. Algumas dessas questões incluem preocupações sobre privacidade e propriedade de dados e segurança sendo especialmente relevantes para dispositivos móveis.

Atualmente, não parece haver nenhuma diretriz publicada que aborda especificamente a condução de uma investigação nestes ambientes, pois o conceito de processamento distribuído de dados gera uma aquisição de evidências e análise cada vez mais complexa, sendo assim, este novo tipo de serviço transforma uma solução a um problema exposto: Como coletar dados nestas estruturas?

Para entender e analisar evidências dentro deste ambiente, os investigadores exigirão uma gama mais ampla de conhecimento técnico em várias plataformas de hardware e sistemas operacionais (Taylor, 2011).

Embora a computação em nuvem possa parecer atraente para um negócio ela também possui seus próprios problemas e preocupações únicas. O armazenamento de

dados corporativos sensíveis em um servidor remoto suscita preocupações quanto à privacidade e acessibilidade desses dados por uma segunda parte não autorizada.

A empresa que contrata este serviço geralmente não tem conhecimento da localização física dos dados, da mesma forma eles podem não conseguir discernir quais políticas / procedimentos estão em vigor para recuperar dados se um servidor falhar ou for comprometido.

Na maioria dos casos, a sede da empresa pode estar localizada em um estado e os servidores podem estar localizados no exterior. Portanto, a pergunta "Onde estão os meus dados?" pode não ser fácil de responder.

Apesar dos provedores assegurarem a confiabilidade e a segurança das informações e quando estas estruturas estão associadas de uma forma ou outra a um crime, a coleta de informações se torna um grande problema visto que muitas vezes se encontram distribuídos geograficamente e o acesso às informações, que estão sob a responsabilidade do provedor, podendo se tornar um problema jurídico por questão dos diferentes locais do datacenter.

Atualmente existem inúmeros documentos sobre as técnicas e procedimentos de computação forense, no entanto quando o assunto é a arquitetura de computação em nuvem e forense em dispositivos móveis, onde os dados são armazenados em um ambiente distribuído, surgem muitos desafios relacionados com o local da persistência dos dados, procedimentos de coleta de vestígios e afins.

Segundo Damacena (2014), a preservação da integridade das evidências no ambiente de cloud-computing pode ficar comprometida, uma vez que, ao se compartilhar o ambiente computacional, em alguns casos, torna-se difícil até mesmo a definição do momento em que um incidente ocorreu.

Essa mudança de armazenamento dos dados de uma área local para um lugar remoto é um dos grandes desafios, pois não existe mais um sólido “perímetro de segurança” como se conhecia há alguns anos, mas agora o perímetro de segurança

tornou-se qualquer lugar onde pessoas tenham acesso à rede e a sistemas de serviços que são providos pela Internet (NOGUEIRA, 2017).

Atualmente o grande volume de dados e a facilidade em se obter equipamento, torna o trabalho do perito computacional cada vez mais demorado e complicado, sendo necessário automatizar processos, de modo que sejam realizadas capturas das evidencias e o cruzamento com outras informações, de modo que seja gerado o laudo em um curto espaço de tempo.

Contudo, há ferramentas anti-forense onde estas mascaram as informações de modo que os peritos não consigam ter acesso ou encontrá-las e nos dias atuais os criminosos possuem acesso e conhecimento, visto que esta disseminada na internet (LOPES, 2017).

A investigação impõe inúmeras dificuldades, devido à natureza remota da evidência, a falta de acesso físico, confiança necessária na integridade e autenticidade dos dados torna-se um grande entrave quando se faz necessário a coleta de informações nestes ambientes.

Um processo de resposta aos incidentes de segurança deve ser desenvolvido pelo Gerente de Segurança da empresa provedora do serviço, cujo qual deverá considerar a coleta de informações respeitando a privacidade dos outros clientes.

Este procedimento está intimamente ligado à maturidade de segurança da informação aplicada à estrutura da nuvem e especialmente a disposição de tais a possíveis investigações. No que diz respeito a um ambiente virtual à análise forense pode ser realizada da mesma forma que em instalações do cliente, pois o cliente é o único com acesso às próprias máquinas virtuais.

Se não for possível para um investigador obter o controle do serviço, pode ser possível obter uma imagem dos dados do serviço, no entanto essa abordagem é problemática por questões legais, ou seja,o provedor esta localizado fora da jurisdição.

Segundo (OLIVEIRA & CAIADO, 2013) as discussões sobre segurança das informações em ambientes em nuvem estão aumentando, desde as análises de risco até as implementaçõesde controles, garantindo que as métricas sejam atendidas.

Entretato há alguns riscos previsíveis e preocupantes nestes ambientes entre eles o uso da plataforma por hackers para a hospedagem de botnets ou shells, porém o provedor deve possuir ferramentas que permitam as autoridades para realizar as investigações sem haver grandes entraves com juridições e outros processos burocráticos.

Um aspecto importante está relacionado à auditabilidade dos sistemas, neste contexto, o provedor deve estabelecer periodicidade de armazenamento e formato de logs principalmente nas instalações dos serviços SaaS, em que o acesso do cliente aos registros e informações físicas é mais limitado. Entretanto, é importante que o CSP (Cloud Service Provider) informe o cliente sobre os casos envolvendo incidentes ou tentativas de invasão ao serviço por ele utilizado imediatamente e com documentação completa sobre o incidente.

As respostas forenses devem ser preditas em acordos entre CSPs e investigadores devendo haver uma equipe de profissionais adequados, respondentes de incidentes e órgãos legais, que devem estar no contrato de nível de serviço (SLA) e no contrato.

Neste contexto deverá haver a cooperação entre equipes, considerando os aspectos legais e privacidade de cada cliente, detalhando claramente os contatos dos grupos de resposta e detalhes da legislação dos países em casos de incidentes onde o acesso físico ao dispositivo afetado esteja a milhares de quilômetros do cliente.

Este procedimento estabelece que o indivíduo responsável pela coleta realize-a de forma competente, entretanto esta abordagem de obtenção de evidências em ambientes em nuvem tem outras implicações. O investigador pode ter dificuldade em estabelecer quais informações que são requeridas e a experiência da equipe responsável pela coleta de informações

Com isso em mente, é essencial que haja um profissional competente para recuperar os dados e então capaz de provar a um tribunal de justiça o motivo da emissão de um mandado para se possuir acesso aos servidores considerando à legislação aplicável.

9 FERRAMENTAS

Entrentando há diversas ferramentas livres e comerciais que facilitam a operação dos peritos na execução de uma investigação como, por exemplo, o appliance Israelita Cellebrite onde o mesmo esta sendo utilizado pela Polícia Federal para acesso e extração de dados contidos nos celulares dos suspeitos da operação Lava Jato.

"A informação estratégica é obtida mesmo que tais dados sejam bloqueados por senha ou criptografia, ou ainda que tenham sido apagados da memória do dispositivo pelo usuário", informa um comunicado enviado ao mercado pela Israelense Cellebrite, provedora da ferramenta (COMPUTERWORLD, 2015).

De acordo com pesquisas, a tecnologia UFED (Universal Forensic Extration Device) é usada em mais de 60 países por órgãos de polícia, setores de inteligência, advogados e agentes legais. Esta solução possibilita uma extração e cruzamento de informações entre diversos serviços de modo que apresente relatórios de forma simplificada, porém de múltiplas informações, automatizando e agilizando a investigação.

Segundo (INFOSECINSTITUTE, 2017), há inúmeras outras ferramentas, tanto proprietárias quanto gratuitas para forense em dispositivos móveis entre elas pode citar a "Oxygen Forensic" que realiza coletas de informações do dispositivo, contatos, mensagens (emails, SMS, MMS), recuperar mensagens excluídas, registros de chamadas e informações de calendário.

10 CONCLUSÕES

A evolução dos dispositivos móveis trás consigo soluções para os diversos problemas cotidianos, entretanto é um atrativo à execução de crimes-cibernéticos, pois o

acesso à internet aumenta à sensação de impunidade e a não identificação dos culpados, causando um incentivo a prática de operações ilícitas nestes meios.

Esta situação esta levando profissionais da área e pessoas a se preocuparem gradativamente com a segurança de suas informações, buscando maneiras para protegê-las. Porém, quando isso não for possível e/ou um incidente já tiver ocorrido, a Forense Computacional atuará para realizar a mitigação, entendimento e elucidação dos fatos ocorridos.

Os criminosos estão aperfeiçoando suas técnicas de modo que realizem suas atividades despercebidas pelos investigadores trazendo consigo uma complexidade nas investigações. Os peritos forenses como todo outro profissional de TI devem estar sempre se atualizando das novas tecnologias e equipamentos de modo que estejam sempre preparados para alguma investigação.

Fabricantes de dispositivos, desenvolvedores de sistemas operacionais contribuem massivamente para o aumento da complexidade de execução de coleta de dados e análise. Entretanto o profissional da área, ao decorrer de sua evolução, irá desenvolver técnicas e meios de acesso a informações por intermédio de outros colegas da área, ou seja, troca de conhecimentos.

Este “network” de profissionais é de extrema valia, pois há uma troca de pontos de vista sobre o mesmo problema, por exemplo: Como coletar as informações do equipamento X?

Uma solução para este problema é a criação de seminários ou projetos de pesquisa que possibilitará à formação da base de casos a comunidade de especialistas interessados na formalização e divulgação de seus conhecimentos através do sistema proposto.

Entretanto com advento da tecnologia trouxe consigo novos horizontes relacionados à Forense Computacional e também as diversas áreas que compõem este ramo. Podemos citar, como um dos horizontes, o uso da computação em nuvem que vem se consolidando e com isto havendo a necessidade da criação de padrões de

utilização bem como graus de confiabilidade, privacidade e demais questões de segurança e jurisdições.

Por fim o perito também deve preocupar-se o em adquirir as informações garantindo que todas suas ações não causarão nenhum efeito de perda, modificação ou dano sobre as evidências nas situações mais adversas e respeitando a legalidade das operações.

REFERÊNCIAS

COATNE, Matt. The **Coming AI Revolution in Digital Forensics**. 2017.Disponível em: <http://accessdata.com/blog/the-coming-ai-revolution-in-digital-forensics> Acesso em 25/08/2017

COMPUTERWORLD. **Polícia Federal usa técnica forense para investigar envolvidos na Lava Jato**, 2015. Disponível em: http://computerworld.com.br/policia-federal-usa-tecnica-forense-para-investigar-envolvidos-na-lava-jato Acesso em: 25/10/2017

DAMACENA, Barbara Larissa Candido. **Desafios da perícia forense em um ambiente de computação nas nuvens**. 2017. Disponível em: <http://revista.uniplac.net/ojs/index.php/tc_si/article/view/1911/988>. Acesso em: 31/07/2017

DAVID, BRETT, TADHG, MARK. **Current Challenges and Future Research Areas for Digital Forensic Investigation**, 2016.Disponível em: <http://commons.erau.edu/cgi/viewcontent.cgi?article=1346&context=adfsl>Acessoem: 05/10/2017

DIDONÉ, DENER. **Computação em Nuvem: Desafios e oportunidades para a Forense Computacional**, 2011. Disponível em: <http://repositorio.ufpe.br:8080/bitstream/handle/123456789/2745/arquivo6996_1.pdf?sequence=1&isAllowed=y> Acesso em: 24/08/2017

DIGITAL, Convergência. **Internet das Coisas vai explodir o tráfego de dados na nuvem**, 2017. Disponível em: http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=44028&sid=97 Acesso em: 05/10/2017

ELEUTÉRIO, Pedro Monteiro da Silva; ACHADO, Marcio Pereira. **Desvendando a Computação Forense**. 1. Ed. São Paulo: Novatec, 2011.

EFORENSICSMAG.**Mobile Phone ForensicsChallenges**, 2017.Disponível em: https://eforensicsmag.com/mobile-phone-forensic-challenges/ Acesso em: 06/10/2017

FRAGOLA, Rodrigo. **A sofisticação gerencial do crime cibernético. 2015.** Disponível em: <www.abessoftware.com.br/noticias/a-sofisticacao-gerencial-do-crime-cibernetica> Acesso em: 23/08/2017

FRANCO, Deiviso Pinheiro. **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/>. Acesso em: 19/07/2017

GILLWARE. **Smartphone Forensics**, 2017. Disponível em: https://www.gillware.com/forensics/mobile/smartphone-forensics/ Acesso em: 20/10/2017

Hegarty, R.C, Lamb, D.J, Attwood. 2016, A. **Digital Evidence Challenges in the Internet of Things**, Disponívelem: <https://www.cscan.org/openaccess/?id=231>Acessoem: 04/10/2017

HP. **O que é Internet das Coisas?**, 2017. Disponível em: https://www.hpe.com/br/pt/what-is/internet-of-things.html Acesso em: 01/10/2017

HYPPOLITO, Thiago.**O maior problema da segurança da informação somos nós**. 2017. Disponível em: https://cryptoid.com.br/banco-de-noticias/o-maior-problema-da-seguranca-da-informacao-somos-nos/ Acesso em: 31/10/2017.

INFOSECINSTITUTE. **22 Popular Computer Forensics Tools**, 2017. Disponível em:http://resources.infosecinstitute.com/computer-forensics-tools/#grefAcesso em: 07/10/2017

LOPES, Petter Anderson. **PERÍCIA FORENSE COMPUTACIONAL**, 2016. <Disponível em: https://periciacomputacional.com/pericia-forense-computacional-2/>. Acesso em 31/07/2017

MADEIRA, Mauro Notarnicola. **O que é Computação forense e sua importância no âmbito empresarial**. 2017 <Disponível em: https://www.uaberta.unisul.br/eadv3/security/units/23035/downloadMaterialDidaticoId.processa?materialDidaticoId=28686> Acesso em: 30/07/2017

Mahalik, Heather. **Mobile Forensicsand Its Challanges**.2016.Disponível em: https://www.packtpub.com/books/content/mobile-forensics-and-its-challanges> Acesso em: 25/08/2017

NOGUEIRA, José Helano Matos. **Investigação Pericial no cenário de computação nas nuvens. 2017** Disponível em: <http://tibahia.com/tecnologia_informacao/conteudo_unico.aspx?c=ART_TECH&fb=B_FULL&hb=B_CENTRA&bl=LAT1&r=ART_TECH&nid=35767> Acesso em: 31/07/2017.

OLIVEIRA, José A. M. M. e CAIADO, Marcelo. B. **Best Pratice and Challenges for Process Efficiency of Investigations and Digital Foresensics**, 2013. Disponível em: http://icofcs.org/2013/ICoFCS-2013-003.pdf Acesso em: 15/11/2017

REIS, Marcelo de Abdalla. **Forense computacional e sua aplicação em segurança imunológica, 2003**<Disponível em: http://repositorio.unicamp.br/bitstream/REPOSIP/276322/1/Reis_MarceloAbdallados_M.pdf> Acesso em: 29/07/2017

RIBEIRO, João Vitor Assis. **Os discos de estado sólido e a forense computacional**, 2017. Disponível em: <http://www.migalhas.com.br/dePeso/16,MI256965,11049-Os+discos+de+estado+solido+e+a+forense+computacional> Acessem: 25/08/2017

RICKER, Thomas. **Samsung's building the first national network dedicated to smart cities**, 2016. Disponível em: <https://www.theverge.com/2016/5/24/11759272/Samsung-commercial-smart-city-network> Acesso em: 04/10/2017

SCAR.**InternetOf Things Mobility Forensics**, 2017.Disponível em: <https://articles.forensicfocus.com/2017/05/17/internet-of-things-mobility-forensics/> Acesso em: 04/10/2017

TAYLOR, Mark. Haggerty, John. **Gresty, David. Lamb, David. Forensic investigation of cloud computing systems**, 2011 Disponívelem: <http://www.sciencedirect.com/science/article/pii/S1353485811700241>Acessoem: 24/08/2017