Internet das Coisas: novos desafios na análise forense

Marco Antonio Andrade Dias[1]

Resumo

Na Computação Forense (CF), existem etapas definidas para a realização da investigação digital. A Internet das Coisas (IdC) trouxe novos fatores que afetaram a CF. Com o crescimento de dispositivos interconectados e a inserção de inteligência em ambientes: casa, shopping e etc., novos obstáculos foram gerados para os peritos digitais. Por exemplo, uma rede interna de uma empresa que sofre invasões através do sensor de um termostato. Esse hipotético caso é um dos vários desafios da chamada quarta geração tecnológica. Os objetivos deste artigo são identificar aspectos da forense tradicional que possam ser absorvidos na forense em IdC e apresentar alguns dos novos desafios. Novos modelos para análise forense em IdC têm surgido com os procedimentos da CF

Abstract

In Computer Forensics (CF), there are execution steps for digital investigation. The Internet of Things (IoT) brought new factors that affected CF. With the growth of interconnected devices and the insertion of smart environments: home, shopping, etc., new obstacles have been created for forensic experts, for example, an internal network of a company that is hacked through the sensor of a thermostat. This hypothetical case is one of several challenges of the so-called fourth generation technology. The purpose of this paper is to identify aspects of traditional forensics that can be absorbed in IoT and present some of the new challenges. New models for forensic analysis in IoT have emerged with the CF procedures in IoT, but the difficulties of analyzing data in various formats and storing it in any datacenter anywhere

1 Graduado em Ciência da Computação e especialista em Banco de Dados; em Segurança da Informação; e em Computação Forense & Perícia Digital. É analista de Segurança da Informação no Centro de Gestão e Estudos Estratégicos (CGEE), onde exerce atividades de natureza técnica especializada em grau de complexidade ligadas à proposição, execução e acompanhamento de projetos.

em IdC, porém, as dificuldades em analisar dados com vários formatos e em armazená-los em algum datacenter localizado em qualquer parte do mundo, além da imensa quantidade de sensores conectados a qualquer coisa se comunicando através da rede, tornaram-se uma grande adversidade para os profissionais forenses digitais.

Palavras-chave: Computação Forense. Crime Digital. Internet das Coisas.

in the world, besides the sheer number of sensors connected to any communicating over the network have become a major adversity for digital forensics professionals.

***Keywords**: Computer Forensics. Cybercrime. Internet of things.*

1. Introdução

Diante da evolução da tecnologia e do surgimento da internet, acessar e obter informação tornaram-se tarefas mais viáveis e muito mais rápidas. A facilidade em pagar um boleto, enviar mensagens e assistir a filmes com apenas alguns cliques otimizou o tempo, mas esses avanços tecnológicos causaram novos desafios na área de segurança da informação. Várias formas e vários tipos de ataques foram desenvolvidos após a popularização da internet. Criminosos passaram a utilizar computadores para cometer seus crimes, estimulados, em grande parte, pela quase impunidade resultante dos poucos avanços na legislação brasileira sobre tais delitos. Eleutério e Machado (2011) diferenciam as formas como um computador pode ser utilizado nessas circunstâncias: como ferramenta de apoio (sonegação fiscal, compra de votos, etc.) ou como meio (ataques a *sites*, *phishing*, etc.) para a realização de um crime. Diante desse cenário, observa-se um crescimento na demanda por perícias digitais. Na CF, existem algumas etapas definidas para a realização da perícia, conforme descritas a seguir: (1) identificação, (2) preservação, (3) análise e (4) apresentação. Segundo Costa (2011), identificação é a emissão de um instrumento legal para gerar a busca e apreensão de evidências; preservação é a manipulação das evidências; análise é a realização dos exames; e apresentação é a materialização da prova por meio do laudo pericial.

Com o crescimento de ambientes inteligentes, os dispositivos obtêm seu próprio Endereço de Protocolo da Internet (Endereço IP) [do idioma inglês, *Internet Protocol address* (*IP address*)] e, com isso, qualquer coisa pode estar conectada à internet. Por exemplo, uma geladeira conectada na rede pode enviar um pedido ao supermercado, informando a falta de polpa de fruta e, em uma situação de vulnerabilidade, pode haver a invasão criminosa da rede interna

por meio do IP daquela geladeira. Essa é a realidade da chamada quarta geração da internet, a Internet das Coisas (IdC).

Peres e Sleiman (2017) afirmam que a IdC tem como base sensores conectados às "Coisas". O termo "coisas", de acordo com Hung (2017), diz respeito a "objetos físicos dedicados que contêm tecnologia embarcada para a comunicação". Atualmente, com o uso da IdC, a conexão de milhares dispositivos através da internet vem crescendo, porém, devido a esse aumento na troca de informações, foram ampliados também as vulnerabilidades e os ataques sobre essa tecnologia.

De acordo com Zulkipli, Alenezi e Wills (2017), os casos de *cybercrime* com o uso de dispositivos de IdC vêm aumentando. Consequentemente, o número de desafios para os profissionais da forense cresce no mesmo ritmo, em razão da imensa quantidade de sensores conectados a qualquer coisa e que se comunicam através da rede em qualquer parte do mundo.

Assim, os objetivos deste artigo são identificar aspectos da forense tradicional que possam ser absorvidos na forense em IdC e apresentar alguns dos novos desafios. O artigo foi estruturado em seis seções: (1) Introdução; (2) Referencial teórico que conceitua tecnologias contidas no tema; (3) Aspectos da forense; (4) Casos em ambientes inteligentes; (5) Desafios; e (6) Conclusão.

2. Referencial teórico

Foram selecionadas algumas definições, com o objetivo de facilitar a compreensão do contexto deste artigo.

2.1. Forense digital

De acordo com Bem, Feld, Huebner e Oscar (2008), o primeiro registro de caso de crime com utilização de um computador foi no Texas, Estados Unidos, em 1966. Com o progresso da tecnologia, crimes com a utilização do computador evoluíram. Claramente esse tipo de delito tinha características de um novo campo de conhecimento. Ainda segundo os mesmos autores, esse campo ficou conhecido como Computação Forense. Em 2005, na conferência *Digital Forensic Research Workshop* (DFRWS), o termo Forense Digital (FD) passou a ser mais comumente utilizado. A definição deste último termo será abordada no decorrer do presente artigo.

FD é um campo que lida com investigação de crimes relacionados à tecnologia (ORIWOH, JAZANI; EPIHANIOU, 2013). A FD é basicamente representada pela aplicação de disciplinas de ciências forenses em cenas de crimes fundamentados em eletrônica e que seguem certos procedimentos legais (HARBAWI; VAROL, 2017).

Sadiku, Tembely e Mussa (2017) afirmam que:

> A forense digital é um campo multidisciplinar e interdisciplinar que abrange diversas disciplinas, como criminologia, direito, ética, engenharia da computação e tecnologia da informação e comunicação, ciência da computação e ciência forense.

A partir das definições citadas neste artigo, considera-se a FD como um campo multidisciplinar que lida com investigação forense de evidências tecnológicas. Tais evidências, por sua vez, seguem procedimentos legais.

2.2. Computação Forense

Kondapally (2019) afirma que a CF lida com a identificação, coleta, análise e apresentação de evidências digitais de vários tipos de mídia de armazenamento digital em um *cybercrime* ou em incidentes de segurança da informação.

Costa (2011) acompanha essa afirmação:

> A CF é ciência que, através de técnicas especializadas, trata da coleta, preservação e análise de dados eletrônicos em um incidente computacional ou que envolvam a computação como meio, apresentando a prova do fato através de laudo pericial para a justiça.

Informação similar é exposta por McKemmish (1999) quando afirma que "a CF é o processo de identificar, preservar, analisar e apresentar evidências digitais de uma maneira legalmente aceitável".

A partir das definições citadas, considera-se CF como a ciência que, por meio das técnicas especializadas nomeadas como *preservar, analisar* e *apresentar as evidências digitais*, demonstra a prova do fato por intermédio de um laudo pericial.

2.3. Internet das Coisas

Em 1999, o termo Internet das Coisas foi apresentado primeiramente por Kevin Ashton, do Massachusetts Institute of Technolog (MIT) [Instituto de Tecnologia de Massachusetts], em uma exposição sobre RFID (acrônimo para *Radio-Frequency IDentification* ou, em Língua Portuguesa, Identificação por Rádio Frequência)) e a cadeia de suprimentos de uma grande companhia (CAVALCANTE, 2018).

Para Ashton (apud SILVA; SZESZ JUNIOR, 2018):

> A IdC se baseia na ideia de que estamos presenciando o momento em que duas redes distintas – a rede de comunicações humana (exemplificada na internet) e o mundo real das coisas – precisam se encontrar. Um ponto de encontro onde não mais apenas "usaremos um computador", mas onde o "computador se use" independentemente, de modo a tornar a vida mais eficiente. Os objetos – as "coisas" – estarão conectados entre si e em rede, de modo inteligente, e passarão a "sentir" o mundo ao redor e a interagir.

E, sobre o mesmo termo, Silva e Szesz Junior (2018) afirmam:

> A IdC é como uma rede de dispositivos físicos conectados, que permitem a interação entre si e com objetos externos, através de interfaces de controle e sensoriamento, possibilitando grande quantidade de dados e diversas formas de interação entre o mundo virtual e o real.

Peres e Sleiman (2017) também expõem conceito semelhante:

> A IdC se baseia em sensores conectados às "Coisas" e que, através de interfaces eletroeletrônicas de comunicação e controle, possam ser interligadas às redes, inclusive à Internet, para que os dados coletados pelos sensores possam ser tratados e correlacionados a outros dados e informações de outros objetos IdC ou de Bases de Dados existentes, através de aplicativos "Apps" e se transformarem em utilidades práticas para os usuários.

Como ponderam Santaella, Gala, Policarpo e Gazoni (2013), a IdC está se popularizando. Segundo os autores:

> [...] (vii) casas passam a ter sistemas inteligentes que regulam o funcionamento de seus aparelhos eletrônicos, elétricos, alarmes, climatização, janelas, portas etc.; (viii) veículos passam a ter direção inteligente, com capacidade de autocontrole em suas rotas, além de escolher os melhores caminhos possíveis; (ix) roupas inteligentes podem registar as mudanças de temperatura no exterior e ajustar-se de acordo com elas; (x) fábricas passam a ter inteligência

> e grande autonomia em seus processos; (xi) cidades passam a ser concebidas de modo inteligente [...]

Assim, a partir dessas definições, considera-se a IdC como uma rede de dispositivos físicos conectados que permitem a interação entre si e com objetos externos. Os objetos – as "coisas" – estarão conectados de modo inteligente e passarão a "sentir" o mundo ao redor e a interagir, inclusive conectados à internet, para que os dados coletados pelos sensores possam ser tratados e correlacionados a outros dados e outras informações de outros objetos.

3. Computação Forense para a Forense em IdC

Na CF, existem etapas definidas para a realização da perícia, que são: identificação, preservação, análise e apresentação.

- **Identificação:** é a primeira etapa da CF. Reconhecer a presença de uma evidência, onde e como ela está armazenada é vital na determinação de quais processos devem ser empregados para facilitar a sua recuperação (MCKEMMISH, 1999). Outra função dessa etapa é a emissão de um instrumento legal para estabelecer a busca e apreensão das evidências, indicando o que será apreendido. Ao executar a busca e apreensão, as evidências serão identificadas, documentadas e apreendidas (COSTA, 2011).

- **Preservação:** nesta etapa, se dá a manipulação das evidências por meio de coleta, documentação de custódia, embalagem, transporte e remessa para a perícia (COSTA, 2011).

  A respeito da etapa de Preservação, como expõe McKemmish (1999):

  > É obrigatório que qualquer exame dos dados armazenados eletronicamente seja feito da maneira menos intrusiva. Há circunstâncias em que as alterações nos dados são inevitáveis, mas é importante que ocorra a menor quantidade de alterações. Em situações em que a mudança é inevitável, é essencial que a natureza e a razão da mudança possam ser explicadas.

- **Análise:** fase em que serão analisados os exames e as evidências (COSTA, 2011). Por exemplo, quando é feita a clonagem de um disco rígido, os dados contidos dentro da

imagem ainda requerem processamento para que sejam extraídos de uma maneira legível para humanos (MCKEMMISH, 1999).

– **Apresentação:** é a etapa final, quando é realizada a materialização da prova por meio do laudo pericial (COSTA, 2011). De acordo com Mckemmish (1999), envolve a apresentação real em um tribunal. Esse processo inclui a forma de apresentação, a perícia e as qualificações do perito, além da credibilidade dos processos empregados para produzir a evidência que está sendo oferecida.

As etapas da Computação Forense são estruturadas para os dispositivos computacionais e não contemplam todos os dispositivos. Na Tabela 1, é apresentada uma possível visão da Computação Forense utilizando suas etapas na forense em IdC.

Tabela 1. Seções da forense em IdC

Etapas	*Comparação entre:*	
	Computação Forense	*Forense em IdC*
Identificação	Celulares, disco rígidos, redes, etc.	Sensores, televisão ou geladeira inteligentes, drones, etc.
Preservação	Equipamentos ou *softwares* (FTK, EnCase, etc.) que bloqueiam a escrita	*Hardware* e *software* proprietários entre os dispositivos
Análise	Com base nas teorias e nos princípios da tecnologia da informação	Dependem da natureza física e mecânica das coisas
Apresentação	Demonstrações em computadores ou telefones celulares	Demonstrações experimentais com as coisas que estavam envolvidas

Fonte: Adaptado de Liu (2015).

Considerando os dados da Tabela 1, um caso hipotético pode ser citado como exemplo: uma geladeira, conectada na rede, pode enviar um pedido ao supermercado, informando o estabelecimento sobre a falta de polpa de fruta. Nesse caso, em uma suposta situação de vulnerabilidade, um criminoso pode invadir a rede interna por meio do IP da geladeira, acessar o roteador e conseguir todo o controle dos dispositivos inteligentes da casa, sendo esse episódio considerando uma invasão de um ambiente inteligente. Nesse contexto, é apresentada a seguir uma análise básica de como seria uma forense em IdC usando as etapas da CF:

- **Identificação:** a geladeira é um novo dispositivo de tecnologia incorporada que não é um computador com o qual estamos habituados, mas sim um dispositivo que tem tecnologia suficiente para se comunicar com a rede interna, receber os comandos e os transmitir (WATSON; DEHGHANTANHA,2016).

- **Preservação:** Após identificar a evidência, é necessário preservar e coletar os dados. Uma possível coleta de dados poderia envolver os *logs* de rede entre a geladeira e o roteador.

- **Análise:** Analisar as evidências coletadas e preservadas.

- **Apresentação:** Desenvolver um relatório da análise.

Diante dessa análise pode-se imaginar o grande desafio para a forense em IdC.

Outra visão entre CF e Forense em IdC é demonstrada na tabela 2. Nota-se que algumas situações são similares como a Jurisdição e Propriedade, e outras são diferentes, como são destacados alguns aspectos: número de dispositivos na CF: bilhões de dispositivos; na forense em IdC: 50 bilhões, podendo chegar em 2020 a trilhões; quantidade e tipos de dados na CF: acima de *terabytes*; na forense em IdC: acima de *exabytes*; tipos de evidência na CF: documentos eletrônicos e formato de arquivo padrão; na forense em IdC: todos os formatos possíveis.

Considerando a tabela 2, constata-se a falta de padronização e o crescimento dos dados e dispositivos que, visivelmente, impactarão na análise forense em IdC.

Tabela 2. Seções da forense em IdC

Etapas	*Comparação entre:*	
	Computação Forense	*Forense em IdC*
Fontes de evidência	Computador, nuvem, virtualização, dispositivos de comunicação móvel, clientes da Web, redes sociais, servidores de autorização	Eletrodomésticos, carros, tags, leitores, sensores de sistemas embarcados, redes de sensores, implantes médicos em humanos e animais, etc.
Jurisdição	Individual, redes sociais, sociedade, empresa, governo	Individual, redes sociais, sociedade, empresa, governo
Número de dispositivos	Bilhões de dispositivos	50 bilhões até 2020 para trilhões de dispositivos
Tipos de evidências	Documentos eletrônicos, formatos de arquivos padrão, por exemplo JPEG, mp3 etc.	Qualquer e todos os formatos possíveis.

Etapas	*Comparação entre:*	
	Computação Forense	*Forense em IdC*
Quantidade e tipo de dados e evidências	Acima de *terabytes* de dados	Acima de *exabytes* de dados.
Protocolos	*Ethernet*, *wireless* (802.11 a,b,g,n), *bluetooth*, IPv4 and IPv6	RFID, RIME
Propriedade	Indivíduos, grupos, empresas, governos, etc.	Indivíduos, grupos, empresas, governos, etc.
Limites da rede	Limites relativamente definidos e linhas de propriedade	Linhas de limite cada vez mais desfocadas

Fonte: Adaptado de Oriwoh Jazani e Epihaniou (2013).

4. Forense em IdC

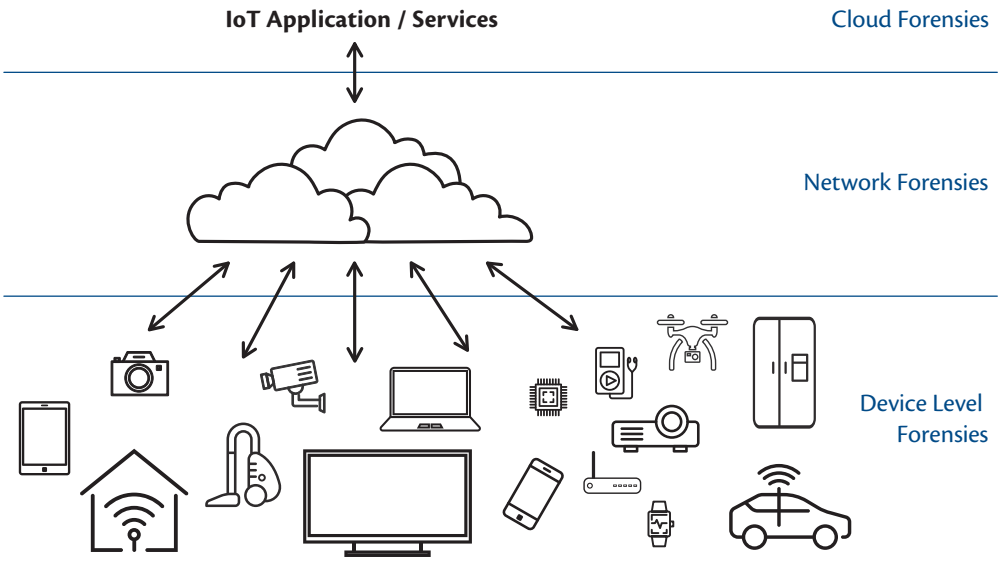
Com o avanço tecnológico e o crescimento da IdC, a perícia forense digital não está mais limitada aos exames em computadores, celulares, e-mails e sites eletrônicos. Atualmente, a perícia pode ser feita em relógios ou fechaduras inteligentes, drones, etc. É valiosa a diversidade de dados que esses dispositivos podem prover com base na interatividade com o usuário nas atividades diárias (BABUN, SIKDER, ACAR, ULUAGAC, 2018).

Por exemplo, um controle de acesso inteligente revela todos os usuários que entraram em um hospital durante um período.

Segundo Chi, Aderibigbe e Granville (2018), a forense em IdC é o processo de execução de procedimentos forenses digitais no paradigma da IdC.

A forense da IdC consiste em três seções: perícia em nuvem, perícia em rede e perícia em nível de dispositivo, como mostra a Figura 1.

Figura 1. Seções da forense em IdC



Fonte: Adaptado de Zawoad e Hansan (2015).

A respeito da perícia forense digital, Zawoad e Hansan (2015) afirmam que:

> Perícia na nuvem: como a maioria dos dispositivos de IdC tem baixo armazenamento e capacidade computacional, os dados gerados pelos dispositivos IdC e pelas redes IdC são armazenados e processados na nuvem.
>
> Perícia de rede: a origem de diferentes ataques pode ser identificada pelas informações que trafegam na rede. Existem diferentes tipos de redes: Rede de Área Corporal (BAN), Rede de Área Pessoal (PAN), Redes de Área Residencial/Hospitalar (HAN), Redes de Área Local (LAN) e Redes de Área Ampla (WAN).
>
> Perícia em nível de dispositivo: um investigador pode precisar coletar dados da memória local dos dispositivos IdC. Quando uma peça crucial de evidência precisa ser coletada dos dispositivos, ela envolve a perícia em nível do dispositivo.

A tabela 3 mostra uma visão que emprega as seções da forense em IdC juntamente com as etapas da CF, utilizando como exemplo o caso hipotético da seção anterior:

Tabela 3. Visão seções da forense em IdC juntamente com etapas da CF

Seções	*Forense em IdC*	
Perícia na nuvem	*Identificar*	*Dados armazenados*
	Preservar	
	Analisar	
	Apresentar	
Perícia de rede	*Identificar*	*Dados trafegados da rede LAN e WAN*
	Preservar	
	Analisar	
	Apresentar	
Perícia em nível de dispositivo	*Identificar*	*Dispositivos inteligentes: TV, geladeira, fogão, fechadura, lampâdas, aspirador de pó*
	Preservar	
	Analisar	
	Apresentar	

Fonte: Elaborada pelo o autor.

4.1. Modelos da forense em IdC

4.1.1. *Forensic-Aware IoT* (FAIoT):

No tocante a *Forensic-Aware IoT* (FAIoT), Zia, Liu e Han (2017) afirmam:

> O modelo FAIot contém dois módulos: Preservação Segura de Provas e Proveniência Segura. O primeiro monitora todos os dispositivos registrados e mantém o repositório de evidências. O segundo preserva o acesso às evidências para garantir sua integridade.

4.1.2. *Forensic State Acquisition from Internet of Things* (FSAIoT)

Meffert, Clark, Baggili e Breitinger (2017) ponderam, sobre *Forensic State Acquisition from Internet of Things* (FSAIoT), que:

> O modelo FSAIot contém um controlador centralizado *Forensic State Acquisition Controller* (FSAC) e três métodos de coleta de estado, cujo estado se refere ao estado atual de um dispositivo de IdC (Ex: porta aberta ou fechada). Os métodos são: controlador para o dispositivo IdC, controlador para a nuvem e controlador para o controlador.

4.1.3. *Forensics* Edge Management System (FEMS)

No que diz respeito a *Forensics Edge Management System* (FEMS), Zia, Liu e Han (2017) explicam que:

> No modelo FEMS, as duas principais funções são: serviços de segurança e forense. O primeiro inclui monitoramento de rede, detecção e prevenção de invasão, registro de dados e ferramentas de segurança. O segundo consiste em funções forenses como compressão de dados, análise, diferenciação, criação de cronograma, escalonamento de incidentes, preparação e apresentação de relatórios.

4.1.4. *Privacy-aware IoT-Forensics* (PRoFIT)

Com relação a *Privacy-aware IoT-Forensics* (PRoFIT), Nieto, Rios e Lopez (2018) expõem:

> No modelo PRoFIT, considera-se uma série de princípios de privacidade que são aplicados em todo o ciclo de vida dos dados pessoais, a fim de permitir que os cidadãos mantenham o controle das informações confidenciais armazenadas em seus dispositivos de IdC enquanto colaboram com uma investigação.

O PRoFIT foi avaliado na propagação real do malware em uma cafeteria habilitada para IdC (YAQOOB, HASHEM, AHMED, KAZMI e HONG, 2019).

4.1.5. *IoT Forensic Model*

No que se refere à *IoT Forensic Model*, Li, Choo, Sun, Buchanan e Cao (2015) esclarecem que:

> O *IoT Forensic Model*, a princípio, tem uma classificação rígida, onde os papéis da IdC são classificados em: IdC como um alvo, IdC como uma ferramenta e IdC como uma testemunha. Em seguida, cada dispositivo relacionado e os aplicativos complementares são examinados usando o processo das quatro etapas da Computação Forense. Além disso, todos os artefatos forenses adquiridos são armazenados em um repositório de evidências criptografado.

4.2. Casos de forense em ambiente inteligente

4.2.1. Sistema de transporte inteligente

Como exemplo de aplicação de sistema de transporte inteligente, alguns países, como Singapura, têm adotado esse modo de organização da mobilidade, por meio da configuração e instalação, em seus sistemas de transporte, de dispositivos inteligentes e configurados para gerenciar o tráfego e evitar o problema de congestionamento das grandes metrópoles.

A respeito do tema, Yaqoob, Hashem, Ahmed , Kazmu e Hong (2019) declaram:

> A precisão é um dos parâmetros mais importantes que devem ser considerados no sistema de transporte inteligente. Informações incompletas e erradas podem causar acidentes graves nas estradas. No caso de acidente, o investigador forense é obrigado a saber o que e como algo deu errado. A investigação pode ajudar a mitigar problemas causadores de acidentes ou outros problemas, como congestionamento de tráfego.

4.2.2. Sistema de monitoramento de saúde inteligente

De modo a facilitar a compreensão a respeito do funcionamento desse sistema, considera-se como exemplo de caso o de um jovem com diabetes e que necessite utilizar um dispositivo que monitora o teor de açúcar de sangue. Este jovem mora em uma casa e tem acesso aos dispositivos de um hospital inteligente, conectados na internet.

Nesse caso hipotético, Zawoad e Hansan (2015) afirmam que:

> Pode ser criado um malware inteligente para coletar dados dos dispositivos inteligentes da assistência médica do hospital. Primeiro, ele infecta a geladeira inteligente da casa, conecta-se com o dispositivo que monitora a glicose do jovem, através da rede compartilhada e, finalmente, infecta o referido dispositivo. Mais tarde, quando o jovem vai ao hospital para trabalhar, o malware procura outros dispositivos que compartilham a mesma rede que o dispositivo. Desta forma, o malware é capaz de infectar centenas de dispositivos médicos inteligentes localizados no hospital e roubar registros médicos eletrônicos confidenciais.

Percebe-se que a investigação se torna um desafio diante da variedade de dispositivos e dos registros de rede gerados entre eles.

4.2.3. Sistema em lugares inteligentes

Ainda com o objetivo de facilitar a compreensão a respeito desse exemplo, faz-se necessário explicar o conceito sobre testemunha digital.

Segundo Nieto, Roman e Lopez (2016):

> Parece razoável definir casos em que vários dispositivos se comportam como testemunhas humanas. Por isso, definimos a testemunha digital como um dispositivo que é capaz de colaborar no gerenciamento de evidências eletrônicas, tanto do ponto de vista tecnológico quanto legal.

De acordo com Nieto, Rios e Lopez (2018), o principal objetivo da abordagem das testemunhas digitais é implantar a cadeia de custódia digital (documentação de todas as informações coletadas) na IdC.

No caso a seguir, o PRoFIT é aplicado em uma abordagem de testemunha digital. Nesse novo exemplo, o ambiente é um shopping center, onde uma jovem passeia entre as lojas, portando o seu celular. Esse exemplo é assim descrito por Nieto, Rios e Lopez (2017):

> Joana tem um telefone celular com o PRoFIT instalado. Suponha que Joana entre em uma cafeteria na qual existem vários dispositivos de IdC, tanto pessoais quanto não-pessoais. Durante sua permanência na loja, o celular de Joana detecta um ataque que vem de um dispositivo de ambiente. Depois de detectar o ataque, o PRoFIT decide armazenar as informações relativas a ele. Além disso, faz um hash das evidências coletadas e alerta Joana. Parece que algum dispositivo no ambiente está infectado e tenta espalhar um worm aproveitando-se de uma vulnerabilidade no aplicativo, que utiliza tecnologia Bluetooth para escanear outros dispositivos no ambiente e, assim, conhecer as ofertas do dia e o número de unidades de alimentos disponíveis (por exemplo, em geladeiras).

5. Desafios da análise forense em IdC

5.1. Dados

5.1.1. Localização dos dados

Os dados podem estar armazenados em celulares, ou em qualquer coisa que tenha um dispositivo de armazenamento, ou mesmo na nuvem (CHI, ADERIGIGBE E GRANVILLE, 2018). Considerando que a nuvem pode estar em diferentes países e que os dados, por sua vez, podem ser movidos entre os países, há um risco de problema de jurisdição dos dados.

5.1.2. Quantidade e tipos dos dados

A quantidade de dispositivos interconectados na rede e a imensa troca de informação geram uma grande quantidade e tipos de dados.

5.1.3. Extração dos dados

A maioria dos fabricantes de dispositivos desenvolve diferentes *hardwares* e sistemas operacionais. Com essa despadronização, a extração de dados se torna um problema.

5.1.4. Formato dos dados

Existem vários formatos de dados na análise em IdC. O formato que está armazenado na nuvem pode ser diferente do formato dos dados gerados pelo dispositivo.

Segundo Chi, Aderibigbe e Granville (2018):

> Para se ter uma análise padronizada, os dados precisam ser retornados ao seu formato original antes que a análise possa ser executada. Devido à segurança limitada em dispositivos IdC, as evidências podem ser modificadas ou excluídas. O que poderia tornar a evidência não admissível ao tribunal.

5.1.5. Dados perdidos

A vida útil dos dados armazenados nos dispositivos de IdC é curta e esses dados podem ser facilmente sobrescritos, com possibilidade de perda de evidências.

De acordo com Alabdulsalam, Schefer, Kechadi e Lekhac (2018):

> Um dos problemas é o período de sobrevivência das evidências em dispositivos IdC antes de serem sobrescritos. Transferir os dados para a nuvem pode ser uma solução fácil para resolver esse desafio. No entanto, apresenta outro desafio relacionado à garantia da cadeia de evidências e como comprovar que as evidências não foram alteradas ou modificadas.

5.2. Evidencia digital

5.2.1. Localização da evidência

Outro desafio é o armazenamento de dados em datacenters localizados em diversos países com suas respectivas jurisdições. De acordo com Oriwoh, Jazani e Epihaniou (2013), esse fato já é um problema reconhecido pelos peritos devido às possíveis distorções nas leis aplicadas nesses locais. Esse desafio será espelhado na IdC devido à quantidade de dados armazenados na nuvem.

5.2.2. Tipos de evidência

Segundo Alabdulsalam, Schefer, Kechadi e Lekhac (2018), na primeira etapa da CF, geralmente são identificados os computadores e celulares como fonte de evidência. Como mencionado no caso citado no item sobre *Computação Forense para a Forense em IdC*, uma geladeira pode ser uma evidência no cenário de Forense em IdC.

Outros eletrodomésticos podem se tornar fontes de evidências, como máquinas de lavar louça, aspiradores de pó, monitores de bebê, etc. (ORIWOH, JAZANI e EPIHANIOU, 2013).

Conforme Chi, Aderibigbe e Granville (2018), alguns desses dispositivos poderiam ser muito pequenos e, erroneamente, ignorados ou, ao contrário, muito grandes a ponto de dificultar o transporte para o laboratório, de modo que fosse realizada a aquisição, configurando outro desafio para os peritos em termos de criação de espaço.

5.3. *Hardware* e *software*

Devido à ampliação do número de dispositivos, houve um aumento também no número de fabricantes com suas diferentes arquiteturas de *hardware* e, consequentemente, surgiram

heterogêneos sistemas operacionais. Além disso, existem diversos fornecedores e múltiplos padrões de *software* e *hardware* proprietários.

5.4. Dispositivos

5.4.1. Desligar um dispositivo

Caso um dispositivo seja considerado fonte de ataques maliciosos, um provável procedimento de segurança seria desligá-lo, mas, por motivos variados, talvez esse dispositivo não possa ser desligado. Nesse caso hipotético, Yaqoob, Hashem, Ahmed, Kazmu e Hong (2019) descrevem dois cenários:

> Fábrica inteligente: um frigorífico é identificado como uma fonte de geração de pacotes maliciosos. O alimento pode estragar se a câmara fria for desligada. Portanto, o proprietário pode não permitir que os investigadores desliguem a máquina.
>
> Sistema de Transporte Inteligente: os dispositivos não podem ser impedidos de funcionar, mesmo que algo seja identificado como suspeito por alguns motivos.

Lidar com esses cenários será um desafio para o perito. Em razão da criticidade do equipamento, a análise forense deverá aguardar o momento oportuno para desligar o dispositivo, porém, considerando a possibilidade de que esse tempo poderá destruir as evidências.

5.5. Jurisdição

De acordo com Oriwoh, Jazani e Epihaniou (2013):

> Existe um aumento na complexidade jurídica, tendo em vista que os dispositivos se encontram em países diferentes. Com a IdC, percebe-se um aumento no número de dispositivos usados entre as redes privadas, pessoais e públicas.

Em virtude do aumento do número de dispositivos com a IdC, essas questões certamente correspondem a um novo desafio para a jurisdição mundial, resultando em inúmeras e ainda mais complexas relações e discussões jurídicas.

5.6. Nuvem

5.6.1. Autenticação

No que diz respeito à autenticação, Alabdulsalam, Schefer, Kechadi e Lekhac (2018) explanam:

> A maioria das contas é de usuários anônimos porque o serviço de nuvem não exige as informações precisas do usuário para se inscrever em seu serviço. Isso pode levar à impossibilidade de identificação de um criminoso. Por exemplo, mesmo que os investigadores encontrem uma evidência na nuvem que prove que um determinado dispositivo de IdC na cena do crime é a causa do crime, isso não significa que essa evidência possa levar à identificação do criminoso.

5.7. Big Data

Segundo Yaqoob, Hashem, Ahmed, Kazmu e Hong (2019):

> A capacidade de analisar uma enorme quantidade de dados da IdC ajuda os investigadores a lidar com muitas informações que poderiam ter um impacto na investigação e, assim, reduz a taxa de criminalidade dentro da cidade. A maior complexidade envolve o processamento de big data para executar a análise dos dados disponíveis para a investigação. Além disso, a escalabilidade dos algoritmos analíticos poderia ter um grande impacto na investigação.

6. Conclusão e trabalhos futuros

Foi observado que as etapas identificação, preservação, análise e apresentação da Computação Forense são estruturadas para os dispositivos computacionais e não contemplam todos os dispositivos em IdC, mas podem ser absorvidas na perícia em Internet das Coisas por meio da análise das seguintes seções: perícia em nuvem, perícia em rede e perícia em nível de dispositivo.

Foram apresentados alguns modelos e estudos de caso. Dentre esses, destaca-se um exemplo cujo modelo PRoFIT usa uma abordagem de testemunha digital. Isto significa que o *software* analisa a comunicação entre os dispositivos, coleta e armazena os dados, informando ao usuário a possibilidade de qualquer ataque. Caso aconteça algum crime, os dados consolidados serão fontes de evidência. A abordagem testemunha digital implementa uma cadeia de custódia digital usando dispositivos pessoais.

Foram avaliados alguns dos desafios em forense e identificadas as dificuldades em analisar os dados com vários formatos e em armazená-los em datacenter localizado em qualquer parte do mundo. A imensa quantidade de sensores conectados a qualquer coisa que se comunique através da rede tornou-se uma grande adversidade para os profissionais forenses digitais.

Para sugestões de trabalhos futuros propõe-se a análise de um modelo de forense em *Internet of Nano-Things* usando a abordagem testemunha digital.

Referências

ALABDULSALAM, Saad; SCHEFER, Kevin; KECHADI, Tahar; LEKHAC, Nhien-An. Internet of things forensics: challenges and case study. *In:* IFIP INTERNATIONAL CONFERENCE ON DIGITAL FORENSICS, 14., Nova Delhi, India, 3-5 Jan. 2018. Publicado em: **Advances in Digital Forensics XIV**, Heidelberg, Germany, Springer, p.53-66, 2018. Disponível em: *https://arxiv.org/ftp/arxiv/papers/1801/1801.10391.pdf*.

BABUN, Leonardo; SIKDER, Amit K; ACAR, Abbas; ULUAGAC, Selculk. IoTDots: A digital forensics framework for smart environments. 2018. **ACM Internet of Things Journal (ACM IoT)**. Disponível em: *https://arxiv.org/pdf/1809.00745.pdf*.

BEM, Derek; FELD, Francine; HUEBNER, Ewa; BEM; Oscar. Computer forensics - past, present and future. **Journal of Information Science and Technology**, v. 5, n. 3, p. 43-59. 2008. Disponível em: *http://www.cis.gsu.edu/rbaskerville/cis8630/Bernetal2008.pdf*.

CAVALCANTE, Jean Wilson Aguiar. **Emprego de Internet das Coisas, como ferramenta de Monitoramento da Poluição sonora visando ao planejamento de Política Pública, na Área de Segurança.** Artigo apresentado ao CAESP da Secretaria de Segurança Pública, em cooperação técnica com a Universidade Estadual de Goiás, como requisito parcial para obtenção do título de especialista em Gestão de Segurança Pública. 2018, 29p. Disponível em: *https://www.academia.edu/37623063/Emprego_de_Internet_das_Coisas_como_Ferramenta_de_Monitoramento_da_Polui%C3%A7%C3%A3o_Sonora_visando_ao_Planejamento_de_Pol%C3%ADticas_P%C3%BAblicas_na_%C3%81rea_de_Seguran%C3%A7a*.

COSTA, Marcelo Antonio Sampaio Lemos. **Computação forense – a analise forense no contexto da resposta a acidentes computacionais.** 3. ed. Campinas: Millennium, 2011. Disponível em: *http://www.millenniumeditora.com.br/produtos_descricao.asp?codigo_produto=556&so=Normal*.

CHI, Hongmei; ADERIBiGBE; Temilola; GRANVILLE, Bobby C. A Framework for IoT data acquisition and forensics analysis. *In:* IEEE International Conference on Big Data (Big Data), 2018. Seattle, WA, USA, 10-13 Dec. 2018. **Proceedings...**2018. Disponível em: *https://ieeexplore.ieee.org/document/8622019.*

ELEUTÉRIO, Pedro Monteiro da Silva ; MACHADO, Marcio Pereira. **Desvendando a computação forense.** 1. ed. São Paulo: Novatec, 2011. 200 p. ISBN: 978-85-7522-260-7.

HARBAWI, Malek; VAROL Asaf. An Improved digital evidence acquisition model for the internet of things forensic i: a theoretical framework. *In:* International Symposium on Digital Forensic and Security (ISDFS), 5., Tirgu Mures, Romania, 26-28 apr 2017. **Proceedings...** 2017. Disponível em: *https://ieeexplore.ieee.org/document/7916508.*

HUNG, Mark. **Leading the IOT gartner insights on how to lead in a connected world.** 2017. 29p. Disponível em: *https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf.* Acesso em: 25 abr 2019.

KONDAPALLY, Bhanu Prakash. **What is Iot forensics and How is it diferente from Digital Forensics.** 2018. Disponível em: *https://cover2investigations.com/what-is-iot-forensics-and-how-is-it-different-from-digital-forensics/.* Acesso em: 08 mai 2019.

LI, Shancang; CHOO, Kim-Kuwang Raymond; SUN, Qindong; BUCHANAN, Willian J.; CAO, Jiuxin. IoT Forensics: Amazon Echo as a use case. **IEEE Internet of Things Journal** v. 14, n. 8, p. 1-17. 2015. Disponível em: *http://eprints.uwe.ac.uk/40122/1/iotfR2.pdf.*

LIU, Jigang. IoT Forensics issues, strategies and challenges. *In:* IDF Annual Conference, 12., Tokio. 15 Dec 2015. **Proceedings...** 2015. 20 p. Disponível em: *http://docplayer.net/29316868-Iot-forensics-issues-strategies-and-challenges.html.* Acesso em: 08 mai 2019.

MCKEMMISH, Rodney. **What is Forensic Computing?** Canberra: Australian Institute of Criminology, jun 1999. 6p. (Trends and Issues in Crime and Criminal Justice series: 118). Disponível em: *https://pdfs.semanticscholar.org/2b86/6f239f498d7d0c9a0ebc3622a9e671975se7.pdf.*

MEFFERT, Chistopher; CLARK, Devon; BAGGILI, Ibrahim; BREITINGER, Frank. Forensic state acquisition from internet of things (FSAIoT): a general framework and practical approach for IoT forensics through IoT device state acquisition. *In:* ARES '17 INTERNATIONAL CONFERENCE ON AVAILABILITY, RELIABILITY AND SECURITY, 12., Reggio Calabria, Italy — aug 29-sep 01, 2017. **Proceedings ...** Article n. 56. Disponível em: *https://dl.acm.org/citation.cfm?id=3104053.*

NIETO, Ana; RIOS, Ruben; LOPEZ, Javier. IoT - Forensics meets privacy: towards copperative digital investigation. **Sensors**, v. 18, n. 2, p. 492. 2018. Disponível em: *https://www.mdpi.com/1424-8220/18/2/492*.

NIETO, Ana; RIOS, Ruben; LOPEZ, Javier. PRoFIT: modelo forense-IoT con integración de requisitos de privacidad. *In:* JORNADAS DE INGENIERÍA TELEMÁTICA (JITEL 2017), 8., Valencia (España), 27-29 sep 2017 **Actas...** 2017. 8p. Disponível em: *http://ocs.editorial.upv.es/index.php/JITEL/JITEL2017/paper/view/6449*.

NIETO, Ana; ROMAN, Rodrigo; LOPEZ, Javier. Digital witness: safeguarding digital evidence by using secure architectures in personal devices. **IEEE Network**, v. 30, n. 6, nov 2016 p.34–41. Disponível em: *https://ieeexplore.ieee.org/document/7764297*.

ORIWOH, Edewede; JAZANI, David; EPIPHANIOU, Gregory; SANT, Paul. Internet of things forensics: challenges and approaches. 2013. *In:* IEEE International Conference on Collaborative Computing: Networking, Applications and worksharing,9., 2013, **Proceedings...** 2013, p. 608-615. Disponível em: *https://eudl.eu/doi/10.4108/icst.collaboratecom.2013.254159*.

PERES, João Roberto; SLEIMAN, Cristina Morais. **IOT Investigação forense digital fundamentos e guia de referências.** 1. ed. São Paulo: 2017. 92 p. Disponível em: *http://www.ntsc-br.com/data/documents/e-Book-IoT-Investigacao-Forense-Digital-vPre2c.pdf*. Acesso em: 01 mai 2019.

SADIKU, Matthew N. O.; TEMBELY, Mahamadou; MUSA, Sarhan M. Digital Forensics. **International Journal of Advanced Research in Computer Science and Software Engineering**, v. 7, n. 4, apr 2017 p.274-276. Disponível em: *http://ijarcsse.com/Before_August_2017/docs/papers/Volume_7/4_April2017/V7I4-01404.pdf*.

SANTAELLA, Lucia; GALA Adelino; POLICARPO, Clayton; GAZONI, Ricardo. Desvelando a internet das coisas. **Revista GEMInIS** (Online), v. 1, n. 2, ano 4, p. 19-32, 2013. Disponível em: *http://www.revistageminis.ufscar.br/index.php/geminis/article/view/141/pdf*. Acesso em: 30 apr 2019.

SILVA, Sani de Carvalho Rutz; SZESZ JUNIOR, Albino. Internet das Coisas na educação: uma visão geral. **Ensino de Ciências e Tecnologia em Revista,** v. 2, n. 1. jul/ago 2018. p. 57-69. Disponível em: *http://srvapp2s.urisan.tche.br/seer/index.php/encitec/article/view/2717*.

WATSON, Steve; DEHGHANTANHA, Ali. Digital forensics: the missing piece of the Internet of Things promise. **Computer Fraud & Security,** n. 6, p. 5-8, jun 2016. Disponível em: *https://www.sciencedirect.com/science/article/pii/S1361372315300452?via%3Dihub*.

YAQOOB, Ibrar; HASHEM Ibrahim Abaker Tagior; AHMED Arif; KAZMI S.M. Ahsan; HONG Choong Seon. Internet of things forensics: recent advances, taxonomy, requirements, and open challenge. **Future Generation Computer Systems,** v. 92, mar 2019, p. 265-275. Disponível em: *https://www.sciencedirect.com/science/article/pii/S0167739X18315644?via%3Dihub.*

ZAWOAD, Shams; HASAN Ragib. FAIoT: Towards building a forensics aware eco system for the internet of things. *In:* IEEE INTERNATIONAL CONFERENCE ON SERVICES COMPUTING (SCC). New York, NY, USA, 27 jun-2 jul 2015. **Proceedings...** 2015. Disponível em: *https://ieeexplore.ieee.org/document/7207364.*

ZIA, Tanveer A.; LIU, Peng; HAN Weile. Application-specific digital forensics investigative model in internet of things (IoT). *In:* ARES '17 INTERNATIONAL CONFERENCE ON AVAILABILITY, RELIABILITY AND SECURITY, 12., Reggio Calabria, Italy — aug 29-sep 01, 2017. **Proceedings ...** 2017. Disponível em: *https://pennstate.pure.elsevier.com/en/publications/application-specific-digital-forensics-investigative-model-in-int.*

ZULKIPLI, Nurul Huda Nik; ALENEZI, Ahmed; WILLS, Gary. IoT Forensic: bridging the challenges in digital forensic and the internet of things. *In:* INTERNATIONAL CONFERENCE ON INTERNET OF THINGS, BIG DATA AND SECURITY, 2., – v.1: IoTBDS, Porto, Portugal, 2017. **Proceedings...** 2017, p. 315-324. Disponível em: *http://www.scitepress.org/DigitalLibrary/Link.aspx?doi=10.5220/0006308703150324.*