IoT Investigação Forense Digital

Fundamentos e Guia de Referências

JOÃO ROBERTO PERES
CRISTINA MORAES SLEIMAN

JOÃO ROBERTO PERES
CRISTINA MORAIS SLEIMAN

IoT
Investigação Forense Digital
Fundamentos e Guia de Referências

1ª edição

São Paulo
João Roberto Peres
2017

IoT - Investigação Forense Digital

Fundamentos e Guia de Referências

Este e-book foi produzido com o objetivo de garantir a maior acessibilidade possível para todos os interessados.

O formato PDF empregado atende aos requerimentos das Normas Internacionais ISO 32000-1:2008, e ISO 14289-1:2014.

Este e-Book também será publicado em outros formatos.

Para consultar a obra no cadastro Internacional do ISBN acesse o link: < https://www.cblservicos.org.br/isbn/pesquisa/ > selecione consulta por ISBN e digite o código ISBN= 9788592315818

IoT - Investigação Forense Digital

Fundamentos e Guia de Referências

Os autores afirmam que mesmo havendo processo de depósito legal de COPYRIGHT ©, e proteção garantida pela constituição federal, amparada na lei 9.610 de 1998, os leitores podem utilizar os textos aqui publicados, desde que citem explicitamente a fonte.

1ª Edição – Novembro de 2017

Dados internacionais de Catalogação na Publicação (CIP)
Catalogação na Fonte por Autores

P512i / S174i
Peres, João Roberto, 1949 – e Sleiman, Cristina Moraes –
IoT – Investigação Forense Digital: Fundamentos e Guia de Referências) / João Roberto Peres – Cristina Moraes Sleiman – São Paulo : Ed. do Autor, 2017.
Recurso Digital - Formato PDF 3,9 Mb. Requisitos do Sistema: Adobe Acrobat Reader ou similar. Modo de Acesso: World Wide Web

Bibliografia.
ISBN: 978-85-923158-1-8 (Recursos Digital)

1.Internet das Coisas - 2. Investigação de Crimes Eletrônicos e Digitais – 3. Perícia Forense Computacional – 4.Apresentação de Caso de Investigação IoT – I. Título.

CDD 347.9:004
CDU 340.6:004

EDIÇÃO PRELIMINAR DOS AUTORES

Declaração

- Este documento foi concebido como contribuição aos interessados nos temas relacionados a de Investigação Forense Computacional em crimes cibernéticos associados a Internet das Coisas IoT" como em assuntos correlatos a IoT/IoE, entre outros. Os autores não se responsabilizam por disponibilizadas por terceiros, em suas fontes de pesquisa, a não ser os direitos de propriedade autorais que são explicitamente citados, o que significa que se houver qualquer discordância quanto a precisão e veracidade das informações, solicita-se que o identificador se manifeste por escrito ao(s) para que se possa validar as discordâncias e efetuar os ajustes correspondes, se for o caso.
- As informações contidas neste documento são destinadas a fornecer apenas um resumo, visão geral e fundamentos sobre os temas propostos. Não há pretensão de se aprofundar ou esgotar os temas. Os constituem e nem devem ser tratados como aconselhamento jurídico, acadêmico ou representam advogados e engenheiros.
- Os autores não são responsáveis por qualquer prejuízo sofrido como resultado da confiança nas desta publicação, por se tratar de uma obra com uma visão geral e não aconselhamento técnico-jurídico dedicado, que por sua vez deve ocorrer especificamente e voltado à peculiaridade de cada empresa. se recomenda procurar aconselhamento profissional específico para se implantar programas de alcancem a Segurança Cibernética e a Conformidade requerida em organizações.
- Evitou-se ao máximo, utilizar formatação e linguagem tipicamente jornalística, jurídica, técnica ou acadêmica.
- Os autores: 1- João Roberto Peres - Professor e Consultor da FGV, especialista em Segurança Corporativa Crimes Cibernéticos, é também owner de empresas ligadas a Gestão e Segurança Empresarial. 2- Cristina Moraes Sleiman, Professora do programa de pós-graduação em Direito Digital e Compliance da Faculdade Damásio, Presidente da Comissão de Educação Digital e 2ª Vice-Presidente da Comissão de Direito Digital e Compliance da OAB-SP.
- Os textos aqui publicados não refletem em nenhuma hipótese a opinião ou concordância das instituições FGV/OAB, entre outras, ou das organizações APOIADORAS, PATROCINADORAS e DIVULGADORAS, mas sim, única e exclusivamente o entendimento dos autores.

- Todas as figuras foram produzidas e tratadas pelo autor 1. Quando se utilizou de figuras de terceiros estas foram de fontes que declaram ser "free" com licença CCO Public Domain - Grátis para uso comercial - Atribuição não como exemplo a biblioteca - Free illustrations on Pixabay, que pode ser acessada via web através do endereço: <https://pixabay.com/pt/ >. Veja também < http://br.freepik.com/ >.
- Uso massivo do "Full Grammarly's Grammer and Plagiarism Checker": < https://www.grammarly.com/plagiarism-checker >

SUMÁRIO

Capítulos

Conteúdo de Terceiros citados sempre em fonte "*Calibri Itálico*" entre aspas "*texto*" .
Textos entre sinais maior/menor < > = indicação de hiperlinks www citados, escritos em fonte Agency BF .
Textos entre colchetes { *xxxxx* } = *notas específicas dos autores.*

Edição preliminar – sem revisões – não comercial

Fundamentos de IoT

- O que é IoT.
- Porque este e-book foi escrito.

• IoT

Neste especial momento da evolução da Internet observamos o desenvolvimento de diversas tecnologias que sustentam o fenômeno que hoje chamamos de "Internet das Coisas - e até porque não dizer a "Internet de Tudo -IoE[2]".

Na prática, a "Internet das Coisas", se constitui na ampliação da capilaridade de da Internet, não somente a smartphones, tabletes, roteadores, impressoras, notebooks, câmeras vídeo IP, TVs, desktops, Servidores, etc., mas agora, em tudo, que se possa ligar sensores e interfaces eletroeletrônicas de conectividade e comando, "coisas" como torradeiras, geladeiras, automóveis, lâmpadas, bicicletas, relógios, roupas, calçados, perucas, óculos, cadeiras, chuveiros, ferramentas, armas civis e militares, fornos, fogões, robôs industriais, aparelhos de ar e calefação, persianas e cortinas, marca-passos e desfibriladores inteligentes, equipamentos colaborativos e de pesquisa, canetas, coleiras de animais domésticos, etc..

Entre milhares de outras possibilidades de conexões da Internet há dispositivos ou o que importa é a integração de dados, gerados nesses dispositivos autônomos, ligando-os as aplicações (App_S) e as inter-relações a outras Bases de Dados (Big Data), para cruzamento e informações de decisão e acionamento de controle remoto, desses dispositivos inteligentes.

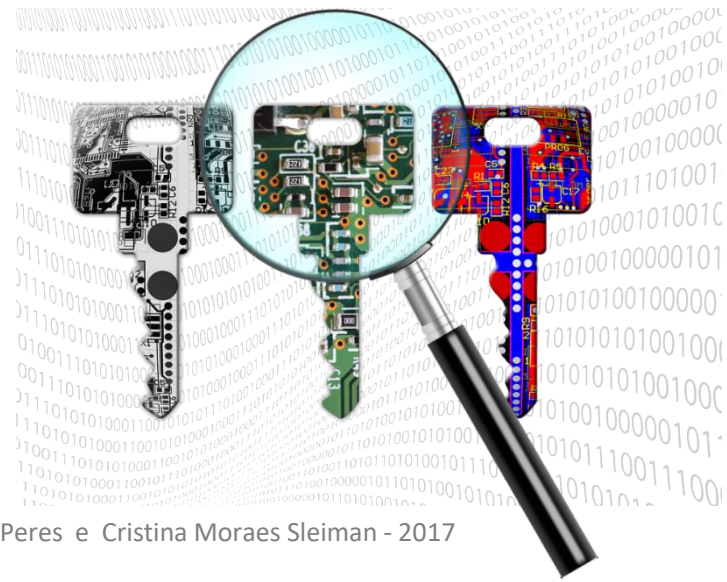
Exemplificada de outra forma, IoT se baseia em "sensores[3]" conectados as "Coisas" e através de interfaces eletroeletrônicas de comunicação e controle, possam ser interligadas as inclusive a Internet, para que os dados coletados pelos sensores possam ser tratados e outros dados e informações de outros objetos IoT ou de Bases de Dados existentes, através de aplicativos "App_s." e se transformarem em utilidades práticas para os usuários.

IoT se caracteriza por possibilitar capacidade de autonomia e de inteligência artificial "Coisas" que podem responder e se modificar as variações do ambiente, desde que estejam devidamente programadas.

A Internet como a conhecemos, tornou mais fácil o cometimento de crimes, oferecendo aos criminosos uma entrada para disseminar ataques com relativa obscuridade, ou seja, com a esperança de serem anônimos. IoT potencializa o fato.

A crescente e evolutiva complexidade da infraestrutura e dos dispositivos de comunicação e de redes, inclusive de IoT, no ambiente global e transfronteiras, da Internet, tornou difícil a investigação de "cibercrimes". Vestígios, pistas de atividades ilegais, e formação de evidências, são muitas vezes submersas em grandes volumes de dados (Big Data) que precisam ser peneirados e garimpados a fim de se identificar a possibilidade de detectar crimes e elencar evidências forenses em provas efetivas.

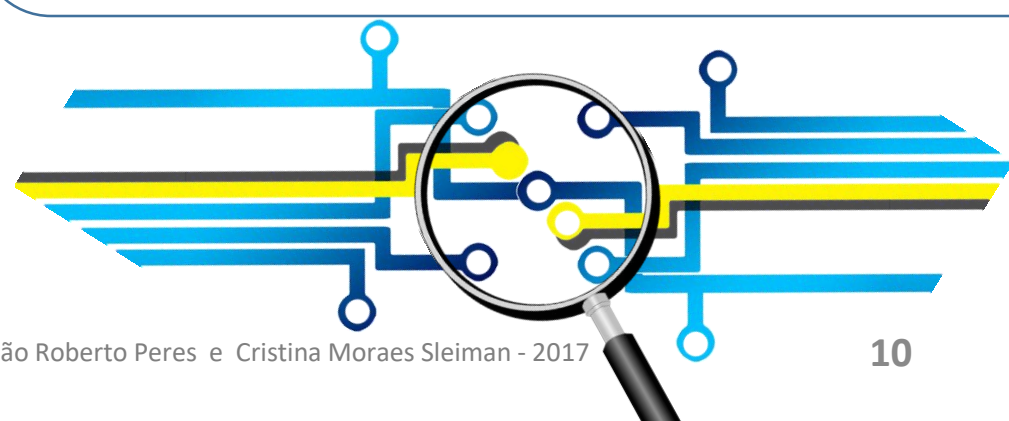
O campo científico da investigação forense digital, principalmente de IoT e da ciber-criminalidade através desses objetos IOT-ware, tornou-se muito importante para se obter a garantia de informações concretas, que sustentem a aplicação das leis locais e internacionais, e para a segurança e defesa da soberania nacional. Investigação digital e a investigação forense cibernética, são áreas multidisciplinares que englobam o direito, informática, finanças, telecomunicações, análise de dados, engenharia eletroeletrônica e mecânica fina, cooperação internacional, governança Global, e vai muito, muito além.



Considerando o contexto exposto, resolvemos escrever estes breves esclarecimentos, neste e-book, conscientes de que ainda não há no mundo consenso sobre os problemas de segurança quando se adiciona IoT/IoE no cotidiano, muito menos da complexidade que possam envolver as investigações de eventos litigiosos, crimes, e ou, outras circunstâncias, para a solução de casos questionáveis.

Neste e-book não se busca o aprofundamento do tema ou a exploração de maior abrangência, pois, ainda tudo é muito novo em "IoT". Mas, com base em visão sistêmica é possível estabelecer uma linha de pensamento adequada na busca de resultados quanto a possibilidade de investigar litígios e crimes cometidos através da Internet, envolvendo aparelhos e artefatos "Coisas" nas bordas da rede, no ambiente sistêmicos de "IoT".

[1]**Internet das Coisas – IoT** – (Internet of Things) expressão cunhada por Kevin Ashton em 1999 durante o desenvolvimento do projeto "Auto-ID" de (RFID) do MIT (Massachusetts Institute of Technology). Seu uso se popularizou.
[2]**Internet de Tudo – IoE** – (Internet of Everything) a expressão é atribuída às estratégias de marketing da gigante de tecnologia Cisco, mas, tem apoio da União Internacional de Telecomunicações (UIT) que afirma que "O mundo hiperconectado da "internet de tudo" começa a se tornar realidade."
[3]**Sensores** – são dispositivos eletrônicos ou mecânicos que respondem a estímulos físicos/químicos de forma mensurável analógica ou digital. (Base de fundamentação Wikipedia)



Os riscos de IoT

- Atuais motivos que afetam objetos IoT e os tornam mais vulneráveis.
- As oportunidades que IoT pode oferecer para as futuras investigações cibernéticas.

Riscos de IoT

A Internet das Coisas se caracteriza por adicionar novos e inéditos objetos "Coisas" conectáveis as redes, inclusive a Internet, na maioria das vezes com baixo custo, no entanto, objeto inteligente conectado as redes poderá ou não ser controlado através de um computador ou smartphone.

A conectividade estabelecida a partir da IoT (Internet of Things) potencializou a sistemática de mensagens de sinalização de sensores, atuadores e controladores, através de fechadas ligadas a Internet, por onde trafegam essas informações, na maioria da vezes abertas e a interceptações Hacker que podem adulterar as mensagens sem deixar vestígios, de forma que a quebra da integridade das informações passe despercebida. Uma informação de um "sensor" adulterada por Hackers/Crackers pode produzir da simples estatística errônea até acidentes inesperados, como um retorno de comando para um atuador girar abruptamente o volante um Automóvel Autônomo em alta velocidade.

Aplicações IoT estão em plena expansão de implantação no mundo corporativos, sendo entendidas como solução para milhares de problemas de digitalização empresarial e também para diversos segmentos de atendimento as necessidades humanas em geral. A cada nova IoT desenvolvida, surgem novos desafios que necessitam ser superados para garantir a CID (Confiabilidade, Integridade e Disponibilidade) das informações sistêmicas transmitidas e

O potencial de riscos que os novos dispositivos de IoT integrados a Internet oferecem é grande, que a comunidade **OWASP**[1] "Open Web Application Security Project" (Projeto Aberto de Segurança em Aplicações Web) desenvolveu um estudo recente sobre o tema, para ajudar desenvolvedores e consumidores a compreender melhor as questões de segurança da IoT. Esse potencial de risco é elevado por inúmeros fatores, mas existem pontos de vital importância que merecem ser avaliados e compreendidos.

Entre os diversos aspectos sobre a segurança de IoT a Fundação OWASP aponta os 10 principais riscos da IoT, que devem ser base para avaliação das organizações ao desenvolverem seus projetos:

1 - Segurança Física dos objetos inteligentes;

2 - Softwares/firmwares vulneráveis dos objetos;

3 - Falta de criptografia e verificação da integridade dos dados;

4 - Configurabilidade insuficiente da segurança dos objetos;

5 - Autenticação/autorização insuficiente dos objetos;

6 - Serviços de redes vulneráveis (privadas ou Internet);

7 - Interfaces de nuvem vulneráveis;

8 - Interfaces de gerenciamento IoT vulneráveis;

9 - Interfaces móveis IoT vulneráveis;

10 - Questões da privacidade de dados dos usuários de IoT.

Disponível em < https://www.owasp.org/index.php/Top_IoT_Vulnerabilities > acesso 10/04/17.

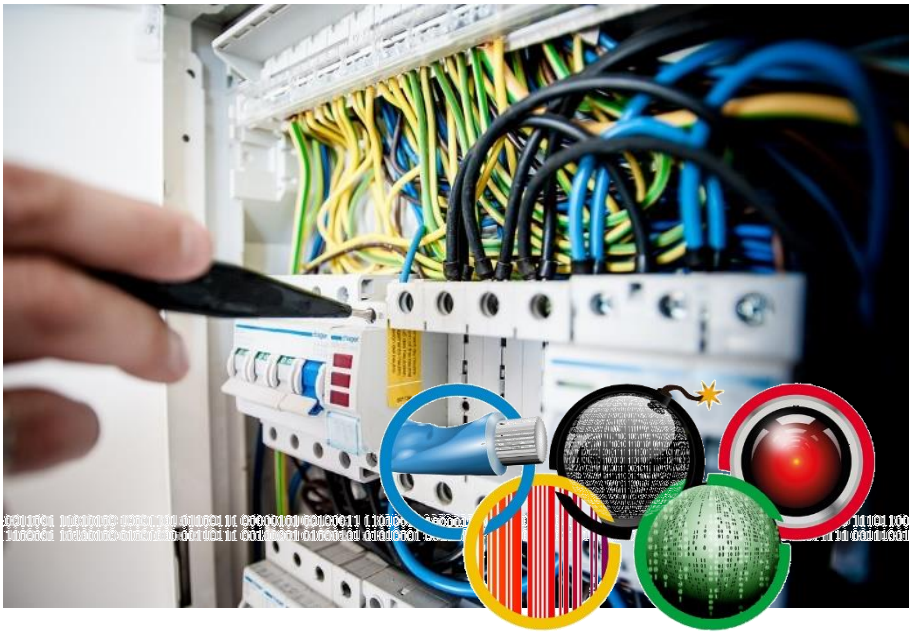
Como se pode observar a maioria dos riscos de IoT apontados, estão de certa forma muito alinhados aos atuais dispositivos hoje conectáveis a Internet, ou seja, um smartphone ao executar qualquer aplicação também está sujeito aos mesmos riscos, no entanto, objetos "Coisas" IoT por serem na maioria das vezes dispositivos mais simples e econômicos, muitas vezes com baixa capacidade de processamento, armazenamento e defesa, efetivamente são mais vulneráveis a todo tipo de ataque[2], inclusive a Malwares, Vírus, Spywares, Trojans...

Ao se analisar o potencial da aplicabilidade de objetos inteligentes IoT, fica evidente que estes também podem ser empregados para a "defesa e ampliação da segurança sistêmica" de aplicações IoT. Como exemplo; em uma rede de dispositivos IoT baseados em sensores, alguns objetos IoT podem ser de controle

e dedicados em armazenar "logs" ou "Cópias Backup" de dados gerados por outros objetos IoT na rede. A estratégia, se devidamente implementada, permitira que em uma rede IoT de grande porte, alguns objetos IoT sejam "melhor qualificados" quanto a segurança, com uso de criptografia forte, armazenamento seguro, entre outros aspectos. A ideia se fundamenta para rede fechadas, com tecnologias específicas de comunicação como ZigBee (IEEE 802.15.4 para a camada de enlace), LoRaWan (Long Range Wide Area Network), UNB[3] (Ultra Narrow Band) como a rede da Sigfox, entre outras que devem surgir, antes que os dados produzidos por objetos IoT trafeguem através da Internet, para serem tratados, integrados e correlacionados com grandes bases de dados.

O uso de objetos IoT específicos, para a defesa de sistemas IoT de grande porte, também abre uma grande oportunidade para a Indústria Eletrônica de Segurança e Serviços, para que se possa fornecer Hardwares Especializados e Serviços de Auditoria, Avaliação de Conformidade (Compliance) e inclusive alcançar melhor fundamentação nos trabalhos de Investigação de eventos delituosos nessas redes fechadas.

[1]**OWASP** - < https://pt.wikipedia.org/wiki/OWASP > acesso em 10/04/2017 as 10:30 horas.
[2]**Ataques** – vide artigo disponível em: <http://cio.com.br/tecnologia/2017/01/16/dispositivos-de-iot-ameacam-as-redes-locais/> acesso em 10/04/2017 as 11:00 horas.
[3]**UNB** – vide artigo disponível em: <http://www.mobiletime.com.br/11/04/2017/brasil-tera-rede-dedicada-a-iot-cobrindo-95-da-populacao-ate-2018/469342/news.aspx> acesso em 10/04/2017 as 11:15 horas.



Investigação de Crimes Eletrônicos

- O que é crime eletrônico?
- O que é Investigação digital e ou cibernética?
- O que é Perícia Digital e ou Cibernética?
- Diferenças entre crimes eletrônicos, digitais e cibernéticos.

Conteúdo Técnico fundamentado principalmente na publicação de 2013 "Roteiro de Atuação sobre Crimes Cibernéticos" divulgado pelo Ministério Público Federal - 2ª Câmara de Coordenação e Revisão - Matéria Criminal e Controle Externo da Atividade Policial. Coordenação e Organização de: Raquel Elias Ferreira Dodge, Subprocuradora-Geral da República – BRASIL.

Investigação de Crimes

Crimes Informáticos / Cibernéticos

O conceito de crime é amplo e seu estudo jurídico nos leva à diversas definições e particularidades. De forma geral compreende a transgressão ou delito, ao qual se possa tipificar culpa, por prática de ação ou omissão que possa ser imputável através de Lei penal. No conceito doutrinário "crime é um fato típico, ilícito e culpável"[1].

Conforme definição da Wikipédia[2]

> "*Crime informático, Crime cibernético, e-crime, Cibercrime (Cybercrime em inglês), crime eletrônico ou crime digital são termos utilizados para se referir a toda a atividade onde um computador ou uma rede de computadores é utilizada como uma ferramenta, uma base de ataque ou como meio de crime*".

Investigação digital e ou cibernética

O conceito de investigação está ligado ao ato prático de investigar, que compreende a análise rigorosa sobre algum fato ou questionamento, sendo a análise geralmente realizada por métodos de pesquisa técnico-científica. No âmbito policial, investigar compreende a busca ou detalhado para averiguar e apurar detalhes sobre algo ou alguém, em algum lugar. No universo jurídico, investigar compreende os procedimentos ou diligências, para reunir vestígios e de provas com o objetivo de atestar fatos e ou circunstâncias legais.

No caso da investigação digital e ou cibernética, o processo de análise é sobre os fatos ocorrências criminosas e suas consequências, na utilização de computadores ou equipamentos (Digitais) e ou na rede mundial Internet (Cibernética). A investigação utiliza as mesmas técnicas intuitivas, dedutivas, indutivas, quantitativas, sempre apoiadas por métodos de pesquisa outras ferramentas especiais. É obvio que para a investigação Digital e ou Cibernética, o devera possuir profundos conhecimentos técnicos multidisciplinares, mas principalmente de da Computação.

Perícia Digital e ou Cibernética

O termo Perícia[3] significa a:

> **"***Execução de uma habilidade com prática aprimorada***"** originada **"***no termo latino "perìtia", derivada por sua vez de "perìtus" ou "experto" compreende a análise técnica de uma situação, fato ou estado conduzida por um especialista numa determinada disciplina, denominado "Perito". A perícia é um exame realizado por profissional especialista, legalmente habilitado, destinada a verificar ou esclarecer determinados fatos, apurar as causas motivadoras do mesmo, ou o estado, a alegação de direitos, ou a estimação da coisa que é objeto de litígio ou processo.***"** (3-Wikipédia)

Para o trabalho do Perito é fundamental que este seja habilitado, credenciado e requisitado por autoridade policial ou do Ministério Público, de maneira formal, para a investigação forense.

A Perícia Digital e ou Cibernética Forense emprega profissionais Peritos, que atender as exigências de aplicar métodos consolidados nas "Ciência(s) Forenses" e nas "Ciência(s) da Computação", para garantir a aquisição, preservação, análise e evidências obtidas nos processos investigatórios.

Segundo o documento "Roteiro de Atuação sobre Crimes Cibernéticos[4]" do Ministério Publico Federal, para uma perícia cibernética:

> **"***É necessário cumprir com alguns requisitos para que as evidências digitais de uma investigação sejam juridicamente válidas. Segundo a RFC 3227 1 , que oferece uma série de recomendações para procedimentos de coleta e preservação de provas em meio digital, a evidência eletrônica deve ser (tradução livre):*
>
> ***1. Admissível:*** *ou seja, estar em plena conformidade com a lei para que possa ser apresentada à justiça.*
>
> ***2. Autêntica:*** *as provas devem ser comprovadamente relacionadas ao incidente/crime investigado. O trabalho de uma documentação de qualidade é essencial para o cumprimento deste item.*
>
> ***3. Completa:*** *o conjunto de evidências deve fornecer uma apresentação completa acerca do evento investigado. Nunca deve depender de elementos faltantes ou duvidosos. Deve "contar a história" completa, e não apenas fornecer perspectivas particulares.*

4. *Confiável:* *não deve haver incertezas acerca da autenticidade e veracidade das evidências, bem como sobre as formas como foram coletadas e posteriormente manuseadas durante a investigação.*

***5. Convincente**: além de todas as características anteriores, deve ser documentada e apresentada de forma clara e organizada.”*

Ainda no mesmo documento, o MPF esclarece, os termos “Vestígios, Indícios e Evidências” considerando:

“*Os termos mencionados acima são por vezes utilizados como sinônimos, embora carreguem semânticas formais distintas. Cabe ao investigador a clara compreensão destas diferenças. Comecemos nossa reflexão sobre este tema analisando a seguinte proposição:*

"*Enquanto o vestígio abrange, a evidência restringe e o indício circunstância*." |Filho 2009|

Segundo o autor, o vestígio abrange no sentido que, em termos periciais, este conceito "mantém a característica abrangente do vocábulo que lhe deu origem, podendo ser definido como todo e qualquer sinal, marca, objeto, situação fática ou ente concreto sensível, potencialmente relacionado a uma pessoa ou a um evento de relevância penal, e/ou presente em um local de crime, seja este último mediato ou imediato, interno ou externo, direta ou indiretamente relacionado ao fato delituoso".

No contexto da investigação de crimes computacionais, onde notadamente o objeto sensível é quase sempre representado pelo intangível, têm-se que o vestígio é majoritariamente apresentado como um registro digital que existe em decorrência de uma prévia intervenção humana, tratada aqui como agente motivador direto ou indireto daquele evento. Estes vestígios podem ser, por exemplo, os logs armazenados por um software, ou uma mensagem recuperada na Web. Uma vez que o investigador extraia - por meio de apurações analíticas – as informações dispostas nestes vestígios, poderá ver-se autorizado a inferir objetivamente sobre o vínculo destes com o delito em questão, apresentando assim evidências de que, por exemplo, aquela mensagem postada na Web partiu indubitavelmente daquele computador periciado. Cabe ressaltar que a abrangência dos vestígios deve ser podada na medida do que se considere necessário e suficiente para a construção lógica da evidência, esta que deve apresentar-se portanto restrita à sua utilidade no processo.

> *No Código de Processo Penal, o indício é apresentado como "a circunstância conhecida e provada, que, tendo relação com o fato, autorize, por indução, concluir-se a existência de outras circunstâncias." Concordamos portanto com [Filho 2009], quando este deduz que "a evidência é o vestígio que, mediante pormenorizados exames, análises e interpretações pertinentes, se enquadra inequívoca e objetivamente na circunscrição do fato delituoso. Ao mesmo tempo, infere-se que toda evidência é um indício, porém o contrário nem sempre é verdadeiro, pois o segundo incorpora, além do primeiro, elementos outros de ordem subjetiva."*

(Textos contidos no Capitulo 3 – páginas 164 a 167) – {importante leitura}.

Diferenças entre crimes eletrônicos, digitais e cibernéticos

No contexto deste e-book optamos por expor entendimentos sobre as diferenças sutis dos termos "Crimes Eletrônicos", Crimes Digitais" e "Crimes Cibernéticos", por julgarmos conveniente e adequado para a devida compreensão sobre os processos de Investigação Forense Digital sobre IoT "Internet das Coisas".

No caso, do termo "Crimes Eletrônicos", entendemos como os crimes praticados ou ocorridos através de equipamentos eletroeletrônicos, mesmo que estes não sejam necessariamente Digitais ou estejam ligados diretamente a redes, inclusive a Internet, ou possam ser caracterizados como cibernéticos.

Um exemplo típico com dispositivos que se baseiam em "sensores", como o "sistema de Controle térmico de um Alto-forno", estes empregam em grande parte sensores de "Pares Termoelétricos" e atuadores. Uma alteração proposital criminosa no ajuste fino desses dispositivos, pode produzir grandes prejuízos em uma indústria, queimando o material depositado no forno. Estamos falando no caso de um crime Eletromecânico ou Eletroeletrônico.

O mesmo "Alto-forno" controlado pelos mesmos sensores e atuadores, cujo resultado de medição térmica seja convertido para sinais binários (digitais) e controlados por "microcontrolador programável", caso o programa residente seja comprometido propositalmente por um invasor, poderá também produzir o mesmo desastre. No caso, estamos falando de "Crime Digital".

Ainda com base no mesmo exemplo do "Alto-forno", com sensores e atuadores, com medição térmica convertida para digital através de "microcontrolador programável", e em seguida os dados transmitidos em rede para um sistema informatizado de controle e gestão, se houver invasão na rede local ou pela Internet, no sistema informatizado de controle, produzindo o mesmo desatre, estaremos falando de "Crime Cibernético".

O exemplo, para que seja útil em IoT, é importante compreender que se o crime for cometido no dispositivo "Coisa" de medição e controle de temperatura que não seja digital, merece um destaque como "Crime Eletroeletrônico", da mesma forma que se a medição for digital, será "Crime Digital", ou ainda possa ser caracterizada como informatizada ou cibernética, conforme o caso. Na prática os objetos "Coisas" IoT, ligados a Internet, serão sempre cibernéticos, em última análise, independente do local do crime.

1 – Disponível em < https://isabelaescolano.jusbrasil.com.br/artigos/188967993/dos-crimes-classificacao-e-tipificacao > acesso em 10/04/2017 as 13:30 horas
2 – Disponível em < https://pt.wikipedia.org/wiki/Crime_inform%C3%Altico > acesso em 10/04/2017 as 13:40 horas
3 – Disponível em < https://pt.wikipedia.org/wiki/Per%C3%ADcia > acesso em 10/04/2017 as 13:50 horas
4 – Disponível em < http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/roteiro-atuacoes/docs-cartilhas/crimes_ciberneticos_web.pdf > acesso em 10/04/2017 as 14:20 horas (publicação digital do MPF com 475 páginas)

Investigação Forense Digital

- O que é Investigação Forense Digital
- O que é Forense Computacional Corporativa "FCC"
- Perfil profissional do Investigador Forense Computacional

Investigação Forense Digital ou Computacional

Na prática, investigação é investigação, seja ela Digital ou Computacional que possuem mesmo significado e objetivo, mas, no entanto, quando se adiciona o termo "Forense" se novas e rígidas regras operacionais, para que a investigação ocorra de forma segura na vestígios, evidências e formação de indícios que possam garantir fielmente as informações correlacionadas, na obtenção de possíveis provas aceitas judicialmente em tribunais.

Forense Computacional Corporativa

As grandes organizações vivenciam violações de conduta operacional de seus colaboradores, todos os dias, e com diversas intensidades de comprometimento nos sistemas informatizados, sendo responsabilizadas pelas consequências. O fato é que a empresa possui responsabilidade objetiva por seus colaboradores, prevista no art. 932 do Código Civil, ou seja, é responsável pelos atos de seus empregados e prepostos quando estão no exercício de suas Desta feita, observa-se o crescimento da procura e contratação de profissionais capazes de investigações Digitais ou Computacionais, de forma transparente e preventiva, buscando a fraudes ocupacionais e digitais no âmbito corporativo.

O trabalho de investigação Forense Computacional Corporativa "FCC", objetiva que ao se investigar qualquer suspeita sobre os colaboradores, terceiros, ou de possíveis invasões Hackers, mantenham os critérios para garantir a admissibilidade das Evidências em ações judiciais, caso elas façam necessárias.

Na maioria dos casos, nas corporações, a ação de Investigação Forense Computacional Corporativa é desenvolvida por profissionais "Security Officers", que tenham sido habilitados e certificados em cursos de Forense Computacional.

O trabalho preventivo de Forense Computacional Corporativa, prepara o ambiente apuração de evidências para a o futuro trabalho do "Perito Judicial", caso necessário.

Perfil profissional do Investigador Forense Computacional

No ambiente de trabalho corporativo, os profissionais dedicados aos processos de Investigação Forense Computacional, necessitam atuar com extrema ética e discrição, de forma a criar animosidade com os demais colaboradores, visto que as investigações sempre serão suspeitas apontadas por monitoração de ambientes ou através de demandas hierárquicas.

Todos os processos de Investigação Forense Computacional Corporativa deverão portanto, sobre segredo absoluto, sendo essa capacidade de dissimulação e sigilo um dos principais atributos do Investigador. Também é obvio que o profissional que conduz a investigação detenha conhecimentos teóricos e práticos sobre como realizar esse importante trabalho.

A base de conhecimentos para um profissional Investigador Forense Computacional, costuma requerer a formação Acadêmica (superior) em áreas de Tecnologias da Informação, Engenharia, Direito ou outras correlatas e que sejam complementadas por cursos livres de específicas em "Análise Forense Computacional", em especial com certificações como:

- ACFEI (American College of Forensic Examiners Institute)
- CCFP (Certified Cyber Forensics Professional), da (ISC)²
- CCFT (Certified Computer Forensic Technical)
- CEH (Certified Ethical Hacker)
- CHFI (Certified Hacker Forensic Investigator)
- GCFA - GIAC (Certified Forensic Analyst), da SANS
- GCFE - GIAC (Certified Forensic Examiner), da SANS
- ... Diversas outras disponíveis no mercado nacional e internacional

Preferencialmente o profissional deverá possuir pós-graduação, Mestrado, MBA, e outros cursos sobre "Metodologias Forenses" focados ou correlacionados as atividades de desenvolvidas.

Em especial, os profissionais Investigadores "Forense Computacional" que **venham a trabalhar em casos específicos de IoT** "Internet das Coisas" deverão buscar se aprofundar em conhecimentos ligados a:

- Dispositivos e Tecnologias de Comunicação, considerando a arquitetura, protocolos e demais aspectos, principalmente neste momento, quanto aos padrões: Bluetooth Low Energy (*Wireless personal area networks* – PANs), ZigBee, LoRaWan (Long Range Wide Area Network), UNB (Ultra Narrow Band), inclusive Wi-Fi (Wireless Fidelity Network) e 3G/4G/5G em Telefonia Celular.
- Tecnologias de Redes (RSSF) Rede de Sensores Sem Fio, redes (LLN) Low-Power and Lossy Networks, protocolos "6LoWPAN" da IETF, "RoLL" Routing over Low-Power and Lossy Links da IETF, etc.
- Protocolos da camada de aplicações para IoT, considerando: "CoAP" (Constrained Application Protocol), "REST" (REpresentational State Transfer), "MQTT" (Message Queue Telemetry Transport), entre outros.
- Tecnologias de desenvolvimento de hardware, considerando componentes eletroeletrônicos, sensores, microcontroladores programáveis, microprocessadores, atuadores, baterias, modems, bacons, Colheita de Energia (Energy Harvesting), etc.
- Arquiteturas e padrões para IoT, considerando as propostas "IoT reference models da ITU-T ", Internet of Things Architecture (IoT-A), Internet of Things Architecture (WS02), Adaptive Internet of Things Architecture (AIoTA), entre outras.
- Tecnologias de desenvolvimento de Softwares básicos e Aplicativos, em especial Ambientes de Desenvolvimento para IoT. Considerando linguagens, compiladores, interpretadores, etc.

- Sistemas Operacionais especializados como: "Contiki" (sistema leve de código aberto para sistemas embarcados de rede, com mecanismos para o desenvolvimento de softwares para IoT), "Android" (plataforma de código aberto para dispositivos móveis que inclui, middleware e aplicativos), "TinyOS" (sistema operacional de código aberto para redes de sensores e objetos inteligentes), entre outros.
- Sólida base de Física: mecânica, eletricidade, ondulatória, termologia, ótica...
- Sólidos conhecimentos dos requerimentos legais/jurídicos (nacionais e internacionais) exigidos em atividades de investigação Forense Computacional, que garanta a "preservação probatória" dos processos de aquisição, identificação, extração e análise de dados eletrônicos, na busca de pistas virtuais que possam indicar a autoria de ações ilícitas.

Na prática, os conhecimentos exigidos dos "Peritos Judiciais em Forense Computacional", não diferem muito dos requeridos para profissionais Investigadores Forense Computacional Corporativos. Para se tornar um "Perito" do juízo nos tribunais o profissional deverá se candidatar apresentando "curriculum" aos Diretores das Varas dos Tribunais ou a um Juiz, mostrando interesse em ajudar com laudos para orientar e fundamentar magistrados nos processos que possam se valer de sua expertise e perspicácia.

Pode-se afirmar que é muito relevante a notoriedade do profissional quanto sua reputação proveniente de ações, opiniões e publicações em mídias, consideradas valorosas pela sociedade e a opinião de outros profissionais sobre si, da mesma classe trabalhista.

A nomeação de um "Perito Judicial" no Estado de São Paulo, sempre ocorre através de um "Juiz" de primeira instância, e sempre na esfera judicial, com base no Provimento nº 797/2003 do Conselho Superior de Magistratura, que estabelece os procedimentos prévios de habilitação. Para os interessados em maiores informações, recomenda-se o acesso ao site da Associação dos Peritos Judiciais do Estado de São Paulo, na seguinte página:

Disponível em < http://www.apejesp.com.br/paginas.aspx?id=50 > acesso 10/04/2017.

Perícia Forense Computacional

- Aspectos Jurídicos da Investigação IoT
- Aspectos Técnicos da Investigação IoT
- Aspectos Metodológicos da Investigação IoT

Perícia Forense Computacional

- **Aspectos Jurídicos da Investigação**

De modo geral a atuação profissional de um Perito Judicial ocorre quando ambas as de um Processo Civil requerem ou quando determinada por oficio de um Juiz, ou ainda, as expensas uma das partes, conforme determina o **C**ódigo de **P**rocesso **C**ivil de 2015. O artigo 370, caput do CPC estabelece que "*caberá ao juiz, de ofício ou a requerimento das partes, as provas necessárias ao julgamento do mérito*".

É muito comum em casos que envolvam litígios ou suspeitas de crimes eletrônicos/cibernéticos que as partes contratem por seus Advogados, Peritos Assistentes (Extrajudicial), exigindo muitas vezes que o Juiz também nomeie um Perito oficial para balizamento. aceitação dos Peritos Assistentes Extrajudicial colabora com o "Princípio do Contraditório e da Defesa", conforme artigo 5º, inciso LV da Constituição Federal do Brasil - 1988, como segue.

> "**Art. 5º -** Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> **LV** - aos litigantes, em processo judicial ou administrativo, e aos acusados em geral são assegurados o contraditório e ampla defesa, com os meios e recursos a ela inerentes;"[1]

Os juízes não possuem a obrigação de conhecerem em profundidade as mais recentes tecnologia de TIC, portanto, o amparo de Peritos Assistentes para as partes e para o entendimento próprio Juiz se faz necessário.

É fundamental entender que o Perito Forense Computacional, atuando como nomeado por Juiz, sempre deverá conduzir as investigações, pautado nos mais rígidos conceitos jurídicos[2] e normas aplicáveis, seguindo procedimentos consistentes, válidos, lícitos e éticos. se que um Perito Forense Computacional, não possuindo formação em DIREITO, deverá imprescindivelmente contar com apoio de um Advogado experiente em Direito Digital, que deve acompanhar a investigação desde a identificação inicial do fato criminoso, até a denúncia.

Considerando a complexidade do tema sobre os aspectos Jurídicos da Investigação Forense Digital, recomenda-se a leitura do capítulo 4 (quatro) do "Roteiro de Atuação Sobre CRIMES CIBERNÉTICOS" do MPF, entre as páginas 304 a 386, documento que pode ser obtido conforme indicação e link da 4ª (quarta) referência indicada na página 19 deste e-book.

- **Aspectos Técnicos da Investigação**

A investigação pericial em Forense Computacional requer a perfeita identificação do ambiente global onde possa ter ocorrido a suspeita do crime Digital. No caso da Internet das Coisas "IoT" é fundamental compreender o ecossistema da aplicação "IoT" alvo, e planejar adequadamente como a investigação será conduzida.

A DFI (Digital Forensic Investigation) deverá observar em especial para IoT, no ambiente onde os objetos "Coisas" estão operando, exigindo muitas vezes que a investigação ocorra incialmente no campo e posteriormente em Laboratório, caso necessário. As investigações sobre IoT devem considerar a possibilidade de coletar evidências caracterizadas em 4 (quatro) grupos:

1 – Evidências coletadas no ambiente onde os objetos IoT estão instalados, principalmente quanto as questões de segurança física-mecânica;

2 – Evidências coletadas a partir dos dispositivos inteligentes, em microcontroladores, firmwares (memórias ROM/RAM/etc.), transmissores, atuadores e sensores;

3 – Evidências coletadas em hardwares e softwares que habilitam a comunicação entre dispositivos inteligentes e o mundo externo (como exemplo; Computadores, Smartphones, Firewalls, IPS, IDS, Roteadores, e outros), que estão inclusos na forense computacional tradicional;

4 - Evidências coletadas de hardware e software que estão fora da rede sob investigação. Considerar redes sociais, ISPs, fornecedores de serviços móveis e principalmente nuvens Internet para prestação de serviços SaaS, PaaS e IaaS, IoTaaS, etc.

Observe que "IoT Forensics" expande a área de Investigação principalmente nas bordas.

É importante compreender que o grande desafio da DFI IoT reside na dificuldade da coleta de dados no campo, principalmente quando os dispositivos IoT possuem acesso restrito devido a alçadas proprietárias dos ambientes, sejam por questões operacionais, contratuais, de Geolocalização ou Jurisdição Extraterritorial legal.

IoT forensics possui uma amplitude estendida em relação a "computer forensics" clássica. Além do tipo tradicional de redes - com fio, Wi-Fi, sem fio e ou móvel, IoT também pode abranger redes de sensores RFID. Objetos "IoTware" diversificados tais como dispositivos médicos, produtos estocados com etiquetas RFID inteligentes, sensores inteligentes de controle e gestão, sistemas CFTVIP, entre outros, também devem ser considerados como fontes de evidência.

Da mesma forma, a perícia forense computacional de IoT tem como objetivo principal determinar a dinâmica, as correlações e a materialidade dos fatos, e principalmente a autoria de ilícitos que possam ter validade probatória em juízo.

Para a investigação "IoT forensics" de objetos que possam ser examinados em Laboratório, recomenda-se que o "Laboratório" tenha um espaço físico real, como uma sala, com acesso físico controlado, onde se deve alojar recursos materiais e tecnológicos (ferramentas de Hardware e Software) bem como acesso lógico controlado a Internet, para cooperação de Laboratórios Virtuais Remotos "WebLabs[3]" de Universidades Internacionais (diversas), onde não há componentes físicos, mas unicamente ambientes e componentes modelados matematicamente por programas de computador. O uso integrado e cooperativo de Laboratórios físicos e virtuais tem possibilitado um avanço significativo nos processos de pesquisas e investigatórios cibernéticos.

Por questões de objetividade e isenção mercadológica, não vamos explanar sobre produtos e ferramentas de Hardware e Software investigativo, mesmo que livres ou gratuitas, disponíveis no mercado mundial.

- **Aspectos Metodológicos da Investigação**

Para a realização de qualquer investigação "IoT forensics" o profissional investigador ou Perito deverá estar apoiado em metodologias ou Frameworks que estabeleçam procedimentos padronizados, com reputação de melhores práticas e aceitável judicialmente, como processo operacional confiável.

A comunidade acadêmica e tecnológica internacional já ha muitos anos pesquisa, desenvolve, estuda e publica documentos de referência que objetivam apoiar o trabalho de investigação "computer forensics".

Na publicação já citada, "Roteiro de Atuação Sobre CRIMES CIBERNÉTICOS" do MPF do Brasil, existe uma indicação de que o Centro Judiciário Federal dos Estados Unidos (Federal Judicial Center) disponibiliza o documento "Reference Manual on Scientific Evidence", 2ª edição, contendo 647 páginas. A atualização da 3ª Edição é composta por 1034 páginas e pode ser baixada a partir do link, Disponível em:

<http://www.au.af.mil/au/awc/awcgate/fjc/manual_sci_evidence.pdf> acesso em 30/04/2017 as 16:00 horas.

Existem diversos padrões metodológicos e frameworks que merecem ser considerados, estudados e integrados de forma evolutiva para se obter os mais atualizados e consistentes processos operacionais.

Entre as organizações internacionais que publicam referências, recomendamos:

- SWGDE[4] - Scientific Working Group on Digital Evidence
- NIST[5] - Forensic Science - DIGITAL & MULTIMEDIA EVIDENCE
- SANS[6] - Integrating Forensic Investigation Methodology into eDiscovery
- ENISA[7] - The European Union Agency for Network and Information Security
- ENFSI[8] - The European Network of Forensic Science Institutes

A Polícia Federal do Brasil também aplica e dispões de padrões, documentados, aceitáveis no país. (SEPINF / SRCC).

Em particular optamos por utilizar em nossos trabalhos um padrão metodológico de alta reputação acadêmica e científica, publicado em 2006 e desde então evoluindo e até se tornar hoje o que chamamos de "Estado da Arte" em racionalidade operacional para "computer forensics". O padrão foi denominado de modelo "FORZA[9] Framework", onde FORZA significa "**FOR**ensics-**Za**chman model". O modelo se fundamenta na Arquitetura Corporativa (Enterprise Architecture) de ZACHMAN[10] e no padrão do framework de Segurança "SABSA Model[11]" (Systems And Business Security Architecture).

Neste momento não entraremos em detalhes do modelo FORZA, mas no capitulo "**Exemplo: Caso de Investigação IoT**" deste e-book, no desenvolvimento do "case", haverá indicações sobre o padrão.

No quadro a seguir encontram-se os links indicados no texto deste capítulo.

Disponível em < endereço > confirmação de acesso em 11/04/2017

1 – Disponível em < http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm > acesso em 11/04/2017 as 08 horas.
2 – Disponível em < http://www.veredictum.com.br/materias/direito-geral/conceitos-juridicos-fundamentais.html > acesso em 11/04/2017 as 08:10 horas.
3 – Disponível em < http://www.ib.usp.br/vinces/weblabs/weblab.htm - http://bdtd.ibict.br/vufind/Record/USP_628d18809afe12f574046a7cabd50afe - http://weblab.deusto.es/website/ > acesso em 11/04/2017 as 08:20 horas.
4 – Disponível em < https://www.swgde.org/documents > acesso em 11/04/2017 as 08:30 horas.
5 – Disponível em < https://www.nist.gov/topics/digital-multimedia-evidence > acesso em 11/04/2017 as 08:40 horas.
6 – Disponível em < https://countuponsecurity.com/2014/08/06/computer-forensics-and-investigation-methodology-8-steps/ > acesso em 11/04/2017 as 08:50 horas.
7 – Disponível em < https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/digital-forensics-handbook > acesso em 11/04/2017 as 09:00 horas.
8 – Disponível em < http://enfsi.eu/wp-content/uploads/2016/09/1._forensic_examination_of_digital_technology_0.pdf > acesso em 11/04/2017 as 09:10 horas.
9 – Disponível em< https://www.dfrws.org/sites/default/files/session-files/paper-forza_-_digital_forensics_investigation_framework_that_incorporate_legal_issues.pdf > acesso em 11/04/2017 as 09:20 horas.
10 - Disponível em < https://www.zachman.com/about-the-zachman-framework > acesso em 11/04/2017 as 09:30 horas.
11 - Disponível em < http://www.sabsa.org/ > acesso em 11/04/2017 as 09:40 horas.

Exemplo: Caso de Investigação IoT

- Exemplo de caso fictício, fundamentado em investigação real de IoT realizada recentemente.

{Os dados de referência e explanação do desenvolvimento e de conclusões são meramente ilustrativos, didáticos e fictícios. Nomes, marcas, modelos, sistemas, componentes e outros detalhes da investigação não representam a realidade e não estão vinculados a nenhuma pessoa ou organização.}

Exemplo: Caso de Investigação IoT

Investigação da suspeita de:

Fraude em Sistema Inteligente para a Individualização da mensuração do Consumo de Água em Condomínio Residencial

Optamos por apresentar um exemplo prático, no entanto, não vamos nos aprofundar detalhes técnicos para que a leitura deste e-book seja proveitosa para todos os tipos de público.

Histórico Factual

A Empresa especializada em "Segurança da Informação" denominada "**KSI Segurança Ltda**" (nome fictício) recebeu uma solicitação de um potencial cliente para entender uma necessidade específica de investigação, exigindo total sigilo quanto aos fatos, e se houvesse condições de realizar o solicitado, que apresentasse proposta comercial. O Cliente exigiu uma de contato no escritório da KSI, para evitar suspeitas e manter o sigilo necessário.

A reunião com o potencial cliente foi agendada e ocorreu conforme o requerido, onde a necessidade foi apresentada aos profissionais da KSI por dois representantes de um Condomínio Residencial, mais especificamente o Síndico e o Subsíndico.

A exposição dos dois representantes do Condomínio, levou os profissionais de KSI aos seguintes cenários de entendimento:

1º - Havia uma contundente Suspeita de "Furto" de grande volume água, de forma sistemática, ao longo de muitos meses, através de burla (fraude) no sistema de individualização "Hidrômetros Inteligentes" do Condomínio Edifício Residencial de alto padrão "LunarWave" (nome fictício).

2º - A suspeita era focada em uma determinada unidade condominial, pois era consenso que o consumo de água daquela unidade deveria ser muito maior, do que o apresentado nas faturas empresa (instaladora) gestora do sistema de medição individualizada.

3º - Os Antecedentes – o Edifício foi construído em 2011, portanto, antecedia a Lei 13.312 de 12/07/2016 que torna obrigatória a medição individualizada do consumo hídrico nas novas edificações condominiais no Brasil. No entanto, devido a variabilidade de consumo de água entre as unidades condominiais, e as constantes desarmonias e questões entre os condôminos, sempre alegando que os outros consumiam mais água, a Administração pesquisou e propôs a "**hidrometração individualizada**" para a medição do consumo através da instalação de sistema inteligente eletrônico. eletrônico.

4º - O edifício - Edifício Residencial com 15 pavimentos - já com previsão inicial em projeto, de alto consumo de água, para os padrões brasileiros.

Fotos Ilustrativas não representando a realidade.

5º - Os apartamentos – 1 por andar - com 496 m^2 composto por dependências como:

- 04 quartos suítes (**todos com hidromassagem**)
- 02 salas - estar/jantar
- 01 sala adega climatizada
- 01 sala íntima para Home Theater
- 01 escritório
- 01 varanda gourmet com **solarium + jacuzzi** (pequena piscina 1,2m^3)
- 01 lavabo
- 01 cozinha
- 02 quartos de empregada
- 02 banheiros de empregada
- 01 lavanderia completa
- 05 vagas de garagem

6º - Medidas Adotadas - pela Administração do Condomínio - A empresa e as tecnologias de individualização do controle de consumo de água, foram selecionados e implantado em maio de 2015, através da instalação de Hidrômetros com sensores eletrônicos acoplados, com transmissão de dados das medições volumétricas de água, através de rede de comunicação "Low-Power Wide-Area Network" (LPWAN).

7º - O sistema proposto - pela empresa vencedora da licitação, considerava que em cada unidade habitacional (apartamento individual) fosse instalado hidrômetros inteligentes diferenciados para água fria e água quente, um para cada prumada de tubulação, que se alojavam nos 4 (quatro) Shafts da edificação, totalizando 8 (oito) hidrômetros por apartamento.

{Existem diversos fabricantes e modelos de Hidrômetros inteligentes no mercado. Optamos por um diferente do real utilizado no caso.}

Dispositivo esquemático - ilustração

8º - O sistema instalado, denominado **"AquaMeter"** (nome fictício) operava com um dispositivo **Repetidor de Sinais**, por pavimento, que se integravam na captura da leitura dos dados dos **Hidrômetros Inteligentes (8 oito)** e os transmitiam para a unidade central **"Concentradora"** de Processamento e transmissão via Internet. As unidades repetidoras e concentradora operavam de forma similar aos sistemas WiFi em uso normalmente, apenas com faixas de frequência de transmissão diferenciadas. A Unidade Concentradora, de fato, era um ROUTER (roteador) que também se ligava a um link de **Internet fixo**, com um site exclusivo da empresa medidora do consumo, ou seja, da própria empresa fornecedora do sistema.

Figuras Fictícias

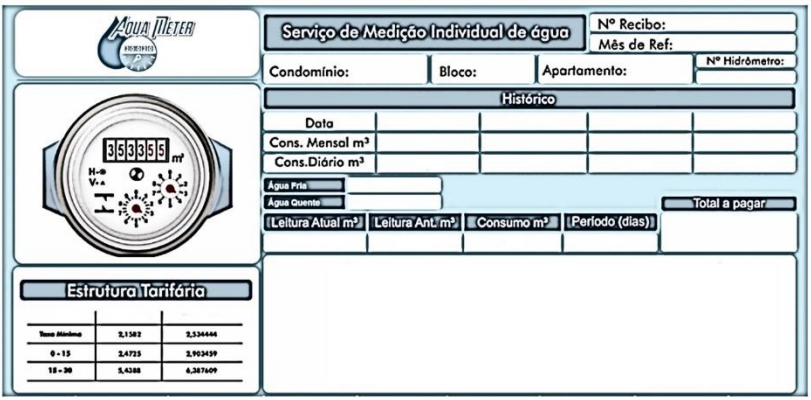
9º - Sistema de Leitura, controle e faturamento - A leitura dos hidrômetros poderia ser acompanhada com totalização horária, por prumada, disponível através de aplicativo 'App" no telefone celular. A totalização temporal poderia ser feita por acesso ao site web da fornecedora.

A fatura de fechamento de consumo seria mensal e apresentada separadamente com base no consumo de água fria e água quente por hidrômetro. O custo da água quente sempre teria maior valor, por ser tratada e aquecida, através de caldeira central e única para todos os apartamentos, consumindo gás GLP.

O custo do gás GLP seria rateado pelas unidades com base no consumo em litros de água quente registrada nos hidrômetros.

10º - A empresa gerenciadora - do sistema de medição individualizada, a "AquaMeter", era remunerada mensalmente, para apresentar a Administração do Condomínio, os extratos das faturas individualizadas por unidade habitacional, indicando o consumo em cada relógio hidrômetro inteligente da edificação. O relatório mensal para controle, sempre apresentavam divergências entre o total medido pela "AquaMeter" e o total medido como fornecimento pela empresa pública concessionaria de água. A margem de erro prevista em contrato era de até 3% (três por cento) considerando as variações da precisão das medidas, tanto dos hidrômetros inteligentes, quanto ao processo de medição e faturamento da concessionaria.

- Extrato – Relatório de Faturamento Individualizado – modelo



11º - Medidas Administrativas – Ao se fazer a análise ao longo do tempo, a Administração do Condomínio vinha observando uma maior variação entre o total medido pela "AquaMeter" e o faturamento do fornecimento de água, que superava gradativamente os 5% (cinco por cento) já bastante superior ao previsto. As justificativas dos técnicos da gerenciadora foram diversas, até aventaram a hipótese de vazamento de água nas caixas inferiores do edifício, antes da água passar por nenhum hidrômetro instalado nas unidades. O fato fez com que fosse contratada uma nova empresa especializada em vazamentos para tentar localizar o provável problema.

O trabalho de analise de possíveis perdas de água por infiltrações ou problemas nas tubulações e na impermeabilização das caixas inferiores e superiores, concluiu que não havia nenhum tipo de irregularidade nas partes examinadas.

Com base no diagnóstico a Administração solicitou a "AquaMeter" uma ampla revisão no sistema instalado para verificar a regularidade funcional dos Hidrômetros e dos demais elementos sistêmicos da solução.

A "AquaMeter" prontamente atendeu ao requerido e programou uma agenda de visitas as unidades e instalações em área comum do edifício "LunarWave".

12º - Revisão da "AquaMeter" – O processo de visita e inspeção da fornecedora do sistema de "hidrometração individualizada" ocorreu conforme o previsto, onde os técnicos da empresa registraram a vistoria e visitaram todos os Shafts verificando todos os hidrômetros quanto a vazamentos, vestígios de adulteração física na mecânica da parte móvel do relógio, para travamento da medição, entre outros detalhes. Segundo o relatório apresentado no final do trabalho, também foram analisadas individualmente por hidrômetro inteligente, o devido funcionamento da comunicação de dados entre eles a Repetidora e Concentradora, bem como, com a "AquaMeter" através da Internet.

A conclusão foi que o sistema de "hidrometração individualizada" estaria funcionando corretamente, salvo a observação de que havia um grande desnivelamento de consumo de água de uma das unidades condominiais, em uma única "coluna" de água quente. Essa unidade condominial de nº15, consumia muito menos que as demais, porém a inspeção no hidrômetro não observou nenhuma anomalia ou vestígios de adulteração.

13º - Análise da Administração – Com fundamentação no relatório da "AquaMeter" se passou a observar o comportamento das variações de consumo individualizados desde a implantação do sistema em maio de 2015. A avaliação mostrou que de fato a unidade 15, já no segundo mês de medição, ou seja, desde julho de 2015 vinha apresentando um consumo muito inferior as demais unidades exatamente na prumada de tubulação do quarto "Shaft" que fornecia agua quente para a jacuzzi (pequena piscina). O fato ficou mais complexo quando se observou que mesmo nos meses de verão o consumo de água quente se mantinha muito próximo das medições anteriores, com total disparidade entre as demais unidades habitacionais.

14º - Providências da Administração - Considerando o resultado das analises tanto da "AquaMeter", quanto próprias, optou-se por averiguar de forma sutil, através de conversas informais, com o "Engenheiro Walter", proprietário da 15º unidade (cobertura) e outros, quanto ao uso e manutenção do espaço social interno da unidade, nos meses de verão, considerando que havia um crescente numero de visitantes nas unidades do "LunarWave".

Da conversa informal entre diversos condôminos, se observou que os visitantes eram familiares e amigos e que estes elevavam as despesas em consumo de bebidas e alimentação, mas o lado social era importante para todos. O Engenheiro Walter, fez comentário que procurava economizar, mantendo a "jacuzzi" desativada, reduzindo assim os seus custos. Essa observação foi determinante para ampliar a desconfiança, pois, o consumo de água quente se mantinha estável durante todo o período analisado. Considerando que a quantidade de metros cúbicos de água quente, seria muito grande apenas para o uso normal, de pia da cozinha gourmet e lavabo, consumidos na prumada de tubulação do quarto "Shaft" da unidade 15, caso a jacuzzi não fosse utilizada.

15º - Medidas Excepcionais – A Administração, única e exclusivamente entre Síndico e Subsíndico, sem envolver o Conselho, optou por buscar ajuda investigativa de terceira parte, para procurar apurar o que poderia estar acontecendo, isto porque seria responsabilidade da Administração que vinha sendo cobrada veementemente por alguns condôminos, quanto aos critérios de rateio e dos desvios de medição, entre a gerenciadora da individualização e a concessionaria fornecedora de água.

Com base na validação do entendimento da demanda, a "KSI Segurança Ltda" desenvolveu e apresentou proposta comercial ao "LunarWave", considerando várias hipóteses e cenários, com condições específicas de atuação, que foi aceita como vencedora, após o processo de licitação promovido pela Administração do Condomínio.

Como a KSI desenvolveu o procedimento Investigatório

Com base no cronograma de planejamento da investigação, a KSI iniciou os trabalhos no meio do mês de dezembro de 2016 com previsão de conclusão até o final de março do ano seguinte (2017).

Equipe envolvida no projeto

A KSI com base no Framework FORZA ("**FOR**ensics-**Za**chman model"), alocou profissionais e requereu a participação de pessoas na equipe de trabalho considerando:

1 - Líder do Caso - Coordenador de Investigação da KSI;

2 - Contratante - Responsáveis pela investigação - Síndico e Subsíndico

3 - Conselheiro Jurídico - Advogado especialista em Direito Digital da KSI;

4 - Especialista em Forense Digital - Engenheiro perito profissional da KSI;

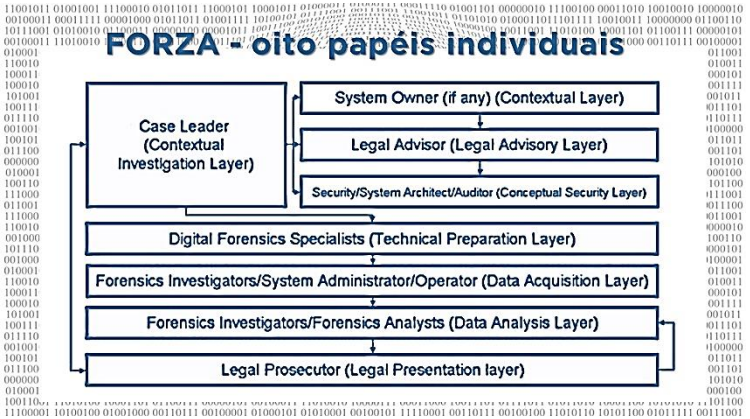
5 - Analista de Sistemas - profissional dedicado aos casos de softwares - KSI;

6 - Especialista em Sistemas Embarcados - Hardware - engenheiro eletrônico KSI;

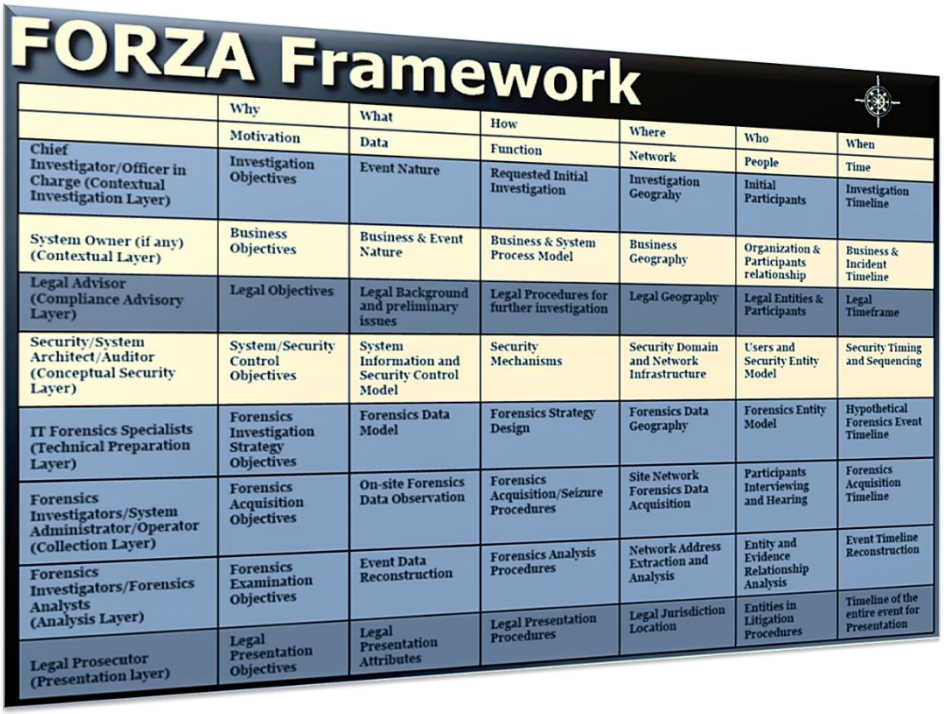
7 - Analista Forense Digital de Campo - especialista investigador KSI;

8 - Advogado procurador do Condomínio "LunarWave" (terceiro contratado).

Esses oito níveis de profissionais é mandatório na metodologia que fundamenta o para que haja total envolvimento e compreensão dos processos investigatórios, garantindo a dos resultados apurados. O envolvimento da equipe vinculada ao projeto explicita papeis muito para cada profissional considerando a atuação em cada camada metodológica.



A Metodologia que fundamenta o FORZA se baseia na matriz de Zachman que questiona: (5W1H) O que, Por quê, Como, Quem, Onde, Quando, relacionados aos diversos parâmetros nas 8 (oito) camadas, uma para cada especialidade de profissional envolvido nos procedimentos de investigação.

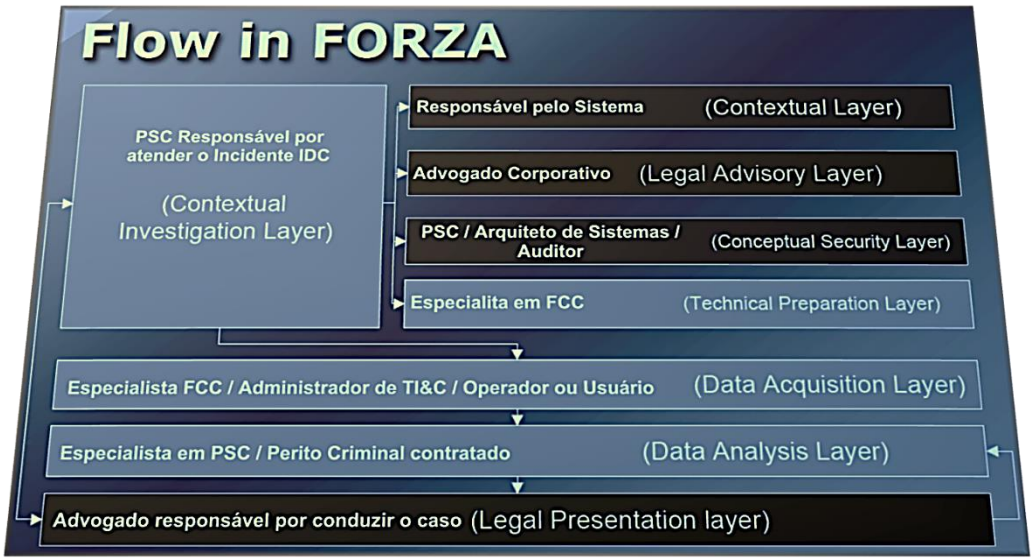


FORZA Framework

	Why	What	How	Where	Who	When
	Motivation	Data	Function	Network	People	Time
Chief Investigator/Officer in Charge (Contextual Investigation Layer)	Investigation Objectives	Event Nature	Requested Initial Investigation	Investigation Geograhy	Initial Participants	Investigation Timeline
System Owner (if any) (Contextual Layer)	Business Objectives	Business & Event Nature	Business & System Process Model	Business Geography	Organization & Participants relationship	Business & Incident Timeline
Legal Advisor (Compliance Advisory Layer)	Legal Objectives	Legal Background and preliminary issues	Legal Procedures for further investigation	Legal Geography	Legal Entities & Participants	Legal Timeframe
Security/System Architect/Auditor (Conceptual Security Layer)	System/Security Control Objectives	System Information and Security Control Model	Security Mechanisms	Security Domain and Network Infrastructure	Users and Security Entity Model	Security Timing and Sequencing
IT Forensics Specialists (Technical Preparation Layer)	Forensics Investigation Strategy Objectives	Forensics Data Model	Forensics Strategy Design	Forensics Data Geography	Forensics Entity Model	Hypothetical Forensics Event Timeline
Forensics Investigators/System Administrator/Operator (Collection Layer)	Forensics Acquisition Objectives	On-site Forensics Data Observation	Forensics Acquisition/Seizure Procedures	Site Network Forensics Data Acquisition	Participants Interviewing and Hearing	Forensics Acquisition Timeline
Forensics Investigators/Forensics Analysts (Analysis Layer)	Forensics Examination Objectives	Event Data Reconstruction	Forensics Analysis Procedures	Network Address Extraction and Analysis	Entity and Evidence Relationship Analysis	Event Timeline Reconstruction
Legal Prosecutor (Presentation layer)	Legal Presentation Objectives	Legal Presentation Attributes	Legal Presentation Procedures	Legal Jurisdiction Location	Entities in Litigation Procedures	Timeline of the entire event for Presentation

De forma didática se apresenta o papel do "Conselheiro Jurídico" envolvido - As perguntas na matriz compreendem: Objetivos legais (Porquê)-Qual é o objetivo da disputa? - Enquadramento jurídico e questões preliminares (Quais) - Que dados devem ser coletados? - Procedimentos legais para investigação posterior (Como) - É necessário qualquer mandado, mandado de busca? - Geografia jurídica (Onde) - Isso está dentro da jurisdição do país? - Pessoas jurídicas e participantes (Quem) - Quem é / é o (a) requerente / inquirido (a)? - Prazo legal (Quando) - Qual é o prazo do caso? - Entre muitos outros...

Ainda de forma didática se apresenta o fluxo de envolvimento profissional, no procedimento investigatório, considerando as camadas propostas na metodologia. Na figura a seguir, usamos outra forma de nomear os profissionais envolvidos, em investigações empresariais ou FCC.



Camadas da investigação:

Similar a Figura da pagina 41

1 – Contextual Investigatio Layer - Líder do Caso – Coordenador de Investigação
2 – Contextual Layer - Contratante – Responsáveis pela investigação-contratação
3 – Legal Advisory Layer – Conselheiro – Advogado especialista em Direito Digital
4 – Conceptual Security Layer - Analista de Sistemas – casos de softwares
5 – Tecnical Preparation Layer - Especialista em Forense Digital – Engenheiro
6 – Data Acquisition Layer - Especialista em Sistemas Embarcados - Hardwares
7 – Data Analysis Layer - Analista Forense Digital de Campo – investigador
8 – Legal Presentation Layer - Advogado procurador do Contratante ou cliente

É importante compreender que a alocação de profissionais especializados em cada camada metodológica é função do Líder do Caso – Coordenador da Investigação.

Planejamento da Investigação

Para iniciar os trabalhos, houve uma reunião preliminar de "Kick-off", com a equipe alocada ao projeto, considerando inclusive a participação do Contratante e do Advogado procurador do Condomínio. A reunião ocorreu na sede da KSI, tendo como pauta, o alinhamento de todos os envolvidos quanto a metodologia FORZA, em seus papeis e como passos consecutivos, a apresentação e discussão da proposta de Planejamento e aprovação do Cronograma detalhado do desenvolvimento da investigação.

As hipóteses de problemas analisadas no planejamento, indicaram as seguintes raízes:

a) Deficiências ou falhas de projeto das tecnologias aplicadas de Comunicação e Processamento da "hidrometração eletrônica individualizada" comercializada;

b) Adulteração da relojoaria mecânica dos hidrômetros ou dos módulos de Processamento e Comunicação utilizados;

c) Falhas e ou invasões nos sistemas de Comunicação e Processamento remoto envolvendo a Internet e o site da fornecedora/gerenciadora.

O Planejamento da Investigação, discutido, apontou as estratégias de atuação em 4 (quatro) frentes, sendo duas paralelas e duas consecutivas, considerando:

1ª - Abordagem velada técno-comercial, convencional, junto a "AquaMeter" a ser realizada por investigadores da KSI, objetivando entender a organização, seus processos e conduta ética e moral, inclusive de seus colaboradores, considerando a hipótese de conluio ou venda de facilidades aos condôminos.

2ª - Investigação paralela da KSI, não intrusiva na intimidade, sobre a atuação profissional e de negócios, considerando a reputação de mercado e profissional do "Engenheiro Walter", proprietário da unidade 15 sob suspeita. O objetivo seria averiguar se as oportunidades do "Diamante da Fraude" levariam o individuo ao processo de corrupção e cometimento de crimes.

3ª - Concluídas as frentes 1ª e 2ª, a abordagem seria da Administração do Condomínio "LunarWave" junto a "AquaMeter", através de notificação extrajudicial requerendo reunião para tratar do assunto "limite de variação de 3% das medições, prevista em contrato". Com base nos resultados da 1ª frente, já se teria o perfil operacional da empresa gerenciadora e neste caso, se a atitude operacional fosse ética e integra, se poderia pedir a colaboração e atuação conjunta nos próximos passos investigatórios. Caso contrario, a discussão caminharia exclusivamente, para o pedido da substituição dos Hidrômetros, por outros de outras tecnologias, criando um impasse comercial, mas significativo, para a efetiva solução do problema.

4ª - Esta quarta frente, que seguiria paralela a 3ª, implicaria na efetiva Investigação no interior das unidades do condomínio, iniciando como vistoria de rotina da gerenciadora, porém, com procedimentos direcionados em buscar o esclarecimento dos fatos. Como hipóteses operacionais a proposta de análise conduziu aos seguintes raciocínios e sugestões de procedimentos:

a) Averiguação detalhada e documentação fotográfica em alta resolução de todos hidrômetros completos (relógio mecânico + módulo eletrônico) nos seus respectivos Shafts, em todas as unidades condominiais (15) e áreas comuns.

b) Por questões estratégicas, seriam removidos os atuais "módulos de comunicação eletrônicos" e substituídos por novos. A retirada seria protocolada, onde seriam "**vinculados os números**" do apartamento, dos Shafts, dos relógios mecânicos dos Hidrômetros e dos Módulos de Comunicação dos respectivos hidrômetros. O protocolo sempre seria formal na presença de dois técnicos, que assinariam em conjunto com um responsável pela unidade habitacional. Essa operação exigiria a participação da "AquaMeter".

c) Os novos "módulos de processamento e comunicação" seriam instalados e protegidos contra acesso e remoção não autorizados com aposição de etiquetas adesivas, não violáveis e ostensivas, ou outras soluções, que poderiam ser estudadas.

d) O Módulo de Processamento e Comunicação de agua quente da unidade habitacional 15 do quarto Shaft, seria separado para investigação detalhada. Da mesma forma, mais dois qualquer outras unidades seriam sorteados para análise. A investigação pericial em Laboratório ocorreria sobre a Documentação Fotográfica e sobre os 3 (três) módulos de comunicação e processamento retirados.

e) O resultado da análise da Documentação Fotográfica poderia apontar intervenções fraudulentas, de forma "física mecânica" atuando sobre os hidrômetros em sua "relojoaria", para paralisar o processo de medição mecânica/eletrônica. Dessa forma, mesmo funcionando os Módulos de Processamento e Comunicação enviariam informações errôneas ao sistema de transmissão e controle.

f) O resultado da análise dos Módulos de Processamento e Comunicação, em suas funcionalidades, poderiam indicar falhas de componentes eletrônicos em especial dos sensores, da programação depositada nas "Flash Memory" (memórias) do controlador, no chip de ou mesmo no sistema de alimentação por bateria, entre outros.

g) Da analise e correlação dos dados e das investigações anteriores (abordagem 1ª e 2ª), teria os vestígios, evidências e indícios apurados. Neste momento, se poderia estabelecer as estratégias de atuação frente aos resultados:

g1) Caso **não haja** identificação de fraudes, buscar solução amigável com a empresa fornecedora da solução;

g2) Caso haja identificação de fraudes, buscar recuperação financeira por prováveis falhas na mensuração eletrônica que distorceu resultados superior a 3% contratuais;

g3) Caso haja identificação de fraudes por quaisquer motivos, ou por parte, buscar alternativa não litigiosa para reparar os danos financeiros aos

g4) Caso haja identificação de fraudes por quaisquer motivos, por qualquer parte, buscar solução judicial civil e criminal, estando o processo dos procedimentos investigatórios preservados, apoiando novas perícias judiciais.

Planejamento Investigatório Aprovado

Considerando mínimos ajustes de entendimento de todos os integrante da equipe constituída, foi aprovado o planejamento e determinada a data para efetivamente o colocar em

Para melhor compreensão das especificidades do framework FORZA é importante compreender os valores de base quanto a segurança da informações e garantia de idoneidade dos vestígios, evidências e indícios apurados através da coleta, exame, análise e apresentação de conforme aceitação judicial no mundo todo. A figura a seguir, aponta a relação entre Integridade, Confidencialidade e Disponibilidade requeridas em Segurança das Informações e os demandados da "Digital Forensics", no FORZA quanto as mesmas informações.

Todos os trabalhos realizados por profissionais envolvidos em processos de digital deverá considerar a busca do trinômio de Segurança da Informação "CID" - Confidencialidade, Integridade e Disponibilidade, da mesma forma, o trinômio da investigação Digital "3R Forensics" - Reconhecimento, Confiabilidade (Reliability) e Relevância.

Inicio Operacional da Investigação

Com base no cronograma foram iniciadas as frentes 1ª e 2ª partindo para as convencionais da empresa fornecedora e do proprietário

suspeito. Para tanto, se utilizou de diversos artifícios investigativos, pesquisas em base de dados de fontes abertas, fontes comerciais fechadas, coleta de dados e pareceres de diversos clientes, inclusive visitas as instalações da "AquaMeter", tentativas de negociações escusas, entre outras.

O resultado da apuração da "AquaMeter" da primeira frente, demonstrou a idoneidade operacional da empresa, que dispunha de um bom Código de Conduta Operacional e que o gerenciava adequadamente, e em nenhum momento se observou a possibilidade de desviou de conduta ética e moral de nenhum profissional envolvido nas supostas negociações. As visitas as instalações da empresa mostraram o cuidado com a segurança da informação, inclusive com a segregação de ambientes para a operação e recepção de dados de leitura hidrométrica de seus clientes. Em todos os questionamentos, as respostas foram prontas e positivas, sem deixar duvidas técnicas ou operacionais. Observou-se os certificados de registros de "faixas de frequências" homologadas da ANATEL, a certificação de qualidade operacional "ISO 9001", entre outras.

A investigação sobre o proprietário da unidade habitacional 15 da segunda frente, mostrou que ele era sócio de uma empresa desenvolvedora de projetos e prestadora de serviços técnicos, ligada a área da construção civil, em especial em automação predial. O fato de ser engenheiro e sócio de uma empresa na área de automação, levou a um natural aprofundamento das análises, para verificar outros aspectos socioeconômicos da empresa e também de ordem pessoal.

A empresa da qual o engenheiro Walter era sócio majoritário, denominada "BACBr - Building Automation Company Brasil" (nome fictício) era uma empresa de porte médio, que atendia as grandes construtoras de edifícios residenciais e comerciais, em áreas de projeto e execução de instalações elétricas, automação e segurança patrimonial eletrônica. A investigação bancaria e cartorial, mostrou que a empresa não estava em uma boa fase, com dívidas e apontamentos, isso devido a grande crise no setor da construção civil e de alguns litígios com clientes quanto a qualidade e conclusão de projetos.

Concluindo, a situação financeira de manutenção mensal do proprietário da unidade 15, não deveria ser das melhores, no entanto, não foi possível avaliar em maior profundidade as questões patrimoniais e reservas financeiras. A investigação não identificou nenhuma questão de desvios éticos e morais da empresa ou sobre a pessoa investigada.

Inicio da 3ª frente junto a "AquaMeter"

Considerando os resultados apurados, a notificação extrajudicial foi enviada para a "AquaMeter", solicitando urgente reunião de alinhamento, o que foi prontamente atendido. Ainda mesma semana foi realizada uma reunião nas instalações da KSI com a participação dos Condomínio "LunarWave", e representantes em nível de diretoria da "AquaMeter" e da KSI.

A reunião se fundamentou nos desvios de margem de 3% da tolerância das medições, argumento para a cooperação da "AquaMeter" em atender as reinvindicações do "LunarWave" no desenvolvimento da Investigação interna no condomínio. Não foi exposto a "AquaMeter" a sobre o morador da unidade nº 15.

A "AquaMeter" acreditava não ser necessária a substituição dos Módulos de e Comunicação dos hidrômetros por serem novos. A KSI concordou em parte, mas justificou a necessidade de investigar alguns hidrômetros específicos, sem citar explicitamente quais. Na negociação ajustou-se a troca de 10 (dez) peças das 140 (cento e quarenta) instaladas e que das 10 peças retiradas na substituição, 3 (três) seriam sorteadas e examinadas no laboratório de perícia da KSI, bem como, a manutenção do total sigilo sobre a investigação, o que foi aceito por todos.

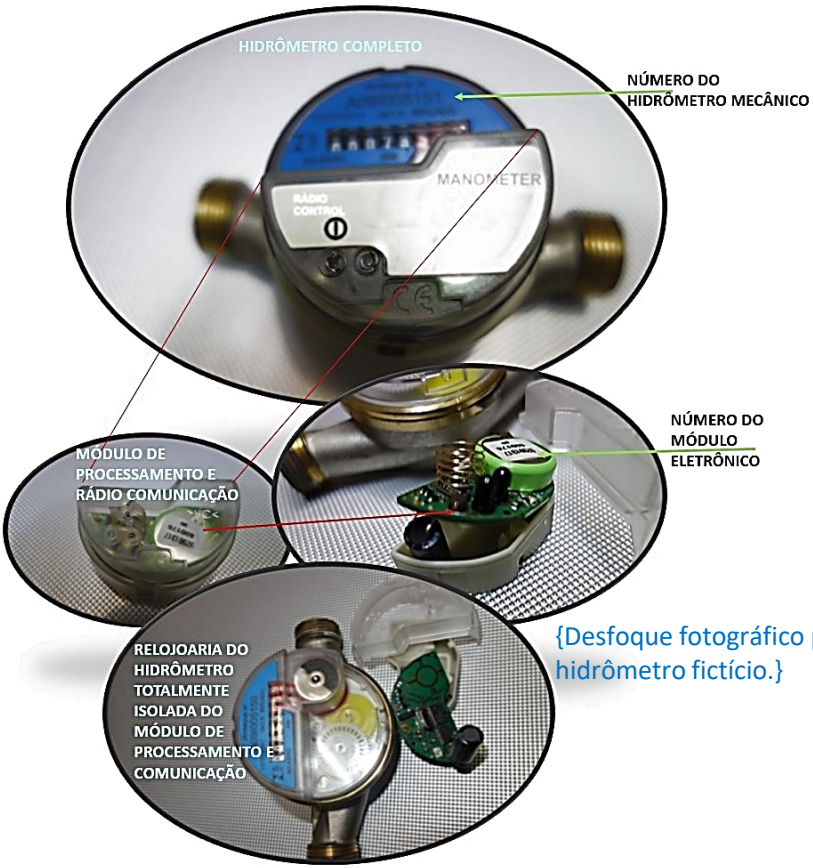
Na citada reunião, se estabeleceu um cronograma para a inspeção de rotina do sistema "**hidrometração individualizada AquaMeter**", no edifício "LunarWave", onde estrategicamente a KSI KSI solicitou acompanhar e interagir ativamente na troca dos Módulos de Processamento e Comunicação, iniciando os trabalhos do 15º pavimento para baixo. Também, se agendou uma reunião alinhamento dos técnicos da KSI com os técnicos da "AquaMeter" para entendimento do do sistema, principalmente da parte eletrônica de processamento, transmissão de dados na rede (LAN) e na Internet, para posterior tratamento e totalização das informações da metrificação individualizada.

Após a reunião dos técnicos envolvidos, a Administração do Condomínio emitiu circular condôminos comunicando a data de inicio da inspeção da "AquaMeter", para verificação de vazamentos, ajustes e ou

substituições de hidrômetros ou partes, se necessário, solicitando o aceite formal dos condôminos em face das questões de precisão hidrométrica.

Inicio das atividades da 4ª frente da investigação

Com base no processo de inspeção agendada no apartamento 15 (quinze) se fez as verificações necessárias, se procedeu o processo de foto documentação, bem como, se substituiu o Módulo de Processamento e Comunicação do hidrômetro suspeito. Para se entender a composição física dos hidrômetros inteligentes, seguem fotos do desmonte ilustrativo:



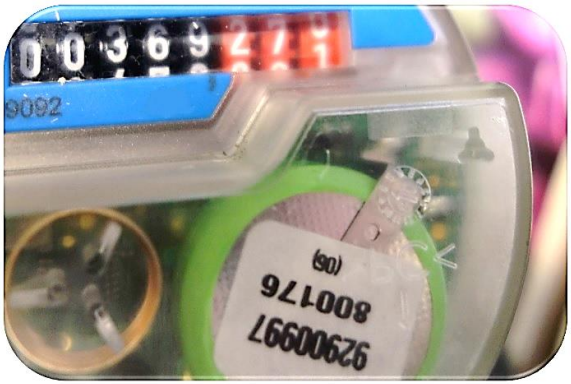
{Desfoque fotográfico proposital. hidrômetro fictício.}

A retirada e substituição dos Módulos de Processamento e Comunicação dos Hidrômetros foi muito simples, pois havia um sistema de encaixe com uma trava móvel, que quando mudada de posição liberava o Módulo. O novo Módulo era encaixado e a trava mudada de posição para fixá-lo. A providência inicial foi colocar uma etiqueta de segurança "Inviolável" entre o Módulo e o Hidrômetro para garantir a identificação de remoção indevida.

Os Módulos de Processamento e Comunicação ao serem retirados, foram acompanhados por gravação de vídeo com áudio, onde além de se mostrar claramente os números dos Hidrômetros mecânicos, estes eram lidos para constar no registro de áudio. Da mesma forma com os números dos Módulos Eletrônicos.

O registro de custódia de cada um dos dez Módulos Eletrônicos de Processamento e Comunicação retirados, foram realizados através de protocolo em 3 (três) vias, contendo os números do Apartamento, do Shaft, do Hidrômetro mecânico e do Módulo retirado a ele associado, constando data, hora, nome e números de documentos dos técnicos, e principalmente nome, dados de documentos e assinatura dos responsáveis pelo imóvel. Não foram aceitas assinaturas e dados de serviçais, como indicado na circular interna do condomínio para os proprietários.

Na oportunidade do desenvolvimento do trabalho de inspeção, a KSI questionou os técnicos da "AquaMeter" sobre o registro numérico constante na relojoaria mecânica dos Hidrômetros e sobre o seu controle. A justificativa foi que o sistema eletrônico era muito preciso, portanto, o registro mecânico numérico não era controlado ou considerado. Os técnicos da KSI solicitaram incluir nos dados da inspeção os números do registro mecânico de cada Hidrômetro, para posterior averiguação.



Outro questionamento da KSI foi sobre o significado dos números, se eram litros ou metros cúbicos de água, e a resposta foi que a relojoaria mecânica dos Hidrômetros registrava em "Litros", mas o "contador" do sistema eletrônico acumulava 10 (dez) litros, para enviar dados, reduzindo assim o consumo de energia da bateria do Módulo. Portanto, a cada 10 (dez) litros registrados no Hidrômetro, o Módulo de Processamento e Comunicação enviava um "string" de dados pelas redes.

O trabalho de inspeção programado durou dois dias, e após a KSI selecionou 03 (três) dos 10 (dez) Módulos Eletrônicos de Processamento e Comunicação, obviamente, incluído o da unidade habitacional suspeita, para exame em Laboratório. Os procedimentos de registro de custódia e garantia do isolamentos físico de cada Módulo, em embalagem individual numerada e lacrada, foi seguido dentro dos tramites legais, sendo todos os procedimentos filmados.

Exame dos Módulos e das Fotos em Laboratório

A KSI dispunha de Laboratório adequado para perícias digitais, com características alinhadas requerimentos da norma ISO/IEC 17025, "General Requirements for the Competence of Testing and Calibration Laboratories, Second edition 2005-05-15" e das recomendações do documento da - Model Quality Assurance Manual for Digital Evidence Laboratories - Version: 3.0, entre outras.

O exame da Documentação Fotográfica, buscava avaliar principalmente se havia perfuração ou vestígios de adulteração física nas carcaças plásticas de revestimento dos em qualquer área, para acesso interno a mecânica da relojoaria, que pudesse travar o mecanismo contador. A burla para fraudar Hidrômetros mecanicamente é conhecida no mercado com "Fraude Sargento".

Todo processo de documentação fotográfica, atendeu aos Procedimentos Operacionais (SOP), recomendados no documento "SWGDE" Photographic Equipment and Infrastructure Recommendations - version 1.0, entre outros, conforme a necessidade do caso.

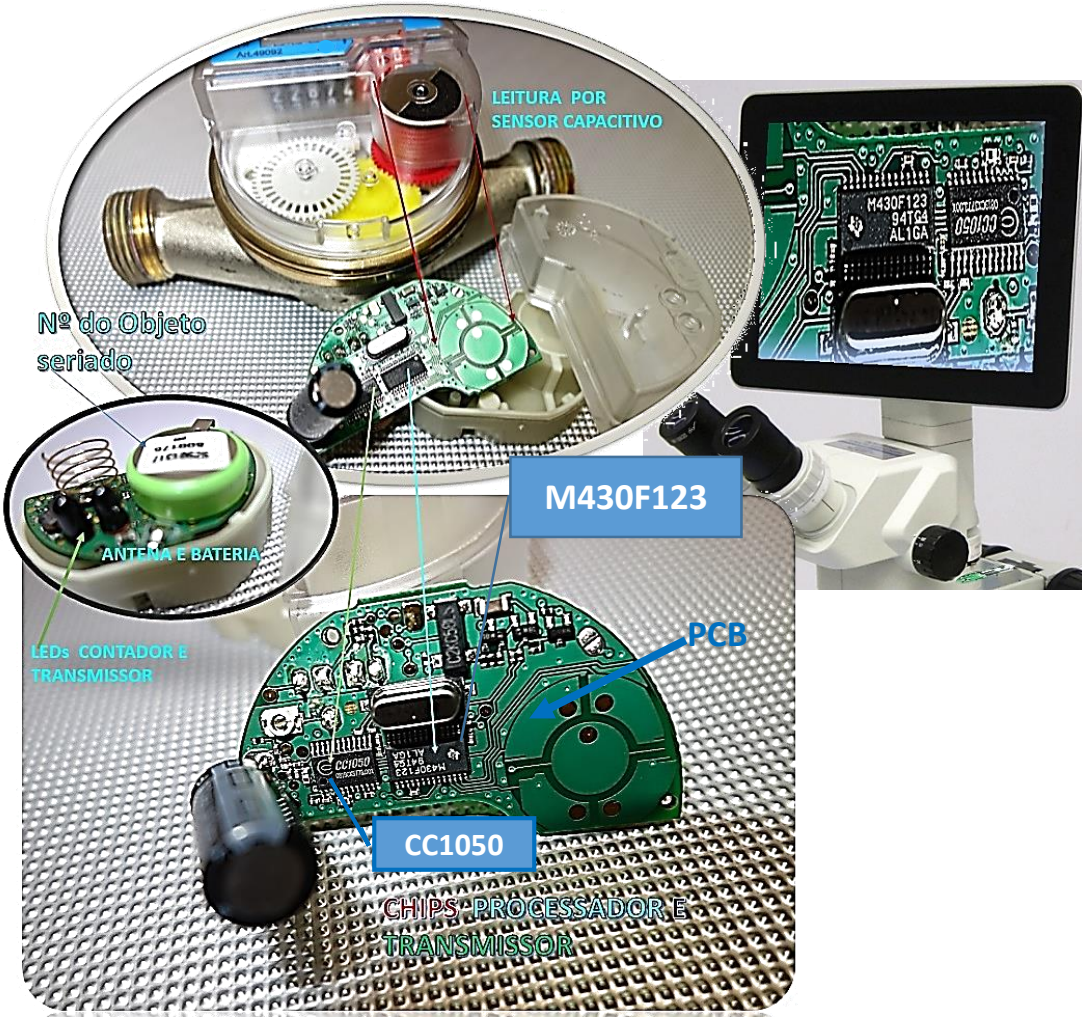
Os resultados da analise das fotos não evidenciou em nenhum dos 140 Hidrômetros, qualquer tipo de anomalia, o que significava não haver tentativa de intrusão física-mecânica sobre os Desse ponto, restava para a KSI entender a possibilidade de eventos adversos em outras partes do sistema de "hidrometração eletrônica individualizada", tais como; intervenção nos Módulos Eletrônicos, na rede interna de repetidores e concentrador, na transmissão pela Internet ou na "aplicação" (App) de recepção dos dados no site da gerenciadora.

Na sequência de análises os 03 (três) Módulos Eletrônicos foram periciados, considerando diversos aspectos mecânicos, inclusive com a análise fotográfica, quanto a vestígios de abertura da carcaça plástica, que não apresentou nenhuma irregularidade, portanto, se os Módulos foram abertos, estes foram devidamente manuseados, sem que as travas tenham sido forçadas.

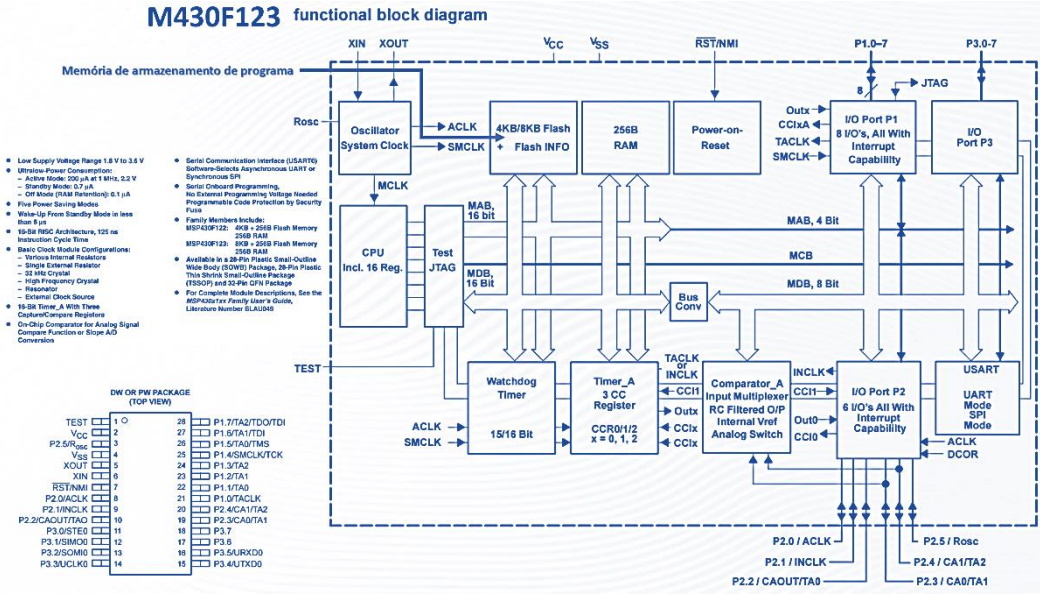
O exame pericial das PCBs ("**P**rinted **C**ircuit **B**oard", ou seja, placa de circuito impresso) foi minucioso, considerando detalhes e características específicas do projeto, fornecidas pelos "AquaMeter", que contribuíram muito nos

resultados obtidos.

Efetivamente a PCB alojava diversos componentes eletrônicos, mas em especial "dois chips", conforme se pode observar:

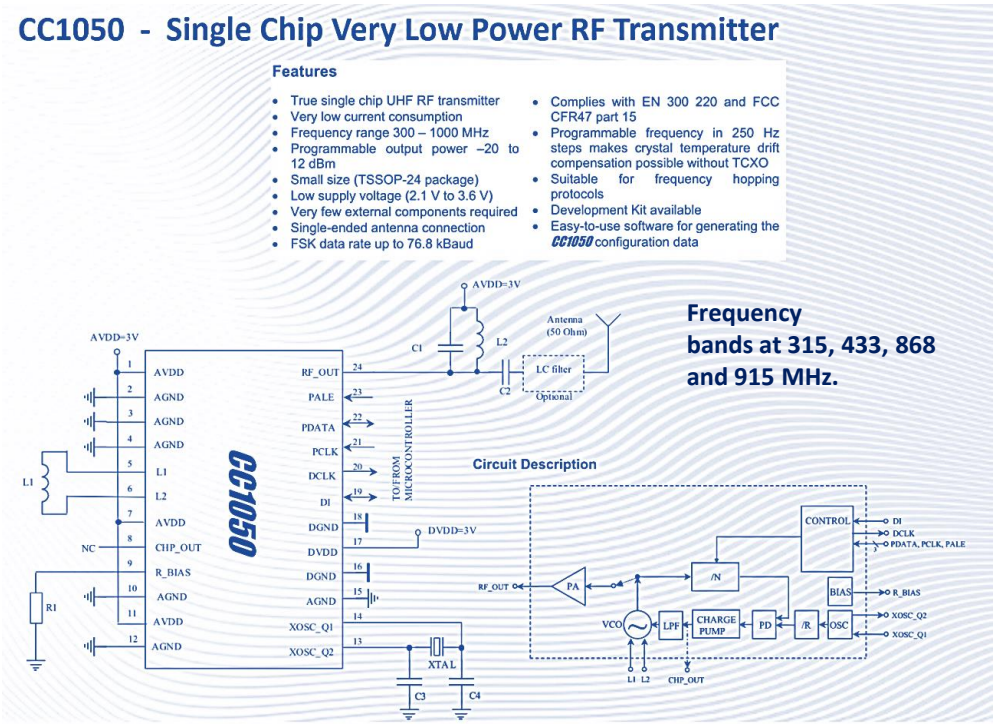


Na análise dos principais microchips da PCB se observou o uso do microcomtrolador da "Texas Instruments", identificado como **M430F123** cujo "data-sheet" (manual) de julho 2001 o identifica como "MSP430x12x MIXED SIGNAL MICROCONTROLLER". O documento pode ser obtido em <http://www.datasheetcatalog.com/datasheets_pdf/M/S/P/4/MSP430XI2X.shtml > acesso em 12/04/2015 as 16 horas.



Esse microchip é na verdade, um quase completo **microcomputador de 16 Bits de arquitetura RISC**, de baixa capacidade, baixa velocidade, baixo consumo de energia e baixo custo, mas que habilita o desenvolvimento de projetos sofisticados com eletrônica embarcada. O importante é observar e entender que o exame do chip M430F123 mostrou que na memória Flash (8Kb)se alojava o programa referido pelos técnicos da "AquaMeter" que continha um "contador" que acumulava a contagem de 10 litros de água para executar um ciclo de transmissão de dados.

O segundo microchip identificado de vital importância na PCB foi o CC1050 produzido pela "Chipcom products", uma divisão da" Texas Instruments", cujo "Data-Sheet" o especifica como "CC1050 - Single Chip Very Low Power RF Transmitter". O documento pode ser obtido em < http://www.datasheetcatalog.com/datasheets_pdf/C/C/1/0/CC1050.shtml > acesso em 14/04/2017 as 17:00 horas.



Este microchip é responsável por **transmitir** os dados produzidos pelo microcontrolador de forma wireless (sem fios) para a o repetidor da rede interna do edifício. Todos os detalhes de operação e faixas de frequência podem ser parametrizados através do software fornecido pelo fabricante do chip.

Na PCB do Módulo de Processamento e Comunicação da "AquaMeter" existem diversos outros componentes eletrônicos que são requeridos para o correto funcionamento, no entanto, além dos microchips, se destacam visualmente componentes, como:

- O sensor capacitivo que consegue identificar uma volta completa do semi-disco metálico da relojoaria do Hidrômetro mecânico;
- A micro antena de 50 Ohm;
- A bateria de 3.6 volts;
- Os dois LEDs de sinalização de contagem e de transmissão;
- O grande capacitor eletrolítico de 1800 microfarads -10 volts.

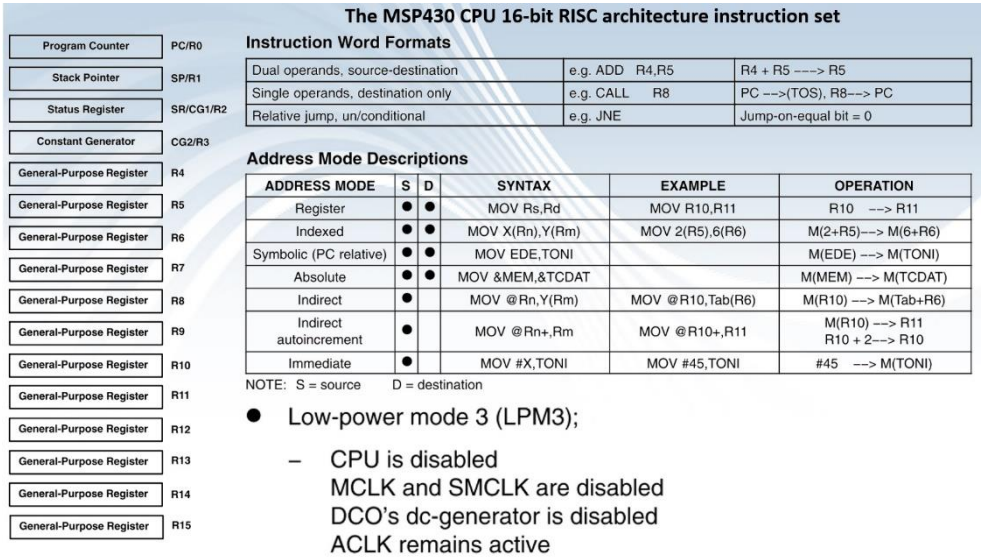
A análise do Módulo eletrônico de Processamento e Comunicação, buscou indícios de falhas de projeto que permitissem levar a erros de leitura, bem como, no processamento e transmissão dos dados. Do ponto vista de design e projeto o PCB e componentes eletrônicos, se mostram muito bem calculados e dimensionados, portanto, descartou-se falhas nesses quesitos.

Restou portanto, na análise do Módulo eletrônico, a avaliação e entendimento de funcionamento do pequeno programa depositado na memória flash do microcontrolador M430F123.

Com base nas informações e indicações dos técnicos da "AquaMeter", seria possível acessar e interagir com o "Firmware", na memória flash onde reside o programa, sem necessidade de remover os microchips da PCB, pois na PCB existiam pontos de acesso para leitura e gravação de dados e configurações.

Com a localização dos pontos de acesso na PCB, para a interação com a área de 8 KB Flash de armazenamento de programa do microchip M430F123, foi efetuada uma leitura dessa área de 8 KB para um notebook, diretamente para um "Pen drive" totalmente livre. Durante a leitura se efetuou a soma de verificação (Checksum – MD5 - função hash criptográfica) para que os dados de destino no Pen Drive pudesse ser validado como cópia integra da origem.

Os dados capturados no "Pen Drive", passaram por processo de "decomplição / Disassembly" através de ferramenta do fabricante do chip, "Visual Disassembler MSP430" considerando que o código executável em síntese é simples, pois a programação possui um "set" reduzido de instruções – 51 instruções com três formatos e sete modos de endereçamento.



The MSP430 CPU 16-bit RISC architecture instruction set

Program Counter	PC/R0
Stack Pointer	SP/R1
Status Register	SR/CG1/R2
Constant Generator	CG2/R3
General-Purpose Register	R4
General-Purpose Register	R5
General-Purpose Register	R6
General-Purpose Register	R7
General-Purpose Register	R8
General-Purpose Register	R9
General-Purpose Register	R10
General-Purpose Register	R11
General-Purpose Register	R12
General-Purpose Register	R13
General-Purpose Register	R14
General-Purpose Register	R15

Instruction Word Formats

Dual operands, source-destination	e.g. ADD R4,R5	R4 + R5 ---> R5
Single operands, destination only	e.g. CALL R8	PC --->(TOS), R8---> PC
Relative jump, un/conditional	e.g. JNE	Jump-on-equal bit = 0

Address Mode Descriptions

ADDRESS MODE	S	D	SYNTAX	EXAMPLE	OPERATION
Register	●	●	MOV Rs,Rd	MOV R10,R11	R10 ---> R11
Indexed	●	●	MOV X(Rn),Y(Rm)	MOV 2(R5),6(R6)	M(2+R5)---> M(6+R6)
Symbolic (PC relative)	●	●	MOV EDE,TONI		M(EDE) ---> M(TONI)
Absolute	●	●	MOV &MEM,&TCDAT		M(MEM) ---> M(TCDAT)
Indirect	●		MOV @Rn,Y(Rm)	MOV @R10,Tab(R6)	M(R10) ---> M(Tab+R6)
Indirect autoincrement	●		MOV @Rn+,Rm	MOV @R10+,R11	M(R10) ---> R11 R10 + 2---> R10
Immediate	●		MOV #X,TONI	MOV #45,TONI	#45 ---> M(TONI)

NOTE: S = source D = destination

- Low-power mode 3 (LPM3);
  - CPU is disabled
    MCLK and SMCLK are disabled
    DCO's dc-generator is disabled
    ACLK remains active

Informações sobre o processo de "Disassembly" podem ser obtidas no endereço: < https://www.eclipse.org/forums/index.php/t/5817/ > acesso em 14/04/2017 as 17:30 horas.

Para melhor compreensão deste processo de análise, se esclarece que:

"O software Visual Disassembler para o Texas Instruments ©MSP430 é um eficiente desassemblador multi-passos, interativo e de fácil uso, para a família de microcontroladores MSP430. O usuário não edita o texto diretamente. Comentários e rótulos do programa são adicionados por endereço através de caixas de diálogo. Cada entrada mostra um resultado imediato na visualização

de texto. Os rótulos do programa são resolvidos e apresentados em todo o arquivo examinado. O trabalho intermediário pode ser salvo e retomado depois, ou a qualquer momento. Após a conclusão da desmontagem, o arquivo pode ser salvo como um arquivo de texto de listagem de montagem. A listagem de montagem pode ser facilmente editada para criar um arquivo de origem de Assembly novo, porém com hash muito diferente. Resumindo, o usuário simplesmente abre um arquivo hexadecimal padrão Intel e o arquivo é desmontado e colocado em uma exibição de texto."

Considerando o exposto, todos os 03 (três) Módulos Eletrônicos, tiveram os seus programas residente na área de 8 KB Flash de armazenamento do microchip M430F123 "desassemblados" e comparados. Não se identificou mudanças no alinhamento da programação, exceto que em um deles, um dos "registradores" o "R8" apresentava valor diferente.

O "Registrador 8" é de proposito geral e a análise o identificou que no programa foi utilizado como parâmetro do "contador" de litros de água identificados pelo sensor de medição, ou seja, em um dos Hidrômetros (exatamente no suspeito) a contagem de litros não finalizava em 10, mas sim em 100, significando que esse parâmetro havia sido alterado, de forma que a cada 100 litros medidos, era enviado um "string" de dados para transmissão como se tivesse medido 10 litros. Apenas um pequeno detalhe com grande impacto.

Os investigadores da KSI questionaram os técnicos da "AquaMeter" para saber se a empresa utilizava Módulos Eletrônicos com parâmetros diferentes de litros ou se havia Hidrômetros e Módulos Eletrônicos diferenciados para medir grandes volumes de água, com contagem de 100 em 100 ou de 1000 em 1000 litros. A resposta foi pronta e segura, de que não, os Hidrômetros eram todos iguais mecanicamente e os Módulos Eletrônicos vinham com programação similar de fabrica e não existia outro padrão.

Considerando a situação, mostrou-se evidente que houve "adulteração" no parâmetro de controle de litros medidos pelo Módulo Eletrônico de Processamento e Comunicação, exatamente no Hidrômetro suspeito.

A KSI propôs então realizar um estudo mais aprofundado no chip

Microcontrolador M430F123, seguindo as recomendações para leitura de dados em microchips "SWGDE Best Practices for Chip-Off " Version: 1.0 (February 8, 2016). Disponível em <https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Chip-Off > acesso em 14/04/2017 as 19:00 horas.

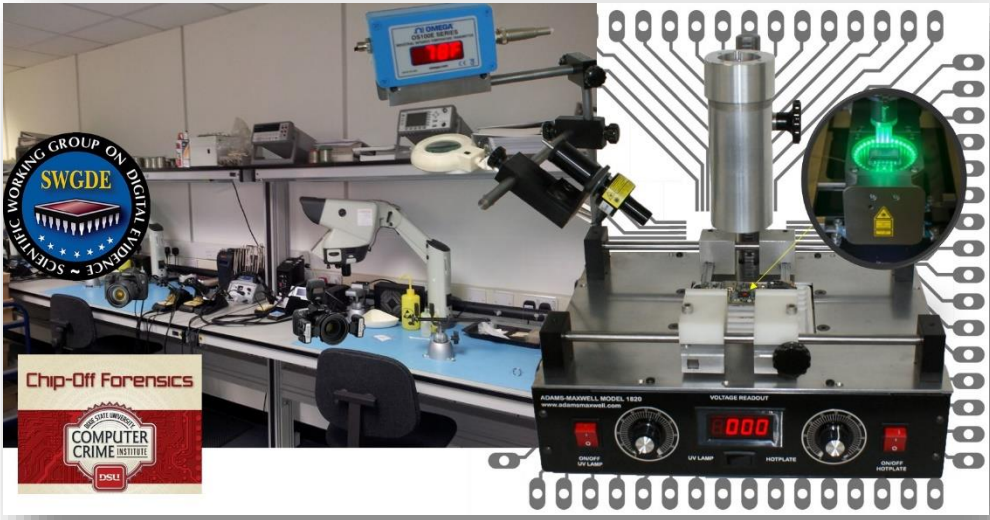
O microchip foi removido da placa PCB (Chip-Off) com base nas mais modernas técnicas e pode ter a memória Flash lida por equipamento leitor adequado e os dados transferidos com "hash" para uma memória "micro-SD" de 1 Gb, a menor disponível, que apos a gravação foi travada, ficando apta apenas para leitura. O arquivo de saída extraído após o processo "chip-off "pode ser importado como um arquivo binário em outro software forense para análise, o que foi realizado.

Do processo mais apurado, por analise de software forense, se concluiu exatamente a mesma modificação visualizada anteriormente no registrador 08.

Considerando as conclusões estabelecidas em Laboratório, onde todos os procedimentos foram filmados, e nas demais frentes de Investigação já realizadas, resultou a elaboração da apresentação audiovisual do laudo e do Relatório preliminar de Resultados.

O relatório desenvolvido com fundamentação no framework FORZA, que também se alinha as melhores práticas da SANS "Methodology for IT Forensic Investigations", abordou sistematicamente: a verificação e aceite do caso pela KSI, a descrição das estratégias e sistemáticas adotadas na investigação, os processos de aquisição de vestígios e evidências em todas as frentes de investigação, tendo todas as informações fundamentadas na linha do tempo em que foram realizadas ou fatos ocorridos, os processos de análise dos artefatos custodiados, o exame dos dados e cadeias binarias de caracteres digitais coletados, bem como, os cuidados para manutenção e recuperação de evidências e indícios que poderão ser utilizados em novas perícias demandadas judicialmente.

Para a conclusão da análise preliminar do relatório, a KSI desenvolveu uma apresentação audiovisual executiva e convidou todos os integrantes da equipe de investigação (8 profissionais já citados) e em especial o Advogado procurador do Condomínio "LunarWave", para entendimento e discussão das conclusões.



Microchip removido da placa PCB (Chip-Off) em laboratório FCC.
Abaixo - equipamentos e softwares - uso em campo e laboratórios.

FERRAMENTAL DE HARDWARE E SOFTWARE PARA INVESTIGAÇÃO DIGITAL FORENSE – CAMPO E LABORATÓRIO

Conclusão da Investigação

A apresentação audiovisual consolidou todos os passos percorridos pelos investigativos, permitindo a última revisão e ajustes de conceitos, entendimentos e conclusões diversos níveis.

Um dos pontos de vital importância na apresentação audiovisual da KSI foi o "estudo de impacto" sobre as próximas medidas que seriam adotadas pela Administração do Condomínio "LunarWave", considerando as questões de recuperação financeira das perdas sofridas, imagem coletiva dos condôminos, imagem do condomínio frente a "AquaMeter" e mercado, investimentos e desgastes em ações judiciais, entre outras.

A KSI se mostrou convencida da materialidade das evidências e indícios de fraude apurados, inclusive, crendo no embasamento pericial e metodológico, para suportar novas investigações, caso o Advogado procurador do Condomínio "LunarWave" e os Administradores quisessem avançar judicialmente. Da mesma forma se posicionou quanto as vantagens de "Arbitragem", junto aos litigantes, com base na Lei nº 9.307/96, Artigos. 267, VII, 301, IX e 520, VI, do do CPC, agilizando a recuperação financeira, sem grandes alardes ou desgastes.

Para a KSI era evidente que pelo conhecimento técnicos do proprietário da unidade 15, este entenderia que era mais fácil arcar com as responsabilidades, do que partir para um embate judicial. E para a Administração do Condomínio seria melhor justificar brandamente, aos demais condôminos, diversas falhas sistêmicas e ações em várias frentes para recuperar as perdas sem criar animosidades. Sugeriu também a busca do retorno financeiro do prejuízo em um espaço tempo maior, isso porque, o montante que deveria ser recuperado era muito significativo, para que houvesse imediato retorno. Seria interessante pactuar um parcelamento com o possível réu.

A questão ética e moral, costuma nesses casos falar mais alto e exaltar os ânimos, no entanto, a lógica e o bom senso devem prevalecer, não justificando uma desgastante disputa mesmo quando se tem certeza dos resultados.

Mesmo com a posição da KSI em caminhar para a Arbitragem, os Administradores ficaram inconformados, e discutiram arduamente com o Advogado, procurador do Condomínio. Eles queriam penalizar de alguma forma moral e financeiramente o responsável pelo crime. No fechamento da reunião, optaram por melhor discutir as medidas a serem tomadas em outra oportunidade.

Com base nas conclusões e ajustes de entendimento a KSI desenvolveu o Relatório Final de Conclusão do caso e o entregou aos contratantes.

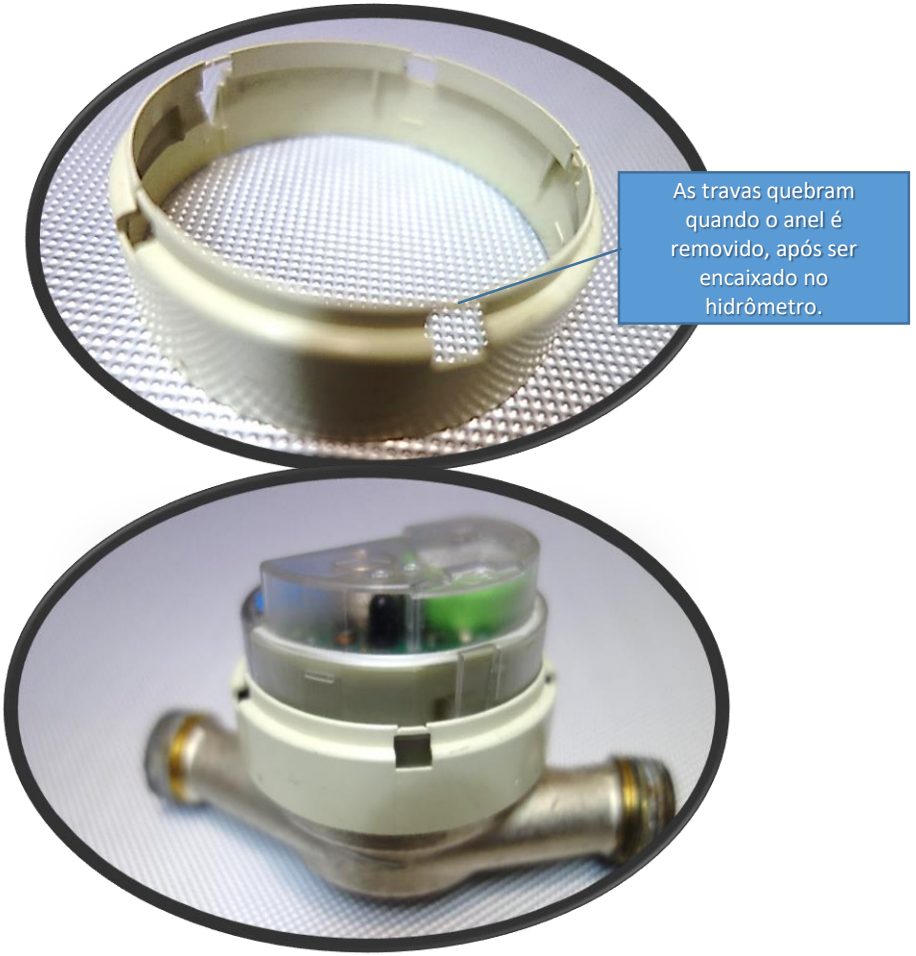
Alguns dias depois, a KSI foi convidada a participar de uma reunião fechada no escritório do Síndico do "LunarWave", com a presença do subsíndico, do Advogado procurador e do "Engenheiro Walter" da unidade 15. A reunião foi na parte da manhã em uma quarta feira, onde, praticamente os demais proprietários não ficaram sabendo da reunião ou presenciariam alguma anormalidade, no caso de manifestações intempestivas.

A reunião foi conduzida pelo Advogado procurador do condomínio, que se valeu da apresentação audiovisual da KSI e demostrou inequivocamente os fatos, fazendo com que o Engenheiro Walter se manifestasse altamente constrangido. Apesar das evidentes escusas e evasivas, o acusado prontamente se prontificou a ressarcir os prejuízos, querendo saber o montante apurado.

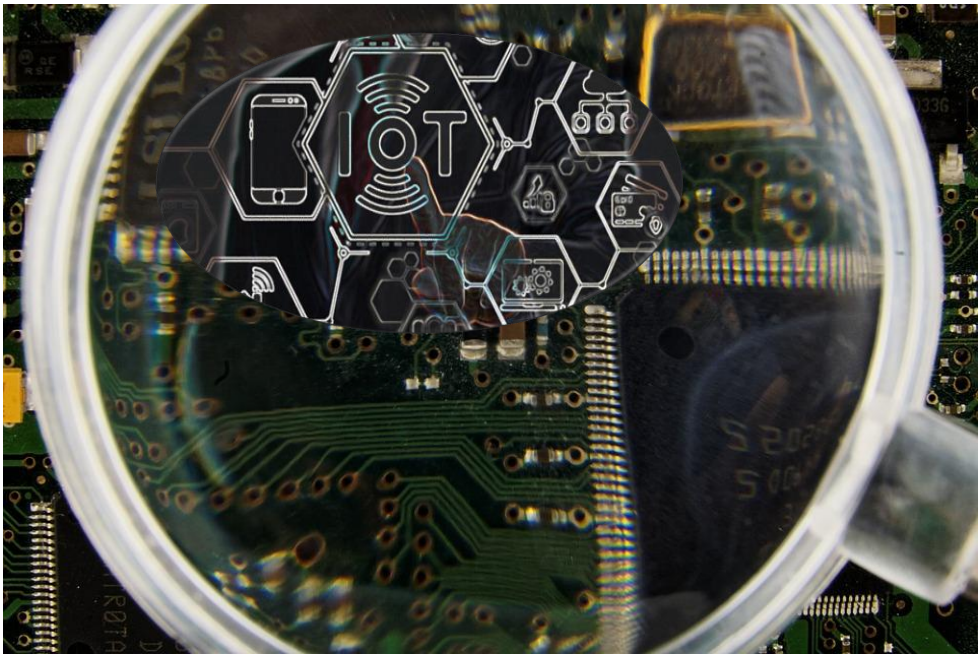
O Sr. Walter obteve a clara visão de que se recusasse em assumir a responsabilidade, o caso seria levado a uma ação judicial, portanto, aceitou pagar o valor de forma parcelada em 10 vezes. No ato, assinou notas promissórias a favor do Condomínio, que seriam resgatadas mensalmente.

Mediante aos acontecimentos, informado parcialmente sob sigilo, a "AquaMeter" resolveu aperfeiçoar o nível de segurança física de seus "objetos IoT", ou seja, os Hidrômetros inteligentes a parir de então receberam um "anel de segurança inviolável" que permite facilmente observar a tentativa de acesso ou remoção do Módulo Eletrônico, como se apresenta a seguir:

Melhor nível de segurança Física necessária em projetos IoT



Esperamos que o caso exposto de Investigação IoT, possa ter contribuído para o entendimento dos interessados no tema.



Considerações Finais

Considerações

Como se prevê a Internet das Coisas "IoT" com seu elevado potencial de inovação, ter um crescimento vertiginoso de propagação de "objetos ou coisas IoT" instaladas, conectadas, autonomamente gerenciadas, que deverá ultrapassar seguramente a marca de 100 bilhões até o 2025.

O número de aplicações práticas, para objetos inteligentes conectados, muito provavelmente promoverá no mundo real e virtual, inúmeros casos e possíveis crimes e litígios partes, que com certeza, também, ultrapassará a nossa capacidade de prever tais hipóteses.

O desenvolvimento contínuo de novas tecnologias, que na prática estão sendo evolutivamente aplicadas aos objetos inteligentes IoT, passam a exigir dos Investigadores Digitais Peritos Computacionais, uma constante e sistemática atualização de conhecimentos, bem como, capacidade de elencar e aglutinar instrumentação de hardware e software atualizadas e ajustadas suporte aos processos investigativos e periciais, conforme a especificidade dos casos e aplicações serem examinadas.

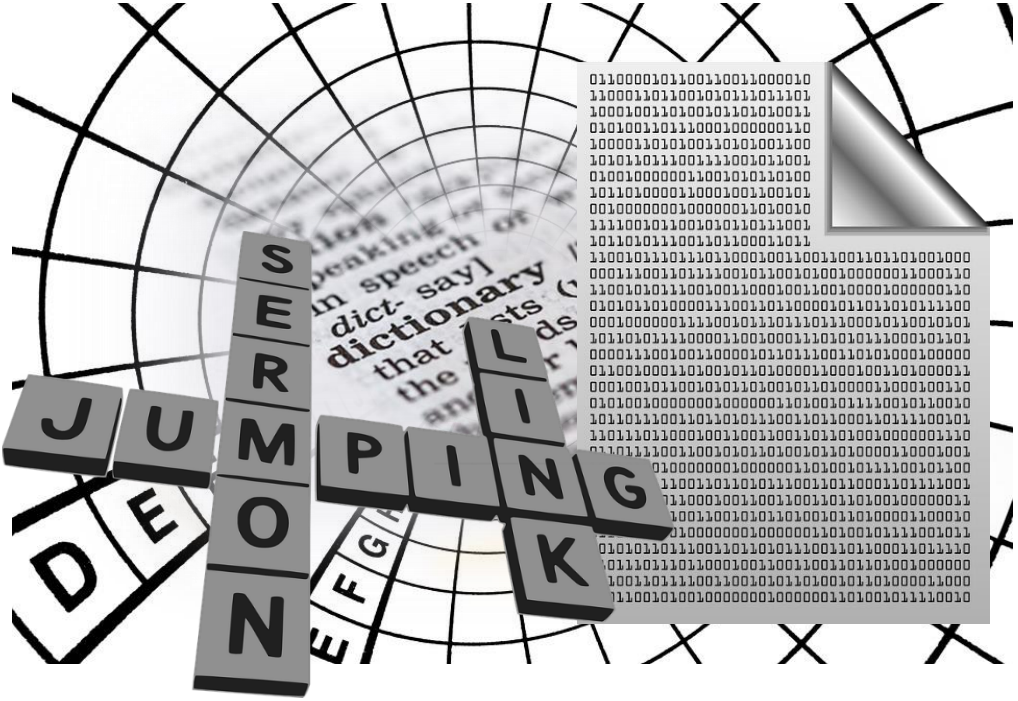
O avanço de "IoT", tem trazido muita preocupação em seus aspectos de Segurança da Informação e principalmente, sobre a **Privacidade dos Dados** e informações trafegadas, fato que levado a comunidade acadêmica e científica, as entidades profissionais e da indústria, em buscar caráter de urgência, novas alternativas de prevenção e proteção para "IoT", até com o uso de tecnologias Blockchain.

Da mesma forma, juristas, advogados, governos e sociedade civil, já estão em debate sobre medidas regulatórias e legais sobre o tema no mundo todo. Portanto, as empresas e profissionais de Computação Forense não podem negligenciar nas questões preventivas no âmbito tendo em vista a necessidade de conduzir investigações concretas com provas admissíveis em judiciais. Desta feita, o acompanhamento de profissional do direito que detenha conhecimentos específicos e aprofundados de Direito Digital, será um forte aliado para qualquer projeto de IoT.

Nos aspectos do desenvolvimento de procedimentos operacionais investigatórios de campo e em laboratório, diversas organizações e institutos já estão com seus comitês específicos estudando e buscando caminhos consolidados e efetivos para aperfeiçoar perícias em objetos "IoT" e enfrentar o grande e crescente desafio de combater a criminalidade.

Esperamos que esta pequena contribuição, exposta neste e-Book, seja efetivamente útil para todos.

Obrigado pela leitura!



Termos Aplicados em "IoT"

Termos usuais em IoT

3G (Third Generation) - Tecnologia das comunicações móveis, que inclui, entre outros, UMTS.

4G (Fourth Generation) - As comunicações móveis que ultrapassam o 3G e destinam-se principalmente a ligação à Internet ultra-banda-larga com velocidades de 100 megabits por segundo para usuários móveis.

5G (Fifth Generation) - Compreende o futuro padrão para comunicações móveis de voz e dados, para telefonia celular. Os principais objetivos da 5G é possibilitasse redes IoT Massivas, redes de críticas de IoT, acesso a Banda Larga de Internet "Wireless Fixo" (1 Gbps ou maior). Iniciou teste em 2016 e deverá estar disponível de forma plena em 2020.

6LoWPAN - Protocolo de comunicação que comprime pacotes "IPv6" para pequenos dispositivos de baixo consumo, para permitir que eles se comuniquem dentro de redes IoT.

6LoWPAN (header compression) - Protocolo que suporta IPv6 sobre redes de área pessoal sem fio de baixa potência. É um Mecanismo de compressão que permite enviar e receber IPv6 via rádio de baixa potência usando o padrão IEEE 802.15.4, que funciona com largura de banda muito baixa e de consumo de energia.

Active digital entity (Entidade digital ativa) - Qualquer tipo de código ativo ou programa "software", geralmente de acordo com uma lógica de negócios.

Actuator (Atuador) - Os atuadores transformam sinais elétricos em diferentes formas de energia, tais como Movimento ou pressão. Isso é o oposto do que os sensores fazem, ou seja, capturar as características físicas e transformá-las em Sinais.

Address of Device (Endereço do Dispositivo) - Um endereço é usado para localizar e acessar - "conversando com" - um dispositivo, um recurso ou um serviço. Em alguns casos, o ID e o endereço podem ser o mesmo, mas conceitualmente eles são diferentes.

AAL (Ambient Assisted Living) ou (Ambiente Assistido ao Vivo) - A AAL preocupa-se com o desenvolvimento de sistemas inteligentes especialmente para os idosos. Isso é feito através de tecnologias inteligentes. Os campos de aplicação são segurança (por exemplo, funcionalidade (interruptores automáticos de luz), bem como entretenimento.

AMI (Ambient Intelligence) ou (Ambiente Inteligente) - São os ambientes controlados eletronicamente, que são são sensíveis e responsivos a presença de pessoas. Uma visão desenvolvida na década de 1990.

API - (Application Programming Interface) - Conjunto de requisitos que administram como uma aplicação pode pode se comunicar e interagir com outra. Nos termos mais simples, as APIs são conjunto de protocolos, rotinas e ferramentas que o software pode usar para se comunicar com outros softwares.

Gerenciamento de API - Supervisão de tarefas relacionadas à publicação, documentação e manutenção de interfaces de programação de aplicativo (APIs). Uma empresa que publica uma API precisa mantê-la em um ambiente escalável e seguro para que os desenvolvedores usem.

Architectural reference model in IoT (modelo de referência Arquitetônico de IoT) - O modelo de arquitetural "IoT-A" descreve a metodologia com a qual o Modelo de referência e a arquitetura de referência são derivados, incluindo a utilização dos requisitos internos e externos tecnológicos, bem como, das partes interessadas.

Big Data - Qualquer grande quantidade de dados que devem ser gerenciados, armazenados ou processados por por sistemas de computador. O termo não se refere a uma quantidade específica, mas é frequentemente usado em relação a petabytes (1000 terabytes) e exabytes (1 milhão de terabytes) de dados. Os dados grandes são descritos frequentemente por "3 Vs": volume, variedade, e velocidade. O volume é a quantidade, a variedade, os diferentes tipos de dados e a velocidade, a velocidade na qual ele deve ser gerenciado.

BLE (Bluetooth Low Energy) - O BLE (Bluetooth 4.0) Bluetooth BLE é um padrão de comunicações sem fio em uma uma versão de baixo consumo de energia, que é executado constantemente, anunciando a presença de um dispositivo em sensores locais e no alcance da força da Bateria do dispositivo em questão. Na IoT, o BLE permite a localização e rastreamento de recursos sem redução da vida útil da bateria.

Brillo - Anunciado em 2015 pelo Google - Brillo é um Backbone para o IoT, peso leve, bastante básico que irá integrar dispositivos Android com suporte Wi-Fi e Bluetooth de baixa energia.

BTS (Base Transceiver Station) Estação de Antena Transceptora - É uma máquina que permite a comunicação sem fio bidirecional entre equipamentos de usuários, por exemplo entre um smartphone e um computador, se conectados com a rede GSM. Os dados são recebidos, e é então processada e transmitida máquina BTS (Antena Transceptora) para criar uma Conexão sem fio entre dispositivos.

CSS - (Cascading Style Sheets) - Um arquivo usado para dizer a um navegador como formatar uma página da web. Um link para o arquivo é incorporado na página da web ou processado em linha, e o navegador usa as informações neste arquivo para formatar atributos da página da Web, como fontes, cores, posicionamento borda e assim por diante.

CoAP (Constrained Application protocol) Protocolo de Aplicação Forçada - É um protocolo de software que é usado em pequenos dispositivos eletrônicos. Ele serve a comunicação interativa entre esses dispositivos determinante.

Computação em Nuvem - Geralmente, a entrega de serviços de computação hospedados pela Internet em vez de em um computador individual ou na localização de uma organização individual. Uma variedade de serviços de computação podem ser requisitados "na nuvem", de servidores de rede a aplicativos de Computação em Nuvem - Semelhante à computação de borda, a computação em nevoeiro toma a analogia da nuvem e aproxima-a do mundo físico: névoa. Normalmente, a computação em névoa está usando a potência computação em um nó de nevoeiro ou gateway IoT para filtrar ou processar dados e, em seguida, enviar os dados necessários para a nuvem.

Cyber-physical Systems (CPS) - Sistemas que combinam aspectos relacionados a controles de computadores sobre dispositivos mecânicos. Um Smartphone, por exemplo, combina software, hardware, podem controlar Dispositivo físicos, como uma geladeira. Em geral, muitas tecnologias móveis ou controlando Dispositivos físicos podem ser chamados de Sistemas Cibernéticos-Físicos, múltiplos. Os geralmente incluem algum tipo de sensor que podem transferir atributos do mundo real para a esfera Hoje os chamamos de dispositivos "IoTware".

Convergência OT / TIC - À medida que a Internet das Coisas se desenvolve, cada vez mais os grupos de tecnologia operacional (OT) e de tecnologia da informação (TIC) dentro das organizações precisarão juntos para capturar e comunicar os dados necessários para as decisões empresariais.

Device (dispositivo ou objeto ou coisa) - Componente físico técnico (hardware) com comunicação para outros sistemas de TIC. Um dispositivo pode ser ligado ou dentro de uma entidade física, ou monitorar uma entidade física em sua vizinhança.

DevOps - A combinação de tarefas tradicionalmente realizadas por uma organização de desenvolvimento separado e equipes de operações. À medida que as operações se tornam mais programáveis (e porque o IoT exige uma mudança na programação de operações de protocolos proprietários para idiomas e protocolos), essas duas equipes devem trabalhar juntas. Novos trabalhos podem misturar tanto desenvolvimento de softwares e habilidades de engenharia de operação de sistemas, em uma única posição.

Domotics - (Domótica) - Tecnologia que indica as confluências entre "doméstico" e "robótica" e forma a Base de muitas inovações de IoT. Estes incluem Sistemas robôs de serviço autônomo como o aspirador "Roomba", Sistemas de segurança em rede. Em IoT, esses dispositivos geralmente têm Capacidade de comunicação a máquina (M2M).

Edge Computing - A "borda da Rede" é onde o mundo físico encontra o mundo digital. Em termos de IOT, a borda é onde os dados de um sensor ou de uma máquina em tensão ou corrente são transformados em **uns e zeros** (binários)) que um computador precisa para processá-lo. Edge computing significa filtrar ou processar esses dados diretamente em dispositivos como controladores de automação programáveis (PACs) localizados na de modo que gateways intermediários e software não sejam necessários. O processamento de dados serem enviados para a nuvem reduz o tráfego nas redes e na Internet, reduzindo a quantidade de dados enviados. Também aumenta a eficiência, segurança e conformidade.

Endereço IP - Um endereço de protocolo Internet, que é um identificador numérico para um dispositivo em rede em uma rede TCP / IP. Tipicamente composto de quatro números de 3 dígitos separados por pontos decimais (IPv4), com uma versão mais recente composta de seis números separados por decimais (IPv6) de dígitos que serão amplamente utilizados em IoT.

Ethernet - Uma tecnologia de rede local (LAN) usada para conectar digitalmente dispositivos de computação. Tipicamente implementado sobre cabos de cobre de par trançado de Categoria 5 ou 6 com conectores RJ45 em cada extremidade, e composto de transceptores para controlar a passagem de bits ao mesmo tempo evitando colisões de dados. Consulte IEEE 802.3, CSMA /CD.

EAN (European Article Number) - Regra ou Norma usada na Europa para marcar e identificar produtos. Desde 2009, é Chamado GTIN (Global Trade Item Number). O número é geralmente encontrado em códigos de barras composto por até 13 dígitos (código de barras EAN 13). Em IoT há proposta que os objetos "IoTware" sejam identificados por esse padrão.

Embedded computing systems (Sistemas Embarcados) - Um termo para computação que é dedicado a um único propósito, como oposição à computação de propósito geral. Computadores embutido ou embarcados Sistemas especiais que contêm apenas o software e Hardware necessário para atingir um fim. Em IoT, sistemas são desenvolvidos para fins específicos e feitos para trabalhar em conjunto com outros

Energy-harvesting Technologies - Tecnologia conhecida como colheita de energia ou limpeza de energia é o processo pelo qual a energia é derivada de fontes externas (por exemplo, Energia térmica, energia eólica, gradientes de salinidade, etc), sendo capturada e armazenada. Frequentemente, esse termo é aplicado a consumos de energia, como a utilizada ou capturada para pequenos dispositivos autônomos sem fio, como usados em Eletrônicos Wearable (vestíveis) e redes sem fio de sensores IoT.

EPCglobal - É uma organização sem fins lucrativos fundada pela GS1 (ex-EAN International) é a GS1 US (antigo UCC). Objetiva contribuir em melhorar e padronizar Tecnologias RFDI (Radio Frequency Identification) e apoiar Comunicação de dados recolhidos através da Internet.

EPCIS repository (Electronic Product Code Information Services) ou (EPCIS Repositório Eletrônico de Informações de Produto e código de Serviços) - Um padrão para acessar e compartilhar dados conectados Códigos de produto eletrônicos que são armazenados em, por exemplo, tags RFID. O repositório EPCIS é um de banco de dados para armazenar Informações sobre produtos e seus serviços.

GitHub - uma plataforma open-source de controle de versão e colaboração para desenvolvedores de software. O GitHub foi iniciado em 2008 e foi fundado no Git, um sistema de gerenciamento de código aberto criado por Linus Torvalds para tornar o software mais rápido.

HTML - (linguagem de marcação de hipertexto) - Uma linguagem web utilizada por servidores web e navegadores da Web para apresentar informações aos usuários. Páginas HTML são servidas aos Web (clientes) de um servidor da Web. O código HTML exibido em uma página HTML informa um navegador da web como e onde exibir texto e outros recursos em uma página da Web.

HTTP e HTTPS - (Protocolo de Transferência de Hipertexto e HTTP Seguro) - Um protocolo de aplicação utilizado para sistemas de informação hipermídia distribuídos e a base de comunicações de dados na World Web. HTTP é um protocolo baseado em texto, é baseado em um modelo de comando / resposta e é identificado pelo prefácio "http: //" em comunicações, Como na barra de endereço do seu navegador da Web. HTTPS é as comunicações HTTP em uma conexão criptografada pela camada de transporte de segurança evitar espionagem de dados transmitidos.

Internet das Coisas (IoT) - Uma rede de objetos físicos - dispositivos, veículos, Edifícios, máquinas e outros itens - incorporados com eletrônica, software, sensores e conectividade de rede que permite que esses coletem e troquem dados. Em seus termos mais simples, o IoT é sobre "coisas" físicas com a capacidade de sentir, atuar e comunicar. O IoT funciona através da infraestrutura de rede existente nas empresas e na criando oportunidades para uma integração mais direta do mundo físico em sistemas baseados em ou sistemas cibernéticos, resultando em maior eficiência, precisão e benefício econômico para a

Java - Uma linguagem de programação de alto nível de propósito geral desenvolvida pela Sun Microsystems, Java é uma linguagem orientada a objetos semelhante a C ++, mas simplificada para eliminar os recursos de linguagem que causam erros comuns de programação. Arquivos de código-fonte Java são compilados em um formato chamado bytecode que pode então ser executado por um interpretador Java. O código Java pode ser executado na maioria dos computadores, pois existem intérpretes Java e ambientes de tempo de execução, conhecidos como Java Virtual Machines (JVMs), para a maioria dos sistemas operacionais.

JavaScript - Uma linguagem de scripts orientada a objetos e multi-plataforma desenvolvida pela Netscape que geralmente é mais fácil de usar e mais rápida de codificar do que linguagens ou compiladas como C e C ++. O código JavaScript pode ser incorporado em páginas HTML e praticamente todos os navegadores da Web fornecem mecanismos JavaScript para executar o computador do cliente e não no servidor. (Executando o script no cliente reduz a carga sobre o servidor.) Intitially JavaScript fornecido para interatividade em páginas web visualizados em um navegador web , mas w om node.js, JavaScript agora também pode ser executado em um servidor quando necessário .

JSON - (JavaScript Object Notation) - Um formato leve de intercâmbio de dados que é fácil para seres humanos ler e escrever, e para máquinas de analisar e gerar. O JSON é baseado na notação de objeto da linguagem JavaScript. No entanto, ele não requer JavaScript para ler ou escrever porque formato de texto que é independente de linguagem. Mas simplificado para eliminar os recursos de linguagem que causam erros comuns de programação. Arquivos de código-fonte Java são em um formato chamado bytecode que pode então ser executado por um interpretador Java. O Java compilado pode ser executado na maioria dos computadores, pois existem intérpretes Java e ambientes de tempo de execução, conhecidos como Java Virtual Machines (JVMs), para a maioria sistemas operacionais. ript para ler ou escrever porque é um formato de texto que é linguagem.

MGD - (Machines Data Generated) São dados gerados por máquinas - Informações produzidas por dispositivos mecânicos ou digitais, dispositivos de função única ou sistemas de controle industrial. dispositivos que geram dados de máquina são cada vez mais capazes de conversar uns com os se conectar com a infraestrutura de TIC que transfere, armazena e analisa os dados de uma

Microcontroller (microcontrolador) - Microcontrolador é um pequeno computador em um único circuito integrado contendo um núcleo de processador, memória e periféricos de entrada / saída. Memórias na forma de NOR flash ou OTP ROM para armazenar programas, também são incluídas no chip, bem como uma pequena quantidade de RAM. Os microcontroladores são para aplicações objetivas e focadas, em contraste com os microprocessadores utilizados em Computadores ou outras aplicações de propósito geral. Os microcontroladores são utilizados em produtos e dispositivos automaticamente controlados, exemplo; Sistemas de controle do motor automóvel, dispositivos médicos implantáveis, Controles remotos, máquinas de escritório, eletrodomésticos, ferramentas elétricas e brinquedos. Reduzidos em tamanho e custos os microcontroladores tornam mais econômicos projetos de dispositivos e processos Microcontroladores de sinais mistos (MIXED SIGNAL MICROCONTROLLER) são comuns, integrando componentes analógicos necessários para controlar sistemas eletrônicos não-digitais.

MQTT - (Message Queuing Telemetry Transport) - Um protocolo de mensagens simples e leve, originalmente projetado para comunicação de baixa largura de banda e alta latência através de conexões TCP / IP. MQTT é baseado em um modelo de publicação / subscrição em vez de um modelo comando / resposta como HTTP. MQTT requer um corretor para facilitar a publicação e assinatura tópicos de dados, enquanto HTTP é cliente / servidor.

Network - body area (BAN) ou (rede em área corporal) - BAN é uma rede de área corporal, também referida como uma área de corpo sem fios (WBAN) ou, uma rede de sensores corporais (BSN), é finalmente uma rede de dispositivos portáteis de computação. Os dispositivos BAN podem ser dentro do corpo, por implantes ou pode ser montado na superfície do corpo em uma posição fixa (adesivada), ou empregando tecnologia wearable, ou pode ser ligada no acompanhamento de dispositivos que os seres humanos podem transportar em diferentes posições, como nos bolsos roupas, à mão ou em outros locais próximos ao corpo.

Node.js - Uma fonte aberta, Ambiente de tempo de execução multiplataforma que executa aplicativos JavaScript em servidores. Permite que programas escritos em JavaScript sejam em várias plataformas de servidor diferentes, incluindo Windows, OS X, Linux e Unix.

Node - RED - uma ferramenta de programação visual de fluxo de dados, open source, desenvolvida pela IBM, que pode ser usada como uma interface homem-máquina (HMI) para node.js. Node-RED é para IoT, porque ele facilmente conecta sistemas heterogêneos distribuídos. Esta ferramenta baseada na Web é ideal para conectar dispositivos de hardware, APIs e serviços on-line de maneiras novas e interessantes.

Operational Technology (OT) - Hardware e software que monitora e controla o desempenho dos dispositivos físicos. Também o departamento ou grupo que instala, programa e mantém esse software; Automação industrial (IA). Tradicionalmente, os sistemas OT são proprietários e não em rede com o sistema de computador de uma organização. Estes sistemas podem até ser mecânicos em vez de automáticos.

REST - (Representational State Transfer) - Um conjunto de restrições arquitetônicas usadas para desenvolver aplicações web. Concebido como um padrão de desenvolvimento comum para usadas na Internet, o REST restringe os desenvolvedores a um conjunto específico de regras ou arquitetônico.

RESTful - (Arquitetura) - Quando um site ou API está de acordo com as restrições da arquitetura REST, é dito ser um sistema RESTful.

SSL / TLS - (Secure Socket Layer / Transport Layer Security) - Protocolos para criptografar transmissões de dados através de redes. TLS criptografa a comunicação usando chaves são geradas exclusivamente para cada conexão.

Tecnologia da Informação e Comunicações (TIC) - Hardware, software, infraestrutura e processos usados para criar, proteger, processar e comunicar todos os tipos de dados eletrônicos. Também como nome do departamento ou grupo dentro de uma organização que instala, programa e esses sistemas.

TCP / IP - (Protocolo de Controle de Transmissão / Protocolo de Internet) - O protocolo de comunicação mais utilizado da Internet e redes de área local (LANs); Amplamente responsáveis pelo estabelecimento e manutenção de conexões, pela formulação de pacotes de dados a serem pela reordenação de pacotes na recepção. Valorizado por sua capacidade de ser roteado através de muitas redes diferentes.

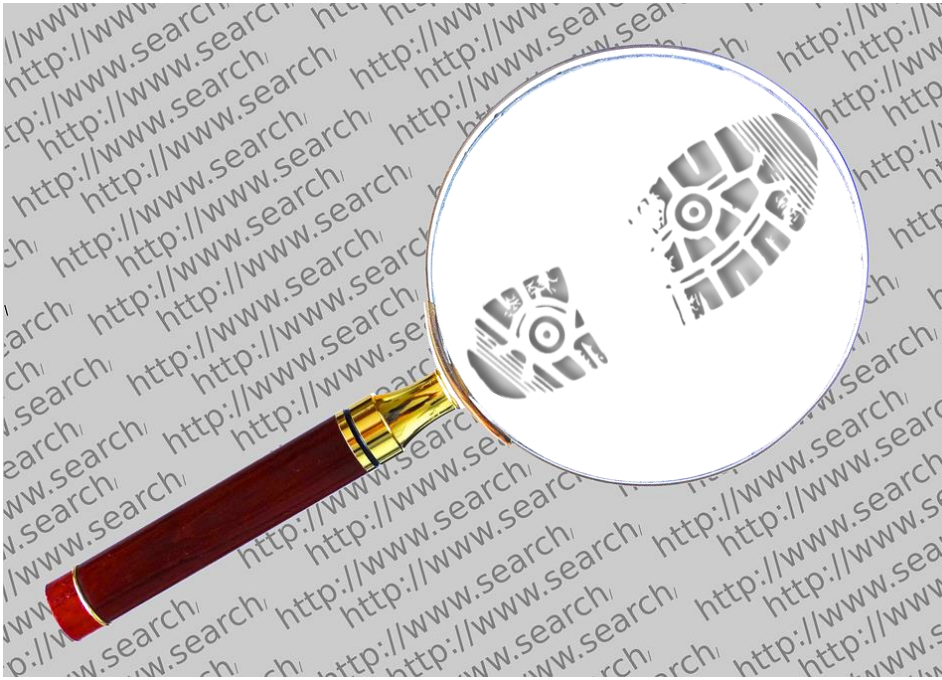
WiFi HaLow - É uma nova tecnologia emergente que utiliza espectro sem licença, de 900 MHz e padrão 802.11ah, para menor potência WiFi. Espera-se que a "HaLow" promova uma nova geração de dispositivos de uso doméstico, graças à menor potência necessária para se conectar a eles, ao WiFi atual nas faixas de 2,4 e 5 GHz. A frequência mais baixa também promete maior alcance.

Wireless - comumente referido como **Wi-Fi** podendo empregar outras tecnologias. Usado em aplicações como uma alternativa sem fio a uma rede baseada em cobre, como Ethernet. Wireless ondas de rádio de ultra alta frequência para se comunicar e transmitir dados.

Wireless sensors and actuators network (WSAN) ou Rede de Sensores - São redes de nós que sentem e potencialmente, controlam o meio ambiente. Eles "sensores" comunicam as informações através de links sem fio permitindo a interação entre pessoas ou computadores e o ambiente circundante.

ZigBee - Um protocolo de rádio de baixa potência para pequenas quantidades de dados, utilizando o padrão IEEE 802.15.4 inserido em chips de rádio comunicação. Tem baixo consumo de energia, permite que o dispositivo alcance cerca de 100 metros e possui uma largura de banda de 250 kbps. Objetos como o termostato "Nest" e as lâmpadas "Hue" usam chips Zigbee.

...



Termos Aplicados em Forense Computacional

Pesquisa dos principais termos, realizada em diversas fontes abertas,
Parafraseadas com tradução livre.

Este pequeno conjunto de termos e ou jargões ligados a Forense Computacional objetiva apenas apresentar o que consideramos essencial para a compreensão básica, para todos os tipos de leitores, sejam leigos ou técnicos. Foram utilizadas diversas fontes de pesquisas internacionais, mas as definições foram traduzidas, ajustadas e parafraseadas.

Admissibilidade – Conjunto de características associadas aos vestígios, evidências e indícios, que obtidos através do uso efetivo de metodologias apropriadas, possam ser consideradas admissíveis em processos judiciais.

Análise Profunda – Uso de padrões e técnicas científicas admissíveis e validadas, para se apurar vestígios, que possam constituir e determinar evidências concretas, ligadas ao objetivo da investigação.

Análise a Quente ou Viva (Live/On Line) - compreende a coleta de dados que possam ser voláteis um equipamento eletrônico em funcionamento, através da leitura/cópia de dados da memória RAM. Existe o risco de se adulterar os dados na memória.

Análise Fria ou Off Line – compreende a análise realizada em equipamento eletrônico desligado, se examinar e ou produzir cópia de dispositivos de armazenamento, através de processos seguros e ferramentais adequadas.

Aquisição de Dados - compreende o estágio em uma investigação forense Digital em que os dados envolvidos são coletados na constituição de informações analisáveis. É comum utilizar cópia "bit-by-bit" do firmware, do disco rígido ou outras mídias envolvidas no caso sob investigação.

Aquisição de evidência digital - É o processo pelo qual informações ou itens físicos, são coletados, armazenados e custodiados para posterior exame. A indicação do termo "Evidência" implica que o processo utilizado pelo agente investigador possa ser reconhecido nos tribunais. A coleta formal e custodiada é considerada um instrumento de ordem legal se devidamente aplicada.

Bit - É a menor unidade de dados, que em eletrônica digital pode representar o elemento binário "Zero" ou "Um".

BIOS - é o acrônimo de "Basic Input/Output System", ou seja é um programa de inicialização de um dispositivo eletrônico microcontrolado/processado, capaz de fazer a configuração inicial do equipamento e ativar o seu funcionamento. Esse programa normalmente é residente em memória tipo firmware ou flash ROM/CMOS.

Bitstream ou Bit-by-Bit - compreende o conjunto da sequencia de dados binários, obtidos através de leitura para execução de cópia de áreas de armazenamento temporário ou permanente de equipamentos eletrônicos. Seria a cópia exata do conteúdo de memórias, firmwares, discos rígidos, etc., sendo vulgarmente chamada de espelhamento.

Buffer - área de memória RAM de armazenando temporário de dados. A cópia desses dados de um arquivo buffer só pode ser realizada seguramente através da Análise a Quente.

Byte - É o conjunto de oito (8) bits (elementos binários) necessários para a representação de um caractere legível (letras ou números) em um equipamento eletrônico. A quantidade de Bytes pode expressa em Kb (kilobyte ou 1000 bytes), Mb (megabyte ou 1.000.000 de bytes), Tb (terabyte), Pb (petabytes)...

Cache - Compreende a técnica para usar uma área de memória para deposito de dados temporariamente. Ela pode ser utilizada para compensar as diferença de velocidade entre um computador, bem como, aplicada para armazenar paginas web que se visitou a pouco tempo para que ao ser revisitada, possa ser recuperada mais rapidamente (ex.: cache de páginas web). Normalmente os últimos dados de cache não são perdidos e podem ser acessados e recuperados.

Cadeia de Custódia - Compreende a documentação cronológica do movimento, localização, coleta e posse de objetos ou dados que possam constituir provas.

Cracker - Nome atribuído a um especialista capaz de burlar a segurança de softwares comerciais, quanto a sua proteção contra o uso ilegal. É também o nome mais apropriado para caracterizar os "invasores criminosos" de sistemas na Internet, ao invés de Hacker, que normalmente atuam para proteção e desenvolvimento ético de softwares.

Dados Ambientais - São as informações do "sistema operacional" sobre os usuários de um dispositivo eletrônico (microcomputador) que normalmente não podem ser acessadas por ele. dados podem ser tecnicamente recuperados através de acesso a slack de arquivos, memórias espaços de discos não alocados, etc. sendo muito úteis em investigações.

DONGLE (hardlock) - Dispositivo do tipo "pen drive" (podendo utilizar portas seriais, paralelas ou USB) que se conecta a um computador para validar a licença de uso de determinados softwares Só quem possui o DONGLE correto, ligado ao numero de série do software, pode executar o A duplicação do DUNGLE é de alta dificuldade.

Criptografia - Aplicação de técnicas matemáticas capazes de ampliar os processos de segurança de dados e informações. Normalmente dados criptografados podem dificultar investigações, mas também, podem reforçar indícios de acobertamento de informações críticas ou criminosas, caso em estudo.

Criptologia - Compreende a ciência matemática que abrange a criptoanálise para tornar claro (legíveis) dados criptografados, assim como, o desenvolvimento de algoritmos criptográficos para ocultar dados e informações.

Cybernetica - Compreende a ciência que estuda sistemas biológicos e mecânicos, incluindo a eletrônica, de forma que a correlação entre os dados sistêmicos possam oferecer retorno mesmo através da redes e ou da Internet. Normalmente nas investigações digitais, se considera ambiente cybernetico quando os dados se relacionam entre os homens e as máquinas (robótica / cybercrimes / cyberespaço...).

Dados de Exfiltração - Compreende a propriedade de que os dados adquiridos estão completos, intactos e podem ser considerados confiáveis, de forma que não houve modificação ou adulteração forma acidental ou não autorizada. Técnica também empregada por Crackers e adicionada de técnicas de "chunking" e "ofuscação", para mascarar a legitima aquisição de dados, furtados em fontes corporativas.

Digital Forensics - Emprego de Técnicas e Processos especializados para a aquisição, recolha, retenção de dados digitais (binários) relacionados a investigações, para se tornarem provas em Pode ser definido também como o trabalho de um grupo de profissionais apoiados em modelos (frameworks) com padrões para a coleta, preservação, analise, correlações e processamento de informações, baseadas em dados digitais, de forma a se apurar as evidências de crimes cometidos ou através de meios eletrônicos.

Endereço IP - É a denominação dada a uma localização exclusiva de um computador ou dispositivo eletrônico (IoT) atribuída pelo IP (Internet Protocol) em uma rede local ou pública. A localização dos endereços IPs podem ser georrefenciadas através das coordenadas das conexões da Internet dos

Exploits - Programas que utilizam técnicas que podem explorar vulnerabilidades de sistemas digitais em hardware e software. Alguns programas dessa classe podem ser empregados em Forensics, como ferramenta, para apurar o cometimento de fraudes e outros delitos.

File Signature - Termo que identifica a assinatura de arquivos em um computador, através de dados ligados ao arquivos, como formato, tamanho, data de criação, modificação, hash, etc. não para garantir a integridade do arquivo.

Firmware - Nome atribuído a um dispositivo de memoria que armazena um programa, para somente leitura e execução (ROM). Hoje dispositivos eletrônicos que utilizam microchips de alta integração, possuem em seus circuitos áreas de armazenamento de programas funcionais e operacionais para funcionalidades.

Hidden Files - Arquivos Ocultos, são normalmente atributos de sistemas operacionais, que permitem que algumas classes de arquivos não apareçam listados normalmente nas sua pastas ou localizações em um sistema eletrônico ou computador.

HUB - Normalmente o termo se refere a um concentrador de dados. Pode ser um software ou hardware capaz de controlar a distribuição de informações em uma rede. Em IoT o termo é no lugar de Router, e pode ser periciado.

Image (Forensics) - Compreende a reprodução fiel dos dados copiados de um dispositivo suspeito, para outro, que possa ser analisado pericialmente, sem intervenção no original.

IMEI - É um número de 15 dígitos, sendo identificador único para seriar dispositivos que utilizam tecnologia GSM/LTE de comunicação móvel. Seu significado é "International Mobile Equipment Identifier". Identifica junto com o endereço IP a localização de um dispositivo único em redes celulares.

IMSI - É um identificador único global "International Mobile Subscriber Identity" que identifica um usuário cadastrado nas operadoras de telecomunicações (GSM, UTMS, LTE...).

Log File - Arquivo controlado por Sistema Operacional que registra todas as operações realizadas no equipamento. Esse arquivo pode ser analisado para se apurar o cometimento de delitos

Metadatas - Dados incorporado em um arquivo (como Assinatura), que descreve as propriedades de um arquivo ou diretório, que pode incluir os locais onde o conteúdo é armazenado no datas e horas na criação e uso, informações específicas do aplicativo e permissões vinculadas aos usuários.

Multimedia Evidence - Evidências coletadas em dispositivos multimídia, onde dados digitais, analógicos, musica e filmes podem ser correlacionados em uma investigação forense. Ex.: Um Smartphone é um dispositivo multimídia.

Photogrammetry - Fotogrametria/Videogrametria é a ciência que envolve tecnologias para obtenção de informações confiáveis através do estudo de objetos físicos e ambientais, através da análise, "medição" e estudo, de imagens fotografadas ou filmadas, com base em padrões outros fenômenos identificáveis. É aplicada em processos de Digital Forensics.

Proficiency Test - Teste empregado para avaliar o conhecimento de Investigadores e Analistas em Digital Forensics, com base em padrões internacionalmente aceitos.

Reference Material - Materiais de referência indicam as fontes de literatura e metodologias publicadas mundialmente, empregadas nas investigações, com fundamentação em documentação hardware e software, analises práticas do conjuntos de hash, conjuntos de cabeçalho, e outras aplicáveis. É fundamental constar nos Laudos desenvolvidos.

Source Code - Código fonte é o conjunto de instruções de um programa escrito em linguagem nativa, que possa ser compilada ou interpretada por um microcontrolador / microprocessador.

Timeline Sequence Reconstruction - Reconstrução de ocorrências na linha do tempo é o processo que permite relacionar dados, imagens, áudio ou outras informações ambientais, entre si, em uma sucessão logica de eventos cronologicamente ordenados.

Traditional Enhancement Techniques (Forensic) - Compreende o emprego de técnicas metodológicas avançadas e mundialmente aceitas em processos de investigação forense.

Validation - Compreende o processo da examinar e desenvolver ensaios para garantir que os resultados de uma técnica forense proposta ou de uma nova ferramenta alcançam os objetivos estabelecidos em eficácia e confiabilidade.

Write Block/Write Protect - Representa a aplicação de métodos em Hadware e Softwares que garantam a proteção contra escrita, através de bloqueio para que não haja modificações durante a aquisição de dados em investigações Digital Forensics.

Principais "NORMAS" e Padrões IoT

Principais Normas e Padrões para IoT

O objetivo deste conteúdo é fornecer algumas indicações, das centenas de referências existentes no mundo, que buscam estabelecer padrões e regulamentação para o desenvolvimento projetos de IoT.

<Acesso confirmado em 12/05/2017>.

- **Internet Protocol for Smart Objects (IPSO) Alliance** - Padrão de "Internet Protocol" para a Rede de Conexão de "Smart Objects", com Consumidores, com cuidados de saúde, e com a industrial Aplicações.

http://www.ipso-alliance.org/

- **Industrial Internet Consortium (IIC)** - M2M standardisation - ligação padrão máquina a máquina.

http://www.iiconsortium.org/

- **AllSeen Alliance (AllJoyn)** - Grupo sem fins lucrativos, dedicado ao Suporte para a Internet de tudo.

http://www.allseenalliance.org/

- **Thread Group** - Certificação de produto para garantir a Segurança e Interoperabilidade dos produtos "IoTware" domésticos.

http://www.threadgroup.org/

- **Open Interconnect Consortium (OIC)** - Grupo de estudo para Desenvolvimento de padrões para descoberta, conectividade e autenticação de dispositivos IoT, ligados ao projeto "IoTivity".

http://www.openinterconnect.org/

- **IEEE Standards Association P2413** - Este projeto de norma define uma arquitetura para a Internet das Coisas (IoT), incluindo a descrições de vários domínios IoT, definições de IoT, domínio abstrações, bem como a identificação de pontos comuns entre diferentes domínios IoT.

https://standards.ieee.org/develop/project/2413.html

- **International Telecommunication Union (ITU)** - Grupo de Estudo ITU-T que aborda a estandardização e requisitos sobre a Internet das Coisas.

http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx

- **Open Connectivity Foundation (OCF)** - Uma colaboração da Indústria, gerando a oportunidades para os consumidores e negócios com dispositivos IoT, sendo, uma maneira rápida de todos obterem e adotarem um padrão único e aberto.

https://openconnectivity.org/

- **Open Source Application Development Portal (OSADP)** - O OSADP é um Programa e outras fontes outras fontes de recursos para apoiar o uso e desenvolvimento de "Veículos Conectados" e aplicações ITS relacionadas ao "USDOT ITS" (sistema inteligente de transporte do Transporte Norte Americano).

https://www.itsforge.net/

- **oneM2M** - OneM2M é uma inciativa para a solução global de padrões, que abrangem requisitos, Arquitetura, APIs e especificações de Segurança e soluções de interoperabilidade para "Máquina Máquina" (M2M) e tecnologias IoT. OneM2M foi constituída em 2012.

http://www.onem2m.org/

- Normalização da IoT na Austrália – Disponivel em < https://www.austrian-standards.at/en/infopedia-topic-center/infopedia-articles/internet-of-things-iot/ >
- IoT-A - WSO2 – ITU-T– padrões de Arquitetura de IoT que merecem ser conhecidos e avaliados. Estão disponíveis em:
  < http://sbrc2015.ufes.br/wp-content/uploads/Ch3.pdf >
  <
  http://cocoa.ethz.ch/downloads/2014/01/1524_D1.3_Architectural_Reference_Model_update.pdf > ou < http://wso2.com/wso2_resources/wso2_whitepaper_a-reference-architecture-for-the-internet-of-things.pdf > ou ITU-T Y.2060 <
  https://www.itu.int/rec/T-REC-Y.2060-201206-I > .
- IoT Security Foundation – objetiva apresentar as melhores práticas em segurança para quem especifica, cria e usa produtos e sistemas IoT. Esta disponível em <
  https://iotsecurityfoundation.org/ >
- OTA - Online Trust Alliance - organização que ajuda na educação e recomendações de padrões para a indústria. IoT é a sua principal iniciativa. Disponível em :<
  https://otalliance.org/initiatives/internet-things >.

Outros e-Books publicados

GUIA - SEGURANÇA CORPORATIVA OAB
http://www.komp.com.br/data/documents/GuiaSegCorp_OAB_KOMP.pdf

COMPLIANCE - Fundamentos
http://www.komp.com.br/data/documents/e-BooK-I-COMPLIANCE-Fundamentos.pdf

COMPLIANCE - Corrupção e Fraudes no Mundo Empresarial
https://www.komp.com.br/gallery/ccfme-v1-ebook2a.pdf

MANIFESTO - Direitos Globais de IoT (Internet das Coisas)
http://www.komp.com.br/data/documents/e-Book-IoT-MANIFESTO-EdicaoIqp.pdf

...

Contato, indicações, manifestações...

kontato@komp.com.br

Este e-BOOK é uma

Edição Especial

Divulgada preliminarmente durante o
III Congresso de Direito Digital
A INTERNET DAS COISAS E A INDÚSTRIA
17 de maio de 2017

http://hotsite.fiesp.com.br/direito-digital/

EDIÇÃO PRELIMINAR DOS AUTORES

Os autores são integrantes do Grupo de Estudos Temáticos de Direito Digital e Compliance, coordenado pelo Dr. Coriolano A. A. C. Santos, Conselheiro do Conselho Superior de Assuntos Jurídicos e Legislativos (CONJUR) da FIESP.