A profissão do futuro: Como ser um perito digital ou perito em informática e iniciar na carreira (2021)

COMO COMECEI A ATUAR ÁREA?

Atuo com perícia em informática há 21 anos. Tive o prazer de aprender muito com grandes nomes na área, pessoas pioneiras que nunca se negaram em compartilhar conhecimento. Sinto-me no dever de contribuir com os jovens interessados na área de *digital forensics* ou em que desejam se tornar um perito digital.

Atualmente, coordeno Pós-graduações no tema e ministro cursos de extensão em ferramentas *open source* e proprietárias para computação forense.Além disso, atuo com perícias judiciais e administrativas em todo o Brasil e tenho um time de *firstresponders* e peritos para atuar em todos os casos que temos.

Novos e desafiadores casos são apresentados semanalmente. Não foi fácil iniciar na área, busquei certificações, fiz especialização, mestrado e sou doutorando na área de ciência da informação e tecnologia, mas, também, me especializei em Direito.

Hoje concluo que o perito digital não pode ser apenas um técnico, muito menos o jurista. É preciso ter conhecimentos de projetos, ter especialidade em conduzir o processo de perícia, avaliando os interesses e dados das partes, mediar e ser um profundo conhecedor da Ciência da Informação.

A área é incrível e apaixonante, mas o profissional que não sabe lidar com a rotina e falar a linguagem forense do

destinatário do trabalho, que é o JUIZ (em perícias judiciais), não consegue atuar por muito tempo e acaba limitando seu campo às perícias internas ou corporativas e assistência técnica.

Ser perito forense é mais do que conhecer a técnica. É coordenar os fluxos de informação do caso, transformar artefatos em evidências e ser um expert *witness*, defendendo tecnicamente o cliente, com a persuasão necessária.

Vamos lidar com advogados e o sistema judiciário, sendo que conhecer estas relações é fundamental. E, principalmente, a nossa missão é auxiliar o juízo no entendimento da questão técnica controvertida ou mesmo ajudar as partes a lograrem êxito em suas ações e processos judiciais, que envolvam tecnologia.

QUAIS SÃO AS NORMAS E BOAS PRÁTICAS SOBRE COMPUTAÇÃO FORENSE

Quando comecei, havia apenas recomendações da SWGDE, IOCE, um manual muito importante da SANS (anote, é referência em computação forense). Hoje, temos o NIST, que testa ferramentas forenses e aborda melhores práticas há 14 (catorze) anos. Também, temos um guia interessante da União Europeia, chamado "Best Practice Manual fottheForensicExaminationof Digital Technology",a RFC 2227, e interessantes artigos publicados, como este http://ieeexplore.ieee.org/document/6274340/?reload=true

Existe, atualmente, uma família de normas ISO relacionadas à computação forense, que devem ser observadas pelos profissionais, sendo elas:

- ISO/IEC 27037 concerns the initial capturing of digital evidence.This standard offers guidance on the assurance aspects of digital forensics e.g. ensuring that the appropriate methods and tools are used properly.
- ISO/IEC 27041 offers guidance on the assurance aspects of digital forensics e.g. ensuring that the appropriate

methods and tools are used properly.
- ISO/IEC 27042 covers what happens after digital evidence has been collected i.e. its analysis and interpretation.
- ISO/IEC 27043 covers the broader incident investigation activities, within which forensics usually occur.
- ISO/IEC 27050 (in 4 parts) concerns electronic discovery which is pretty much what the other standards cover.
- British Standard BS 10008:2008 "Evidential weight and legal admissibility of electronic information.

Além disso, o profissional deverá conhecer as normas e regulamentos vigentes em sua localidade, bem como as normas processuais, sobretudo em relação a coleta e produção válida de provas, aplicada aos meios digitais. Um perito que desconhece os limites de sua atuação pode causar grandes danos às partes.

AUTORES, ARTIGOS E PESQUISADORES INTERNACIONAIS ESSENCIAIS

MARK REITH, também, tem um artigo essencial para quem pretende trabalhar na área, denominado "*Anexaminationof digital forensics models*", em que ela faz um comparativo sobre as disciplinas e metodologias de perícias na área: https://www.just.edu.jo/~Tawalbeh/nyit/incs712/digital_forensic.pdf.

GARFINKEL escreveu um artigo indispensável a todos os futuros peritos em informática, qual seja*, Digitalforensicsresearch: The next 10 years*.

MORIOKA publicou em 2016 um importante artigo sobre computação forense em nuvem, área da perícia digital que vem crescendo muito: https://ieeexplore.ieee.org/document/7568909.

MILAGRE e CAIADO, publicaram um importante artigo sobre Computação Forense na em "*Cloud Computing*" (Desafios e melhores práticas – ICoFS-2013): https://www.forensicfocus.com/articles/current-challenges-in-digital-forensics/.

SOTYANOVA et al, escreveram importante artigo sobre os desafios e abordagens da forense em Internet das Coisas: https://ieeexplore.ieee.org/document/8950109.

NHIEN-NA LE-KHAC et al, tratam dos desafios da computação forense em veículos inteligentes: https://www.sciencedirect.com/science/article/abs/pii/S0167739X17322422.

Estes são alguns artigos estruturais, mas o profissional deve estar sempre atento à produção científica na área.

Não tenho dúvida que o profissional e auditor em informática forense de sucesso será aquele que não sejaum mero "Operador de Ferramentas". Mas será aquele que conheça as técnicas aplicadas pelas ferramentas e, principalmente, as teorias da informação por trás de um objeto de análise. Por isso, publiquei um artigo, com meu orientador denominado: "As contribuições da Ciência da Informação na perícia em Informática no desafio envolvendo a análise de grandes volumes de dados – Big Data", publicado na UFPB (https://periodicos.ufpb.br/index.php/itec/article/view/22846). É leitura basilar.

Estes são importantes aportes teóricos e basilares para iniciar uma consultoria em perícia digital, que, com certeza, trarão a base para outras leituras mais específicas.

CADEIA DE CUSTÓDIA

Recentemente, o Código de Processo Penal, aplicado quando da realização de perícias na área criminal, sofreu profundas alterações em razão do advento da Lei nº 13.721, de 2018, conhecida como Pacote Anticrime.

Agora, há a descrição da cadeia de custódia, isto é, o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e

manuseio a partir de seu reconhecimento até o descarte (art. 158-A). Os artigos 158-B e seguintes do Código de Processo Penal disciplinam a cadeia de custódia e deverá ser também observado pelo perito digital.

O QUE FAZ O PERITO DIGITAL?

A função da perícia digital ou forense digital, carreira que mescla a formação jurídica com a tecnologia da informação é reconstruir o passado, constatar a materialidade e apurar a autoria de conflitos, fraudes, furtos e agressões que são cometidas por intermédio de dispositivos informáticos e telemáticos, como computadores, notebooks e dispositivos móvel celular.

A ciência que possui, aproximadamente, dezenove anos no país, antes era destinada apenas a auxiliar a criminalística na atuação de crimes eletrônicos, agora passa a ser considerada uma área corporativa, ligada a segurança da informação, governança, risco e conformidade, em razão do crescente número de fraudes informática cometidas no âmbito corporativo.

Cumpre destacar que são crescentes as infrações cometidas sob o suposto anonimato virtual. Contudo, as pessoas ainda insistem em classificar a perícia digital ou forense computacional como mero resgate científico de dados ou clonagem de discos, o que é uma premissa incorreta.

QUAL É O CAMPO DE ATUAÇÃO?

No que se refere às áreas de atuação, o perito digital pode atuar na área pública ou privada.

Para atuar na área pública, o profissional pode peticionar em juízo sua habilitação que será ou não deferida pelo juiz. Em São Paulo, a norma que regulamenta a perícia é o Provimento nº 2306/2015. Lembrando que o peticionamento dos peritos já é realizado pela via eletrônica, razão pela qual o perito precisa conhecer sobre PROCESSO ELETRÔNICO.

Em algumas comarcas, pode auxiliar o Ministério Público e Delegacias não especializadas, necessitando apresentar, em petição escrita instruída de curriculum, os antecedentes criminais e casos que atuou.

Além disso, o perito digital pode atuar como assistente técnico das partes em juízo.

Ainda, há a possibilidade de ser um perito policial, integrante do Instituto de Criminalística dos Estados ou da Polícia Federal, sendo que o ingresso é somente mediante concurso.

Por sua vez, na área privada, os profissionais de forense corporativa normalmente integram uma equipe multidisciplinar composta por profissionais da área jurídica e técnica, de nível estratégico e gerencial, e que estão inter-relacionados com o Time de Resposta a Incidentes da Empresa, previsto na norma ISO 27001.

Importante destacar, ainda, que a recém publicada norma ISO 27701, que estabelece o Sistema de Gestão da Privacidade da Informação, ratifica em seu item 6.13.1.17 as diretrizes da ISO 27002, no que diz respeito a manutenção de processos claros de coleta de evidências:

"Convém que procedimentos internos sejam desenvolvidos e seguidos quando tratando de obter evidências para os propósitos de ações legais ou disciplinares.

Geralmente os procedimentos para evidência fornecem processos de identificação, coleta, aquisição e preservação de evidências, de acordo com diferentes tipos de mídia, dispositivos e situação dos dispositivos, por exemplo, se estão ligados ou desligados. Convém que os procedimentos levem em conta:

a) a cadeia de custodia;

b) a segurança da evidência;

c) a segurança das pessoas;

d) papéis e responsabilidades das pessoas envolvidas;

e)competência do pessoal;

f) documentação;

g) resumo do incidente.

Quando disponível, certificações ou outros meios de qualificação de pessoal e ferramentas são buscados, para aumentar o valor da evidência preservada.

Evidência forense pode ir além dos limites da organização ou da jurisdição. Em tais casos, convém que seja assegurado que a organização tem direito de coletar as informações requeridas como evidência forense. Os requisitos de diferentes jurisdições podem ser considerados para maximizar as chances de admissão ao longo das jurisdições relevantes."

Assim, o perito forense computacional também pode atuar nas áreas relacionadas à proteção de dados pessoais e segurança da informação, buscando solucionar problemas relacionados a incidentes, como vazamento da dados, na identificação do motivo e da autoria.

Vale ressaltar que nem tudo na perícia são crimes informáticos. Hoje o perito pode atuar com:

a) Valoração de ativos digitais;

b) Apuração de autoria de fraudes;

c) Análise de contrafações de sistemas e softwares;

d) Comparação de softwares;

e) Análise de controvérsias em implementações de

sistemas;

f) Perícias envolvendo concorrência desleal;

g) Perícias envolvendo uso indevido dos ativos de TI;

h) Fraudes em meios de pagamentos;

i) Atuação em processos trabalhistas;

j) Controvérsias em relações de consumo na web;

k) Análise de sanitização de bases de dados;

l) Controvérsias envolvendo proteção de dados pessoais.

FORMAÇÃO EM PERÍCIA DIGITAL

Em relação à formação do perito digital, a legislação nacional não exige formação específica em tecnologia, sendo que no novo Código de Processo Civil até a expressão "nível universitário" fora reprimida. Agora, conforme o art. 156 do novo Código de Processo Civil, os peritos serão nomeados entre os profissionais legalmente habilitados.

No entanto, isso não significa "carta" branca para aventureiros, pois os tribunais avaliarão, periodicamente, três fatores:

a) formação profissional: conjunto de formações do perito para atuação na área, sendo que aqui contam graduações, pós-graduações e certificações;

b) atualização do conhecimento: o quão atualizado o profissional se encontra, o que pode ser demonstrado com cursos e certificações recentes;

c) experiência: o que pode ser quantificado pelo número de trabalhos técnicos já realizado.

A despeito do que está previsto em lei, é imprescindível um

conhecimento multidisciplinar, a fim de evitar que erros sejam homologados pelos juízes e cortes brasileiras, bem como a produção de laudos superficiais, que geram quesitos a serem explorados por bons advogados em Direito Digital, que irão destituir as provas e, principalmente, cooperar com a impunidade. Precisamos, realmente, de pessoas qualificadas.

Além do perito digital ter uma formação aprofundada em tecnologia, deve demonstrar experiências em frameworks, *compliance* e melhores práticas previstas na tecnologia da informação como SOX, COBIT, ITIL, PCI, ISO 27001, bem como da legislação básica brasileira, Código Civil, Código Penal, Consolidação das Leis do Trabalho, e principalmente, normas processuais e procedimentais que regulamentam a produção da prova pericial no Brasil.

Dessa forma, a formação ideal do perito digital deve ser a técnica, com aportes de conhecimento processual/jurídico (caso atue na área forense), já que, mais do que saber agir tecnicamente ou conhecer a intimidade das falhas dos sistemas, o profissional precisa atuar na linha tênue que separa uma perícia homologada de uma produção probatória nula, ilícita ou ilegítima.

Nos treinamentos que ministramos, constatamos profissionais altamente treinados para coleta de evidências, mas que possuem dificuldades em preservá-las, classificá-las, analisá-las em uma escala de prioridade e, principalmente, não conseguem elaborar um laudo técnico pericial.

Vale ressaltar que a profissão do perito digital compreende a habilidade de escrever e dar significado a zeros e uns para um juiz ou *sponsor*. Além disso, há peritos com formação jurídica tendem a fazer laudos repletos de fundamentação legal, e esquecem de analisar os pontos técnicos solicitados pelas partes.

Assim, a perícia digital não pode ser mais vista como um “box”

separado da segurança da informação e das normas de governança em TI.

Não recomendaria uma Pós em computação forense que só trate de Direito ou apenas teorias. O aluno precisa ter contato com *threats*e casos simulados, de modo a setornar um projetista quando tiver que lidar com casos reais, rapidamente, estruturando em sua mente suas técnicas e ferramentas a utilizar, considerando todos os princípios da disciplina e, principalmente, ciente de que tempo é sim fundamental.

Quanto aos conhecimentos que reputo indispensáveis para um perito digitallisto: redes e arquitetura TCP/IP, sistemas de arquivos, sistemas operacionais baseados em Unix, conhecimentos de fundamentos de algoritmos e linguagem de programação. Muitas ferramentas *opensource* já homologadas pela comunidade estão em plataforma Unix, logo, um perito que opere somente e plataforma Windows, pode em determinados casos, preterir ferramentas e técnicas que seriam essenciais para o caso.

ONDE CURSAR COMPUTAÇÃO FORENSE

Não se tem a disciplina de computação forense ou perícia digital nos cursos de graduação em tecnologia da informação (alguns já contam com a disciplina de segurança da informação). Igualmente, algumas pós-graduações em Segurança da Informação adotam a computação forense como disciplina. Não recomendo cursar uma pós apenas pela disciplina, embora o conhecimento de Segurança da Informação seja muito relevante para aqueles que desejam se especializar em computação forense.

De início, eu preciso deixar claro que você não necessita de uma pós-graduação em computação forense para atuar. Existem importantes certificações que passo no meu curso EAD de PERÍCIA E INVESTIGAÇÃO FORENSE DIGITAL (https://cyberexperts.com.br/curso-pericia-digital/), que

podem contribuir muito para a formação profissional. O Curso é feito pela CYBEREXPERTS, referência e uma das primeiras empresas no Brasil focada em Reputação Online e Computação Forense. Mais informações, entre em contato comigo, pois as turmas são extremamente limitadas.

Hoje, é interessante que você desenvolva cursos de extensão ou mesmo certificações na área, sendo as da SANS e da e-COUNCIL (https://www.eccouncil.org/programs/computer-hacking-forensic-investigator-chfi/) as mais conhecidas, além das certificações focadas em ferramentas. Participe, também, de eventos sobre o tema, sendo que hoje existem inúmeros eventos online e, provavelmente, alguns na sua região.

CURSO PERÍCIA E INVESTIGAÇÃO FORENSE DIGITAL

O meu treinamento -"PERÍCIA E INVESTIGAÇÃO FORENSE DIGITAL"- tem como objetivo fornecer ferramentas para que os profissionais atuantes na área – ou que nela pretendam ingressar – possam se capacitar neste ramo, atendendo com excelência as exigências do mercado. Estas ferramentas proporcionarão os conhecimentos necessários para a análise de mídias, recuperação de evidências e elaboração e análise de Laudos Periciais.

Além disso, é um curso que atua não só com forense open source, mas com ferramentas proprietárias muito utilizadas no mercado. Se você for trabalhar como terceirizado para grandes consultorias ou mesmo busque um emprego como analista o perito forense digital, certamente deverá comprovar conhecimento nestas ferramentas.

Caso opte por uma pós graduação, antes de ingressar, pesquise sobre os docentes. Uma Pós que atua só com agentes públicos passará ao aluno uma visão limitada do mercado e dos casos envolvendo computação forense e perícia digital.

Portanto, escolha um curso que possa conhecer como é a perícia em informática no setor público (Polícia, Receita Federal,

Fazenda, Exército, Ministério Público), mas também, que possa ter contato com docentes que estão no mercado corporativo de perícia digital, a fim de ter um contato não só sobre as áreas, mas como são conduzidos processos de investigação forense (fase de preparo, coleta, preservação, análise e reporte).

Não preciso dizer que o networking também é essencial, pois profissionais do mercado poderão demandar seus serviços. Já na área pública, só existe o ingresso mediante concurso público.

QUANTO GANHA UM PERITO FORENSE COMPUTACIONAL?

Na área pública, as perícias judiciais são pagas através de honorários. Ou seja, o juiz, a partir do momento em que entenda que é caso de perícia, oferece oportunidade para o perito estimar. Considere neste caso dividir o trabalho em fases e estime horas para cada fase, totalizando ao final. Mas o profissional que pretenda atuar como perito judicial deve saber, que comumente os honorários são menores que as perícias privadas e o recebimentoburocrático (mediante guias de levantamento).

Em relação aos peritos policiais, a remuneração inicial de um perito da Polícia Federal é R$ 23.692,74 (https://www.estrategiaconcursos.com.br/blog/concurso-policia-federal/) e do Instituto de Criminalística do Estado de São Paulo é R$ 8.699,94 (http://www.recursoshumanos.sp.gov.br/retribuicao.asp?pagina=policial4), ambos mensais.

Em média, a remuneração por hora de um perito em informática está em torno de 480,00 (quatrocentos e oitenta reais). Essa hora pode aumentar ou diminuir de acordo coma a especialidade do perito, volume de dados a coletar e analisar, a exemplo, perícias em dispositivos móveis, bancos de dados, redes, cloud computing costumam ter honorários mais elevados. Além disso a quantificação de horas deve levar em consideração quantidade e

diferenças de dispositivos, equipe necessária para o trabalho e demais considerações, valor da causa, etc.Também é possível estimar o trabalho por empreitada.

Aos pretendentes da área, a profissão é rentável, mas exige muito de nós. Podemos ter muitasperícias positivas, mas basta um deslize ou uma evidência clara que não encontramos para que todo o histórico seja destruído. Avisamos que qualquer conduta impensada, como um simples comando para listar o diretório de um sistema operacional, pode significar a perda de dados importantes para o draft final e, consequentemente, milhões para as empresas envolvidas. Por isso, simulações de coleta de dados são sempre estimuladas e bem-vindas, pois, em campo, o profissional estará mais preparado.

PERSPECTIVAS NO MERCADO

No que diz respeito à perspectiva de crescimento da área, o mercado vem crescendo assim como cresceu no mundo. Sobre o tema, fiz o seguinte vídeo: https://www.youtube.com/watch?v=Ik5JyWVOzKM&t=248s.

No mundo, é um mercado que movimentará mais de 9 bilhões de dólares até 2022. E, até 2026, o mercado forense digital está projetado para atingir 11,45 bilhões de dólares. Os principais fatores que impulsionam o mercado forense digital global são: a crescente demanda pela implementação da Internet das coisas, visto que, de acordo com o Relatório de Mobilidade da Ericsson e a Previsão da Internet das Coisas, haverá 18 bilhões de dispositivos conectados até 2022, bem como o aumento de crimes cibernéticos, ataques cibernéticos e outras práticas ilícitas (MARKETSANDMARTEKTS).

As tendências do mercado forense digital, por componente são:

- Hardware
- Sistemas Forenses
- Dispositivos Forenses
- Bloqueadores de escrita forenses

- Outros (inclui cabos, adaptadores, compartimentos de disco rígido, baterias e dispositivos de armazenamento)
- Programas
- Serviços
- Serviços profissionais
- Investigação e consultoria digital
- Resposta ao Incidente
- Integração do Sistema
- Treino e educação
- Suporte e Manutenção
- Serviços gerenciados

No Brasil, o Marco Civil da Internet (Lei nº 12.965/2014) e as Leis que estabeleçam condutas criminosas na Internet tendem a fomentar o perito digital corporativo, apto a atuar em sintonia com o Sistema de Gerenciamento de Segurança da Informação da empresa, avaliando casos e propondo melhorias. Além disso, a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) traz uma série de oportunidade para peritos digitais que se especializem em incidentes e controvérsias evolvendo dados pessoais.

O perito policial e judicial, o primeiro, atuando em investigações e inquéritos que se relacionem com Internet e tecnologia, e o segundo, auxiliando juízes no entendimento técnico de discussões judiciais cíveis, criminais e trabalhistas, possuirão cada vez mais trabalho. O Perito digital será função indispensável à justiça, tal como o advogado, pois através dele inocentes não serão condenados e culpados não serão absolvidos por ausência de provas, que na sua maioria das vezes são digitais.

A perícia digital vem amadurecendo no Brasil, mas ainda muito precisa ser feito para que autoridades de aplicação de leis se aproximem do cibercrime. O Estado precisa preocupar-se mais em capacitar seus profissionais do que comprar ferramentas.

Os casos enfrentados por um perito digital são variados, podendo ser uma mera constatação de contrafação de código fonte ou violação de software, ou a análise de escuta clandestina do tráfego de telefonia celular ou internet wireless, passando por análise de memórias de dispositivos, arquivos de paginação e recuperação de dados apagados ou sobrescritos.

Como a maior parte dos incidentes de segurança decorre de vulnerabilidades, cada vez mais é necessário um profissional de computação forense com profunda bagagem em resposta a incidentes, a fim de auditar logs, profiles e compreender o passado, em busca do entendimento sobre o que, como e quem foi o responsável pelo o ocorrido.

COMO COMEÇAR A TRABALHAR COM PERÍCIA DIGITAL E SE HABILITAR?

Primeiro passo é buscar conhecimento, formação profissional. A profissão deve crescer muito nos próximos anos e a concorrência já é bem maior que há 10 anos atrás.

Importante dizer que perícia em informática não é perícia em engenharia, portanto, não está sujeita a conselhos ou associações de engenharia, sobretudo no que tange à estimativa de honorários. Embora alguns peritos usem tabelas da engenharia para estimar honorários, os salários hoje podem ir de 8 a 35 mil reais por mês, de acordo com a complexidade do trabalho, experiência e tarefas do analista, além de outros fatores.

Os passos básicos para iniciar são:

1) Defina seu foco de atuação e busque cursos de extensão e especialização, se possível uma certificação;

2) Faça seu curriculum técnico e crie igualmente um perfil no Linkedin, buscando contato com empresas e consultorias de perícia;

3) Apresente-se para empresas e escritórios jurídicospara atuar como assistente técnico;

4) Converse com peritos experientes e conheça as normas processuais, de habilitação em tribunais e, principalmente, os principais documentos que um perito faz, como manifestações, resposta a quesitos e laudos.

Em meus treinamentos, também, trago importantes modelos para peritos e profissionais de TI que atuam com crimes virtuais e cibernéticos.

5) Pratique. Associe-se a entidades e associações da área, ou seja, um correspondente de perícia ou acompanhe diligências e perícias digitais, mesmo sem honorários periciais. O que vale é a experiência para conhecer a prática do dia a dia.

6) Software. Monte uma estação forense para análises, com suas ferramentas, lembrando que hoje temos ótimos softwares gratuitos para análises, como KALI LINUX, PTK, *volatility*, *disk digger*, AUTOPSY, dentre outros. Aqui temos 22 ferramentas essenciais para o perito em informática: https://resources.infosecinstitute.com/topic/computer-forensics-tools/#gref.

CRITÉRIOS PARA CONTRATAR

O fator humano é fundamental para o sucesso de uma empresa perícia digital e computação forense, visto que se trata da prestação de serviço extremamente especializado. Os profissionais contratados devem ter formação tecnológica, jurídica e vivência nas áreas pública e privada. Algumas faculdades oferecem cursos de pós-graduação em perícia digital.

O perito digital precisa conhecer a legislação brasileira e o direito internacional já que tudo que está ligado à internet é de escopo global. Com o crescimento do uso de recursos multimídia, o domínio sobre tecnologias de imagem e voz também

é requerido, além de habilidades específicas como a capacidade de análise e síntese de soluções e integridade profissional.

Compreender outras línguas, principalmente o inglês, é outro requisito básico, visto que o perito pode lidar com questões internacionais. Também precisará buscar informações disponíveis em outros idiomas e cooperar com profissionais estrangeiros ou operar tools.

Além da formação acadêmica básica, o profissional poderá (não deverá) obter algumas certificações válidas no mercado mundial de software. As principais são:

– EnCE (EnCaseCertifiedExaminer), do fabricante Guidance;

– ACE (AccessData Certified Examiner), do fabricanteAccessDat;

– CCFT (Certified Computer Forensic Technical);

– GIAC (Global Information Assurance Certification), da SANS;

– CEH (Certified Ethical Hacker);

– CHFI (Certified Hacker Forensic Investigator);

– ACFEI (American College of Forensic Examiners Institute).

– iSC2.

A qualificação de profissionais aumenta o comprometimento com a empresa, eleva o nível de retenção de funcionários e melhora a performance do negócio. O treinamento dos colaboradores deve desenvolver as seguintes competências:

– Capacidade de percepção para entender e atender as expectativas dos clientes;

– Agilidade e presteza no atendimento;

– Motivação para crescer juntamente com o negócio.

Portanto, é evidente que a perícia irá crescer muito e o

profissional que se tornar um perito digital terá um campo de trabalho imenso, desafiador e bem lucrativo, desde que, se prepare a altura.

DESAFIOS FUTUROS

Dados encriptados, *cloud forensics*, Internet das Coisas e o alto volume de dados são indicados como os principais desafios. O alto volume de dados é uma frustração que o perito terá que aprender trabalhar. Costumo dizer que perícia profunda e tempo são intimamente ligados e a qualidade do trabalho cresce na mesma proporção do tempo existente. Infelizmente, grande parte dos trabalhos serão feitos e um curto período de tempo e nem todas as análises possíveis poderão ser realizadas, quer por falta de tempo, quer por falta de orçamento, razão pela qual o perito deverá escolher as análises mais significativas ou que mais contribuem para o caso.

Durante o ano de 2020, vivenciamos uma pandemia causada pelo Covid-19, o que potencializou as relações no ambiente digital. Diversos golpes e fraudes foram aplicados, aparelhos invadidos. Além disso, muitas empresas precisaram fazer o home office, o que fez com que a vulnerabilidade de muitos aumentassem. Assim, a perícia digital estará em alta, considerando a inovação forçada de muitos setores, sem os cuidados básicos com segurança, o que dará margem a atuação de fraudadores e criminosos.

A computação forense e perícia digital é muito dinâmica e a cada ano surgem novos desafios e tecnologias, sendo que os peritos devem se enquadrar nesta dinâmica de atualização constante. Internet das coisas, Drones, GPS, ataques de *ransonware*, Big Data, Inteligência Artificial e Deep Web já são realidades. A criptografia e as novas transações na Blockchain são desafios. Pontos que valem um maior estudo pois profissionais com “respostas” nestas áreas serão extremamente procurados.

O perito que tiver soluções para estes problemas certamente terá muito sucesso em sua atividade. Vale ficar atento em novas tecnologias utilizadas em massa, e quais evidências podem ser coletadas diante de fraudes, golpes e crimes na internet cometidos nestes ambientes.

REFERÊNCIAS

INDICAÇÃO DE LIVROS

Muitos livros foram lançados sobre computação forense. Vou indicar os que eu li e gostei, basilares, e que podem lhe dar o alicerce para outros livros mais específicos:

– Perícia Forense Computacional. Teoria e Prática Aplicada (Dan Farmer)

https://www.amazon.com.br/Per%C3%ADcia-Forense-Computacional-Pr%C3%A1tica-Aplicada/dp/8576051281

– Introdução à Análise Forense em Redes de Computadores (Ricardo Kleber)

https://www.novatec.com.br/livros/analise-forense/

– File system Forensic Analysis (Brian Carrier)

https://www.goodreads.com/book/show/692554.File_System_Forensic_Analysis

– A Forensic Focus (que aliás é item indispensável de leitura do perito em informática) tem uma lista bem interessante de livros na área: http://www.forensicfocus.com/computer-forensics-books-us

– Perícia digital: da investigação à análise forense (Evandro Della Vechia). É um livro fundamental que indico, de um grande perito digital, e tenho prazer de ter escrito meu depoimento no livro.

https://www.editorajuspodivm.com.br/pericia-digital-da-investi

gacao-a-analise-forense-2019?utm_camp=gshop&idgrade=163024&gclid=Cj0KCQiAjKqABhDLARIsABbJrGm3DHs7p1tt1G91ZyCwlYEsvvmcgk_0hReCORYoTTKYtMvyl4JWRMMaAg5cEALw_wcB

AINDA TEM DÚVIDAS? FALE COMIGO

Minha missão é ajudar ao máximo pessoas que pretendam atuar na área de computação forense, resumindo informações que levei anos para descobrir. Espero que este conteúdo possa agregar a muitos profissionais e estudantes que pretendam e sonham em trabalhar com perícia digital ou em informática. Atualizarei esta página continuamente e peço que reverbere este conteúdo compartilhando aos que tem interesse. Bom trabalho a todos e fico à disposição para dúvidas pelo e-mail consultor@josemilagre.com.br. No meu canal no Youtube também publico vídeos semanais sobre computação forense (www.youtube.com/josemilagre).

CYBEREXPERTS

A CyberExperts é consultoria especializada em computação forense, inteligência cibernética, perícia e auditorias em informática. Atuamos para empresas e órgãos públicos na coleta, preservação e análise de evidências digitais, por meio de um rol de peritos com notória experiência profissional. Fale conosco (11) 3254-7616 ou acesso www.cyberexperts.com.br

José Antônio Milagre, perito e assistente técnico em informática, especialista em computação forense, analista de sistemas, técnico em processamento de dados, Pós Graduado em Gestão de Tecnologia da Informação, Mestre e Doutorando em Ciência da Informação pela UNESP. Contato: consultor@josemilagre.com.br e (11) 3513-7844. Instagram @drjosemilagre

Colaboração

Laura Secfém Rodrigues.Pós-graduanda em Direito, Tecnologia e

Inovação com ênfase em proteção de dados, no Instituto New Law. Graduada em Direito pelo Centro Universitário de Bauru/SP, mantido pela Instituição Toledo de Ensino (ITE).

A perícia forense digital na fraude telefônica do “bypass”

É sabido que as operadoras de telefonia legitimamente faturam com ligações móvel-móvel, fixo-móvel e fixo-fixo, cada qual com sua tarifa. Do mesmo modo, uma ligação local não é tarifada da mesma forma que uma ligação interurbana ou internacional.

Quando você utiliza seu celular em São Paulo e liga para um celular de Natal, pagará logicamente a tarifa específica para esta ligação interurbana. A cobrança é feita com base na sua localização, ou seja, uma ERB específica de São Paulo capta seu sinal, sendo identificada também a ERB de destino, no Rio Grande do Norte.

Agora imagine que você pudesse “enganar” todo este sistema de localização e tarifas, confundindo a rede da empresa de telefonia, fazendo com que uma ligação de São Paulo/Natal fosse cobrada como sendo Natal/Natal? Imagine que uma ligação interurbana fosse considerada pela rede como uma ligação local? Agora imagine o mesmo exemplo no cenário internacional. Uma ligação Seattle/São Paulo sendo tarifada como São Paulo/São Paulo?

Exemplo mais didático não poderia ilustrar como funciona a dinâmica da fraude Bypass. Por meio dela, criminosos redirecionam tráfego de origem e destino de chamas, fazendo a rede “enxergar” um cenário que não existe.

A fraude se dá por diversas formas e variantes, mas a mais frequente consiste na aquisição de chips, normalmente com planos corporativos, que são instalados em equipamentos com SIM BOX ou GSM BOX, posteriormente uma configuração é feita nos aparelhos do cliente do fraudador. A partir daí sempre que o cliente utiliza o equipamento para ligações interurbanas ou internacionais o sistema aciona a BOX que escolhe a rede até o ponto local mais próximo do destinatário da chamada, originando então a chamada de um número local.

Normalmente este tráfego utiliza a rede IP (Voip+GSM Gateways) que não é enxergado pela rede. O tráfego só aparece quando volta ao serviço telefônico em um ponto próximo ao destinatário. Algumas modalidades de bypass inclusive são direcionadas a “planos” das operadoras da telefonia móvel, ou seja, são configurados de acordo com as promoções lançadas pelas teles.

Fraudadores montam estas redes e revendem minutos a pequenos e grandes negócios, empresas e comércios, que às vezes sequer sabem que estão utilizando um serviço ilegal. E o pior, muitas empresas são laranjas na compra de chips que são instalados nas boxes e alimentam o mercado do bypass. São milhões e milhões em perdas financeiras com uma operação que é ilegal, inclusive vedada pela Anatel.

As operadores contam com mecanismos antifraude para a detecção remota destes números e redes clandestinas. Mas a melhor forma de perícia é no cliente das operadoras. A comunidade especializada em auditorias e antifraudes já traz alguns critérios como importantes a serem avaliados em perícias desta natureza como:

1. a) Ausência de mobilidade da origem: Não é comum que um telefone celular permaneça sempre ligado na mesma ERB;
2. b) Mobilidade extrema da origem: Aquele celular que de manhã fez ligações de Natal, a tarde originou chamadas do Rio Grande do Sul, e a noite fez chamadas de São

Paulo é muito suspeito;

3. c) Volume de chamadas: Um volume humanamente impossível de chamadas ou mesmo minutagem exagerada é um indício;
4. d) Relação Incoming/Outgoing: Um indício de fraude é quando a relação chamada recebidas e originadas são desproporcionais, com muitas chamadas feitas e um número mínio de chamadas realizadas.
5. e) Análise de IMEI e TAC: As operadoras registram os IMEIs dos aparelhos que originam as chamadas, podendo a perícia forense extrair o *type allocation code (TAC)* e assim identificar que o chip está instalado não em um celular convencional, mas em uma BOX.

Atuamos na fase preventiva, com profissionais especializados para assessorar o anti-fraude na detecção e preservação de provas que apontem anomalias no uso. Detectada a fraude, atuamos como assistentes técnicos em processos judiciais para reparação dos danos em decorrência das operações clandestinas. Do mesmo modo, podemos atuar na produção da prova técnica simplificada, esclarecendo os sujeitos processuais sobre a dinâmica da fraude, em cada caso concreto, incluindo sustentações orais.

Já para empresas que tiveram contas bloqueadas, podemos auditar o sistema e verificar se existem indícios de uso indevido ou irregular das redes ou não e neste sentido, fornecer elementos para apuração da autoria dos responsáveis.

Importante esclarecer por fim que a prova pericial é indispensável em processos desta natureza, considerando a necessidade da certeza técnica ao Magistrado, para que possa decidir sobre casos de reparações de danos, inclusão de nomes em serviços e de proteção ao crédito e até mesmo sobre cancelamento/bloqueio de serviços telefônicos.

Por Legaltech