Revista Interdisciplinar do Pensamento Científico. ISSN: 2446-6778
Nº 2, volume 5, artigo nº 15, Julho/Dezembro 2019
D.O.I: http://dx.doi.org/10.20951/2446-6778/v5n2a15

PERÍCIA FORENSE COMPUTACIONAL E CRIMES CIBERNÉTICOS

Kamille da Silva Pereira[1]
Graduanda em Sistemas de Informação

Fábio Machado de Oliveira[2]
Doutor em Cognição e Linguagem

Resumo - Tendo em vista que o aumento da utilização das tecnologias, e o descuido das pessoas físicas e jurídicas em relação aos riscos frequentes, torna-se necessária uma ampla divulgação sobre bom uso das tecnologias e a necessidade em mostrar a origem das instruções que possa ajudar as pessoas a se proteger de crimes. Com isso, tornou-se necessário realizar uma pesquisa sobre a Perícia Forense Computacional e Crimes Cibernéticos, a fim de criar uma aplicação para que as pessoas tenham acesso a informações sobre crimes digitais e também sobre a Perícia Forense Computacional. Para tanto, é necessário entender o contexto da Perícia Forense Computacional, para que possa mapear os riscos da má utilização das tecnologias e disponibilizar orientações sobre os crimes. Realiza-se então uma pesquisa de revisão bibliográfica, sendo de natureza quali-quantitativa. Diante disso, verifica-se que o crime cibernético vem aumentando constantemente, e mesmo diante de todo esse crescimento, as pessoas não temem aos riscos, expondo também pessoas de seu convívio familiar.

Palavras-chave: Perícia forense; crimes digitais; conhecimento; má utilização; tecnologia.

Abstract - Considering that the increased use of technologies, and the carelessness of individuals and corporations in relation to the frequent risks, a broad dissemination on good use of technologies and the need to show the source of the statements that can help people protect themselves from crimes. With this, it became necessary to perform research on Computer Forensics and Cyber Crimes, in order to create an application for people to have access to information about crimes and also about Computer Forensics. To this end, it is necessary to understand the context of Computational Forensics so that you can map the risks of misuse of technologies and provide guidance on the crimes. Performs a search of literature review and quality quantitative nature. Given this, it turns out that the Cybercrime is increasing constantly, and even in the face of all this growth, people are not afraid to risk, exposing your family living people, too.

Keywords: forensic expertise; digital crimes; knowledge; bad utilization; technology.

1. CONSIDERAÇÕES INICIAIS

A globalização, também conhecida como revolução tecnológica, modificou a forma como o ser humano relaciona-se com o mundo e consigo mesmo. As tecnologias fazem parte do dia a dia do homem contemporâneo. Os avanços tecnológicos viabilizam o acesso à comunicação e aos variados tipos de produtos e serviços.

Os Autores Wendt e Jorge (2013), Definem em que pesem inúmeros benefícios, esses mesmos recursos – hoje indispensáveis – apresentam diversos riscos, pois muitos deles podem proporcionar transtornos ou prejuízos para as vítimas. Nestas situações e existindo previsão penal, surgem os denominados crimes cibernéticos, que se caracterizam pela prática de delitos no ou por intermédio do ambiente cibernético, ou seja, da internet. Pode-se afirmar, mesmo que por uma análise empírica, que a ocorrência desses crimes apresenta um crescimento acentuado, seja pelo aumento do número de usuários, pelas vulnerabilidades existentes na rede ou pela falta de atenção do usuário.

Devido a esse crescimento e desconhecimento das pessoas, o índice de crimes virtuais se expandiu. A melhor maneira de propiciar aos usuários de *internet* uma navegação segura é conscientizá-los acerca desses tipos de transgressões, e apresentá-los conhecimentos científicos e tecnológicos empregados para apurar esse tipo de crime. Dentre estes, para a realização do trabalho, optou-se pela aplicação da Perícia Forense Computacional.

A sociedade possui um baixo conhecimento sobre os crimes digitais circulados pelo mundo, muitas delas acreditam que um crime digital é apenas um compartilhamento de fotos íntimas na internet, se baseando no que acontece com alguns famosos. Muitos não acreditam que podem sofrer um roubo na internet ou uma fraude, achando que estão imunes a elas. A partir destas considerações, visa-se responder a seguinte pergunta: Como podemos propiciar as pessoas, conhecimento e instruções sobre crimes digitais?

A criação de um aplicativo e uma aplicação web para maior divulgação de informações sobre crimes virtuais e Perícia Forense Computacional poderá diminuir a incidência dos mesmos e consequentemente elevar o nível de seguimento e bom uso das tecnologias da informação por parte dos usuários.

Justifica-se que com o aumento da utilização dos dispositivos eletrônicos, computadores e computação em nuvem nos dias atuais, pessoas Físicas e Jurídicas andam se descuidando cada vez com relação aos riscos da má utilização desses recursos. Sendo assim, torna-se cada vez mais necessário que cuidados e conhecimentos sobre estas

questões sejam amplamente divulgados e conhecidos por todos. A Perícia Forense Computacional, área responsável por investigar criminosos virtuais, realiza um importante trabalho para a sociedade que muitas vezes desconhece por completo sua existência e sequer conhece um conjunto de instruções e dicas, informadas pela mesma para orientação na defesa contra estes tipos de crimes digitais. Com isso torna-se necessário criar meios para ajudar na divulgação das informações de crimes digitais e também para orientar sobre como se prevenir e defender de crimes e mapear se elas estão sendo vítimas de crimes digitais ou não.

O objetivo geral desta pesquisa é criar um aplicativo e uma aplicação web que permita que as pessoas tenham acesso a importantes informações sobre crimes virtuais e Perícia Forense Computacional.

1. Entender o contexto da Perícia Forense Computacional;
2. Mapear os riscos da má utilização da tecnologia de informação segundo a Perícia Forense Computacional;
3. Criar um Aplicativo Android que faça o mapeamento dos crimes virtuais;
4. Disponibilizar instruções e conteúdos com orientação sobre crimes virtuais através de uma Aplicação Web;
5. Criar um conteúdo de notícias sobre crimes virtuais no App.

A natureza da pesquisa esta classificada em quali-quantitativa onde a pesquisa qualitativa tende a salientar os aspectos dinâmicos, holísticos e individuais da experiência humana, para apreender a totalidade no contexto daqueles que estão vivenciando o fenômeno. A pesquisa quantitativa, que tem suas raízes no pensamento positivista lógico, tende a enfatizar o raciocínio dedutivo, as regras da lógica e os atributos mensuráveis da experiência humana (POLIT et al., 2004, p. 201).

A pesquisa aborda sobre a área da Perícia Forense Computacional, sua importância, e o que ela realiza. Também mostrar o grau de conhecimento sobre a área Forense e os principais crimes digitais.

Para isso, foi realizada uma revisão de literatura, onde aborda sobre a Perícia Forense Computacional e os principais Crimes Cibernéticos.

O referencial teórico deste trabalho foi elaborado em cima de artigos científicos encontrados em bases de buscas como Google Acadêmico, Monografias e livros de autores como Pedro Monteiro da Silva Eleutério, Marcio Pereira Machado, Wilson Leite da Silva

Filho, que abordam sobre a Perícia Forense Computacional e também sobre os Crimes Cibernéticos. Além de ser utilizados alguns sites oficiais de empresas como: CERT.br, MICROSOFT, ÉPOCA NEGÓCIOS.

2. PERÍCIA FORENSE COMPUTACIONAL

A perícia forense computacional é uma área responsável pela investigação de crimes digitais, investigação de seus fatos e coleta dos dados para usar como evidência. Os peritos utilizam vários procedimentos para encontrar o autor do crime, seguindo as regras da investigação, para que a evidência não seja comprometida ou perdida.

Sérgio Marcos Roque conceitua crime de informática como sendo “toda conduta, definida em lei como crime, em que o computador tiver sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material”. (ROQUE, 2007, p. 29).

Define-se Perícia Forense Computacional ou Análise Digital Forense como a modalidade de perícia criada para combater os crimes digitais, utilizando análises e métodos na busca de identificar e coletar evidências comprovadas e eficientes.

Para a perícia criminal da polícia, a computação forense envolve o trabalho investigativo e todo o trabalho pericial, para desvendar os crimes cometidos através do uso do computador. Ela pode ser empregada tanto para fins legais como exemplo investigar espionagem industrial, como também para ações disciplinares internas, por exemplo, uso indevido de recursos de uma empresa. (ELEUTÉRIO; MACHADO, 2011).

2.2. PROCEDIMENTOS DA PERÍCIA FORENSE COMPUTACIONAL

O trabalho da perícia forense computacional, segundo Souza (2017), para obter êxito, deve seguir algumas fases específicas, que são:

Coleta: fase em que o perito realiza busca, coleta e catalogação de dados que podem ser considerados ativos e inativos, ou seja, explícitos e ocultos, devendo os mesmos serem preservados. O perito deve fazer a coleta de acordo com a ordem de volatilidade, considerando primeiramente dados mais efêmeros e depois os equipamentos que devem ser embalados, etiquetados e suas identificações registradas para a realização do exame. Qualquer erro nessa fase prejudicara todo o andamento da investigação, pois qualquer falha na coleta dos dados ira comprometer na decisão da justiça; (SOUZA, 2017).

Exame: fase para procurar os dados, fotos, vídeos e informações escondidas nas evidências coletadas, selecionando e utilizando ferramentas e também técnicas para extração de informações importantes para o caso sempre mantendo a integridade das mesmas; (SOUZA, 2017)

Análise: fase que realiza exames sobre evidências importantes e relevantes para a investigação;

Relatório: fase final que realiza um relatório onde devem ser escritos os procedimentos usados na investigação, quais os dados que foram recuperados durante a mesma contendo relevância para o caso. O relatório deve ser produzido com escrita adequada que garanta a compreensão e o entendimento por parte de todos.

Uma perícia em um computador suspeito envolve uma série de conhecimentos técnicos e a utilização de ferramentas adequadas para a análise, que é justificado pela necessidade indiscutível de não alterar o sistema que está sendo analisado. (SANTOS, 2008, p. 5).

As técnicas de investigação escolhidas pelo perito, durante uma investigação, dependem do tipo de crime que foi cometido. Por exemplo, se o crime for de acesso não autorizado o perito poderá buscar evidências de conexão, de arquivos confidenciais que foram alterados ou roubados, de logs. Se o crime for de pornografia o perito deve identificar, vídeos, fotos, mensagens e muitas dessas analisem são feitas na hora, conhecida como análise ao vivo, que consiste na investigação do equipamento ainda em funcionamento que permite a identificação dos processos em execução, portas abertas no sistema e pela rede. Na análise ao vivo a preservação da evidencia é o principal foco para não alterar logicamente os dados coletados e garantir que não sejam perdidos. Para que isso não aconteça utiliza-se a cadeia de custódia, explicada a seguir, que é uma das principais obrigações que o perito deve cumprir.

Cadeia de custódia: A cadeia de custódia é um registro detalhado das evidências que foram coletadas. Este processo de registro deve conter: a identificação de todas as evidências coletadas; as informações de quais pessoas tiveram acesso às elas (no momento do flagrante); onde elas estavam (fisicamente) no momento da coleta; registro de trânsito das evidências entre os peritos e mídias. Estes cuidados preservam as responsabilidades conhecidas institucionalmente e garantem a qualidade nas fases dos processos de investigação. Assim poderão ser evitados questionamentos no tribunal sobre a legitimidade das informações coletadas na investigação.

Cadeia de custódia é procedimento preponderante e de suma importância para a garantia e transparência na apuração criminal quanto à prova material, sendo relato fiel de todas as ocorrências da evidência, vinculando os fatos e criando um lastro de autenticidade jurídica entre o tipo criminal, autor e vítima. (MACHADO, 2009, p. 18-23).

Propõe que se entenda por cadeia de custódia "o conjunto de procedimentos que visa garantir a autenticidade dos materiais que serão submetidos a exames, desde a coleta até o final da perícia realizada". (BONACCORSO, 2007, p.26).

Segundo Saferstein (2004), cadeia de custódia é "uma lista de todas as pessoas que estiveram de posse de um item de evidência". Para o autor a cadeia de custódia é um documento que contem toda a identificação da evidencia e também do individuo que custodiaram o item. Isto fica evidenciado na figura 1 que demonstra um formulário de cadeia de custódia.

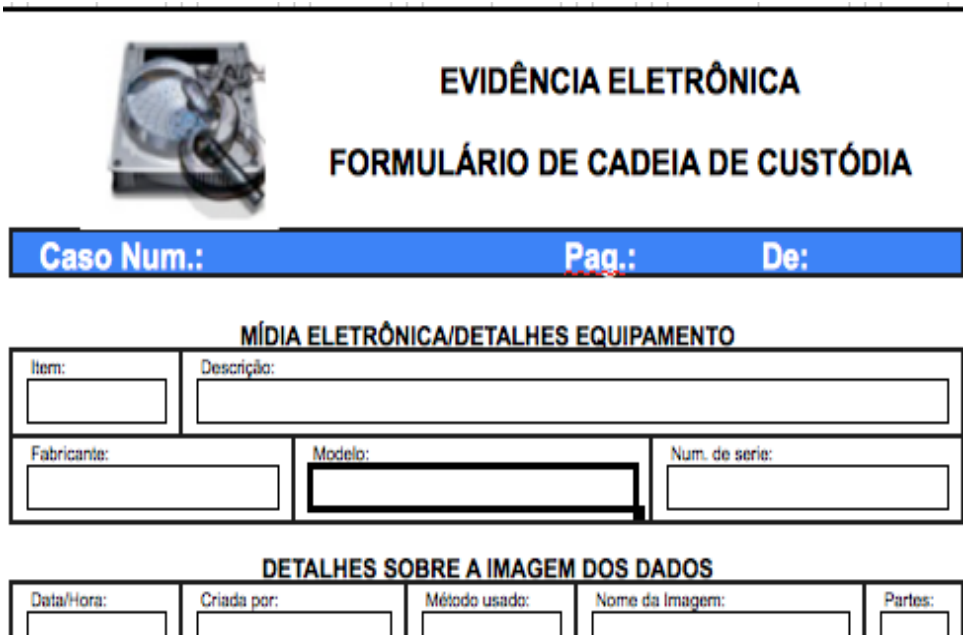


Figura 1: Exemplo de formulário de cadeia de custódia

(Fonte: http://www.fdtk.com.br/files/formulario.xls)

No âmbito da investigação, o Perito deve coletar evidências a serem embaladas e levadas ao laboratório, muitas das vezes, a profissional coleta evidências não necessárias para o desenvolvimento do caso, contudo não deixando de lado qualquer evidência importante, a seguir será abordado oque é uma evidência digital e seus tipos para obter conhecimento das mesmas.

2.3. EVIDÊNCIAS DIGITAIS

No mundo do crime cibernético existem diversos tipos de evidências para se comprovar um determinado delito, e que as mesmas são qualquer tipo de dados armazenados em diferentes dispositivos a fim de ser coletado e devidamente preservado para posterior analise Pericial. Claudemir Rodrigues Dias Filho conceitua evidências como "a evidência é o vestígio que, mediante pormenorizados exames, análises e interpretações pertinentes, se enquadra inequívoca e objetivamente na circunscrição do fato delituoso". (FILHO, 2009). Listamos a seguir alguns tipos de evidências digitais:

Tipos de evidências digitais:

- Documentos;
- Ameaças através de e-mails;
- Softwares maliciosos;
- Pornografia infantil (vídeo/fotos);
- Evidências de conexões de redes estabelecidas entre computadores;
- Mensagens SMS;
- Qualquer dado que possa estar armazenado em dispositivos digitais.

Nas palavras de Mallmith (2007), "as evidências, por decorrerem dos vestígios, são elementos exclusivamente materiais e, por conseguinte, de natureza puramente objetiva".

As evidências são originadas de crimes cibernéticos, praticados por criminosos digitais, a fim de ser utilizada para a solução de um caso, no mundo virtual há uma variedade de crimes que ocorrem diariamente sem o conhecimento dos usuários com isso, a seguir será abordado sobre os crimes cibernéticos e seus tipos para o conhecimento dos mesmos.

3. CRIMES CIBERNÉTICOS

Nos tempos da internet, existem diversos crimes de caráter cibernéticos, isso acontece por que as tecnologias por mais avançadas que sejam elas possuem suas falhas de segurança, permitindo que os criminosos explorem suas vulnerabilidades, por tanto qualquer descuido do usuário pode ser fatal. Mas com o passar dos tempos a pratica dos crimes vem se inovando, os alvos também são variados, mas isso não quer dizer que os crimes tradicionais são deixados de lado, por tanto os usuários ainda tem que ter muito cuidado. Um crime cibernético é qualquer crime envolvendo um computador, sistema, rede de computadores ou qualquer meio eletrônico com acesso não autorizado causando danos a pessoas físicas ou jurídicas. Segundo Gimenes (2013) os crimes cibernéticos são:

Classificação de Crimes Cibernéticos

Crime cibernético puro: É qualquer conduta envolvendo a parte de hardware ou software de um computador, sendo assim toda conduta praticada contra os componentes do computador e seus dados.

Crime cibernético misto: É a conduta que utiliza a internet para realizar o crime, o foco não é computador da vitima, mas todo bem jurídico.

Crime cibernético comum: É a conduta que utiliza a internet como ferramenta para cometer os delitos, o principal deles é a pornografia infantil onde se utiliza varias plataformas desde as salas de bate-papo aos e-mails.

Crime cibernético próprio: É a conduta onde ocorre violação do sistema, contudo é o crime onde ocorre roubo de dados, alteração e exclusão das mesmas.

Crime cibernético impróprio: É a conduta que utiliza o computador para cometer o delito ao bem jurídico como forma de injuria, difamação ou fraude.

Com o crescente numero de usuários no mercado de tecnologia no Brasil, acabou resultando também um aumento de registros de crimes cibernéticos, que por sua vez não é diferente de um crime tradicional, obtendo o mesmo impacto nas vitimas. Uma pesquisa realizada pela empresa de cibersegurança Symantec (2018), através de um questionário online, incluindo projeção e coleta de dados de outras fontes, resultou em que 62,2 milhões de pessoas sofreram crimes cibernéticos no Brasil no ano de 2017. Apesar do numero de vitimas estar crescendo constantemente, os usuários ainda cometem alguns erros em relação ao uso de suas tecnologias.

A imagem a seguir apresenta uma estatística dos principais tipos de ataques ocorridos no Brasil no ano de 2017, pesquisa realizada pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br).

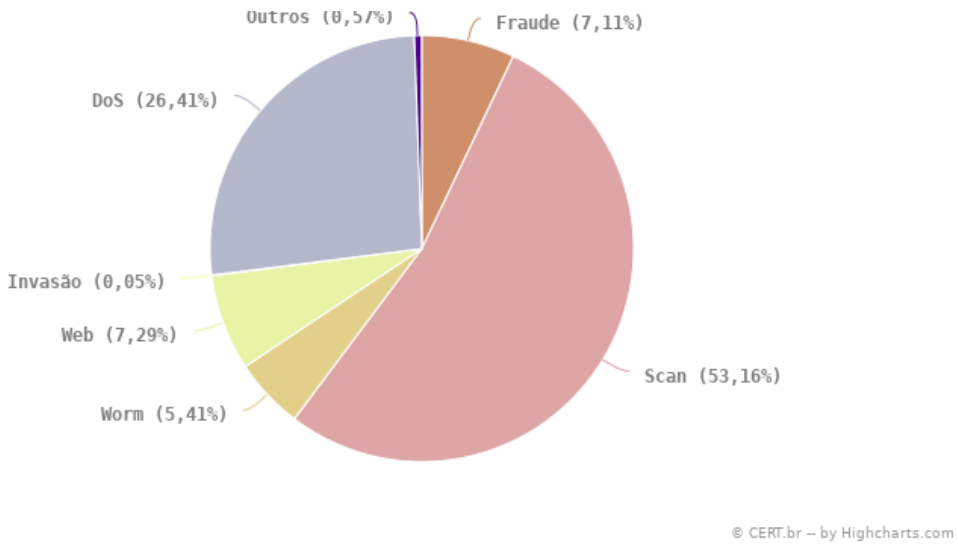


Gráfico 1: Gráfico de incidentes reportados ao CERT.br

Fonte: (CERT.br, 2017).

Paralelo a isso é importante destacar que os crimes que ganharam destaque foram o Scan com 53,16% que tem como finalidade coletar informações dos usuários, a fim de realizar um ataque e Dos com 26,41% cujo foco de operação é tirar um computador de serviço.

De acordo com o próprio CERT (2017), temos o seguinte mapeamento de tipos de ataque:

Scan: É uma técnica que consiste em efetuar buscas minuciosas em redes, com o objetivo de identificar computadores ativos e coletar informações sobre eles como, por exemplo, serviços disponibilizados e programas instalados. Com base nas informações coletadas é possível associar possíveis vulnerabilidades aos serviços disponibilizados e aos programas instalados nos computadores ativos detectados.

DoS(DoS – *Denial of Service*): É uma técnica pela qual um atacante utiliza um computador para tirar de operação um serviço, um computador ou uma rede conectada á internet.

Quando utilizada de forma coordenada e distribuída, ou seja, quando um conjunto de computadores é utilizado no ataque, recebe o nome de navegação de serviço distribuído, ou DDoS (*Distributed Denial of Service*).

Web: Um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet.

Fraude: É aquela na qual um golpista procura induzir uma pessoa a fornecer informações confidenciais ou a realizar um pagamento adiantado, com a promessa de futuramente receber algum tipo de beneficio.

Worm: notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede.

Invasão: um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede.

Outros: notificações de incidentes que não se enquadram nas categorias anteriores.

Um levantamento realizado pela Associação Brasileira de Comércio Eletrônico (2017), o crime de fraude vem aumentando constantemente, e de acordo com o levantamento, uma onda criminosa ocorre a cada cinco segundos no Brasil, sendo um grande problema para os comerciantes no país. Um dos crimes que mais ocorrem são de paginas falsas, onde os criminosos criam essas armadilhas para levar os usuários a sites maliciosos, e induzindo os mesmos a compartilhar os conteúdos com os amigos, obtendo assim seus dados pessoais, sites de empregos são os mais comuns na internet, onde os usuários perante a necessidade e a grande taxa de desemprego no país acabam acessando a página e se tornando vitima, os criminosos usam nomes de empresas famosas para enganar facilmente, realizando processos seletivos, e também usam bancos e redes sociais.

Conforme mostra no gráfico a seguir, o CERT.br teve um percentual muito alto de notificações de tentativas de fraudes no ano de 2017, a situação se agravou com o aumento do crime de páginas falsas perfazendo 85,32%.

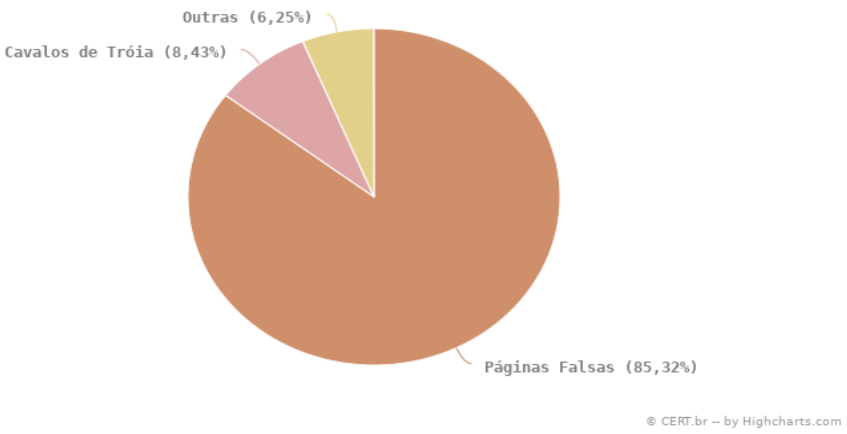


Gráfico 2: Gráfico de tentativas de fraudes reportados ao CERT.br

Fonte: (CERT.br, 2017).

De acordo com o próprio CERT (2017), temos o seguinte mapeamento de tipos de tentativas de fraudes:

Páginas Falsas: Tentativas de fraude com objetivos financeiros envolvendo o uso de páginas falsas.

Cavalos de Tróia: É um programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário.

Outras: Outras tentativas de fraude.

Neste sentido pode-se observar que os dados estatísticos oferecidos pelo CERT.br, que é um grupo de respostas a incidentes de segurança para a internet Brasileira vinculado ao comitê Gestor da internet no Brasil que possui responsabilidade de receber e responder aos incidentes de segurança envolvendo as redes de internet do Brasil, agregando informações e registrando para tomar providências.

Um estudo feito pela *Telecommunications Research Group*, para a *Microsoft Corporation (2018),* analisando os riscos online mostra que o Brasil ficou na 13º posição no que diz respeito à exposição aos crimes das mesmas, com um índice de cidadania de 71%, e sendo o segundo país com jovens e adultos de entre 18 e 34 anos com 81% de exposição aos crimes, sendo os primeiros a crescer no mundo digital, não temendo os riscos oferecidos na internet. Os crimes mais ocorridos no Brasil, de acordo com o resultado da pesquisa, baseado em 23 tipos de riscos online são:

1. Contatos indesejados (51%)
2. Solicitações sexuais (23%)
3. Fraudes (21%)
4. Recebimento de mensagens sexuais indesejadas (21%)
5. Assédio online (não sexual) (20%)
6. Compartilhamento de dados privados (11%)
7. Dano à reputação pessoal (10%)
8. Misoginia (5%)

Segundo o levantamento da pesquisa da *Microsoft Corporation* os adultos foram os mais afetados, entretanto o inimigo esta cada vez mais próximo do que você imagina, 30% da média de crimes cibernéticos estão ligados a parentes e amigos da vitima, levando em conta aqueles conhecidos do mundo virtual, e aquele amigo que fez no *facebook,* o perigo esta

geralmente naquelas mensagens instantâneas, com links maliciosos, noticias de fofocas falsas, dentre outros que dão porta de entrada aos criminosos.

Outro fator preocupante não só pela má utilização das tecnologias, mas pelo percentual dos crimes envolvendo parentes e amigos da vitima que vem crescendo constantemente e isso é devido à confiança das informações enviadas dos mesmos. Com isso os dados estatísticos mostram que 30% dos crimes ocorridos, são de familiares, amigos e conhecidos prejudicando as vitimas.

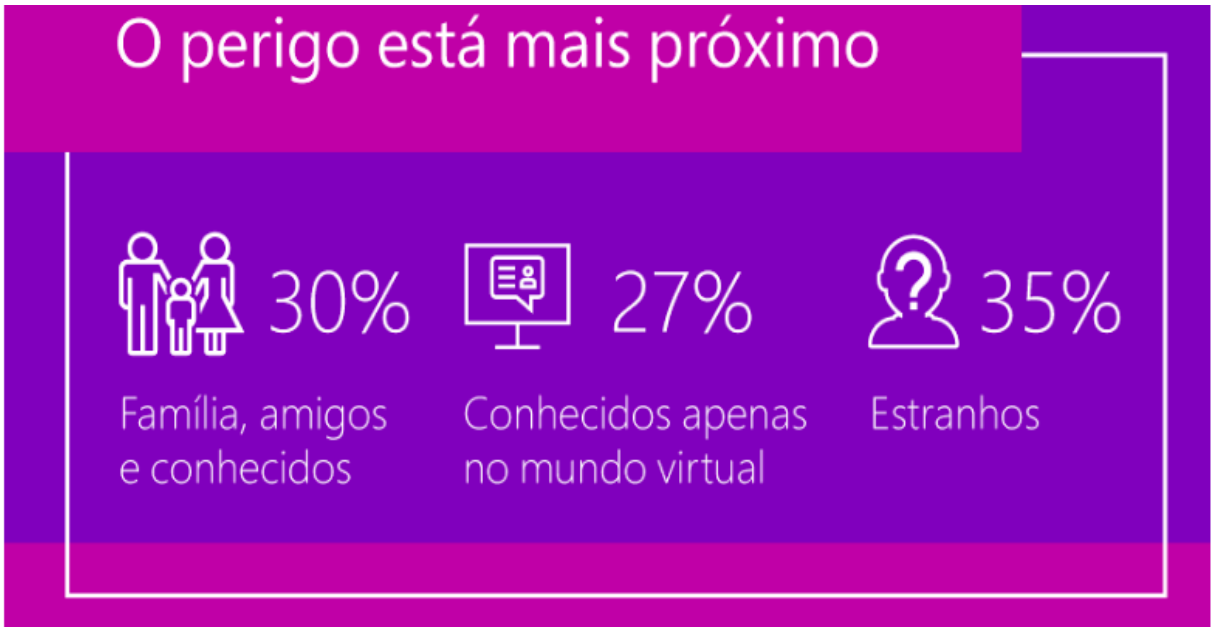


Figura 2: Resultado do índice de cidadania digital no Brasil

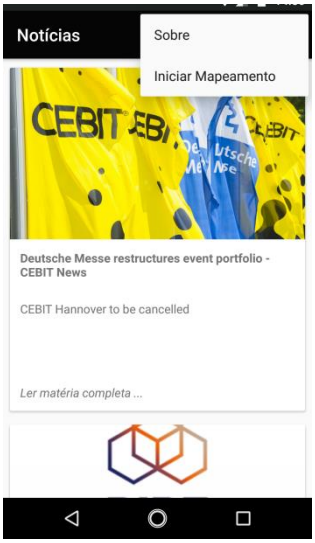
Fonte: Microsoft News Center Brasil (2018)

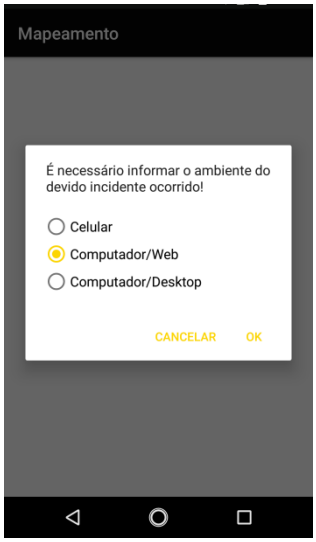
4. DESENVOLVIMENTO

O desenvolvimento é a parte onde se apresenta o embasamento teórico, neste caso, das ferramentas utilizadas para o desenvolvimento do aplicativo, em que foi realizada uma pesquisa de revisão de literatura, com o objetivo de abordar sobre o significado da Perícia Forense Computacional, explicando brevemente o motivo de seu surgimento para tratar tais questões relacionadas a crimes cibernéticos no mundo atual. A fonte da pesquisa foi retirada de artigos científicos, onde os autores definem o conceito da Perícia Forense Computacional, sobre a importância do trabalho dos mesmos no combate aos crimes cibernéticos, mostrando procedimentos importantes para se obter uma investigação de sucesso, e encontrando a fonte verdadeira do responsável pelos crimes, que vem crescendo no mundo todo, sempre renovando suas formas de invasão. Um dos objetivos importantes

dentro da pesquisa é a abordagem dos crimes cibernéticos, com a intenção de mostrar oque é e relacionar os que mais afetam os usuários, apresentando assim dados estatísticos, a fim de ajudar a ter um conhecimento sobre o mesmo para que possa utilizar a tecnologia de forma correta. Com isso, como solução do problema do projeto de estudo, foi criado um aplicativo *android* e uma aplicação *web*, no qual irá divulgar informações importantes sobre os crimes cibernéticos e Perícia Forense Computacional, para que as pessoas possam estar atualizadas sobre as mesmas. Contudo o usuário também poderá realizar um teste de mapeamento para que a mesma possa saber se está sofrendo algum tipo de crime digital.

Na primeira tela do aplicativo o usuário terá acesso ao News de noticias, na segunda tela o usuário irá marcar a opção do tipo de plataforma, em que o mesmo sofreu o possível crime, a fim de reduzir o processo de mapeamento, para que seja mais objetivo. Na terceira tela haverá algumas opções que possa ter acontecido dado aos acontecimentos, o usuário irá marcar as opções que irão identificar os eventos que tenham ocorrido em sua plataforma, portanto ao finalizar este processo a aplicação irá realizar um mapeamento a fim de dar ao usuário o resultado de qual tipo de crime ele sofreu em sua plataforma e o que ele deve fazer, ou qual departamento procurar para resolver seu problema. Veja-se:





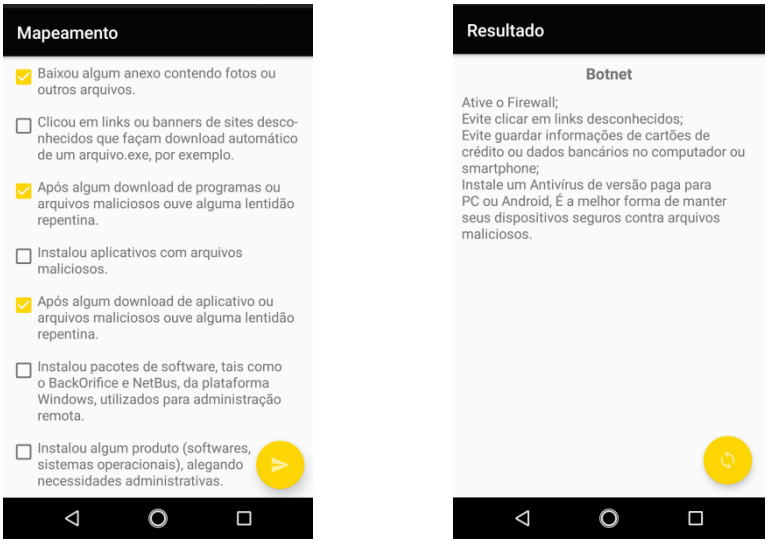


Figura 3: Telas do aplicativo Proteja.se

Na tela principal o usuário terá acesso a informações sobre estudos de crimes digitais para despertar um interesse sobre as informações, a fim de continuar navegando pela aplicação, e também possui informações sobre o aplicativo proteja.se afim de fazer uma propaganda e convencer o usuário a baixar o aplicativo para utilizar o News, quanto o mapeamento. No menu possui 26 opções de pesquisa tanto de ataques quanto de crimes digitais, onde o usuário terá informações sobre o tema, como se prevenir, remover um vírus ou denunciar um crime, para quem não curte uma leitura longa, no final da página possui um vídeo explicando sobre o tema e uma parte de comentário para quem quiser compartilhar alguma experiência ou comentar sobre a aplicação.

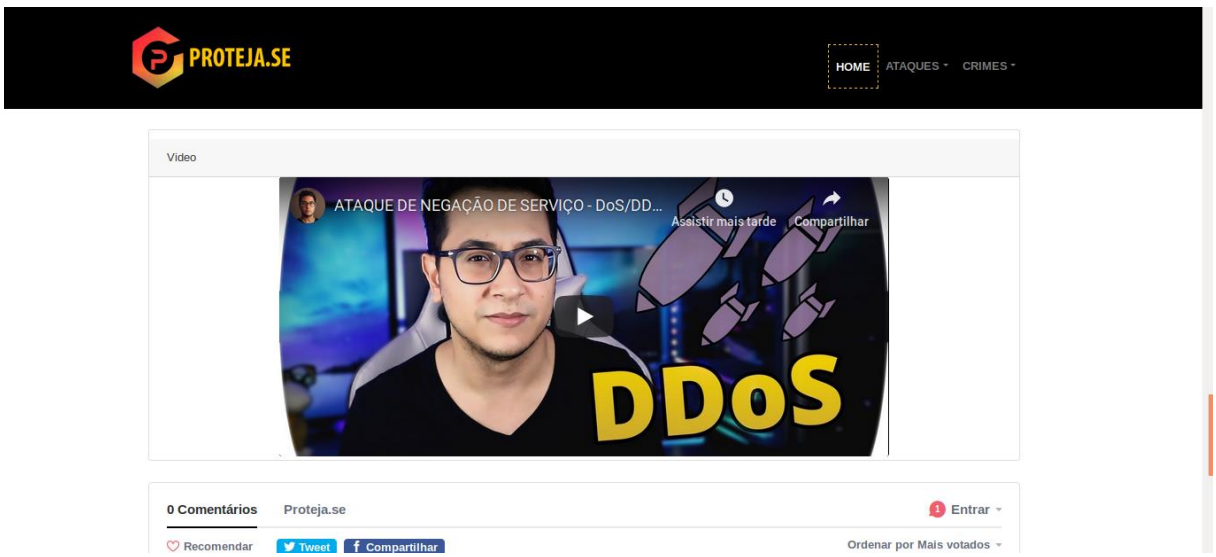


Figura 4: Telas da plataforma proteja.se

Para criar as aplicações, utilizei as seguintes ferramentas:

Linguagem "*Java*": *Java* é uma linguagem de programação criada por Sun Microsystems que permite se comunicar com o computador a fim de realizar manipulação de dados, o *Java* é uma linguagem orientada a objeto isso permite que o desenvolvedor faça modelagem dos objetos no projeto definindo estruturas e operações que dão um importante conceito de herança e polimorfismo que permite o programador selecionar as funcionalidades do sistema para seu funcionamento, contudo também é uma linguagem estaticamente tipada. A vantagem é que o *Java* é uma linguagem simples por ser multiplataforma, o programador consegue ser mais eficiente e produtivo por não precisar se preocupar com a infraestrutura, contudo o programador também pode compilar o projeto em diferentes plataformas, dando um grande desempenho no desenvolvimento da mesma (MENDES, 2009).

Linguagem "*Ruby*": *Ruby* é uma linguagem nova em comparação às outras, uma linguagem limpa e direta, toda orientada a objetos, bem simples de se aprender e trabalhar, multi-plataforma, sendo assim suportada por diversos tipos de sistemas operacionais como Linux, Windows, Solares e outros. Possui muitas *features* interpretantes como o *Ruby Gems* (Biblioteca Gratuita disponível na internet), *Code Blocks*(Bloco de códigos), *Mixins* (Reposta à herança múltipla), tipagem dinâmica e outras características.

**Framework "*Rails*": O *Rails* foi criado pensando na praticidade que ele proporcionaria na hora de escrever os aplicativos para Web. Comparado a outros, ele permite que as funcionalidades de um sistema possam ser implementadas de maneira incremental por conta de alguns padrões e conceitos adotados. Isso tornou o *Rails* uma das escolhas óbvias para projetos e empresas que adotam metodologias ágeis de desenvolvimento e gerenciamento de projeto.

Api "API de Noticias": A API de Noticias é uma API de código aberto, de fácil implementação onde se pode visualizar noticias de qualquer manchete do mundo inteiro, ao vivo, o usuário pode escolher uma ou mais fontes de noticias que deseja receber sobre um determinado tema (NESBITT, 2017).

Banco de dados *"Firebase":* O *Firebase Database Realtime* é um banco de dados fornecido pela *Google,* utilizado para armazenar dados de aplicações *mobile* em tempo real sincronizando os dados. O banco de dados do *Firebase* é uma árvore em formato *JSON,* onde os dados são armazenados em forma de nodos, deixando uma infraestrutura de forma prática, com uma modelagem ágil e simples.

O *Firebase* é uma solução completa de *back-end* para desenvolvimento tanto mobile quanto web. É oferecido como um serviço pela Google, sendo hospedado e mantido em seus *datacenters* (AVRAM, 2016).

Plataforma "*Android*": O *Android Studio* é uma plataforma que originalmente foi construída com base no sistema operacional *Linux*, contendo diversas ferramentas, podendo assim criar aplicações para diferentes dispositivos moveis. As funcionalidades e recursos da plataforma muda ao decorrer das necessidades dos desenvolvedores e usuários.

O *Android* é uma plataforma para tecnologia móvel completa, envolvendo um pacote com programas para celulares, já com um sistema operacional, *middleware*, aplicativos e interface do usuário (PEREIRA; SILVA, 2009, p.3).

5. CONSIDERAÇÕES FINAIS

O desenvolvimento do estudo possibilitou realizar uma pesquisa sobre a importância da Perícia Forense Computacional e seus procedimentos. Além disso, também permitiu que realizasse uma pesquisa sobre os tipos de evidências, e fizesse um estudo sobre os crimes cibernéticos, mostrando dados estatísticos sobre os principais crimes ocorridos ao longo do ano de 2017, e seu nível de impacto na sociedade.

Ao fazer uma pesquisa, verificou-se que numero de crimes relacionados à Dos, Scan e páginas falsas tem aumentado constantemente de acordo com o gráfico 1 e 2 e também um resultado do levantamento do índice de cidadania que registrou a exposição de crimes, levando em conta os usuários mais afetados. Permitindo mostrar que os objetivos propostos foram realmente alcançados.

O estudo conseguiu mostrar que mesmo diante de todos os crimes presente na descrição da pesquisa, os usuários não temem aos riscos oferecidos na internet, resultante do mau uso das tecnologias, mesmo sabendo que os crimes estão presentes no seu dia a dia, os usuários só querem utilizar as novas tecnologias, divulgar informações mesmo sendo falsas propagando assim um aumento dos crimes, pois os mesmos acham que a internet é uma terra sem lei, que podem usar todos os recursos tecnológicos de uma forma incorreta sem se preocupar se isso irá afetar as pessoas ou alguém próximo a elas, e também por não saber que existem leis para crimes virtuais, com isso cabe realizar uma conscientização para que possa diminuir os níveis de incidências, a fim de fazer com que os usuários possa

se cuidar mais em relação à utilização das tecnologias, pois os crimes virtuais são tão prejudiciais às pessoas quanto um crime físico.

REFERÊNCIAS

BONACCORSO, Norma. **Aplicação do exame de DNA na elucidação de crimes e identificação de pessoas**. Encontro Regional de Biomedicina – Mini – Curso. 2007. Disponível em: http://www.ibb.unesp.br. Acesso em:15.08.2010.

CERT.br. **Grupo de Resposta a Incidentes de Segurança para a Internet no Brasil**. Disponível em: <https://www.cert.br/> Acesso em: 19 de junho de 2018.

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

ÉPOCA NEGÓCIOS. **Páginas falsas de emprego enganam mais de 300 mil brasileiros.** Disponível em: <https://epocanegocios.globo.com/Tecnologia/noticia/2018/02/estudo-mostra-que-tentativas-de-fraude-no-e-commerce-brasileiro-acontecem-cada-5-segundos.html> Acesso em: 19 de junho de 2018.

FILHO, CLAUDEMIR. **Cadeia de custódia**: do local de crime ao trânsito em julgado;do vestígio à evidência. 1. ed. [S.l.: s.n.], 2009. 16 p. v. 1.

FILHO, Wilson. **Crimes Cibernéticos e Computação Forense**. 1. ed. Simpósio Brasileiro Em Segurança da Informação e de Sistemas Computacionais: [s.n.], 2016. 38 p. v. 1.

GIMENES, Emanuel Sperandio. **Crimes virtuais**. 1. ed. Juiz Federal Substituto: [s.n.], 2013. 19 p. v. 1.

MACHADO, Margarida Helena Serejo. A Regulamentação da Cadeia de Custódia na Ação Penal: Uma necessidade Premente. Corpo Delito, n.1, p. 18-23, Brasília, 2009.

MENDES, Douglas.**Programação Java com Ênfase em Orientação a Objetos**. 1. ed. [S.l.]: NOVATEC, 2009. 456 p. v. 1

MICROSOFT NEWS CENTER BRASIL. **No Brasil, um terço dos casos de crimes online envolve parentes, amigos ou conhecidos.** Disponível em: <https://news.microsoft.com/pt-br/no-brasil-um-terco-dos-casos-de-crimes-online-envolvem-parentes-amigos-ou-conhecidos/> Acesso em: 19 de junho de 2018

NESBITT, Jordan. **Documentação**. 1. 2017. Disponível em: <https://newsapi.org/docs>. Acesso em: 03 nov. 2018.

PEREIRA, Evandro et al. **Forense Computacional: fundamentos, tecnologias e desafios atuais** . 2006. 51 p. TCC (Graduação em Sistemas de Informação)- Universidade do Vale do Rio dos Sinos, Unisinos, VII Simpósio Brasileiro Em Segurança da Informação e de Sistemas Computacionais, 2006. 1. Disponível em: <http://ceseg.inf.ufpr.br/anais/2007/minicursos/cap1-forense.pdf>. Acesso em: 28 nov. 2017.

PEREIRA, LUCIO CAMILO OLIVA; SILVA, MICHEL LOURENÇO DA. **Android para Desenvolvedores**. [S.l.]: Brasport, 2009. 219 p. v. 1.

ROQUE, Sérgio Marcos. **Criminalidade informática: crimes e criminosos do computador**. São Paulo: ADPESP Cultural, 2007. P. 25.

SAFERSTEIN, Richard. **Criminalistics: introduction to forensic science**. 8. ed. Upper Saddle River: Prentice Hall, 2004.

SANTOS, Herlones et al. **PERÍCIA FORENSE COMPUTACIONAL: METODOLOGIAS, TÉCNICAS E FERRAMENTAS** . 2012. 17 p. Artigo (Bacharel em Ciência da Computação)- Faculdade de Ciências Sociais Aplicadas do Vale de São Lourenço, Revista Cientifica Eletrônica de Ciências Sociais Aplicadas da EDUVALE, 2012. 1. Disponível em: <http://eduvalesl.revista.inf.br/imagens_arquivos/arquivos_destaque/LXkEA5FVHGZF1FB_2015-12-19-2-33-33.pdf>. Acesso em: 16 nov. 2017.

SOUZA, Adriano Gomes. **ETAPAS DO PROCESSO DE COMPUTAÇÃO FORENSE: UMA REVISÃO**. 2016. 13 p. TCC (Bacharel em Ciência da Computação)- Centro Universitário da Bahia, FIB, Acta de Ciências e Saúde, 2016. 2. Disponível em: <http://www2.ls.edu.br/actacs/index.php/ACTA/article/viewFile/138/128>. Acesso em: 07 nov. 2017.

TOLENTINO, Luciano Cordova; DA SILVA, Wanessa; MELLO, Paulo Augusto. **Perícia Forense Computacional**. 2011. 6 p. Artigo (Graduação em Sistemas de Informação)- Faculdade Projeção, Revista Tecnologias Em Projeção, 2011. 2.

WENDT, Emerson; JORGE, Higor. **Crimes Cibernéticos: Ameaças e procedimentos de investigação**. 2. ed. Rio de Janeiro: Brasport, 2013. 364 p. v. 2.