Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

JOÃO PEDRO LOPES VICENTIN

PERÍCIA DIGITAL FORENSE: ESTUDO DE CASO

ASSIS/SP

2020

Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

JOÃO PEDRO LOPES VICENTIN

PERÍCIA DIGITAL FORENSE: ESTUDO DE CASO

Projeto apresentado à Comissão do PIC do Instituto Municipal de Ensino Superior de Assis – IMESA e a Fundação Educacional do Município de Assis – FEMA, como requisito ao ingresso no Programa de Iniciação Científica.

Orientando: João Pedro Lopes Vicentin Orientador: Prof. Me. Fábio Eder Cardoso

Assis/SP

2020

SUMÁRIO

INTRODUÇÃO

Ao longo dos últimos anos, a internet foi uma das áreas que mais conseguiram espaço na vida da maioria das pessoas. Muitos de nossos serviços, atividades, trabalhos que antes nós conseguíamos exercer apenas de forma presencial, hoje podem ser feitos de forma on-line sem precisar sair de sua própria casa.

É indiscutível os benefícios e praticidade que o mundo digital trouxe para nós neste período, e viver hoje sem um smartphone no seu bolso e um computador em sua casa torna-se algo quase impossível.

Porém, ao mesmo tempo que a internet traz muitos pontos positivos para nós, os negativos chegam logo em seguida.

Como o número de atividades que podem ser feitas de forma online só vem aumentando, as pessoas acabam armazenando cada vez mais suas informações pessoais dentro da internet, o que torna os riscos de perda ou vazamentos de dados privados cada vez maiores, pois mesmo que a maioria das pessoas usem as redes online para fins legais, existe ainda, uma parte das pessoas que se aproveitam da fragilidade de um sistema de segurança para cometerem cybercrimes.

E para a investigação de tais crimes, coleta de dados e solução destes problemas, é utilizado a perícia digital ou computação forense.

1. PROBLEMATIZAÇÃO

Pretende-se elucidar os questionamentos abaixo:

• O que é a perícia digital?

• Quem são os criminosos que praticam esses crimes cibernéticos?

• Quais ferramentas são utilizadas por esses criminosos?

• Quais técnicas e ferramentas um perito deve utilizar?

• Quais são as etapas de uma perícia digital?

• Como a perícia digital funciona na prática?

2 . OBJETIVOS

2.1 Objetivo Geral

Acredito que seja essencial ampliar a informação em computação forense para um número cada vez maior de pessoas para que o interesse na área aumente, sendo assim este o objetivo desta pesquisa.

2.2 Objetivos Específicos

Creio que a maioria das pessoas que escolhe estudar e trabalhar na área de TI não tenham tanto interesse ou conhecimento sobre a área de perícia digital, fazendo com que acabassem indo para a área de programação em softwares, hardwares e administração de banco de dados por exemplo.

Além disso, durante a elaboração desta pesquisa, percebi a escassez de material sobre o assunto principalmente em língua portuguesa, fazendo com que tivesse que pesquisar sobre artigos e livros em língua estrangeira, o que na minha opinião limita o acesso das pessoas sobre o assunto.

Com a internet tendo cada vez mais um papel essencial em nossas vidas, acredito que a área de TI precisará ao passar dos anos, de um número cada vez maior de profissionais na área, da mesma forma na perícia digital.

3 . JUSTIFICATIVA

O tema a ser abordado é de extrema importância e relevância devido ao fato que muitos usuários da Internet, bem como de sistemas computacionais são atingidos por crimes digitais. A perícia digital permite a descoberta de vestígios criminais e, com isso, a imputação da pena aos malfeitores que se utilizaram de meios eletrônicos para cometer tais delitos. Conhecer a metodologia de trabalho e as ferramentas corretas que devem ser utilizadas em cada processo é um fator importante para a formação de um perito.

4 . O QUE É A COMPUTAÇÃO FORENSE

De uma maneira geral, a computação forense é um conjunto de técnicas que um profissional formado na área utiliza para a solução de crimes cibernéticos. Tais técnicas podem ser classificadas na seguinte ordem: Coleta e preservação dos dados, análise, e por fim, a formalização das provas e o veredito sobre o caso.

A computação forense pode ser utilizada para a solução de um crime em qualquer dispositivo que contenha um hardware, e que possa armazenar dados, como computadores, celulares, notebooks, tablets, GPSs entre outros.

A utilização da técnica pode ser feita para desvendar diversos crimes realizados por meio de dispositivos eletrônicos como crimes cibernéticos, fraudes virtuais, roubos de identidade, crimes financeiros etc.

Porém também pode ser utilizada para ajudar a solucionar crimes que acontecem dentro do mundo físico. O processo da investigação de muitos dos casos de assassinatos, sequestros ou roubos, passam por coletar aparelhos eletrônicos dos suspeitos de terem cometidos tais crimes como evidências para serem analisadas afim de conseguirem algumas provas para solucionar o caso.

5 . QUEM PRATICA ESTES CRIMES?

Se perguntassem para pessoas que são leigas no assunto, como elas denominariam os criminosos que praticam crimes virtuais, muitos iriam classificá-los como hackers, porém, esta denominação é equivocada. Todos os hackers são assim chamados, por terem a capacidade de modificar ou invadir softwares e hardwares de diferentes dispositivos, mas nem todos eles usam para fins legais, e para diferenciar os “hackers do bem” com os “do mal”, nasceu em 1985 o termo cracker, vejamos a diferença entre os dois:

Hacker

Os hackers utilizam suas habilidades e conhecimentos afim de melhorar o desempenho de um programa ou corrigir uma falha de segurança de maneira legal. Muitas das vezes os hackers também podem contribuir para solucionar crimes de alguns crackers.

Cracker

Diferente dos hackers, estes usam suas habilidades para cometerem atividades ilegais, invadindo e quebrando sistemas de segurança e furtando informações de usuários.

Alguns hackers consideram essas denominações muito subjetivas, assim eles usam outras: o White Hat (Chapéu Branco) seria o hacker, Black Hat (Chapéu Preto) o cracker, e uma nova denominação que colocam é o Gray Hat (Chapéu Cinza) que seria o meio termo entre os dois, teria as intenções boas de um White Hat só que usando ferramentas não legais como o Black Hat.

6 . MALWARES

Muitos dos crimes virtuais cometidos, são possíveis de serem executados graças à programas que são criados para se infiltrarem em dispositivos, alterando ou corrompendo arquivos e programas presentes neles afim de prejudicar de alguma forma o usuário.

Esses softwares são conhecidos como **malwares** (softwares maliciosos), vejamos alguns exemplos:

Ransomware

Com este tipo de malware, o criminoso tem a possibilidade de bloquear um dispositivo e roubar documentos específicos, muito utilizado para crimes de extorsão, fazendo com que a vítima consiga seus dados de volta apenas depois de um pagamento.

Spyware

Capaz de coletar informações sobre atividades feitas no computador de destino sem o conhecimento do usuário. Este malware é muito difícil de ser identificado pois atua de forma discreta no dispositivo. Com esse programa, o criminoso pode monitorar todas as atividades exercidas pela vítima como teclas digitadas, sites visitados, mensagens recebidas e enviadas etc. Estes dados são armazenados para depois serem enviados para os criminosos.

Este tipo de malware serve para roubar dados confidenciais, segredos industriais, informações sobre clientes, dados financeiros, dados de transações de cartão de crédito etc.

Worms

São malwares que trabalham de forma autônoma se espalhando de computador para computador. Eles se instalam a partir de uma rede de computadores, nela, os worms procuram dispositivos com algum tipo de vulnerabilidade no sistema de segurança, ou se copiando por compartilhamentos, envios de e-mails e outras formas.

Normalmente esse malware consegue se infiltrar em dispositivos sem causar quase nenhuma alteração no sistema, porém pode comprometer o desempenho do computador pois consome uma quantidade considerável de sua banda larga e também, tem a possibilidade de se infiltrar na rede e baixar malwares mais comprometedores para o computador como um ransomware.

Cavalo de Tróia

Trojan ou mais conhecido como Cavalo de Tróia, é um tipo de malware que visa ganhar a confiança do usuário, fazendo com que ele acredite que esse programa tenha fins úteis e legítimos para que possa ser instalado, a partir de sua instalação, ele entrega o controle do dispositivo ao criminoso.

Dois exemplos de Trojans seriam os Keyloggers (usados para o roubo de senhas), e os Backdoors (arquivos que possibilitam aberturas de portas para invasão). São tipos de malwares menos limitados que podem ser baixados na tentativa de fazer o download de algum aplicativo ou em algum site de origem duvidosa.

Rootkits

Esse malware é muito usado para esconder ou camuflar processos de identificação de um programa fazendo com que sua detecção por algum antivírus seja mais difícil. Ele funciona também como uma porta de entrada para outros malwares mais agressivos.

7 . FERRAMENTAS USADAS DURANTE UM PERÍCIA DIGITAL

O uso de ferramentas de hardware e software durante uma investigação deste tipo é essencial para a coleta e análise de dados, muitas dessas ferramentas usadas pela polícia podem ser livres para demais pessoas poderem usar, não somente para profissionais que atuam na área, porém ainda sim, existem softwares designados para

uso exclusivo das autoridades.

Hardwares

Os hardwares são importantes para uma investigação criminal pois tem como objetivo a coleta e preservação dos dados encontrados. Neles são armazenadas as evidências do caso para que o perito possa fazer a análise dessas pistas logo em seguida. É muito importante também, a utilização de um outro HD para fazer a cópia dos dados, assim o perito poderá seguir adiante com sua investigação sem que tenha risco de perdas ou alterações não desejadas em algumas evidências.

O uso do SSD para o armazenamento de dados também é possível, em comparação com o HD, este se mostra um dispositivo que consome menos energia e tem uma performance superior, porém sem a mesma capacidade de armazenamento de um HD.

8 . PROCESSOS DE UMA PERÍCIA DIGITAL

Como anteriormente citado, a perícia pode ser dividida em algumas partes para que o processo fique mais organizado e claro de se entender, ela pode ser dividida em quatro etapas que serão mais aprofundadas logo em seguida.

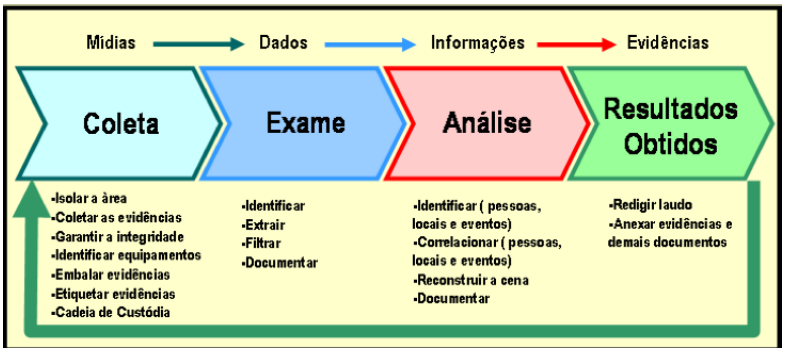

Imagem 1

Fases de uma Perícia Computacional Forense

8 . 1 . COLETA E PRESERVAÇÃO DE DADOS

A preservação dos dados de um caso sobre um crime digital é tão necessária quanto em um caso de algum crime físico, pois quaisquer modificações que aconteça em um dado

importante pode acabar prejudicando a investigação. Durante esta parte, o perito deve ser o mais cuidadoso possível até nas operações mais simples, pois qualquer movimento mal executado, pode modificar partes de um arquivo essencial para o laudo, conectar um pen drive via a entrada USB do computador ou até simplesmente ligar ele, pode modificar arquivos importantes.

Para que isso não ocorra, o perito deve fazer o processo de espelhamento dos dados. O espelhamento consiste em fazer uma cópia perfeita dos arquivos de um dispositivo de armazenamento para outro bit a bit. Para isso, é preciso que o tamanho do dispositivo que está recebendo a cópia seja igual ou maior do dispositivo que está sendo copiado. Caso seja maior, o dispositivo deve passar por um processo de limpeza para que não receba restos de arquivos irrelevantes que possam se misturar com os que realmente são relevantes, esta técnica de limpeza é denominada de wipe. É muito importante também, ter a certeza que o disco rígido está em plenas condições de uso e que não apresentem defeitos em nenhum de seus setores, caso contrário isso pode fazer com que a cópia dos dados seja incompleta.

Além da técnica de espelhamento para a cópia do dispositivo, existe também o processo de duplicação dos discos com o uso de imagens sobre eles, um processo semelhante ao espelhamento, fazendo uma cópia exata dos arquivos do disco. Porém, ao invés de se fazer uma cópia bit por bit dos dados igual ao espelhamento, estes são passados para arquivos de imagens.

Este processo dá para se dizer que contém algumas vantagens em relação ao espelhamento. Com a duplicação, é possível fazer a cópia de apenas uma parte do dispositivo e não necessariamente ele todo, o dispositivo de destino tem a possibilidade de receber arquivos de mais de um dispositivo diferente, a maior facilidade de manipulação dos dados, e também o uso menor de quantidade de espaço do dispositivo de destino.

Existem muitas ferramentas em hardware que ajudam na preservação dos dados no momento da realização da duplicação ou do espelhamento. Os equipamentos Espion Forensics e o Forensic Bridge Tableau são os mais utilizados para bloqueio de escrita em discos, já o software ICS Write Protect Card Reader é o mais utilizado para bloqueio de escrita em cartões de memória.

Os bloqueadores de escrita em disco rígido são os dispositivos mais comuns e simples de serem utilizados. Conectado entre o material questionado e o computador, esse tipo de equipamento possui a garantia, certificada pelo próprio hardware, de que nenhum dado será gravado, necessitando apenas utilizar o programa específico para a cópia do disco.

8 . 2 . ANÁLISE DOS DADOS

O objetivo desta etapa é examinar os dados obtidos durante a fase de coleta, identificar evidências e relacioná-las com o propósito da investigação.

Com a coleta dessas evidências, será possível responder as perguntas feitas pelas autoridades do caso, por isso, é de extrema importância que as pessoas responsáveis pela investigação sejam muito claras e diretas com o perito dizendo exatamente o que elas procuram para que o seu trabalho possa ir direto ao ponto sem a necessidade de perder tempo em analisar arquivos encontrados que são irrelevantes para o caso.

Ir direto ao ponto é essencial para que o perito possa fazer a análise pois muitos dos discos rígidos que são coletados como evidências por menor que sejam, podem conter milhares de arquivos e muitos deles desnecessários, tornando o exame pericial muito difícil de acontecer, para isso são usadas algumas técnicas e softwares com a finalidade de tornar a análise mais eficiente.

Um exemplo de técnica utilizada é o Known File Filter (KFF), que é um utilitário de banco de dados que compara valores hash conhecidos contra uma base de arquivos a ser analisada. Com o uso do KFF você pode identificar tipos de arquivo com base no seu conteúdo com o uso do hash. Técnica muito utilizada quando o objetivo é encontrar imagens de pornografia infantil por exemplo.

Outra técnica utilizada durante este processo é a de busca por palavras-chave, que é disponibilizada em muitos softwares de análises de arquivos.

Softwares

Para a resolução dos crimes digitais, o perito pode usar como ferramenta vários softwares específicos para essa área, como dito anteriormente, podendo ser gratuito e livre para todos usarem, ou sendo um software de uso exclusivo da perícia.

Abaixo listo alguns dos softwares mais utilizados pela polícia durante uma perícia digital, e as funções que cada um contém:

Sistema IPED

Software desenvolvido no Brasil para o uso na Operação Lava Jato, pode ser executado em Windows, Linux ou Mac OS.

Este software tem a possibilidade de:

- Analisar as informações armazenadas nos dispositivos digitais apreendidos;
- Recuperar arquivos deletados;
- Identificar criptografia;
- Localizar palavras;
- Reconhecer caracteres;
- Detectar nudez;
- Cruzar informações;
- Rastrear localizações;

En Case

Um dos softwares mais utilizados pela PF e FBI. É necessário uma licença paga para a utilização desse programa.

Este software tem a possibilidade de:

- Realizar investigações completas em dispositivos eletrônicos;
- Padronizar laudos periciais;
- Organizar o banco de dados de evidências;
- Recuperar arquivos apagados;
- Fornecer senhas de arquivos criptografados;
- Analisar hardwares e e-mails;
- Pesquisar palavras-chave de forma inteligente;
- Fornecer relatórios detalhados;

FTK

Programa de fácil uso sendo gratuito para todos usarem.

Este software tem a possibilidade de:

- Escanear o disco rígido para coletar informações;
- Processar e analisa documentos, gráficos e imagens;
- Recuperar arquivos;
- Criar filtros para gerenciar evidências relevantes;

8 . 3 . FORMALIZAÇÃO E APRESENTAÇÃO DAS PROVAS

Esta é a fase de conclusão da perícia, onde é colocada todas as provas que foram conseguidas durante o processo de análise para a formalização do laudo.

No laudo, é aonde é descrito todos os passos que foram tomados e técnicas utilizadas durante a investigação de forma direta. Nele deverá conter informações relevantes da investigação, como os peritos responsáveis, qual a autoridade responsável e o local que foi realizado o processo. É muito importante a clareza durante a apresentação do laudo, principalmente nos momentos de explicação sobre as fases de coleta e análise pois dependendo dos resultados obtidos, será possível a resolução do caso. Também é importante o uso de uma linguagem adequada pois deve se ter a noção de que o laudo estará sendo apresentados para pessoas que não são especialistas na área.

Laudo Técnico Pericial – Perícia Forense Computacional	
Preâmbulo	Identificação do laudo
Histórico	Fatos anteriores e de interesse ao laudo Quesitos concisos e objetivos
Material	Descrição do material examinado
Objetivo	Principais objetivos da perícia
Considerações técnicas/periciais	Conceitos e informações que podem ser úteis para o entendimento do laudo
Exames	Parte descritiva e experimental do laudo
Respostas aos quesitos/conclusões	Resumo objetivo dos resultados obtidos

Imagem 2

O laudo pode ser dividido nas seguintes etapas

9 . EXEMPLOS DE CASOS REAIS QUE FORAM SOLUCIONADOS COM A AJUDA DA COMPUTAÇÃO FORENSE

Caso #1 – Sharon Guthrie, morta afogada na banheira de sua casa em Dakota, EUA.


Imagem 3

Sharon Guthrie ao lado de seu marido e assassino, o pastor Willian Guthrie.

Em maio de 1999, Sharon Guthrie, de 54 anos, morre afogada na banheira de sua casa em Dakota, EUA. A autópsia realizada no corpo de Sharon, indicou o uso da droga Temazepam usada para auxiliar o sono. Seu marido, o pastor Willian Guthrie, foi quem indicou o medicamento para a esposa.

A polícia então contatou o perito em computação científica Judd Robbins para examinar os computadores utilizados pelo pastor na igreja. Assim, foi descoberto que o acusado havia pesquisado na internet, sites que explicavam como matar de forma eficaz e indolor incluindo o uso do Temazepam. Algumas pesquisas como “acidentes na banheira” e “acidentes domésticos” também foram encontrados no histórico do computador.

Com essas evidências encontradas, o marido da vítima acabou se tornando o principal suspeito de ter cometido o crime, contudo, para que a perícia não cometesse nenhuma injustiça, era necessário saber exatamente a data e hora que essas pesquisas foram feitas, pois o pastor poderia muito bem ter feito essas pesquisas depois do ocorrido. Um laudo bem formulado deve responder as seguintes perguntas: Quando? Onde? Como? Por que? e Quem?

As prováveis técnicas utilizadas para descobrir a data e hora destas pesquisas foram a restauração dos arquivos de backup do registro e a restauração das pastas de histórico do navegador web.

Caso #2 – Mércia Nakashima, encontrada morta na represa de Nazaré Paulista, no Estado de São Paulo.


Imagem 4

Mércia Nakashima ao lado de seu ex-namorado e assassino, o ex-policial e ex-advogado Mizael Bispo de Souza.

No dia 23 de maio de 2010, foi encontrado o corpo da advogada Mércia Mikie Nakashima de 28 anos, após ter sido violentada, e afogada trancada em seu carro na represa de Nazaré Paulista, no Estado de São Paulo. O IML concluiu o laudo afirmando que Mércia foi morta por afogamento após ter desmaiado em consequência de ter recebido um tiro no maxilar. O perito criminal concluiu que a vítima dirigia o veículo e que acabou entrando em luta corporal com o criminoso antes de ter recebido o tiro ainda dentro de seu carro e que, depois, o veículo foi empurrado em direção à represa. O ex-namorado de Mércia, policial militar e advogado, Mizael Bispo de Souza passa a ser o principal suspeito.

A perícia criminal encontra vestígios de algas no sapato do suspeito, mesmo tipo de algas próximas à represa, porém essa pista não é suficiente para provar que Mizael estaria próximo à represa no mesmo momento do crime.

O perito computacional entra na investigação com o objetivo de procurar ligar o suspeito ao local e hora do crime quando ele foi cometido. A estação rádio base (ERB), detectou a presença do aparelho do suspeito próximo a cena do crime (margem de erro de 100 metros).

A prova circunstancial ajudou a condenar o suspeito após ele ter negado que estava próximo da represa no momento do crime.

10 . CONCLUSÃO

Chegando ao final do trabalho pudemos compreender, de maneira resumida, sobre do que se trata a computação forense, o que significa, qual sua importância, e os processos que ela possui.

É importante ressaltar a importância que essa área possui e que irá aumentar ainda mais conforme os anos irão passando. Com o número de informações aumentando cada vez mais dentro da internet, os casos de crimes cometidos virtualmente só tendem a crescer, e para isso, será necessário um número cada vez maior de profissionais dentro do ramo, por isso é muito importante que esse assunto seja abordado com mais frequência.

11 . REFERÊNCIAS

NIKKEL, Bruce. **Practical Forensic Imaging: Securing Digital Evidence with Linux Tools,** 2016.

A. HASSAN, Nihad. **Perícia Forense Digital: Guia prático com o uso do sistema operacional Windows.** Novatec Editora Ltda, São Paulo: Apress Media, 2019.

RODRIGUES DE FREITAS, Andrey. **Perícia Forense Aplicada à Informática,** Edição 1: Brasport Livros, 2006.

NADER DE ALMEIDA, Rafael. **Perícia Forense Computacional: Estudo das técnicas utilizadas para coleta e análise de vestígios digitais,** São Paulo. Disponível em <https://www.passeidireto.com/arquivo/26461384/pericia-forense-computacional-estudo-das-tecnicas-utilizadas-para-coleta-e-anali>. Acesso em: 15 de setembro de 2020.

Imagem 1 - https://periciacomputacional.com/pericia-forense-computacional-2/

Imagem 2 - https://www.imdb.com/title/tt2610702/

Imagem 3 - https://repositorio.uniube.br/bitstream/123456789/384/1/Jean%20Aleff%20Dorneles%20Borges%20e%20Nicholas%20Prado.PDF

Imagem 4 - https://fotos.estadao.com.br/fotos/cidades,relembre-o-caso-da-morte-da-advogada-mercia-nakashima,191013