**ALUNA:** Bruna Lanzarini

**RM:** 83421

Esta tarefa deverá ser feita INDIVIDUALMENTE. Poste o arquivo com as suas respostas no Portal de Trabalhos da FIAP até a data máxima de **8 de Setembro de 2020**. Dê preferência para o formato MS-Word (.DOC).

O intuito dessa tarefa é conhecer sobre as características e boas práticas da arte da perícia digital, profissão específica de quem trabalha com segurança da informação.

**Observação:** Como se trata de opiniões dissertativas sobre um tema, as respostas serão discutidas na próxima aula presencial, dia 9 de Setembro. Somente para referência, não necessariamente todas as respostas precisam estar exatamente iguais. Leia o texto abaixo e encontre o enunciado de sua atividade no final dele.

**OBSERVAÇÃO: No final da página 3 há um link de um vídeo que você PRECISA assistir para completar a Atividade!!**

**A arte da perícia digital**

Profissionais são especialistas em recuperar dados que pareciam perdidos

FDTK – o sistema operacional feito para o Perito Digital

Você acha que, ao apagar seu histórico, todos os seus rastros na internet estão eliminados para sempre? E apagar uma mensagem comprometedora do celular, será que ela nunca mais será lida por ninguém? Bom… para todos nós, usuários comuns, isso pode fazer sentido. Mas para os peritos digitais, recuperar informações é algo que faz parte do dia-a-dia. Eles trabalham para bancos, lojas e empresas que realizam transações online. Perto deles, ninguém tem nada a esconder.

O perito digital é o profissional que descobre evidências em equipamentos eletrônicos a fim de comprovar algum crime online. As ferramentas são variadas, e são capazes de recuperar informações, além de informar quando, onde e como o fato ocorreu. Com uma maleta especial com ferramentas diversas eles são capazes de extrair qualquer dado de um telefone celular: chamadas e mensagens de texto escritas ou recebidas, agenda, música, vídeo e fotos. E mesmo o que já foi apagado pelo usuário pode ser recuperado com técnicas que eles dominam. Você já tá pensando em comprar uma maletinha dessas para descobrir os segredos da namorada, não é? Calma… as coisas não funcionam bem assim!

“Existe uma questão ética e uma questão legal, então você não pode usar um equipamento como este para extrair dados telefônicos de um telefone que não seja seu, sem a autorização dessa pessoa – exceto em casos de solicitação judicial. Um marido não pode pedir que a esposa extraia os dados sem a devida autorização, porque isso é crime”, explica o perito em Segurança Digital, Marcelo Lao.

No caso dos computadores, uma série de ferramentas ajuda na perícia digital. Com uma ferramenta específica é possível fazer um raio-x completo da máquina, desde o mapa de horários em que ficou ligada ou desligada, e que programas já foram instalados aqui nos últimos meses e até nos últimos anos! Isso é fundamental, por exemplo, ao procurar programas-pirata instalados em máquinas indevidas. Mesmo que o programa já tenha sido apagado, esta ferramenta registra o uso dele. Já esta outra ferramenta permite identificar cada um dos dispositivos USB que foram plugados na máquina. Você pode não saber, mas todo pen drive ou equipamento eletrônico possui uma identificação única, e esta marca fica guardada em todos os computadores. Basta plugar uma vez…

“Por meio dessa identificação via número de série, se esse mesmo pen drive foi conectado no equipamento A e tiver sido conectado no equipamento B, numa análise de registros eu irei encontrar essa mesma identificação nos dois equipamentos”, conta Lao.

Um arquivo só é apagado de verdade quando uma nova informação é escrita em cima do espaço que ele ocupava no disco. Mas, mesmo assim, para ter a informação excluída definitivamente, os peritos dizem que seria necessário regravar ou formatar um disco por 25 vezes, utilizando técnicas variadas. Caso contrário, não adianta, eles conseguem recuperar dados. E ainda tem outro detalhe: você já parou para pensar que toda informação digitada ou processada pelo computador passa pela memória RAM? Você acha que ela é apagada ao desligar o PC? Que nada!

“Tudo o que eu faço pelo computador transita pela memória: um chat, o acesso a uma página, a digitação de uma senha. Esses dados podem ser capturados na memória, inclusive os sites acessados. Por mais que eu desligue a máquina, ainda eu posso ter padrões fazendo um ‘dump’ de memória, congelando a memória, analisando essa memória numa ferramenta forense eu consigo identificar vários dados que possam sugestionar o comportamento de usuários daquela máquina. Então os dados podem persistir mesmo após a máquina ter sido desligada ou reinicializada”, conta o perito em segurança digital, José Antônio Milagre.

Para combater a pornografia, a ferramenta é esta: o PornStick. Este pen drive analisa os metadados do arquivo e consegue descobrir imagens suspeitas até mesmo em lugares improváveis. Em nosso teste, ele encontrou uma imagem suspeita. E ela havia sido gravada como se fosse um inocente arquivo de texto, olha só! E ainda falando sobre metadados, que são os códigos binários que formam os arquivos, tem **cracker** que esconde informações aqui. É possível transmitir uma senha ou um recado em texto, alterando estes códigos.

“O perito, se não tiver profundos conhecimentos e não analisar o sistema tão somente na sua interface de usuário, mas transcender camadas e fazer uma busca complexa, ele não vai encontrar informações e nós teremos um criminoso solto nas ruas”, alerta Milagre.

Um pouco mais avançada que os metadados é a técnica chamada esteganografia. Aqui, o criminoso consegue ocultar um arquivo dentro do outro. Esta imagem, por exemplo, traz consigo um arquivo de áudio.

Essa técnica foi muito utilizada pela AL Qaeda de Osama Bin Laden no início da década passada. E hoje, é utilizada para **phishing**. Imagine, por exemplo, a aparentemente inofensiva apresentação em PowerPoint que sua mãe recebeu. Ao executá-la, é possível que outro arquivo também seja executado em conjunto e a partir de então, tudo o que for digitado na sua máquina será enviado para o cracker. Atualmente, não se pode confiar em ninguém, e não se pode clicar em nenhum arquivo vindo de fonte desconhecida.

“São ferramentas que permitem com que eu anexe vários arquivos em um único arquivo. A maioria dos antivírus que não checar a identidade do arquivo, checar só a extensão – ou o próprio IDS, que não faz checagem de assinatura -, vai entender que aquilo é um PPS. O próprio usuário que não tem um antivírus instalado não vai ter nenhuma reação ao abrir um PPS – que vai abrir uma apresentação de qualquer natureza. Só que, paralelamente, ele executou em modo hidden (oculto) um key logger ou outra função que está rodando na máquina e, a partir de então, ele está sendo monitorado. Tudo o que ele digita, principalmente os screens (telas) dele estão sendo encaminhados para o criminoso digital, que vai aplicar fraudes bancárias, financeiras ou até mesmo acesso indevido a dados”, resume Milagre.

E sabe aquela história de criar senhas complexas, que não contenham data de aniversário ou sequências numéricas? A explicação para isso está aqui. Uma das ferramentas mais utilizadas pelos crackers para a quebra de senhas é a John the Ripper. Ela trabalha com uma lista de palavras comumente utilizadas como senhas e com base nessa relação, consegue quebrar 7 em cada 10 senhas online. Mas muitas vezes, descobrir a senha nem é o desafio principal do perito.

“Batendo o olho no hexadecimal, você consegue identificar caracteres que não correspondem a uma imagem, ou são caracteres envolvendo textos. Então no final desse arquivo nós conseguimos identificar exatamente onde foi lançado o código e a senha de esteganografia e, com base nisso, a gente apenas zera essa informação em hexadecimal fazendo com que seja possível acessar o conteúdo oculto. Mais uma vez eu chamo atenção: período digital não é CSI, eu não preciso descobrir a senha. Nesse caso, eu não descobri a senha e nem me importa a senha, o importante era ter acesso ao conteúdo. Nós zeramos a senha da esteganografia em hexadecimal, e conseguimos descobrir o conteúdo que estava embutido dentro de uma imagem”, exemplifica o perito José Antônio Milagre.

O perito digital é, hoje, uma profissão em ascensão. Existem várias universidades no país que oferecem cursos de pós-graduação e até Mestrado na área.

Após ler o texto responda as questões abaixo. Procure responder sem acessar qualquer tipo de informação auxiliar (a própria Internet, livros, cadernos, smartphone, etc.) apenas utilizando como base a leitura do texto. É recomendável que você também acesse posteriormente o vídeo no Youtube sobre ‘A Arte da Perícia Digital’ (programa Olhar Digital exibido pela Rede TV de São Paulo), para verificar as ferramentas e técnicas por meio do link a seguir:

<https://www.youtube.com/watch?v=b9YAK3losaU>

**QUESTÕES**

1. De acordo com o texto apresentado, qual a descrição sobre o profissional chamado “perito digital”?

O perito digital é o profissional que descobre evidências em equipamentos eletrônicos a fim de comprovar algum crime online.

1. Qual é a questão ética que envolve as técnicas da perícia digital?

Não se pode extrair dados que não sejam seus, sem a autorização da pessoa proprietária deles – exceto em casos de solicitação judicial. Um marido, por exemplo, não pode pedir que a esposa extraia os dados sem a devida autorização, porque isso é crime.

1. Como faríamos então para ter certeza de que um único arquivo foi excluído definitivamente de um computador?

Um arquivo só é apagado de verdade quando uma nova informação é escrita em cima do espaço que ele ocupava no disco. Mas, mesmo assim, para ter a informação excluída definitivamente, os peritos dizem que seria necessário regravar ou formatar um disco por 25 vezes, utilizando técnicas variadas. Caso contrário, não adianta, eles conseguem recuperar dados.

1. De acordo com o perito, a memória do tipo RAM\* é apagada ao se desligar a máquina? Qual ou quais procedimentos são utilizados para se recuperar dados em memórias voláteis?

Tudo o que fazemos no computador transita pela memória: um chat, o acesso a uma página, a digitação de uma senha. Esses dados podem ser capturados na memória, inclusive os sites acessados. Por mais desliguemos a máquina, ainda podemos ter padrões:

- Fazendo ‘dump’ de memória;

- Congelando a memória;

- Analisando essa memória numa ferramenta forense.

Então os dados podem persistir mesmo após a máquina ter sido desligada ou reinicializada

1. Qual o significado do termo “esteganografia” mencionado no texto? Quais os perigos e ameaças proporcionados por essa técnica?

Esteganografia é a técnica de ocultar um arquivo dentro do outro. O seu perigo se dá, quando o fato de um arquivo que pode parecer simples e inofensivo, ao ser habilitado ou executado na máquina do usuário, executa em modo hidden (oculto) um key logger ou outra função que está rodando na máquina e, a

partir de então, passa a ser monitorado. Tudo o que ele digita, principalmente os screens (telas), estão sendo encaminhados para o criminoso digital, que vai aplicar fraudes bancárias, financeiras ou até mesmo acesso indevido a dados.

**Notas do professor**:

\*RAM (Randomic Access Memory – Memória de Acesso Randômico ou Aleatório)

\*\*Volatilidade é a propriedade de um líquido transformar-se em vapor ou gás. Há uma relação feita com os dados da memória desse tipo que “evaporariam” ao terem sua fonte de energia extinta.

\*\*\*Cracker é o nome do especialista (muitas vezes mais curioso do que especialista, mas que conhece muito de computadores) que acessa sistemas de computadores para obter informações que não lhes pertencem.

\*\*\*\*Phishing (pescaria) é a técnica utilizada pelos crackers para ‘pescar’ informações alheias, seja por meio de envio de e-mails maliciosos ou infectando computadores por meio de invasão com acesso lógico indevido.

Fonte: Blog do 26, disponível em: <https://www.26notas.com.br/blog/?p=543> . Acesso: 19 Ago, 2020.

“*Que os vossos esforços desafiem as impossibilidades. Lembrai-vos de que as grandes coisas do homem foram conquistadas a partir do que parecia impossível...*”

(Charles Chaplin – ator e diretor Inglês)