Aula 02
Forense Computacional

Conceitos & Legislação

Agenda

- Objetivos
- História
- Forense Digital
- Crime Cibernético
- Legislação
- Atividade

Objetivos

- Certificações e Mercado (3 formas);
  - CCE - **Certified Computer Examiner**
  - CCFE - **Certified Computer Forensics Examiner**
  - CHFI - **Computer Hacking Forensic Investigator**
  - GCFA - **GIAC Certified Forensic Analyst (SANS)**
  - **Access Data, EnCE, EnCEP)**

- Explicar o que é Forense - Arquimedes;
- Esclarecer os principais conceitos de Forense Digital;
- Desenvolver a ideia de Forense Computacional.

História

- **O que é forense?**
  - Antes da definição é interessante saber um pouco da história, como surgiu a forense, suas diversas utilizações e evoluções no decorrer dos tempos.
    - Quando?
    - Como?
    - Quem?
    - Por que?

Princípio da Flutuabilidade

- **Séc. III a.C -Caso da coroa do Rei Heron II de Siracusa**

  - Arquimedes usa o princípio da flutuabilidade para checar se o metal em uma coroa de ouro é tão puro quanto o fabricante alega;

  - O **princípio de Arquimedes** determina que ***"um objeto total ou parcialmente imerso num líquido sofre a ação de uma força vertical, de baixo para cima, de intensidade igual ao peso do fluido deslocado por esse objeto".***

História

1784 - O inglês John Toms foi condenado por assassinato porque uma bucha de pistola, feita de papel amassado, encontrada no ferimento de sua vítima, corresponde ao jornal rasgado no bolso de Tom.

1858 - William Herschel coleta a palma da mão no verso de seus contratos, e no final deste mesmo século Francis Galton elabora um estudo complexo sobre as impressões digitais (5%);

1910 - O criminologista francês Edmond Locard, o homem que descobriu o princípio forense básico de que "qualquer contato deixa uma pista", funda o primeiro laboratório criminal do mundo, em Lyon.

História

1930 – O Austríaco **Karl Landsteiner** descobre que os tipos sanguíneos podem ser divididos em grupos de acordo com caraterísticas próprias (A+, A-, B+, B-, AB+, AB-, O+, O-);

+- 1930 – O Americano **Calvin Goddard** desenvolve um estudo sobre a comparação entre projéteis de armas de fogo.

História

Frank Abagnale JR.

Catch Me if You Can

- **Albert Sherman Osborn** desenvolve uma pesquisa sobre as características e metodologias para análise de documentos;
- **Hans Gross**, que desenvolve o método científico para a realização de investigações criminalísticas;

- **<u>1932</u>**
  - No **FBI**, foi organizado um laboratório para prover serviços de análise forense a todos os agentes de campo e outras autoridades legais Americanas.

- Isso só começa a mudar com o advento da informática e o crescente nível de importância da informação no contexto da atualidade.

Definição de Forense

“Aplicação da ciência física à lei na busca pela verdade em assuntos civis, criminais e de comportamento social, com o fim de que nenhuma injustiça seja feita à nenhum membro da sociedade”.

Handbook of Forensic Pathology College of American Pathologists

Forense Digital

- Ciência que objetiva **identificar, preservar, coletar, examinar, analisar e apresentar** informações sobre uma atividade maliciosa.

- A **investigação** é o processo que provê as informações necessárias para a análise forense, levando à conclusão final que poderá servir como base em decisões judiciais.

Investigação Forense

- "*Uma série metódica de técnicas e procedimentos para coletar evidências de um sistema computadorizado, de dispositivos de armazenamento ou de mídia digital, que podem ser apresentadas em um fôro de uma forma coerente e de formato inteligível*". - Dr. H. B. Wolf

Investigação Forense

- A investigação digital é um processo onde uma hipótese é desenvolvida e testada para responder algumas questões à respeito de uma ocorrência digital.

- A investigação digital tem como objetivo suportar ou desmentir uma hipótese apresentada por uma análise inicial, e muitas vezes superficial, do cenário comprometido.

Investigação Digital X Forense Digital

- A investigação digital difere da forense digital em inúmeros ponto do processo.

  - A Forense Digital procura chegar a uma conclusão final, que permita apresentar um relatório com provas bem fundamentadas e amparadas nas leis vigentes daquele país (para a corte).

  - Já a Investigação Digital tem um foco diverso, mais voltado para a técnica e ferramentas utilizadas do que com o aspecto legal de um processo judicial.

Forense Computacional

- *“Forense Computacional compreende a aquisição, preservação, identificação, extração, restauração, análise e documentação de evidências computacionais, quer sejam componentes físicos ou dados que foram processados eletronicamente e armazenados em mídias computacionais.”*
  Warren G. Kruse II & Jay G**.** Heiser

- “*Preservação, identificação, coleta, interpretação e documentação de evidências computacionais, **incluindo as regras de evidência**, processo legal, integridade da evidência, relatório factual da evidência e provisão de opinião de especialista em uma corte judicial ou outro tipo de processo administrativo e/ou legal com relação ao que foi encontrado*”. Steve Hailey, do Cybersecurity Institute

Problemas da Forense Computacional

- Não existe metodologia internacional;
- Não existe padronização das ferramentas - NIST;
- É mais uma arte do que ciência;
- Ainda está em seus estados iniciais de desenvolvimento;
- Pouco conhecimento teórico sobre o qual as hipóteses empíricas são baseadas;
- Falta de treinamento apropriado;

Por que Forense Computacional?

- "*A forense computacional é o equivalente ao levantamento na cena de um crime ou a autópsia da vítima* ". - James Borek
  - Buscar e identificar dados em um computador;
  - Recuperação de arquivos deletados, **encriptados** ou corrompidos em um sistema;
  - Fundamentar demissões de funcionários que desrespeitam normas organizacionais;
  - Auxiliar na quebra de contratos que não são respeitados;
  - Provar fatos;
  - Fazer cumprir as leis de privacidade.

Crime Cibernético

- Um **crime cibernético** é definido como qualquer ato ilegal envolvendo um computador, seu sistema ou suas Aplicações. E para ser tipificado como crime, o ato deve ser intencional, e não acidental.
  - Três aspectos:
    - Ferramentas do crime
    - Alvo do crime
    - Tangente do crime
  - Duas categorias:
    - Ataque interno
    - Ataque externo

Exemplos e Motivações

- Exemplos:
  - Roubo de propriedade intelectual;
  - Avaria na rede de serviço das empresas;
  - Fraude financeira;
  - Invasão de hackers;
  - Distribuição e execução de vírus ou worm.
- Motivações:
  - Testes ou tentivas de aprender na prática, por script kiddies;
  - Necessidade psicológica;
  - Vingança ou outras razões maliciosas;
  - Desejo de causar problemas para o alvo;
  - Espionagem Corporativa ou Governamental;

Função do Investigador

- O principal objetivo do investigador forense computacional é determinar a natureza e os eventos relacionados a um crime ou ato malicioso e localizar quem o perpetrou, seguindo um procedimento de investigação estruturado.

Conduta do Investigador

- A conduta profissional determina a credibilidade de uma investigação forense;
- O profissional deve demonstrar o mais alto nível de integridade ética e moral;
- Confidencialidade é uma característica essencial que todo investigador deve possuir;
- Discutir detalhes dos casos investigados apenas com as pessoas que possuem permissão para tomar conhecimento do processo;

Legislação

- Entender as principais leis relacionadas à investigação e perícia forense;
- Compreender como o código civil está configurado para abarcar os novos crimes, ditos digitais;
- Adquirir uma visão inicial das leis vigentes no código penal que se aplicam à crimes digitais;
- Entender as principais classificações de crimes digitais;

Legislação

- O primeiro artigo do código penal diz que:
  - *Art. 1º - Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal.*

Se não existe uma lei para definir que tipo de ação é infração, então não existe crime.

Legislação

- O advento da Internet, trouxe a possibilidade de uma pessoa estar em um lugar e cometer o crime em outro.

- No Brasil isso é tratado pela teoria da ubiquidade, acolhida pelo sexto artigo do Código Penal:

  – *Art. 6º - Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado.*

Legislação

- Os Crimes de Informática podem ser:

  - ✓ Crime de informática puro
  - ✓ Crime de informática misto
  - ✓ Crime de informática comum

Legislação

- **<u>Crime de informática puro</u>**
  - Toda e qualquer conduta que vise exclusivamente violar o sistema de computador, pelo atentado físico ou técnico ao equipamento e seus componentes, inclusive dados e sistemas.
  - As ações físicas se materializam, por exemplo, por atos de vandalismos contra a integridade física do sistema, pelo acesso desautorizado ao computador, pelo acesso indevido aos dados e sistemas contidos no computador.

- **Crime de informática misto**

  – São todas as ações em que o uso do sistema de computador é condição essencial para efetivação de um crime.

Por exemplo, para realizar operações de transferência bancária ilícitas pela Internet, é imprescindível o uso do computador para a sua consumação, sendo classificado assim como um crime de informática misto.

Legislação

- **<u>Crime de informática comum</u>**
  - São todos aqueles em que o sistema de computador é uma mera ferramenta para cometer um delito já tipificado na lei penal. Se antes, por exemplo, o crime como pornografia infantil era feito por meio de vídeos ou revistas, atualmente, se dá por troca de fotos via e-mail e divulgação em sites. Mudou a forma, mas a essência do crime permanece a mesma.

Legislação

- Falta de legislação específica
  - Novo Código Civil (Lei no 10.406)
  - Medida Provisória 2.200-2
  - Lei 9.296/96
  - Lei 9.983/00
  - Lei 9.800/99

Legislação

Novo Código Civil (Lei no 10.406)

> ***Art. 225.*** *As reproduções fotográficas, cinematográficas, os registros fonográficos e, em geral, quaisquer outras reproduções mecânicas ou eletrônicas de fatos ou de coisas fazem prova plena destes, se a parte, contra quem forem exibidos, não lhes impugnar a exatidão*.

- Assim, a legislação não exige que o documento seja reconhecido como verdadeiro previamente, o documento agora é considerado verdadeiro até que provem o contrário. O mesmo se aplica para uma evidência eletrônica.

- Entretanto, é necessário que seja aplicada alguma tecnologia no documento para garantir sua integridade e autenticidade, pois sem isso, a parte contrária pode contestar a veracidade da prova.

Legislação

Medida Provisória 2.200-2

Art. *1º - Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.*

- *Essa medida provisória reconhece a assinatura digital baseada na criptografia assimétrica de chave pública e privada para garantir a identificação e a integridade dos documentos eletrônicos, desde que a chave pública esteja em uma autoridade certificadora.*

Legislação

Lei 9.296/96

- *É a primeira lei específica para o meio digital e trata, basicamente, do sigilo das transmissões de dados. O fluxo de comunicações em sistemas de informática e telemática podem ser interceptados somente com autorização da justiça.*
- O Art. 2º desta lei diz que não será admitida a interceptação desse fluxo de comunicação se:
  - Não houver indícios razoáveis da autoria ou participação em infração penal;
  - A prova puder ser feita por outros meios disponíveis;
  - O fato investigado constituir infração penal punida, no máximo, com pena de detenção.
- Sendo constituído crime a interceptação de comunicações telefônicas, de informática ou telemática sem autorização judicial ou com objetivos não autorizados em lei, além da quebra de segredo da justiça.

Legislação

Lei 9.983/00

- Considera como crime o ato de divulgar, sem justa causa, informações sigilosas como senhas ou dados pessoais de clientes, por exemplo, contido ou não nos sistemas de informação.

- Então a publicação de dados reservados, assim definidos por lei, pela Internet ou qualquer outro, é um sistema de informação e infringe a Lei com uma pena de até 4 anos de detenção. Também é crime, de acordo com a Lei 9983/00, a inserção, modificação ou alteração não autorizada de sistema de informações ou banco de dados.

Legislação

Lei 9.800/99

- Revela que o Brasil está tentando acompanhar o progresso científico e o avanço tecnológico ao permitir às partes a utilização de sistema de transmissão de dados e imagens, para a prática de atos processuais, como o envio de petições via correio eletrônico (e-mail) ao Poder Judiciário. Isso implica mais comodidade e economia de tempo no envio de petições aos Tribunais de Justiça.

- Segundo o artigo 4º, quem fizer uso de sistema de transmissão torna-se responsável pela qualidade e fidelidade do material transmitido, e por sua entrega ao órgão judiciário.

Legislação

Projetos de Lei

- ***PL 3.356/00*** - Do Sr. Osmânio Pereira - Dispõe sobre a oferta de serviços através de redes de informação.

- ***PL 3.303/00*** - Do Sr. Antônio Feijão - Dispõe sobre normas de operação e uso da Internet no Brasil.

- ***PL 7093/02*** - Ivan Paixão - dispõe sobre a correspondência eletrônica comercial, entre outras providências.

- ***PL 6.210/02*** - Ivan Paixão - Limita o envio de mensagem eletrônica não solicitada, por meio da Internet

Legislação

- ***PL 1809/99*** - Bispo Rodrigues - dispõe sobre a segurança nas transações bancárias efetuadas por meios eletrônicos e fornece outras providências.

- ***PL 84/99*** - Luiz Piauhylino - Dispõe sobre os crimes cometidos na área de informática, suas penalidades e fornece outras providências

- ***PLS 76/00*** - Leomar Quintanilha - Estabelece nova pena aos crimes cometidos com a utilização de meios de tecnologia de informação e telecomunicações.

Atividade

- **Artigo:** CRIMES INFORMÁTICOS: Legislação brasileira e técnicas de forense computacional aplicadas à essa modalidade de crime
- **Artigo:** Um pouco sobre Leis
- **Artigo:** Como se tornar um profissional de Forense Digital?
- **Texto**: Forense Computacional: Aspectos Legais e Padronização