Aula 03
Forense Computacional

Laboratório Forense

&

Investigação Forense

Agenda

- ✓ Organização do laboratório
- ✓ Segurança do laboratório
- ✓ Auditoria
- ✓ Responsabilidades
- ✓ Equipamentos

Organização do laboratório

- ✓ Para qualquer investigação, seja ela simples ou complexa, é necessário dispormos de uma infraestrutura organizada para conduzir as análises forenses.

Implementação

- ➢ Valor do Investimento;
- ➢ Estatísticas de crimes, para alocação de recursos
- ➢ Espaço ocupado, equipamentos necessários, profissionais, treinamento, software e hardware necessários;
- ➢ A natureza do laboratório

Segurança do laboratório

- ✓ Devemos levar em consideração o design estrutural do laboratório, por vários motivos, sendo um deles a segurança:
  - A sala deve ser em um local seguro;
  - Deve ser construído com materiais sólidos, para evitar invasões;
  - Não deve possuir quaisquer aberturas nas paredes, teto e assoalho;
  - Não deve possuir janelas para o exterior;
  - Tomar cuidado para que as telas dos computadores não estejam voltados para janelas externas ou internas.

Segurança do laboratório

- ✓ Ainda podemos acrescentar outros fatores para determinar uma maior segurança ao laboratório, com os seguintes procedimentos:

  - ➢ Ter apenas uma entrada para o laboratório;
  - ➢ Não deixar janelas abertas, para evitar acesso não autorizado;
  - ➢ Log de entrada de pessoas no laboratório, para armazenar hora, tempo de permanência e nome da pessoa que teve acesso as suas dependências;
  - ➢ Implantação de um alarme de detecção de intrusão;
  - ➢ Equipamento de combate à incêndio, que deve ser disposto dentro e fora do laboratório.

Auditoria em um laboratório

- ✓ Os passos necessários para a realização de uma auditoria em um laboratório de Forense Computacional:
  - ➢ Investigar o teto, assoalho, telhado, paredes internas e externas;
  - ➢ Investigar portas e fechaduras;
  - ➢ Checar se as fechaduras estão funcionando corretamente;
  - ➢ Verificar o log de visitantes;
  - ➢ Examinar os logs de acesso aos locais onde as evidências estão guardadas;
  - ➢ Coletar evidências que não estejam sendo analisadas e armazená-las em local seguro.

Responsabilidades de um Supervisor

- ✓ Algumas delas são as que estão definidas abaixo:
  - Os supervisores devem assegurar a qualidade e eficiência do trabalho;
  - Os supervisores são responsáveis por assegurar a produtividade;
  - Os supervidores são responsáveis pelos profissionais contratados;
  - O desenvolvimento das tarefas da equipe é de responsabilidade do supervidor;
  - Os supervisores devem assegurar a segurança do ambiente de trabalho.

Equipamentos

- Estações de trabalho: de ambos os tipos, para análise forense e de uso geral;
- No-Break, como equipamento de prevenção de falta de energia;
- Estante para livros;
- Softwares necessários;
- Materiais de referência (livros, apostilas e etc);
- Cofre ou locais seguros para armazenamento de evidências;
- Conexão com LAN e Internet;
- Prateleiras para organização de equipamentos que não estiverem sendo utilizados;
- Impressoras;
- Scanners;
- Hard disk, adicionais;
- Drives de fita para backup.

Toolkits

- ✓ Kits de hardware para coleta de evidências e análise forense de dispositivos comprometidos

Investigação Forense Computacional

- ✓ Uma investigação Forense Computacional, pode assumir diversas características, dependendo do contexto onde a investigação é realizada.
- ✓ A investigação pode assumir aspectos diferentes em cada situação.

Investigando um crime computacional

- ✓ Primeiro é necessário definir se realmente houve um incidente, qual tipo de incidente, como foi reportado e quis as informações que a pessoa que reportou teve acesso.
- ✓ A partir desse ponto, é necessário encontrar e analisar as pistas deixadas pelo criminoso.
- ✓ Iniciar uma avaliação preliminar em buscas de evidências, a fim de ter material para análise.
- ✓ Ao longo do processo investigativo, devem haver profissionais que executam papéis bem definidos:
  - Profissional de resposta à incidentes
  - Investigador ou perito forense
  - Técnico forense

Investigando violação de políticas

- ✓ Os passos são os mesmos de uma investigação criminal, porém, alguns aspectos devem ser levados em consideração:
  - ➢ Todos os empregados da companhia, deveriam ser informados da politica organizacional no seu primeiro dia de trabalho;
  - ➢ Empregados que utilizam recursos da companhia para uso pessoal não apenas gastam o tempo da companhia e tais recursos, mas também violam a política organizacional;
  - ➢ Tais empregados, precisam ser rastreados e educados acerca da política vigente na companhia;
  - ➢ Se o problema persistir, alguma ação deve ser tomada.

Passos de uma Investigação

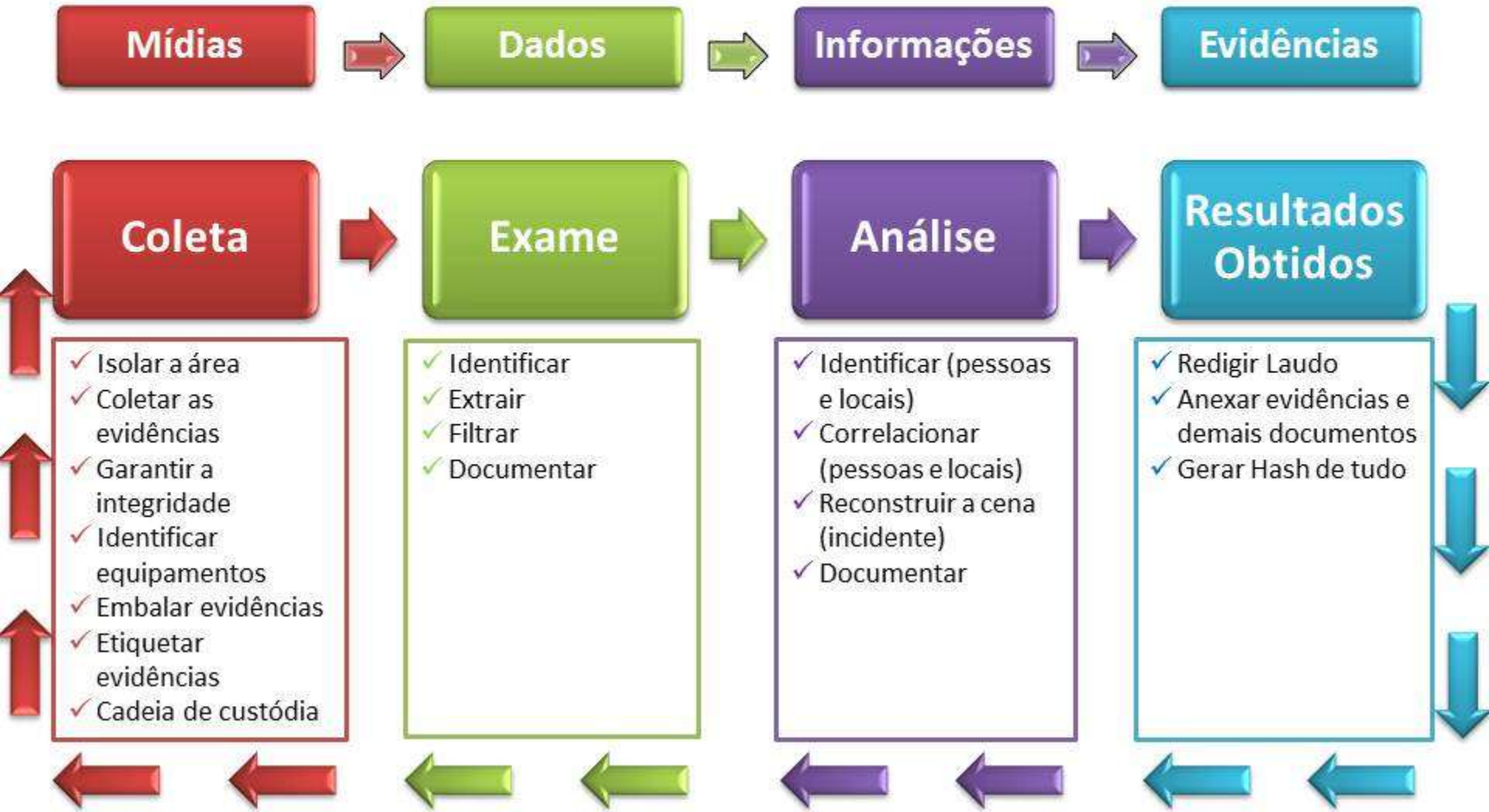
- ✓ Avaliação inicial do caso;
- ✓ Preparar um projeto detalhado;
- ✓ Determinação dos recursos necessários;
- ✓ Identificação dos riscos envolvidos;
- ✓ Investigação das informações recuperadas;
- ✓ Preenchimento do relatório do caso;
- ✓ Conclusão do caso.

  - ➢ O trabalho de processar as evidências é composto de quatro parte básicas, que consistem na Coleta, Análise, Exame e Documentação das mesmas.

Avaliação inicial do caso

- ✓ Situação do caso;
- ✓ Natureza do caso;
- ✓ Questões específicas;
- ✓ Tipo de evidências;
- ✓ Sistema operacional utilizado pelo suspeito;
- ✓ Formato do disco;
- ✓ Localização das evidências;
- ✓ Motivações do suspeito.

Ciclo de uma investigação



Recursos necessários

- ✓ Disponibilidade de profissionais habilitados e com expertise para o caso;
  - ➢ Ter certeza de que o perito tenha capacidade, se necessário, de testemunhar em um tribunal;
  - ➢ O perito é capaz de explicar a metodologia utilizada ao logo da investigação de forma simples e sem fazer uso de terminologias;
  - ➢ O perito é capaz de explicar questões do júri utilizando analogias, como por exemplo, a de arquivos em espaços ocultos (ex. biblioteca);

Recursos necessários (continuação)

- ✓ Disponibilidade dos recursos físicos e lógicos necessários;
  - ➢ Mídias esterilizadas (processo documentado);
  - ➢ Etiquetas para provas;
  - ➢ Câmera fotográfica;
  - ➢ Formulário de cadeia de custódia;
  - ➢ Envelopes para provas;
- ✓ Definir atribuições de cada membro da equipe;
- ✓ Definir qual perito fará o deslocamento se necessário até o local do incidente;

Cena do Incidente

- ✓ Isolar a área;
- ✓ Fotografar todo o ambiente e os equipamentos detalhadamente (conexões, anotações, telas de equipamentos);
- ✓ Se possível filmar o ambiente;
- ✓ Fazer anotações detalhadas do que está sendo visualizado;
  - ➢ Detalhes como fotografias e objetos pessoais podem auxiliar em descobertas de senhas;
- ✓ De acordo com os quesitos, definir a necessidade de mudar o status dos equipamentos a ser investigados (Coleta Live ou puxar o cabo de força Post-Mortem);

Coleta Live

- ✓ Documentar todas as etapas do processo;
- ✓ Fotografar conexões do equipamento;
- ✓ Utilizar Pendrive com Kit de Ferramentas pré-compiladas;
- ✓ Coletar dados voláteis:
  - Data/Hora do sistema;
  - Identificação do equipamento;
  - Sistema operacional;
  - Estado da memoria;
  - Tempo de utilização do equipamento;
  - Tempo de funcionamento;
  - Usuário(s) logado(s);
  - Configuração IP;
  - Estado das conexões;
  - Tabela de roteamento;
  - Utilização do(s) disco(s);
  - Processos em execução,
  - Lista de todos os arquivos do equipamento;
  - Hash de todos os arquivos;

Coleta Post-Mortem

- Documentar todas as etapas do processo (data hora inicial e final);
- Abrir equipamento;
- Fotografar conexões internas e externas do equipamento;
- Desconectar o(s) disco(s) para cópia (modo somente leitura ou utilizar bloqueador de escrita);
- Anotar os dados do(s) disco(s) no Formulário de Custódia;
- Etiquetar o(s) Disco(s);
- Conectar o(s) Disco(s) a estação forense para realizar 2 cópias bit-a-bit;
- Embalar, lacrar e etiquetar o(s) disco(s);
- Fotografar o(s) discos(s) etiquetados;

Atividade

- **Entender todas as novas leis para crimes na internet propostas pelo deputado Eduardo Azeredo no projeto de lei 84/99 -** http://www.terra.com.br/noticias/tecnologia/infograficos/crimes-da-internet/

- **Game Forense**
  - http://real-forensic.com/