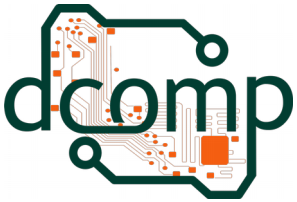
Universidade Federal do Espírito Santo
Centro de Ciências Agrárias – CCENS UFES
Departamento de Computação



Busca e apreensão de provas

Computação Forense

Site: http://jeiks.net
E-mail: jacsonrcsilva@gmail.com

Tópicos

- Mandado de Intimação;
- Provas Digitais: métodos e padrões;
- Técnicas e padrões para a preservação de dados;
- Emissão de relatórios no trabalho de perícia.

Mandado de Intimação

- Mandado de intimação:
  - instrumento pelo qual a autoridade policial dá ciência a alguém que deverá comparecer em sede policial e prestar as informações, reconhecer pessoas ou prestar serviços necessários, como de perícia;
  - Por aplicação analógica, deve o delegado de polícia ou o juiz se valer das disposições dos arts. 351 a 372 do CPP, no que for aplicável, para expedição do mandado de intimação;
  - O amparo legal para expedição deste instrumento encontra guarida no próprio art. 6º, e seus incisos III, IV, V e VI, do Código de Processo Penal, consoante à aplicação do art. 3º do código, que permite a interpretação analógica e a integração harmônica entre os dispositivos atinentes a ação penal e os do inquérito policial.

Mandado de Intimação Exemplo

Processo: 2013.11.182918216315-2

Requerente: Nome da Empresa requerente

O Excelentíssimo Senhor juiz, José da Silva, manda ao oficial de justiça ou a quem for este distribuído, que proceda à INTIMAÇÃO de **Fulano de Tal** para prestar serviço de perícia neste processo, sendo o mesmo responsável por obter as informações listadas no ANEXO I.

O perito intimado possui duas semanas para apresentar seu parecer.

Assinatura do Juiz

Iniciando o trabalho de perícia

- Alguns procedimentos executados pela autoridade policial durante a inquirição são:
  - dirigir-se ao local e preservar o estado e a conservação das coisas até a chegada dos peritos criminais;
  - apreender os objetos que tiverem relação com o fato, após liberados pelos peritos;
  - colher todas as provas que servirem para o esclarecimento do fato e suas circunstâncias;
  - proceder a reconhecimento de pessoas e coisas e a acareações;
  - determinar, se for caso, que se proceda a exame de corpo de delito e a quaisquer outras perícias;
  - …

Iniciando o trabalho de perícia

- Quatro etapas básicas:
  - Coleta:
    - Nesta etapa, o perito deve isolar a área, identificar equipamentos e coletar, embalar, etiquetar e garantir a integridade das evidências, garantindo assim a cadeia de custódia.
  - Exame:
    - Nesta fase, deve-se identificar, extrair, filtrar e documentar os dados relevantes à apuração.
  - Análise:
    - Nesta etapa, o perito computacional deve identificar e correlacionar pessoas, locais e eventos, reconstruir as cenas e documentar os fatos;
  - Resultado:
    - Neste momento deve-se redigir o laudo e anexar as evidências e demais documentos.

Finalizando a coleta...

- Ao terminar o processo de coleta, a autoridade policial fará um “Auto de Busca e Apreensão e Depósito”, informando:
  - A data;
  - O local do crime;
  - O número do processo;
  - O Juiz, a Vara Civil e a requerente;
  - As informações encontradas pelos peritos (ex.: softwares e documentos encontrados);
  - Os objetos que deverão ser apreendidos;
  - Assinaturas da autoridade policial, dos peritos e do(s) requerido(s).

Provas Digitais: Métodos e padrões

- Formatos de armazenamento da evidência digital:
  - RAW: cópia bit a bit dos dados da mídia original de armazenamento.
    - Vantagens: preserva todos os dados; pode ignorar setores com erros da mídia original; pode ser lido por diversos programas forenses.
    - Desvantagens: necessita de espaço de armazenamento igual ou superior à mídia de origem; diversas ferramentas gratuitas não conseguem recuperar os erros da mídia original.
  - Formatos proprietários: várias ferramentas proprietárias de cópia de dados possuem seus próprios formatos para coletar a evidência digital:
    - Vantagens: Costumam fornecer características adicionais, como comprimir a imagem de cópia; dividir a imagem em diversos segmentos; adicionar metadados à imagem (data de aquisição, hash, etc.).
    - Desvantagens: a imagem gerada não pode ser lida por outros aplicativos; o tamanho do arquivo costuma ser limitado (650MB à 2GB).
  - ...

Provas Digitais: Métodos e padrões

- Formatos de armazenamento da evidência digital:
  - Advanced Forensic Format (AFF): formato livre para a cópia da mídia original de armazenamento. Vantagens:
    - criar imagens comprimidas ou não;
    - sem restrições do tamanho do arquivo de cópia;
    - prover espaço dentro da imagem ou de arquivos segmentados para metadados;
    - ter um design simples e extensivo;
    - ser livre para diversas plataformas e Sos;
    - oferecer checagem de consistência interna.

  Mais informações em: <http://afflib.sourceforge.net/>

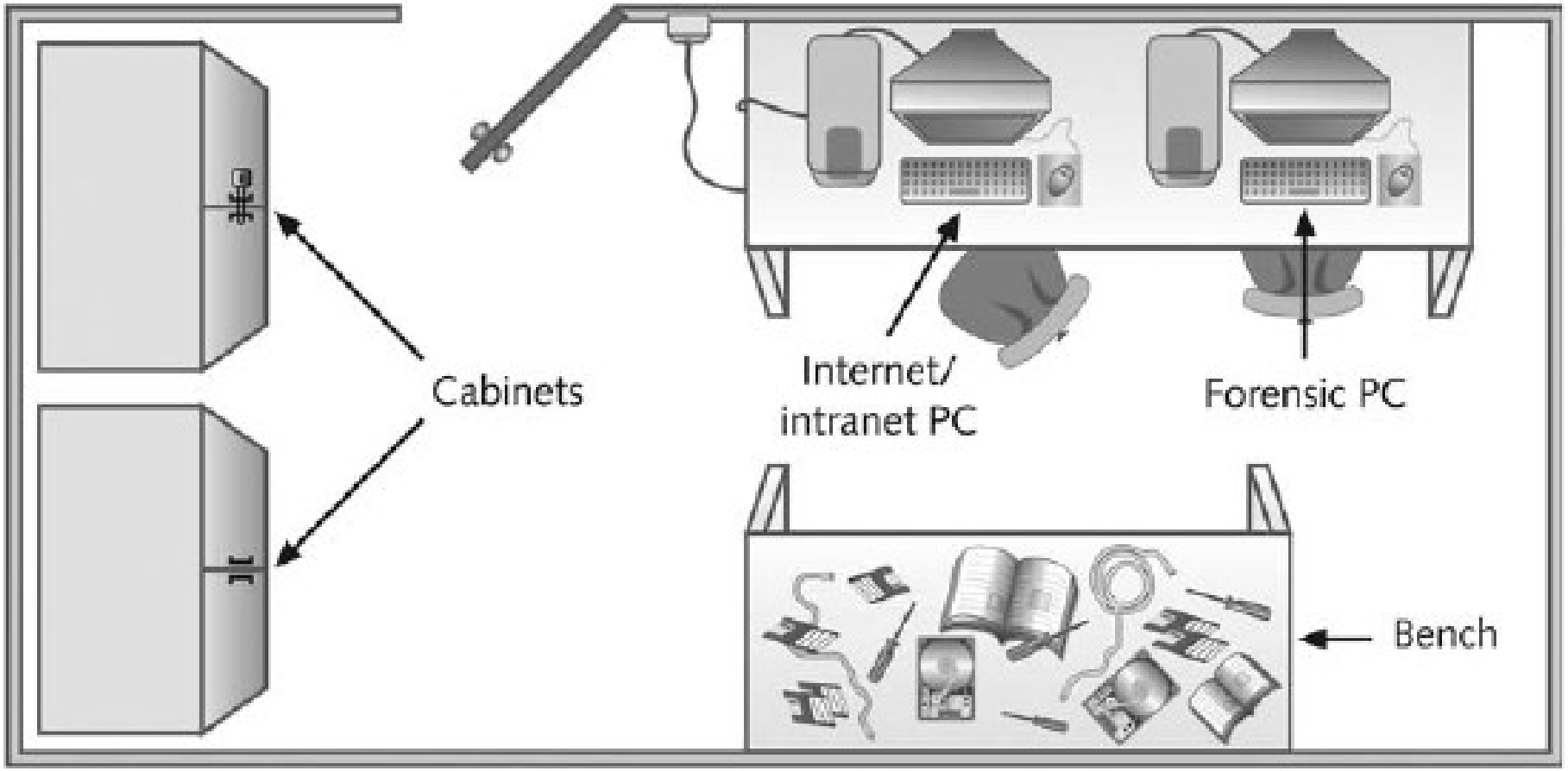
Exame e análise

Após o cumprimento de um mandado de busca e apreensão que tenha resultado na coleta de equipamentos computacionais, deve-se encaminhar o material confiscado para um laboratório de informática capacitado a fim de realizar os exames forenses necessários.

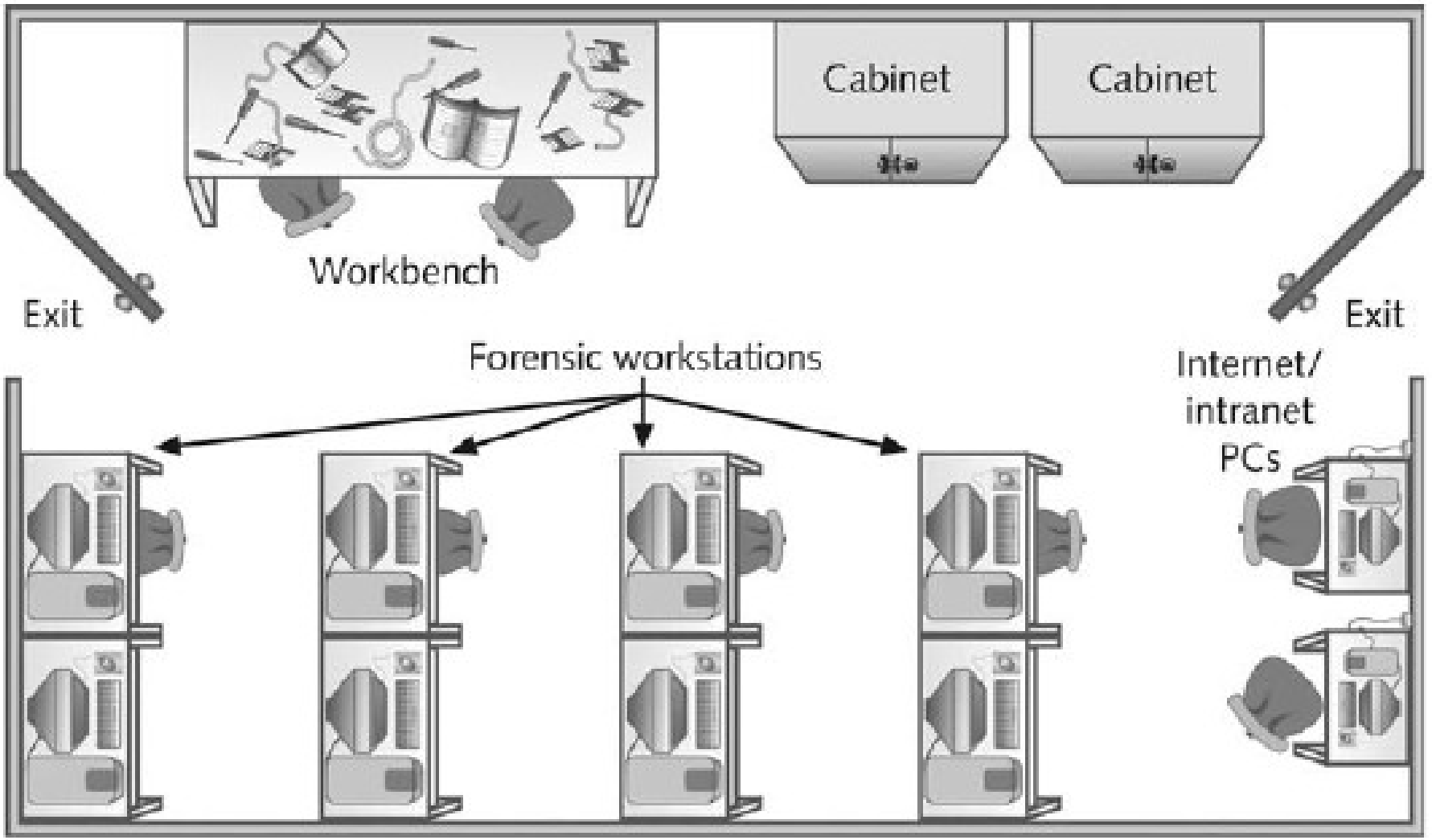
Provas Digitais: Métodos e padrões

- Laboratório Forense:
  - Ser restrito ao seu acesso, pois as evidências do crime estão lá;
  - Deve ser um local para controlar sua evidência e assegurar sua integridade;
  - Deve ser uma sala pequena, com paredes do chão ao teto;
  - Ter um acesso único com um mecanismo de trava, como chave ou código de acesso. A chave e o código de acesso deve ser limitado às pessoas autorizadas;
  - Ter um recipiente seguro, como um cofre ou um armário de arquivos com um cadeado de qualidade que tranque suas gavetas;
  - Ter um registro de visitas, listando todas as pessoas que acessaram o laboratório.

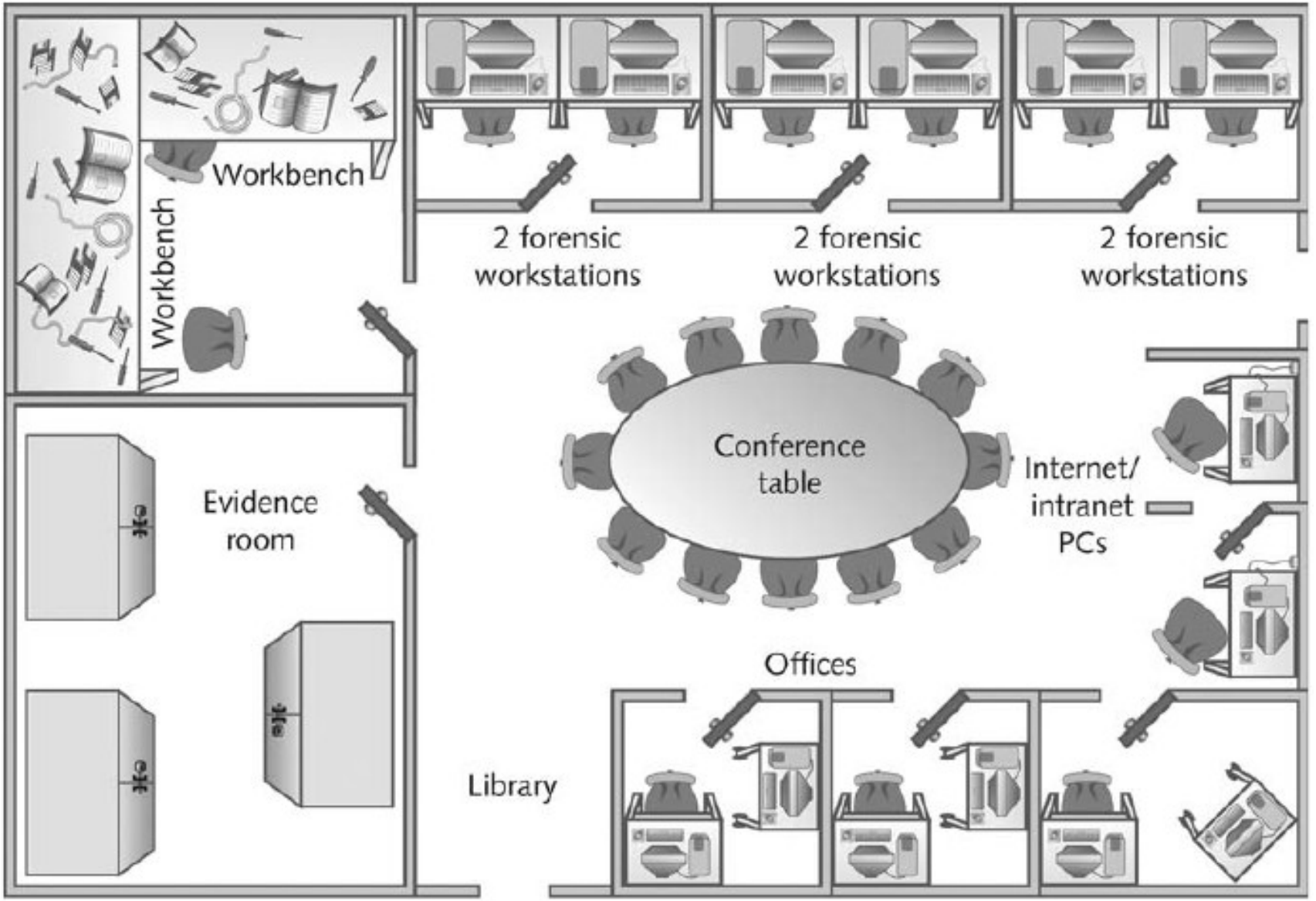
Laboratório pequeno (doméstico)



Laboratório Médio



Laboratório Regional



Laboratório – Periféricos

- Hardware:
  - Cabos IDEs de diversas pinagens, tanto ATA-33, quanto ATA-100, ou mais rápido;
  - Cabos de fita para disquetes;
  - Placas SCSI, de preferência ultra-wide;
  - Placas gráficas, tanto *Peripheral Component Interconnect* (PCI), quanto *Accelerated Graphics Port* (AGP);
  - Cabos de alimentação extras;
  - Diversos discos rígidos (vários para apagar e utilizar à vontade);
  - Pelo menos dois adaptadores para discos rígidos de notebook: IDE/ATA padrão, drives SATA, …;
  - Chaves de fenda, Phillips, soquete, etc.;
  - Uma pequena lanterna;
  - O que mais achar necessário.

Técnicas e padrões para a preservação de dados

- Refrescamento:
  - Transferir a informação de um suporte físico para outro mais atual antes que o primeiro se deteriore ou torne-se obsoleto;
- Emulador:
  - Utilizar emuladores para reproduzir o comportamento de uma plataforma de hardware e/ou software.
- Migração/conversão:
  - Transferir uma configuração de software/hardware para outra tecnologia. Ex.: de HD IDE para SATA.
- Encapsulamento:
  - Preservar a evidência até que ela seja utilizada. Ex.: alguma informação que não possa ser utilizada por ainda não existir emulador existente.

Análise das informações

- Forma segura de analisar os dados:
  - Manter a mídia original em modo somente leitura;
  - Efetuar uma cópia da mídia original;
  - Analisar a cópia e nunca a mídia original;
- Buscar padrões conhecidos com ferramentas forenses.
- Não se prender somente a análise dos arquivos comuns. Buscar resgatar as informações/arquivos que estão escondidos.

Emissão de relatórios no trabalho de perícia

- O laudo de perícia forense, em 3 vias, deverá conter:
  - Nome, CPF e contatos do perito;
  - Período de realização da perícia forense;
  - Breve relato do ocorrido (inclui notícias iniciais);
  - Dados sobre o hardware periciado;
  - Detalhamento dos procedimentos realizados (um segundo perito deverá ter condições de refazer todos os procedimentos, caso alguma autoridade requeira);
  - Dados, fatos e indícios relevantes encontrados;
  - Conclusão e recomendações;
  - Apêndices (inclui certificado de integridade) e anexos. Material produzido pelo perito.

Caso de estudo:

http://eriberto.pro.br/wiki/index.php?title=Forense_caso_00