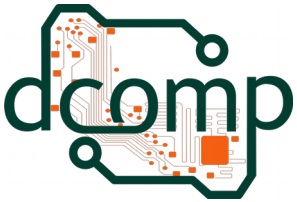
Universidade Federal do Espírito Santo
Centro de Ciências Agrárias – CCENS UFES
Departamento de Computação



Procedimentos Legais

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

Tópicos

- Conceitos utilizados em computação forense;
- Como atuar com evidências;
- Cadeia de Custódia;
- Jurisdições.

Conceitos

- Cadeia de custódia (*Chain of custody*):
  - Documentação cronológica do movimento, localização e possessão da evidência, tanto físicas quanto digitais.
  - Como exemplo, podem ser informações sobre:
    - quem está de posse do disco rígido do computador invadido,
    - onde está guardada a cópia do disco rígido,
    - qual a *hash* criptográfica da evidência original, etc.
- Cena do crime digital (*Digital crime scene*):
  - O ambiente virtual criado pelo software onde existe evidência digital de um crime ou incidente.
- Cena do crime físico (*Physical crime scene*):
  - O ambiente físico onde existe evidência física de um crime ou incidente.

Conceitos

- *Data carving* ou *file carving*:
  - Processo de busca por informações ou conteúdo de arquivos.
- Dados (*Data*):
  - Informação em forma analógica ou digital que pode ser transmitida ou processada.
- Esterilização da mídia (*Media sanitization*):
  - Processo para apagar o conteúdo original da mídia que irá receber a imagem a ser analisada, escrevendo-se zeros, em dígitos binários, no disco, de modo que dados previamente contidos na mídia não influenciem na análise da imagem.

- Esterilizando a mídia -

No Linux, os dispositivos estão presentes no diretório /dev.
Para verificar quais são as partições existentes, pode-se dar o comando:

```
> cat /proc/partitions
```

E para verificar qual a partição do pendrive inserido, basta verificar o último dispositivo reconhecido pelo kernel, com o comando:

```
> dmesg | tail
```

Após encontrar qual é a mídia que deseja esterilizar, pode-se executar:

```
> shred -v /dev/DISPOSITIVO
ou
> dd if=/dev/random of=/dev/DISPOSITIVO
ou
> dd if=/dev/zero of=/dev/DISPOSITIVO
```

Conceitos

- Evidência digital (*Digital evidence*):
  - Informação de valor probatório que é armazenada ou transmitida em forma binária.
  - Informação digital que pode estabelecer que um crime foi cometido, que pode prover um elo entre um crime e a vítima, ou que pode prover um elo entre o crime e o seu executor.
- Evidência física (*Physical evidence*):
  - Objetos ou rastros físicos que podem estabelecer que um crime foi cometido, prover um elo entre um crime e a sua vítima, ou que pode prover um elo entre o crime o seu executor.
- Forense (*Forensic*):
  - Uso da ciência e tecnologia na investigação e estabelecimento de fatos ou evidências em um tribunal.

Conceitos

- Imagem (*Image*):
  - Duplicata bit a bit dos dados originais.
- Incidente (*Incident*):
  - Um evento único ou uma série de eventos de segurança da informação não desejado ou não esperado que tem uma probabilidade significante de comprometer as operações de negócio e de ameaçar a segurança da informação.
- Investigação forense digital:
  - Processo de se responder, de maneira forense, a perguntas sobre estados e eventos digitais, onde os procedimentos e técnicas utilizados irão permitir que os resultados possam ser utilizados em um tribunal.

Conceitos

- Live analysis:
  - Captura, de acordo com a ordem de volatilidade, e análise de informações com o computador ligado
- **MAC**times:

  Timestamps com informações sobre os últimos tempos de:
  - **M**odification time (mtime): última vez que o conteúdo do arquivo ou diretório foi modificado.
  - **A**ccess time (atime): última vez que o arquivo ou diretório foi acessado.
  - **C**hange time (ctime): última vez que informações de metadados do arquivo ou diretório foram modificadas (*chmod*, por exemplo). Pode ser utilizado como aproximação de quando o arquivo ou diretório foi deletado.
  - Delete time (dtime): indica quando o arquivo ou diretório foi deletado.

Utilização do comando stat:
> echo nome > arquivo.txt
> stat arquivo.txt
> chmod +x arquivo.txt
> stat arquivo.txt
> echo outro nome > arquivo.txt
> stat arquivo.txt

Obtenção dessas informações em linguagem C:
> arquivo exemplo: FileStat.c

Somente o MAC obtido em linguagem C:
> arquivo MAC.c

Conceitos

- Ordem de volatilidade (*Order of volatility*):
  - Ordem na qual as informações mais voláteis, de acordo com o seu tempo (expectativa) de vida, vão sendo perdidas.

- Princípio da troca de Locard (*Locard's Exchange Principle*):
  - Princípio que diz que qualquer pessoa ou objeto que entra na cena crime leva algo da cena e deixa algo seu na cena.

- *Post-mortem analysis*:
  - Captura e análise de informações com o computador desligado.

Como atuar com evidências

- Antes da coleta de dados, é necessário:

  1. **esterilizar** todas as mídias que serão utilizadas ou usar mídias novas a cada Investigação;

  2. certificar-se de que todas as **ferramentas** (softwares) que serão utilizadas estão devidamente **licenciadas** e prontas para utilização;

  3. verificar se todos os **equipamentos** e **materiais** necessários estão a **disposição**;

  4. quando chegar ao local da investigação, o perito deve providenciar para que **nada** seja **tocado** sem seu consentimento, com o objetivo de proteger e coletar todos os tipos de evidências;

  5. os investigadores devem **filmar** ou **fotografar** o ambiente e registrar detalhes sobre os equipamentos como: marca, modelo, números de série, componentes internos, periféricos, etc.

  6. manter a cadeia de custódia.

Cadeia de Custódia

- A **Cadeia de Custódia** é um processo usado para:
  - manter e documentar a história cronológica da evidência,
  - para garantir a idoneidade e
  - Para garantir o rastreamento das evidências utilizadas em processos judiciais.
- Procedimentos relacionados à evidência (coleta, manuseio e análise) podem
  - Acarretar falta de integridade da prova,
  - Provocar danos irrecuperáveis no material coletado,
  - Comprometer a idoneidade do processo e
  - Prejudicar a sua rastreabilidade.

Cadeia de Custódia

- Para controlar as fases do processo de coleta de evidências, torna-se necessário adotar uma **Cadeia de Custódia**.
- É utilizada:
  - Para manter e documentar a história cronológica da evidência,
  - Para rastrear a posse e o manuseio dos dados e equipamentos desde a coleta, passando pelo transporte, recebimento e armazenamento, até a análise e entrega do laudo.
- A Cadeia de Custódia refere-se então:
  - Ao tempo em curso no qual os dados e equipamentos estão sendo manuseados e inclui todas as pessoas que os manuseia.
- Esta terminologia vem sendo legalmente utilizada para garantir a identidade e integridade das amostras em todas as etapas do processo.

Cadeia de Custódia

- As evidências devem ser manipuladas de forma cautelosa,
  - Evitando futuras alegações de adulteração ou má conduta que possam comprometer as decisões relacionadas ao caso em questão.
- Sua importância inicia no chamado Princípio da Troca de Locard:
  - O cientista forense Edmon Locard exprimiu a teoria em que

    "através do contato de dois itens, haverá uma permuta”
  - Explica que qualquer pessoa ou qualquer coisa que entra em um local de crime:
    - leva consigo algo do local e deixa alguma coisa para trás quando sai.

Cadeia de Custódia

- O Princípio da Troca de Locard deixa claro que:
  - Todo contato entre quaisquer pessoas ou objetos com a cena do crime pode produzir vestígios, e por menores que sejam, poderão servir como base para o esclarecimento dos fatos de um crime.
- Assim:
  - Tudo que for apreendido deve ser descrito em um documento (denominado auto) pela autoridade competente.
  - Nesse momento, é importante conhecer e utilizar técnicas para a correta descrição dos equipamentos, garantindo sua cadeia de custódia.

Cadeia de Custódia

FORMULÁRIO DE CADEIA DE CUSTÓDIA							
Número do Caso:		20130910					
DETALHES DA MÍDIA OU EQUIPAMENTO							
ITEM	DESCRIÇÃO						
1	HD DO PC COM NÚMERO DE SÉRIE 2153413816						
FABRICANTE		MODELO		NÚMERO DE SÉRIE			
SAMSUNG		SGM2GB		HSGA716214			
SOBRE A IMAGEM DOS DADOS							
DATA	HORA	CRIADA POR		FERRAMENTA UTILIZADA			
10/09/2013	09:43:00	NOME DO PERITO		dd (linux)			
TIPO DE CÓPIA		HASH (md5sum)					
DISCO COMPLETO		33c74d29059b49b647bab5418ba48547					
CADEIA DE CUSTÓDIA							
CÓDIGO	ORIGEM	DATA	HORA	DESTINO	DATA	HORA	
1	LOCAL DE APREENSÃO	10/09/2013	13:05:00	PERÍCIA	10/09/2013	14:00:00	

Como agir no local da perícia

- Evitar a entrada de pessoas estranhas no local sem autorização/supervisão do perito;
- Não ligar equipamentos computacionais que estejam desligados;
- Se necessário, interromper as conexões de rede eventualmente existentes e retirar a fonte de energia dos equipamentos computacionais, desligando-os.
  - Exceto quando há possibilidade de flagrante de delito;
- Não é recomendado utilizar os equipamentos computacionais do local para verificações de evidências;
- Só apreender equipamentos computacionais se houver suspeita de que eles podem conter as evidências;
- Quanto às evidências eletrônicas, saber que informações digitais estão contidas nas mais variadas formas e locais.

Considerações de coleta

- Nada pode ser desconsiderado a princípio.
  - Um computador pode conter uma série de informações, sejam elas em arquivos de texto, lista de contatos, arquivos multimídia, bancos de dados, e-mails, históricos de internet, planilhas eletrônicas e muitos outros formatos de dados.
  - Uma secretária eletrônica contém informações de ligações realizadas e recebidas, agenda com nomes e números, gravações, além de outras informações conforme suas funcionalidades.
  - Até uma simples placa de rede pode comprovar uma transferência de informações entre dois computadores.
  - Em um cartão de memória podem existir vídeos, imagens, sons.
  - O buffer de uma impressora pode fornecer informações sobre arquivos que foram impressos.

Jurisdição e Legislação Brasileira

Jurisdição

- **Jurisdição**:
  - É o poder legal para interpretar e ministrar a lei.
- Considerações:
  - Devido ao crescimento exponencial da tecnologia as leis e estatutos existentes simplesmente não conseguem acompanhar sua taxa de mudança.
  - Quando estatutos ou regulamentos não existem para determinado caso, é utilizada a **Jurisprudência**.
- Jurisprudência:
  - Ciência do direito e da legislação;
  - Maneira especial de interpretar e aplicar as leis.

Jurisprudência

- A jurisprudência permite:
  - Utilizar casos anteriores semelhantes ao atual;
  - Abordando-o e interpretando as leis utilizadas sobre o mesmo para avaliar o novo caso;
  - Assim, cada novo caso pode ser avaliado por seu próprio mérito e questões.

- Mesmo assim, esteja ciente de que a lei caso não envolve novos tipos de crimes que ainda não possuem lei específica.

Exemplos

- A universidade de Rhode Island cita muitos casos em que os problemas ocorridos no passado e que podem ser utilizados como exemplos para casos atuais: <http://dfc.cs.uri.edu>

Um exemplo foi de um investigador que se deparou com fotos de pedofilia em um computador **enquanto** resolvia seu caso de drogas.

Ao invés dele esperar um **novo** mandado para tratar esse novo crime, ele continuou suas investigações sobre tais imagens.

Ao perceber o que ocorrera, o criminoso **apagou** as fotos, **eliminando** as evidências do crime e o **investigador não pôde** fazer **nada**.

Os investigadores atuais devem procurar as leis referentes e se manter atualizados para trabalhar nos casos, além de procurar não repetir casos anteriores, como este.

Legislação Brasileira

- O Brasil é regido por diversas leis que atendem particularmente cada necessidade.
- Nestas leis, como o Código Penal (CP) são descritos
  - Os direitos,
  - As obrigações e
  - As penas para todos os cidadãos brasileiros, salvo aqueles que possuem foro privilegiado.
- As questões relacionadas para o desenrolamento de crime tipificado pelo Código Penal são descritas no Código de Processo Penal (CPP) em vigor a partir da publicação do Decreto de Lei nº 3.689, de 3 de Outubro de 1941.
- Dentre estas questões encontram-se os artigos relacionados à perícia criminal de modo geral.

Legislação Brasileira

- Um perito somente deve atuar caso seja solicitado,
  - De nenhuma forma ele poderá realizar uma perícia baseado apenas em seu instinto;
  - Caso isso ocorra o laudo apresentado não terá nenhum valor jurídico.
- Para que ele possa realizar uma perícia:
  - a autoridade policial ou o Ministério Público deve o requerer formalmente, conforme o Artigo 6º.
- Artigo 6º:
  - “Logo que tiver conhecimento da prática da infração penal, a autoridade policial deverá:

    I – dirigir-se ao local, providenciando para que não se alterem o estado e conservação das coisas, até a chegada dos peritos criminais.”

Legislação Brasileira

- O Artigo 178 descreve que este requerimento deve ser entregue ao responsável pelo instituto de perícias que por sua vez encaminha para o perito da área solicitada.
- Este Artigo se relaciona com o Artigo 159:
  - "Art. 159 - O exame de corpo de delito e outras perícias serão realizados por perito oficial, portador de diploma de curso superior (alterado pela Lei no 11.690, de 09 de junho de 2008).

    § 1° - Não havendo peritos oficiais, o exame será realizado por duas pessoas idôneas, portadoras de diploma de curso superior, escolhidas, de preferência, entre as que tiverem habilitação técnica relacionada à natureza do exame.

    § 2° - Os peritos não oficiais prestarão o compromisso de bem e fielmente desempenhar o encargo."
- "Art. 178 - No caso do art. 159, o exame será requisitado pela autoridade ao diretor da repartição, juntando-se ao processo o laudo assinado pelos peritos."

Legislação Brasileira

- Além do perito não poder atuar de forma autônoma em uma perícia ele deve atender a alguns requisitos, conforme a legislação.
- O preenchimento destes requisitos nada mais serve como uma proteção para que o laudo seja realizado com maior clareza e veracidade possível.
- O CPP traz em seu texto o que é necessário para ter as atribuições de um perito. Quando inexiste este especialista na instituição estadual ou federal para alguma área em especifico,
  - a escolha do perito fica a cargo do responsável do caso, o delegado ou promotor/juiz, que deve nomear algum profissional **capacitado** e **com curso superior** para tomar de posse das evidências e elaborar o laudo pericial.

Legislação Brasileira

- Este profissional, descrito no CPP como perito não oficial, precisa dominar o assunto do qual ele realizará a perícia, não podendo ser:
  - “Art. 279 - Não poderão ser peritos:

    I -os que estiverem sujeitos à interdição de direito mencionada no Art. 47 do Código Penal;

    II - os que tiverem prestado depoimento no processo ou opinado anteriormente sobre o objeto da perícia;

    III - os analfabetos e os menores de 21 (vinte e um) anos”

Legislação Brasileira

- Os peritos, tanto os oficiais como os não-oficiais, são pessoas de **confiança** do juiz, conforme Art. 275.
  - É então necessário que o perito **cumpra** os prazos estabelecidos no CPP.
- O Art. 277 relaciona a **obrigatoriedade** do perito em realizar a atividade quando for escolhido pela autoridade.
- Se **não cumprir** com as obrigações ou se **prejudicar** a perícia,
  - O perito será **enquadrado** nos itens já descritos na legislação.
- O Art. 278 descreve a solicitação de **prisão** do perito caso ele **não compareça** sem justa causa.
- De acordo com o Art. 105,
  - O perito também pode ser excluído por solicitação de alguma da partes,
  - Mas esta deve argumentar e provar os motivos para o afastamento do profissional da atividade que será julgada pelo juiz.

Legislação Brasileira

- Toda essa preocupação também visa que o **laudo** final contenha os fatos **realmente** ocorridos.
- Mais considerações:
  - Art. 275 - O perito, ainda quando não oficial, estará sujeito à disciplina judiciária.
  - Art. 277 - O perito nomeado pela autoridade será obrigado a aceitar o encargo, sob pena de multa de cem a quinhentos mil-réis, salvo escusa atendível.
  - Parágrafo único - Incorrerá na mesma multa o perito que, sem justa causa, provada imediatamente:

    a) deixar de acudir à intimação ou ao chamado da autoridade;

    b) não comparecer no dia e local designados para o exame;

    c) não der o laudo, ou concorrer para que a perícia não seja feita, nos prazos estabelecidos.

Legislação Brasileira

- Mais condutas:
  - Art. 278 - No caso de não-comparecimento do perito, sem justa causa, a autoridade poderá determinar a sua condução.
  - Art. 105 - As partes poderão também **arguir** de suspeitos os peritos, os intérpretes e os serventuários ou funcionários de justiça, decidindo o juiz de plano e sem recurso, à vista da matéria alegada e prova imediata.

Legislação Brasileira

- Objetivo Final do perito (Art. 160):
  - elaborar um laudo minucioso,
  - sempre observando os prazos,
  - explicando todos os detalhes da perícia realizada e das informações encontradas.
- O laudo deve ser elaborado por dois peritos (Art. 159)
  - Se houver divergências entre eles, cada um deve elaborar um laudo em específico com as suas conclusões (Art. 180).
  - Pode também ocorrer de a autoridade solicitar novamente uma perícia para outros peritos, caso ele não se sinta confortável com o laudo inicialmente apresentado ou se os peritos não observarem as formalidades e deixaram obscuras as conclusões (Art. 181).

Legislação Brasileira

- Todas as formalidades relacionadas à perícia sempre devem ser levadas em consideração, pois:
  - O perito é uma pessoa de confiança do juiz sendo ela às vezes o fator decisivo para esclarecer um caso.
- A legislação vigente indica todos os quesitos que o perito deve observar,
  - tanto para preservar a perícia como a ele mesmo,
  - Se houver má fé do perito:
    - Poderá pagar uma multa ou
    - Até ser preso caso se negue ou prejudique a realização da perícia.
- O juiz tem o livre-arbítrio para **aceitar** ou **não** a conclusão do laudo pericial.
  - Art. 182: O juiz não ficará adstrito ao laudo, podendo aceitá-lo ou rejeitá-lo, no todo ou em parte.

Legislação Brasileira

- Notícia de Maio de 2012:
  - Reproduções fotográficas da intimidade da atriz Carolina Dieckmann foram **indevidamente** divulgadas em diversos sítios eletrônicos da rede mundial de computadores.
  - Segundo os fatos noticiados, ocorreu da seguinte forma:
    - após deixar um computador pessoal em um estabelecimento de assistência técnica especializada,
    - violaram a sua conta de correio eletrônico, obtendo as imagens.

      Começaram a chantagear a atriz, sob pena de divulgar as imagens tidas como comprometedoras.

Legislação Brasileira

- Este caso foi a mola propulsora da edição da Lei n. 12.737, de 30 de novembro de 2012 (DOU 03/12/2012).
- Lei apelidada de “Lei Carolina Dieckmann”,
  - “dispõe sobre a tipificação criminal de delitos informáticos;
  - altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal;
  - e dá outras providências”.
- Em seu artigo 2º, o legislador criou uma norma penal incriminadora, que passa a integrar:
  - a Seção IV (“Dos crimes contra a inviolabilidade dos segredos”),
  - do Capítulo VI (“Dos crimes contra a liberdade individual”),
  - do Título I (“Dos crimes contra a pessoa”),
  - do Código Penal.

Lei Carolina Dieckmann

“**Invasão de dispositivo informático**

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:

Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa”.

Mais informações em: <http://jus.com.br/artigos/24406/lei-carolina-dieckmann-e-a-definicao-de-crimes-virtuais>

Legislação Brasileira

- Maio de 2013:
  - Alteração da Lei Carolina Dieckmann.
  - Agora a lei também criminaliza a invasão de sites com interrupção de serviços fornecidos via Internet.
- Porém, para especialistas a mudança legal não foi precisa:
  - "Dispositivos informáticos são computadores, *tablets* e celulares. Mas como fica a questão de furto de dados de redes sociais, quando o servidor não esteja instalado no Brasil?"
  - "Pela mudança, a invasão será crime se tiver como fim a obtenção, adulteração ou destruição de dados ou informações. Ou seja, se você invade e só bisbilhota, não é considerado crime pela nova lei".

<http://www1.folha.uol.com.br/cotidiano/1255833-lei-que-pune-invasao-hacker-em-celulares-e-computadores-entra-em-vigor.shtml>