

# Segurança Computacional

## Computação Forense

Ricardo de la Rocha Ladeira  
{[ricardo.ladeira@ifc.edu.br](mailto:ricardo.ladeira@ifc.edu.br)}



## Computação Forense

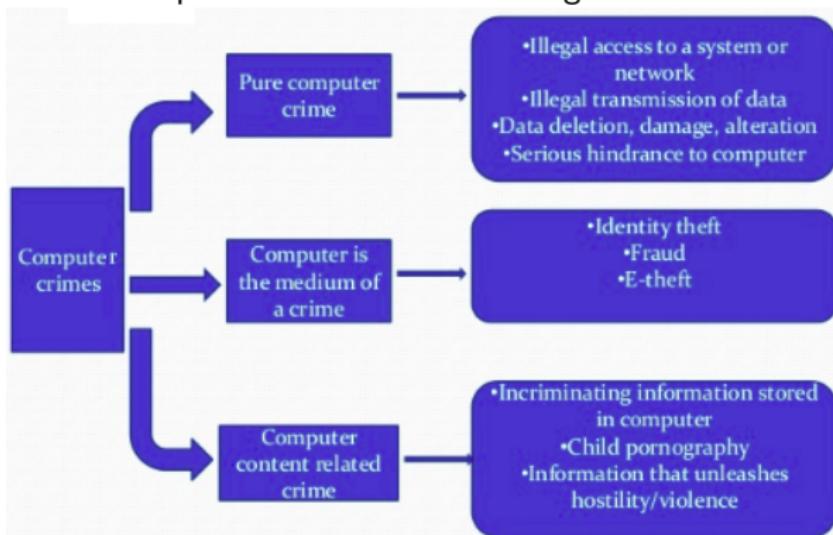
- ▶ Uso do conhecimento científico para análise, identificação, coleta, preservação, recuperação e apresentação de evidências digitais para investigações de eventos criminais.
- ▶ **Forense** significa *relativo ao foro, da justiça, do tribunal*.

# Computação Forense

## Crimes Digitais

► **Crime Digital** é a transgressão da lei por meio de (redes de) computadores.

Adaptado de [reisebuero-dr-hoegemann.de](http://reisebuero-dr-hoegemann.de).



## Computação Forense

- ▶ Esteganografia
- ▶ Esculpimento de dados/arquivos
- ▶ Recuperação de dados/arquivos

## Esteganografia



- ▶ Alguma diferença visível entre as imagens?

## Esteganografia



► Alguma diferença visível entre as imagens?

```
> diff peter.jpg peter2.jpg
```

```
> java -jar ../Programas/f5.jar x -e out.txt peter2.jpg
```

# Esteganografia



- ▶ Imagem IFe.jpg
- ▶ outguess -r IFe.jpg arquivosaída

## Esteganografia

- ▶ Arte de encobrir mensagens.
- ▶ Objetivo: esconder uma mensagem, de forma que terceiros não percebam que ali há uma comunicação.
- ▶ Pode ser em arquivos de texto, áudio, imagem, vídeo, protocolos...

# Esteganografia

## ► Não é criptografia.

- Diferença: esteganografia serve para ocultar a existência da mensagem, enquanto a criptografia serve para ocultar o significado da mensagem.
- Podem ser usadas em conjunto.

## Esteganografia

- ▶ Comunicação (de bandidos, por exemplo);
- ▶ Compressão de Dados;
- ▶ Segurança da Informação (marca d'água, direitos autorais).
  - ▶ Na verdade, há pequenas diferenças entre esteganografia e marca d'água.
    - ▶ A marca d'água pode ser visível.
    - ▶ A marca d'água é relacionada ao objeto; na esteganografia, a mensagem pode não ter relação com o objeto.
    - ▶ A marca d'água tem cardinalidade 1:N; a esteganografia tem, *a priori*, cardinalidade 1:1.
  - ▶ Na prática, as mesmas técnicas e ferramentas podem ser utilizadas.

# Esteganografia

## Abadia usava Hello Kitty para enviar ordens

10 de março de 2008 • 07h48

AAA |

NOTÍCIA

Segundo análise feita pela DEA, agência antidrogas dos Estados Unidos, as mais de 200 imagens da gatinha japonesa Hello Kitty, encontradas no computador do traficante Juan Carlos Ramirez Abadia, continham mensagens de texto e de voz com ordens para movimentar a cocaína entre os países e sumir com pessoas na Colômbia.

- » Justiça rejeita acordo com Abadia
- » Mansões são arrematadas por R\$ 3,65 mi
- » vc repórter: mande fotos e notícias



Segundo o jornal Folha de S.Paulo, a agência ajudou a Polícia Federal porque o Brasil não tinha toda a tecnologia necessária para realizar a investigação. A técnica utilizada pelo traficante é conhecida como esteganografia. A Al Qaeda utilizou esta técnica para preparar os atentados de 2001.

Além de imagens da Hello Kitty, boneca preferida da mulher de Abadia, outro disfarce utilizado pelo traficante eram fotos de crianças.

A descoberta das ordens enviadas através de imagens pode mudar a situação de Abadia no País. Atualmente, ele responde por lavagem de dinheiro, formação de quadrilha e falsificação de documentos.

[mais notícias de polícia »](#)

## Esteganografia

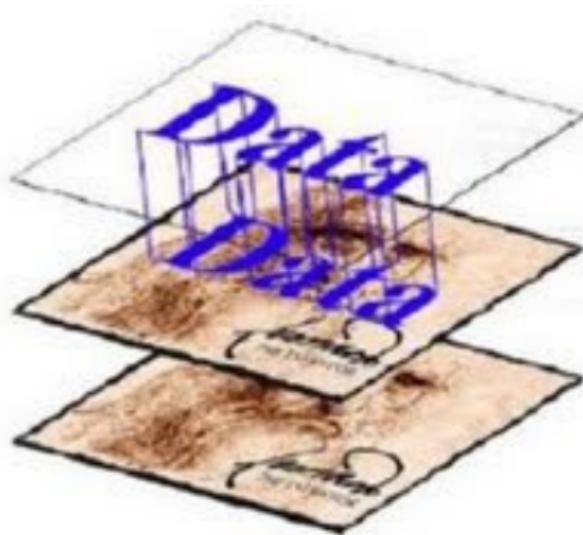
- ▶ **Esteganálise** é a área de estudo do descobrimento de mensagens ocultas.
  
- ▶ Em um processo de comunicação inseguro, o emissor envia um objeto com a mensagem esteganografada e o interceptador que o captura pode esteganalizar o objeto (bem como destruí-lo ou alterá-lo).

# Esteganografia

## Terminologia

- ▶ **Meio de cobertura:** objeto que será utilizado para encobrir a mensagem.
- ▶ **Mensagem:** conjunto de dados que será encoberto pelo meio de cobertura.
- ▶ **Estego-chave:** conjunto de procedimentos que pode encobrir/descobrir a mensagem no meio de cobertura.
- ▶ **Estego-objeto:** produto final, um objeto que resulta da inserção da mensagem no meio de cobertura usando a estego-chave.

# Esteganografia



# Esteganografia

## Classificação

- ▶ Três tipos:

- ▶ **Técnica:** tintas invisíveis e micropontos;
- ▶ **Linguística:** semagrama e acróstico;
- ▶ **Digital:** arquivos de texto, áudio, vídeo, protocolos...

# Esteganografia

Figura: Exemplo de acróstico.

Elizabeth it is in vain you say  
“Love not” — thou sayest it in so sweet a way:  
In vain those words from thee or L. E. L.  
Zantippe’s talents had enforced so well:  
Ah! if that language from thy heart arise,  
Breathe it less gently forth — and veil thine eyes.  
Endymion, recollect, when Luna tried  
To cure his love — was cured of all beside —  
His folly — pride — and passion — for he died.

Fonte: Adaptado de Pinterest.

# Esteganografia

Figura: Exemplo de acróstico.



Fonte: Folha de São Paulo.

## Esteganografia

- ▶ Veremos exemplos de técnicas e ferramentas utilizadas para esteganografia em imagens.

# Esteganografia

## LSB

- ▶ Algoritmo mais “básico” para esteganografar.
- ▶ Insere a informação sempre no bit menos significativo.

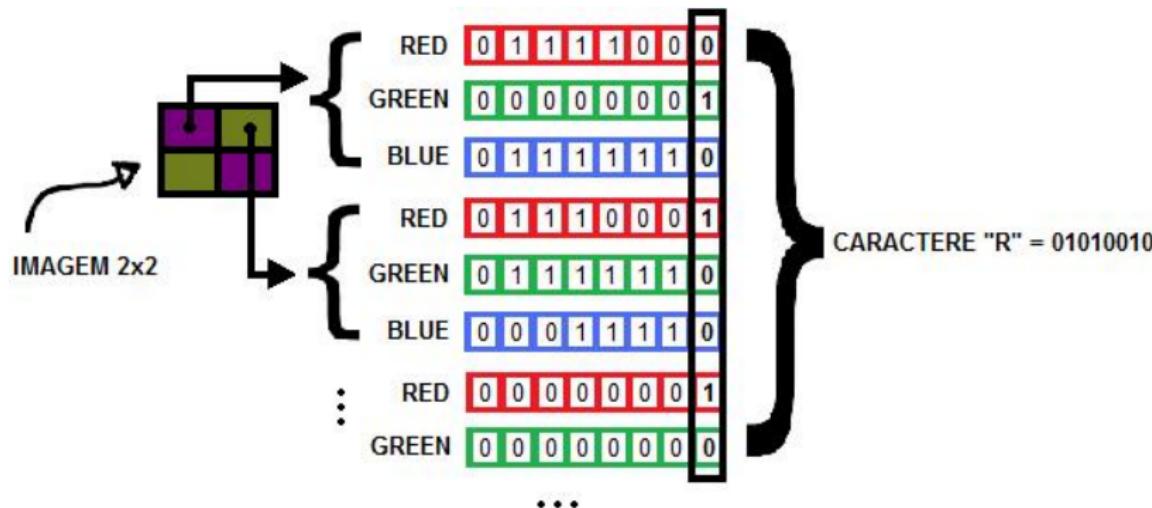


Figura: LSB em imagens RGB24 com texto ASCII.

# Esteganografia

## Outros algoritmos

- ▶ DCT
- ▶ BPCS

# Esteganografia

## Ferramentas

- ▶ JPHS (LSB)
- ▶ F5 (DCT)
- ▶ QTech-Hide&View (BPCS)
- ▶ Outguess (LSB e DCT)
- ▶ Steghide (Teoria dos Grafos)
- ▶ <https://futureboy.us/stegano/encinput.html>
- ▶ <https://futureboy.us/stegano/decinput.html>
  
- ▶ Algumas dessas ferramentas esteganográficas apresentam restrições. Não suportam todo tipo de arquivo de imagem e não suportam mensagens muito extensas.

# Esteganografia

## Ferramentas

► F5

► Esconder um arquivo de texto dentro de uma imagem:

```
java -jar f5.jar e -e msg.txt pic.jpg out.jpg
```

► Recuperar um arquivo de dentro de uma imagem:

```
java -jar f5.jar x -e out.txt out.jpg
```

## Observações

- ▶ Quando temos o meio de cobertura e o estego-objeto é mais fácil identificar que há mensagem esteganografada.
- ▶ Quando não temos mais o arquivo original esta tarefa se torna mais difícil, pois não há uma referência para comparar a imagem.
- ▶ Será que os usuários mal intencionados mantêm os meios de cobertura?

## Exercícios

- ▶ <https://futureboy.us/stegano/encinput.html>
  - ▶ <https://futureboy.us/stegano/decinput.html>
1. Crie um acróstico.
  2. Utilizando as páginas acima, esteganografe, em uma imagem qualquer, uma mensagem contendo alguma frase. Depois, com o estego-objeto, recupere a mensagem.
  3. Pesquise e descubra uma ferramenta esteganográfica que trabalhe com outro tipo de arquivo. Explique como ela funciona. Mostre a ferramenta funcionando.
  4. Pesquise e descubra uma ferramenta de esteganálise. Mostre a ferramenta funcionando.

## Esculpimento de Dados/Arquivos

- ▶ **Esculpimento de Arquivos** ou *File Carving* é uma técnica forense para remontar arquivos corrompidos ou com ausência de dados que os impedem de ser acessados pelo sistema de arquivos.

## Esculpimento de Dados/Arquivos

### ► Ajudam no esculpimento de arquivos:

- ▶ Cabeçalhos conhecidos (*headers*)
- ▶ Rodapés conhecidos (*footers*)
- ▶ Tamanho máximo do arquivo
- ▶ Estruturas conhecidas
- ▶ Reconhecimento de texto

## Esculpimento de Dados/Arquivos

- ▶ **DESAFIO!** Extraia duas imagens do arquivo FileCarving.pdf.

## Esculpimento de Dados/Arquivos

- **DESAFIO!** Extraia duas imagens do arquivo FileCarving.pdf.

```
> file FileCarving.pdf
> evince FileCarving.pdf
# abrir em um editor hexadecimal (ex: Jeex) ou:
> xxd -p FileCarving.pdf > Carving.hex
```

- Arquivos JPEG iniciam por FF D8 e terminam com FF D9.
- Selecionar o trecho e salvar (xxd -p -r Carving.hex > Arquivo)
- Repetir o processo.

# Recuperação de Dados/Arquivos



## Recuperação de Dados/Arquivos

- ▶ Imagine que você tinha arquivos confidenciais em algum dispositivo.

Figura: Arquivos Confidenciais.



Fonte: Adaptado de dreamstime.

## Recuperação de Dados/Arquivos

- ▶ Imagine que você tinha arquivos confidenciais em algum dispositivo. Arquivos que ninguém deveria ver. E você os excluiu, para que ninguém tivesse acesso a eles.
- ▶ Não estão na lixeira, foram removidos diretamente (SHIFT + DEL).
- ▶ Será que é impossível recuperá-los?

## Recuperação de Dados/Arquivos

- ▶ Imagine que você é um perito criminal em computação e recebeu o computador de algum bandido.
- ▶ O bandido, antes de ser surpreendido pela polícia, apagou todos os arquivos do computador.
- ▶ Será que é impossível recuperá-los?

## Recuperação de Dados/Arquivos

- ▶ Acidentalmente você apagou alguns arquivos importantes, tais como trabalhos do IFC.
  
- ▶ Será que é impossível recuperá-los?

## Recuperação de Dados/Arquivos

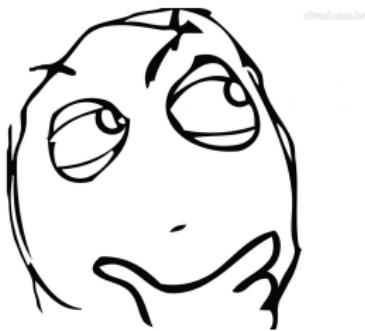
- ▶ Você vendeu seu *smartphone* usado, mas antes apagou todos os arquivos.
- ▶ É possível garantir que o novo dono não conseguirá recuperar os arquivos?

## Recuperação de Dados/Arquivos

- ▶ A resposta para todas as perguntas é **NÃO**.

# Recuperação de Dados/Arquivos

- ▶ A resposta para todas as perguntas é **NÃO**. E **SIM!**



## Recuperação de Dados/Arquivos

- ▶ A resposta para todas as perguntas é **NÃO**. E **SIM!**
  
- ▶ Não existe garantia de que os arquivos excluídos serão recuperados. No entanto, em muitos casos é possível recuperá-los, total ou parcialmente.

# Recuperação de Dados/Arquivos

## Sistema de Arquivos

- ▶ Um Sistema de Arquivos (SA) é um sistema responsável por organizar de forma lógica os arquivos em unidades de armazenamento.
- ▶ Geralmente se preocupam com a consistência dos dados, velocidade de acesso e otimização do espaço, minimizando o desperdício.

# Recuperação de Dados/Arquivos

## Sistema de Arquivos

- ▶ E, quando o usuário apaga algum arquivo, como o SA realiza esta operação?

# Recuperação de Dados/Arquivos

## Sistema de Arquivos

- ▶ E, quando o usuário apaga algum arquivo, como o SA realiza esta operação?
- ▶ Resposta: não realiza.
- ▶ Ele apenas marca, com bits de controle, a área que estava sendo utilizada pelo arquivo como “área livre”, sendo possível, desta forma, que ela seja ocupada por novos arquivos.

# Recuperação de Dados/Arquivos

## Sistema de Arquivos

- ▶ Mas isso só acontece com discos rígidos?

# Recuperação de Dados/Arquivos

## Sistema de Arquivos

- ▶ Mas isso só acontece com discos rígidos? Não.
- ▶ O que interfere neste aspecto é a forma como o SA é implementado.

# Recuperação de Dados/Arquivos

## Sistema de Arquivos

- ▶ Desta forma, pode-se dizer que é possível recuperar dados de
  - ▶ cartões SD
  - ▶ *smartphones*
  - ▶ discos rígidos
  - ▶ *pendrives*
  - ▶ ...

# Recuperação de Dados/Arquivos

## Ferramentas

- ▶ Scalpel.
- ▶ Ferramenta em linha de comando para recuperação de dados.
- ▶ Necessário acesso administrador.

# Recuperação de Dados/Arquivos

## Ferramentas

- ▶ `sudo apt-get install scalpel`
  
- ▶ Edite `/etc/scalpel/scalpel.conf`, descomentando as linhas que contêm o tipo de arquivo que você quer pesquisar.

Recuperação de Dados/Arquivos

## Ferramentas

Figura: scalpel.conf.

```
scalpel.conf X
# Scanning with this setting Foremost are curved and no tree executions
# are used. No footer is defined and the max carve size is 1000 bytes.
#
#      NONE      y      1000      FOREMOST
#
# -----
# GRAPHICS FILES
# -----
#
# AOL ART files
#      art      y      150000      \x4a\x47\x04\x0e          \xcf\xc7\xcb
#      art      y      150000      \x4a\x47\x03\x0e          \xd0\xcb\x00\x00
#
# GIF and JPG files (very common)
#      gif      y      5000000      \x47\x49\x46\x38\x37\x61          \x00\x3b
#      gif      y      5000000      \x47\x49\x46\x38\x39\x61          \x00\x3b
#      jpg      y      20000000      \xff\xdb\xff\xeb\x00\x10          \xff\xd9
#
# PNG
#      png      y      20000000      \x50\x4e\x47?    \xff\xcf\xfd\xfe
#
# BMP (used by MSWindows, use only if you have reason to think there are
# BMP files worth digging for. This often kicks back a lot of false
# positives
```

Fonte: Elaborado pelo autor.

# Recuperação de Dados/Arquivos

## Ferramentas

- ▶ sudo scalpel "dispositivo/diretorio" -o "saida"
  
- ▶ Ex: sudo scalpel "/dev/sda1" -o "saida"

# Recuperação de Dados/Arquivos

## Ferramentas

- ▶ sudo scalpel "dispositivo/diretorio" -o "saida"
- ▶ Ex: sudo scalpel "/dev/sda1" -o "saida"
- ▶ Procura arquivos com a(s) extensão(ões) definida(s) no arquivo de configuração, no dispositivo /dev/sda e envia o resultado para saida

# Recuperação de Dados/Arquivos

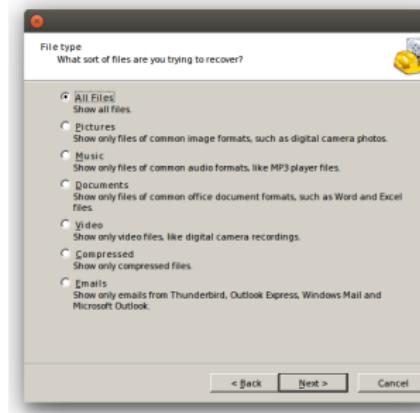
## Ferramentas

- ▶ Recuva.

# Recuperação de Dados/Arquivos

## Ferramentas

Figura: Opções de arquivos recuperáveis pelo Recuva.



Fonte: Elaborado pelo autor.

# Recuperação de Dados/Arquivos

## Ferramentas

- ▶ GT Recovery.
- ▶ Não está mais disponível para Android na Play Store.
- ▶ Ainda é encontrado aqui: <https://gt-recovery-for-windows.softonic.com.br/>

# Recuperação de Dados/Arquivos

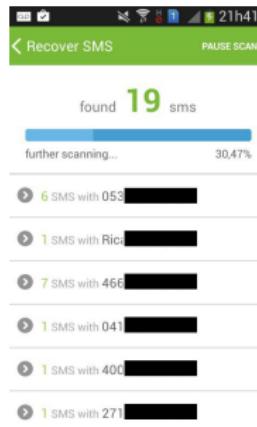
## Ferramentas

- ▶ Exige ROOT!
- ▶ Pode recuperar arquivo TXT, Contato, SMS,

# Recuperação de Dados/Arquivos

## Ferramentas

Figura: Recuperação de SMS no GT Recovery.

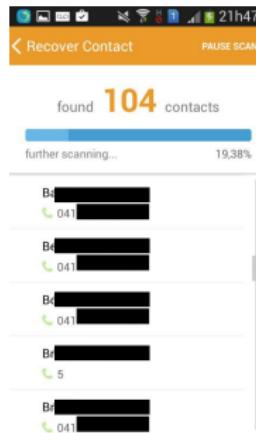


Fonte: Elaborado pelo autor.

# Recuperação de Dados/Arquivos

## Ferramentas

Figura: Recuperação de contatos no GT Recovery.



Fonte: Elaborado pelo autor.

# Recuperação de Dados/Arquivos

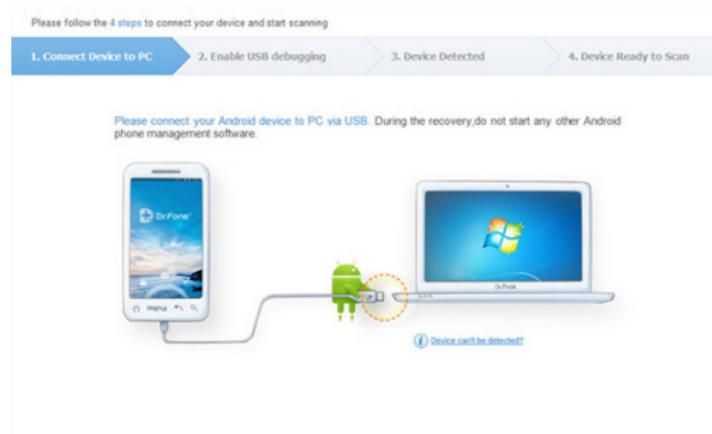
## Ferramentas

- ▶ Android Data Recovery.
- ▶ Disponível para Windows e MAC.

# Recuperação de Dados/Arquivos

## Ferramentas

Figura: Android Data Recovery (Passo 1).



Fonte: Recovery Android.

# Recuperação de Dados/Arquivos

## Ferramentas

Figura: Android Data Recovery: Ativação da depuração USB no smartphone (Passo 2).

Please follow the steps to enable **USB debugging** to continue

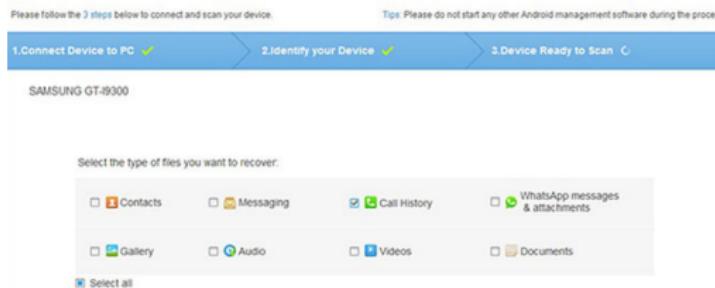


Fonte: Recovery Android.

# Recuperação de Dados/Arquivos

## Ferramentas

Figura: Android Data Recovery: Seleção dos tipos de dados a serem buscados (Passo 3).

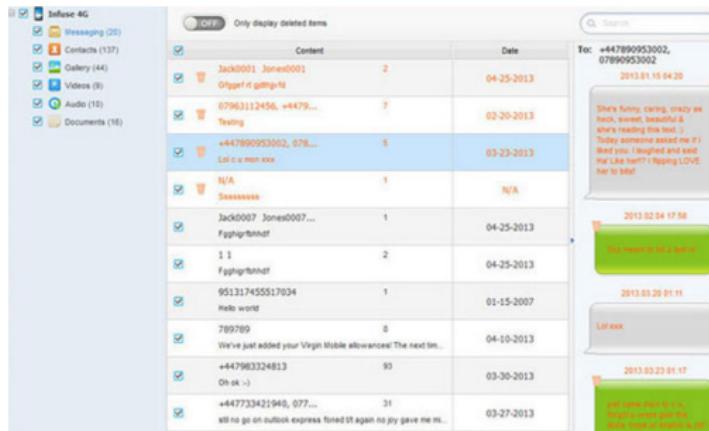


Fonte: Recovery Android.

# Recuperação de Dados/Arquivos

## Ferramentas

Figura: Exemplo de recuperação de dados no Android Data Recovery.



Fonte: Recovery Android.

# Recuperação de Dados/Arquivos

## Ferramentas

- ▶ EaseUS MobiSaver
- ▶ PhotoRec
- ▶ Tenorshare
- ▶ TestDisk
- ▶ Undelete Plus
- ▶ Wise Data Recovery

## Recuperação de Dados/Arquivos

### Backup

- ▶ Implemente alguma forma de backup, pois a recuperação não é garantida.

Figura: Backup.



Fonte: STORCENTER.

# Recuperação de Dados/Arquivos

## Backup

### ► Tipos de Backup (MICROSOFT, [s. d.]):

- **De cópia:** copia os arquivos selecionados e não os marca como arquivos que passaram por backup (o atributo de arquivo não é desmarcado). Útil para fazer backup de arquivos entre os backups normal e incremental, pois não afeta essas outras operações de backup.
- **Diário:** copia os arquivos selecionados que foram modificados no dia de execução do backup. Os arquivos não são marcados como arquivos que passaram por backup (o atributo de arquivo não é desmarcado).

# Recuperação de Dados/Arquivos

## Backup

### ► Tipos de Backup (MICROSOFT, [s. d.]):

- **Diferencial:** copia arquivos criados e alterados desde o último backup normal ou incremental. Não os marca como arquivos que passaram por backup (o atributo de arquivo não é desmarcado). Executando uma combinação dos backups normal e diferencial, a restauração de arquivos e pastas exige o último backup normal e o último backup diferencial.
- **Incremental:** copia arquivos criados e alterados desde o último backup normal ou incremental. Marca os arquivos que passaram por backup (o atributo de arquivo é desmarcado). Para utilizar uma combinação dos backups normal e incremental, exige-se o último backup normal e todos os backups incrementais para restaurar os dados.

# Recuperação de Dados/Arquivos

## Backup

- ▶ Tipos de Backup (MICROSOFT, [s. d.]):
  - ▶ **Normal:** copia os arquivos selecionados e os marca como arquivos que passaram por backup (ou seja, o atributo de arquivo é desmarcado). É possível restaurar todos os arquivos apenas com o último backup normal. Geralmente é executado quando um conjunto de backup é criado pela primeira vez.

# Recuperação de Dados/Arquivos

## Backup

► Segundo a Microsoft ([s. d.]):

- O backup que combina backups **normal** e **incremental** exige menos espaço de armazenamento e é mais rápido. No entanto, a recuperação de arquivos pode ser difícil e lenta porque o conjunto de backup pode estar armazenado em vários dispositivos.
- O backup que utiliza uma combinação dos backups **normal** e **diferencial** é mais longo, principalmente se os dados forem alterados com freqüência, mas facilita a restauração de dados, porque o conjunto de backup geralmente é armazenado apenas em alguns dispositivos.

# Recuperação de Dados/Arquivos

## Backup

### ► Ferramentas:

- ▶ AMANDA – Linux, Windows e MAC OS
- ▶ App Backup & Restore – Android
- ▶ Comodo Backup – Windows
- ▶ Déjà Dup – Linux
- ▶ Retrospect – Linux, Windows e MAC OS
- ▶ Syncthing – Linux, Windows, MAC OS, iOS, Android, Solaris, Darwin e BSD
- ▶ Ultimate Backup Tool – Android

## Recuperação de Dados/Arquivos

### Cópia Forense

- ▶ Cópia que mantém as características originais dos dados e do dispositivo.
- ▶ Útil para obter evidências/provas sobre processos judiciais.
- ▶ Útil pela praticidade, pois não é necessário trabalhar no dispositivo original.

# Recuperação de Dados/Arquivos

## Cópia Forense

- ▶ Para garantir a integridade das evidências, algumas ações devem ser tomadas ao realizar uma cópia forense.
- ▶ Portar um disco secundário, para onde os dados serão copiados.
- ▶ Impedir a inicialização do sistema pelo disco rígido analisado (desabilitar a inicialização do disco na BIOS). Por quê?

# Recuperação de Dados/Arquivos

## Cópia Forense

► Ferramentas:

- EnCase (proprietária)
- DD
- DC3DD (DD mais completo)

# Recuperação de Dados/Arquivos

## Cópia Forense

- ▶ Exemplo de comando com o DC3DD para gerar a cópia forense:
- ▶ O disco destino deve estar formatado, escrito na tabela de partições e deve conter o diretório `meuDiretorio`. Após, a unidade deve ser montada.
- ▶ `dc3dd if=/dev/sda of=meuDiretorio/image.dd progress =on hash=md5 split=1024 iflag=direct log=image.log conv=noerror splitformat=000`

## Exercícios

- ▶ Atividades:
  1. Utilizando os conceitos desta aula, crie uma cópia forense – total ou parcial – do seu HD em algum dispositivo externo. Com um software de recuperação de dados, restaure, a partir da cópia forense, arquivo(s) que havia(m) sido excluído(s).
  2. Criar uma rotina de backup automatizada e mostrá-la em funcionamento. **DICA:** pesquisar por “*How to automatically backup files and directories in Linux*”.

## Referências

- ▶ WIKIPÉDIA. Data recovery. List of data recovery software. Disponível em: [https://en.wikipedia.org/wiki/Data\\_recovery#List\\_of\\_data\\_recovery\\_software](https://en.wikipedia.org/wiki/Data_recovery#List_of_data_recovery_software). Acesso em: 05 ago. 2024.
  
- ▶ MICROSOFT. Tipos de Backup. TechNet. Disponível em: <[https://technet.microsoft.com/pt-br/library/cc784306\(v=ws.10\).aspx](https://technet.microsoft.com/pt-br/library/cc784306(v=ws.10).aspx)>. Acesso em: 13 jul. 2021.

# Segurança Computacional

## Computação Forense

Ricardo de la Rocha Ladeira  
{[ricardo.ladeira@ifc.edu.br](mailto:ricardo.ladeira@ifc.edu.br)}

