Perícia Computacional Forense: Identificando o crime

Prof. Marcos Monteiro

http://www.marcosmonteiro.com.br
contato@marcosmonteiro.com.br

Marcos Monteiro

- A partir da última década, os criminosos estão utilizando os benefícios oferecidos pela tecnologia em suas atividades ilícitas.

- Entre os anos de 2005 e 2006 o CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil), registrou um aumento de mais de 190% nos incidentes de segurança reportados.

Ciência Forense Criminal

- A ciência forense criminal traz a prática da investigação o que chamamos de método cientifico, ou metodologia cientifica, fazendo-se valer dos conhecimentos de diversos tipos de ciências como a matemática, química, física, biologia, medicina, engenharia e nos dias atuais a informática.

Computação Forense

- “Ciência forense destinada a preservar, adquirir, obter e apresentar dados que foram processados eletronicamente e armazenados em dispositivo de computador.”

FBI

Evidencia Digital

- Qualquer dado em meio digital que possa colaborar no sentido de provar que uma fraude ou irregularidade foi cometida e que possa estabelecer vinculo de relação entre a fraude ou irregularidade e a vitima, e entre a vitima e o agente.

EVIDÊNCIA ELETRÔNICA

FORMULÁRIO DE CADEIA DE CUSTÓDIA

Caso Num.: 053203 **Pag.: 01** **De: 05**

MÍDIA ELETRÔNICA/DETALHES EQUIPAMENTO

Item:	Descrição:		
00001	HD de Notebook com 80GB de capacidade		
Fabricante:	Modelo:	Num. de serie:	
TOSHIBA	MK4026GAX	85MC7639T	

DETALHES SOBRE A IMAGEM DOS DADOS

Data/Hora:	Criada por:	Método usado:	Nome da Imagem:	Partes:
20/5/2007 15:30	Paulo A. Neukamp	dcfldd	053203_01.dd	01
Drive:	HASH:			
Disco Completo	d243367072088feae98364977441d736			

CADEIA DE CUSTÓDIA

Seqüência:	Data/Hora:	Origem:	Destino	Motivo:
001	Data: 20/5/2007	Nome/Org.: Sigilo	Nome/Org.: Lab. Perí. Unisinos	Investigação sobre denuncia de Pedofilia
	Hora: 16:00	Assinatura:	Assinatura:	

Perito

- A Ciência Forense possui diversas àreas de atuação;

- Segundo KRUSE II e HEISER, a “ Forense Computacional compreende a aquisição, preservação, identificação, extração, restauração, análise e documentação de evidências computacionais, quer sejam componentes físicos ou dados que foram eletronicamente processados e armazenados em mídias computacionais” .

Habilidades de um Perito em Computação Forense

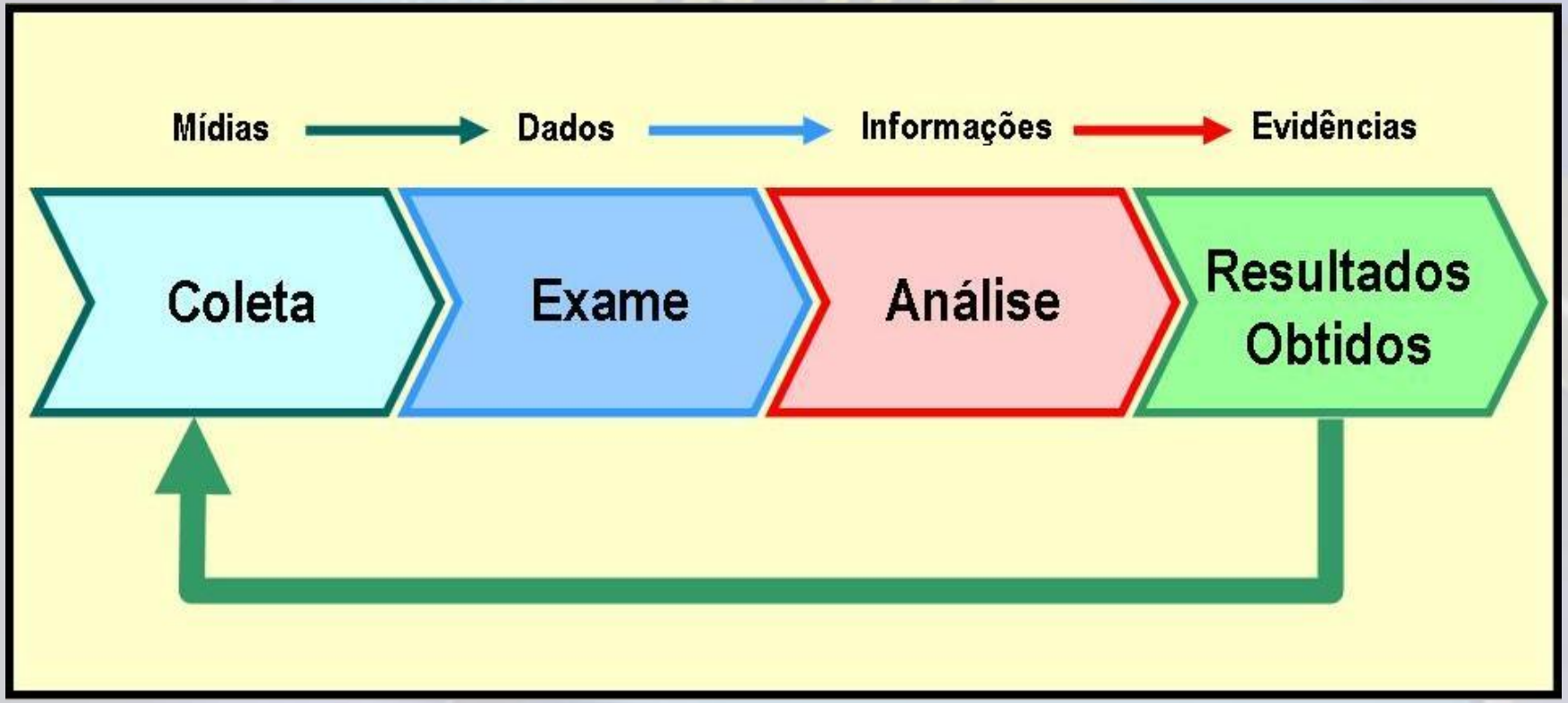
- Segurança da Informação;
- Resposta a Incidentes
- Auditoria de Sistemas

Marcos Monteiro

Campos de atuação da Computação Forense

- Sistemas Operacionais
  - Ambiente Windows
  - Ambiente Unix-Like
- Funcionalidade do S.O.
  - Computadores domésticos e pessoais
  - Computadores corporativos ou servidores em geral
- Conectividade
  - Computadores não rede
  - Computadores em Rede
- Tipos de rede
  - Maio de cabo
  - Sem fio

Etapas de uma Investigação



Técnicas Forenses

- Preparação
- Chegada ao local da Investigação
- Coleta dos Dados
- Exame dos Dados
- Análise das Informações
- Redação do Laudo

Chegada ao local da Investigação

- **Isolar a área** → alteração e contaminação
- **Fotografar ou Filmar** → próximas etapas
- **Registro dos detalhes** → reconstrução da cena
- **Manter o estado dos equipamentos** → prioridade

Marcos Monteiro

Coleta dos Dados

- **Dados voláteis**
  - Data hora;
  - Conexões de rede;
  - Memória;
  - Configuração da rede;
  - Processos em execução;
  - Arquivos abertos;
  - Sessão de Login.

- **Dados não-voláteis**
  - Log, temporários e de configuração;
  - Textos, planilhas, imagens, etc…

Coleta dos Dados cont.

- **Formas de coleta dos dados**
  - Cópia lógica (Backup) → arquivos e pastas
  - Imagem → bit-a-bit

- **Coletando dados voláteis** → Rootkits & alterações
- **Coletando dados não-voláteis** → RO
- **Integridade dos dados** → Hash

Exame dos Dados

- Extração dos dados →Localizar → Filtrar → Extrair → Recronstrução dos eventos

- Localizando os dados → Conhecimento sobre extensões e localização

Análise das Informações

- A etapa de análise das informações, ocorre muitas vezes, paralela à etapa de exame;

- Finalidade de recriar o(s) evento(s) que estão sendo investigado(s).

Redação do Laudo

- **Finalidade do relatório** → Objetivos da Investigação;
- **Autor(es) do relatório** →Especialidade e responsabilidades;
- **Resumo do incidente** → Incidente e suas conseqüências;
- **Estado das evidências** → Como, quando e por quem;
- **Detalhes** → Quais evidências, métodos, procedimentos;
- **Conclusão** → Evidências que comprovem;
- **Anexos** → Toda documentação.

Passo-a-Passo Analise com a distribuição Linux FDTK

Etapa	Descrição Técnica	Ferramentas na FDTK
Preparação para a investigação	Esterilizar todas as mídias que serão utilizadas na investigação	wipe, air, secure-delete
	Certificar-se de que todas as ferramentas (softwares) que serão utilizadas estão devidamente licenciadas para o uso.	FDTK
	Certificar-se de que todo o equipamento necessário para a investigação está em ordem e funcionando plenamente	Notebook, câmera fotográfica
Coleta dos Dados	Data hora do sistema operacional	dvol.sh & dvol.cmd (na raiz do CD)
	Conexões de rede ativas	
	Tabela de roteamento	
	Módulos do Kernel carregados	
	Configuração de rede	
	Processos em execução	
	Arquivos abertos	
	Sistemas de arquivos montados	
	Coleta de informações do equipamento	discover1, lshw-gtk, blktool
	A imagem das midias ou imagem *bit-a-bit* dos dados das mídias	dd, dd_recue, dcfldd, aff-tools, sdd, air, gddrescue
	Geração de Hash (integridade das evidências)	md5, sha1sum
	Cadeia de Custódia	Formulário de Custódia
	Captura de screenshots	gnome-screenshot

Marcos Monteiro

Exame dos Dados	Recuperar arquivos deletados ou armazenados nas áreas livres ou não utilizadas das mídias	testdisk, Scrounge-NTFS, fatback, magicrescue, e2undel, recover
	Recuperar arquivos expecíficos	recovergz, recoverjpg
	Manipulacao de dados em sistemas de arquivos NTFS	ntfsprogs, scrounge-ntfs
	Visualizar imagens	comix,gthumb, imageindex
	Acessar arquivos compactados	xarquive, zoo, p7zip, unshield, unrar-free, unzip, unarj, unace
	Extrair informações de arquivos jpg	exif, exiftags, jpginfo, exifprobe, exiftran, exiv2
	Extrair imagens cruas de cameras fotograficas	dcraw
	Criptoanálise	outguess, stegdetect, xsteg
	Decriptar arquivos	bcrypt, ccrypy, cryptcat
	Quebar senhas de arquivos	medussa, jonh, ophcrack
	Quebar senhas de arquivos do NT	chntpw
	Quebar senhas de arquivos zip	fcrackzip
	Manipular arquivos pdf	pdftk
	Coletar mac time de arquivos e diretórios	mactime, mac-robber
	Detecção da presença de rootkits	chkrootkit, rkhunter
	Acessar arquivos de forma binária	ghex2, biew, hexdump, hexcat
	Leitores para varias extensões proprietária da MS	readpst, antiword, mdbtools, tnef, fccu-docprop, fccu-evtreader, regtool, regp.pl, dumpster_drive.pl, mscompress

Análise das Evidências	Gerarção de um timeline das evidencias	sleuthkit
	Localizar atacantes através de seus ip's	xtraceroute
	Analizar bases de dados de email MS	eindeutig
	Analisar cookies do windows	galetta, cookie_cruncher.pl
	Analisar cache do IExplorer do windows	pasco
	Analisar arquivos INF2 do windows	rifiuti
	Script perl para ler arquivo history.dat do Firefox	mork.pl
	Visualizador de históricos de bowser' s	browser-history-viewer
	Tollkit's para tarefas de várias finalidades	autopsy, pyflag
Total de Etapas = 4	Total de areas de atuação = 42	Total de Ferramentas = 95

Marcos Monteiro

Vamos Peritar !!

- Zerar a Senha do Usuário local do Windows
  - **Hiren's**

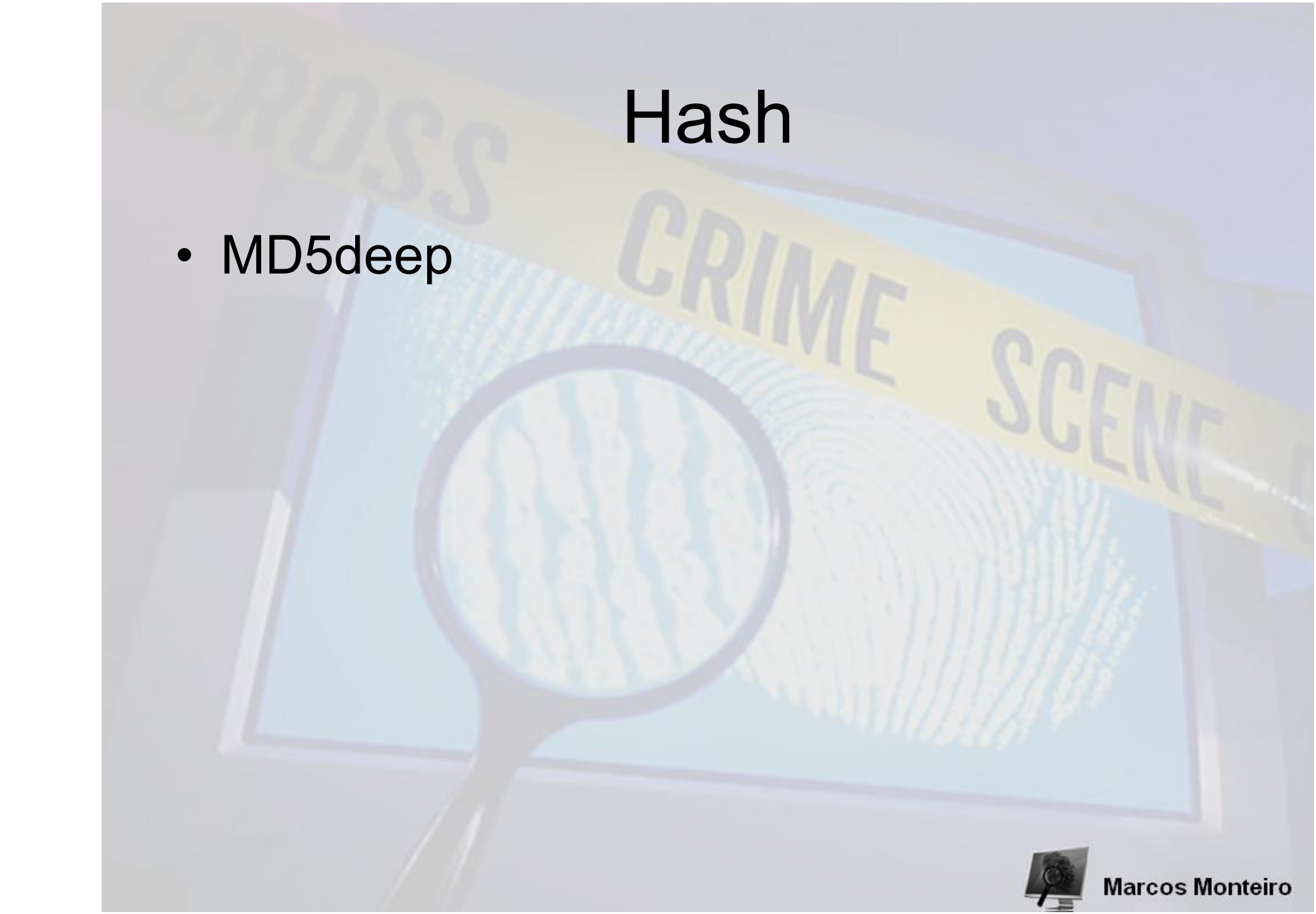
Marcos Monteiro

Vamos Peritar!!!

- Identificando o seu sistema.
  - **WinAudit**
  - **Windows Forensic Toolchest™ (WFT)**

Hash

- MD5deep



Vamos Peritar!!

- Os arquivos mais recentes criados na maquina.
  - **RecentFilesView**

Marcos Monteiro

- As ultimas linhas de registro que foram modificadas
  - RegScanner

- Monitorando Arquivos que estão sendo executados em tempo real para analise.
  - **Filemon**

Identificando o perfil de acesso do usuário a Internet

- Histórico de Internet
  - pasco
  - IECacheView
  - MozillaCacheView

- Ultimas pesquisas feitas na internet
  - MyLastSearch

- Identificando Senhas de Usuário
  - **mailpv** - senha outlook;
  - **Pspv -** senhas de internet ou outocompletar;
  - **WirelessKeyView –** Conexões Wireless;

- Arquivos que foram deletados para a lixeira
  - **rifiuti**

- Recuperando arquivos Deletados
  - GetDataBack

- Identificando Acesso do Pen Drive
  - **USBDeview**

- Identificando arquivos com atributos
  - **Attrib**

Esteganografia

- **Esteganografia** (do grego "escrita escondida") é o estudo e uso das técnicas para ocultar a existência de uma mensagem dentro de outra. Em outras palavras, esteganografia é o ramo particular da criptologia que consiste em fazer com que uma mensagem seja camuflada, mascarando sua presença.
  - **Camouflage**

Distribuições Linux para Perícia Computacional Forense

Distribuições Linux Analisadas				
Nome	Baseada	Versão	Data	Nomenclatura
DEFT	Ubuntu	1.0	22/3/2007	Digital Evidence Forense Toolkit
BackTrack	Slackware	2.0	06/03/2007	N/A
INSERT	Knoppix	1.3.9b	16/02/2007	Inside Security Rescue Toolkit
nUbuntu	Ubuntu	6.10	21/11/2006	Network Ubuntu
FCCU	Knoppix	11.0	19/10/2006	Federal Computer Crime Unit
Helix	Knoppix	1.8	06/10/2006	N/A
Operator	Knoppix	3.3.20	01/10/2005	N/A
PHLAK	Morphix	0.3	07/05/2005	Professional Hacker's Linux Assault Kit
L.A.S Linux	Knoppix	0.5	06/03/2004	Local Area Security
Knoppix-STD	Knoppix	0.1	21/01/2004	STD - Security Tools Distribution

PERGUNTAS ?

Marcos Monteiro
contato@marcosmonteiro.com.br
http://www.marcosmonteiro.com.br