

**Anti-Forensics - Falhas atuais de perícias
técnicas em sistemas de informações**

***H2HC SE – Hackers 2 Hackers
Conference Second Edition***

Domingo Montanaro

São Paulo-SP, 03 de Novembro de 2005



Introdução - Motivação

- **Analísadores - Operadores de Ferramentas**
- **Delinqüentes - Técnicas Ascendentes**
- **Brasil – Realidade no Crime Organizado**
- **Governo - Ações Policiais**
- **Internet – Informação de Fácil Aquisição e Compreensão**











Agenda

- **Introdução – Know How**
- **Datas de Arquivos**
- **Sobreposição de dados**
- **Slack Space**
- **Steganografia**
- **Páginas de Memória**



Introdução – Know How

- Estrutura SO – Páginas de Memória
- Estrutura de um FileSystem
- NTFS – [ADS](#) (Só um feature, não é técnica de esteganografia)

<input type="checkbox"/>	12	 \$AttrDef		File, Internal
<input type="checkbox"/>	13	 \$BadClus^\$Bad		File, Invalid Cluster, Stream
<input type="checkbox"/>	14	 \$BadClus		File, Internal
<input type="checkbox"/>	15	 \$Bitmap		File, Internal
<input type="checkbox"/>	16	 \$Boot		File, Internal
<input type="checkbox"/>	17	 \$LogFile		File, Internal
<input type="checkbox"/>	18	 \$MFT		File, Internal
<input type="checkbox"/>	19	 \$MFTMirr		File, Internal

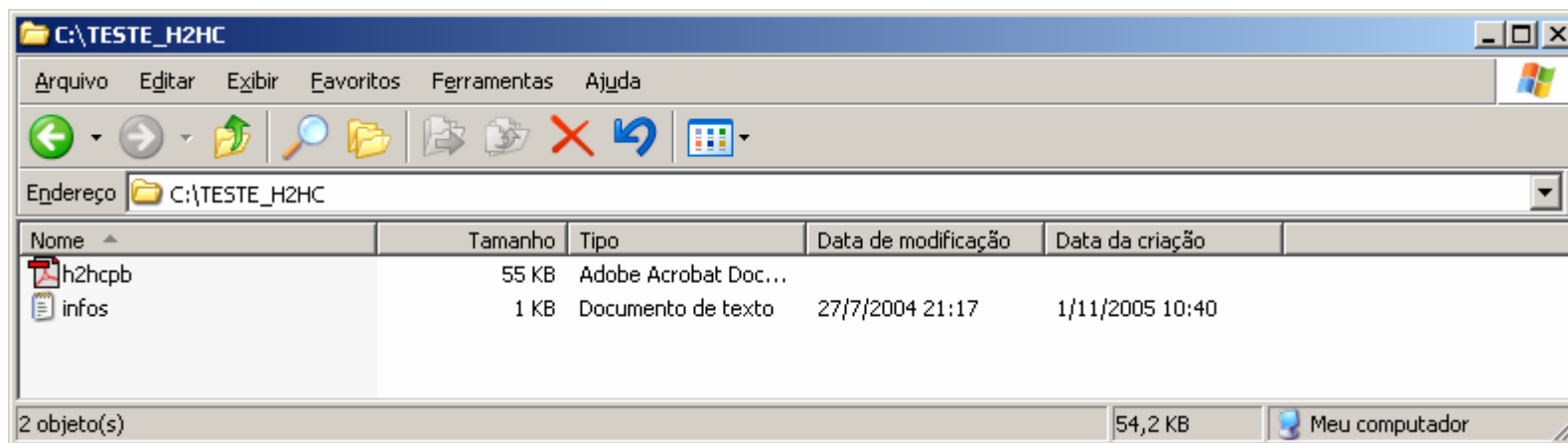


Datas de Arquivos

- **Fundamentais para elaboração de laudos**
- **Ferramentas de análise utilizam “Timelines” que guiam peritos na linha de tempo dos acontecimentos**
- **Problema: Datas são facilmente manipuláveis**
 - **NtQueryInformationFile()**
 - **NtSetInformationFile()**



Demonstração - TimeStomp



	File Name	Last Accessed	Last Written	File Created	Entry Modified
<input type="checkbox"/> 1	h2hcpb.pdf				
<input type="checkbox"/> 2	infos.txt	11/01/05 10:40:03	07/27/04 09:17:44	11/01/05 10:40:03	11/01/05 10:40:04



Por que?

- **Maioria das ferramentas de análise utiliza SIA (Standard Information Attributes) no registro do arquivo na MFT**
- **Outros registros de data ficam no atributo de “FN” (FileName), porém a utilização dessas datas requer operações em “RAW I/O”**



O que ocorre quando um arquivo é gravado?

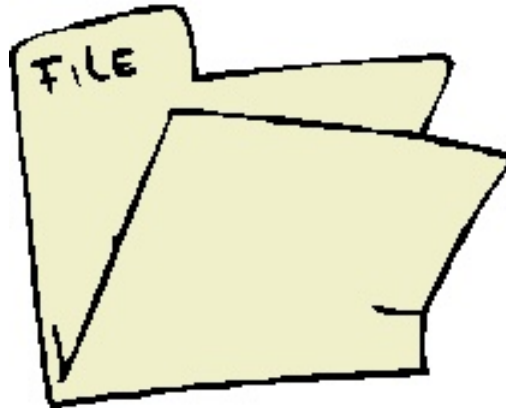
1

FAT



2

Diretório



3

Dados



1 - Primeiro Passo

FAT =

File Allocation Table

Tabela de alocação de arquivos

**Índice de localização de trechos de arquivos na
área de dados do disco rígido**

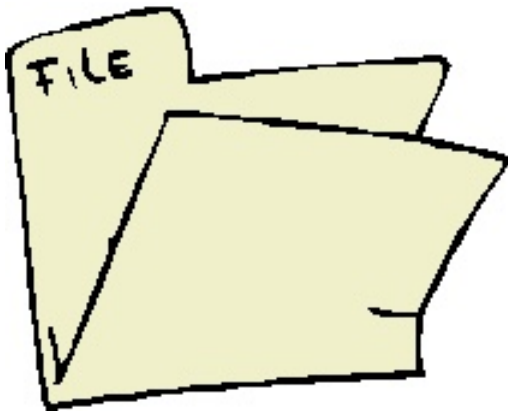


**Entrada criada na FAT com a localização do
arquivo à ser gravado**



2 - Segundo Passo

Diretório = Localização lógica do arquivo no disco



Criado um registro no diretório indicando:

- Tamanho
- Nome
- Datas (Acesso, Modificação, Criação)
- Permissões



3 - Terceiro Passo

Dados =

Conteúdo binário do arquivo



O conteúdo do arquivo que está sendo gravado é escrito na área de dados do disco.



E quando o arquivo é deletado?

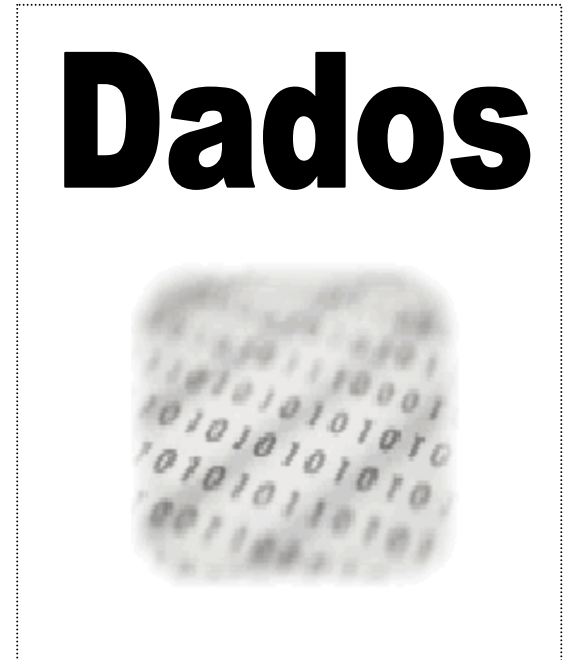
1



2



3



E quando o arquivo é deletado?



A entrada na FAT é excluída

Indicação de trecho disponível
para gravação



E quando o arquivo é deletado?



O registro no diretório é alterado

O primeiro caractere do nome do arquivo no diretório é trocado por um caractere especial (Ex: E5 Hexadecimal [Fat32])



E quando o arquivo é deletado?

Dados



Os dados permanecem!

Os trechos do arquivo continuam na área de dados do disco rígido até outro arquivo ser gravado no mesmo lugar



Nível Magnético

Causas:

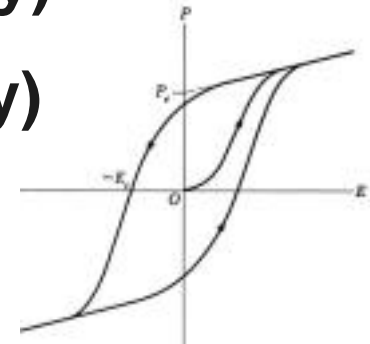
- **Sobreposição de dados:**
 - **Re-utilização por outros usuários**
 - **Mudança de sistema operacional e filesystem**
 - **Doação e ferramentas de Wipe**



Nível Magnético

Método:

- **STM (Scanning Tunneling Microscopy) 2-3**
- **SPM (Scanning Probe Microscopy)**
- **MFM (Magnetic Force Microscopy)**
- **Blue Laser Scanning (Convar)**



HISTERESE (HISTÓRIA MAGNÉTICA)

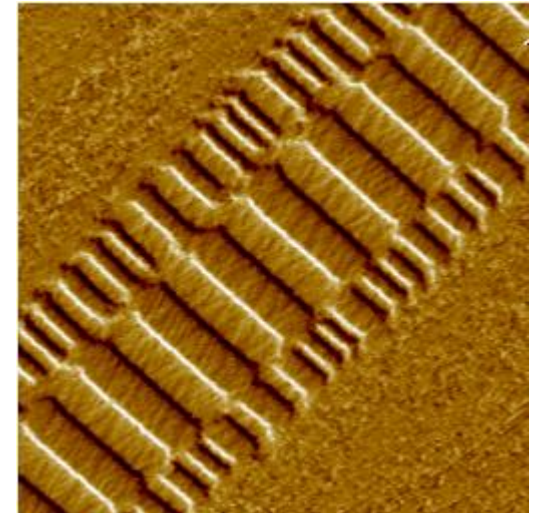
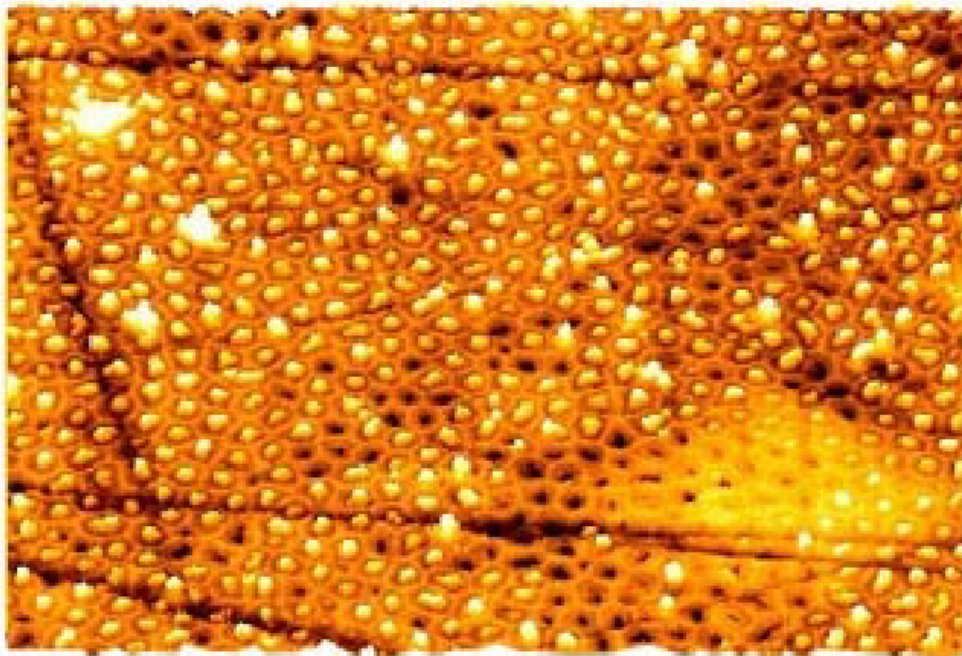
Estudo: Curvas de Histerese Ferromagnética



Realidade

- **Wipe Randômico de 1 Passo? – Novas Densidades**
- **Informação Digital, Tecnologia de Suporte (Storage) Analógica**

FIGURE 1:
AN ATOMIC FORCE IMAGE OF MAGNETIC RECORDING MEDIA SHOWING THE SUSPENDED
MAGNETIC PARTICLES (used courtesy of Park Scientific Instruments, [http://shell7.ba.best.com/
~wwwpark/appnotes](http://shell7.ba.best.com/~wwwpark/appnotes))



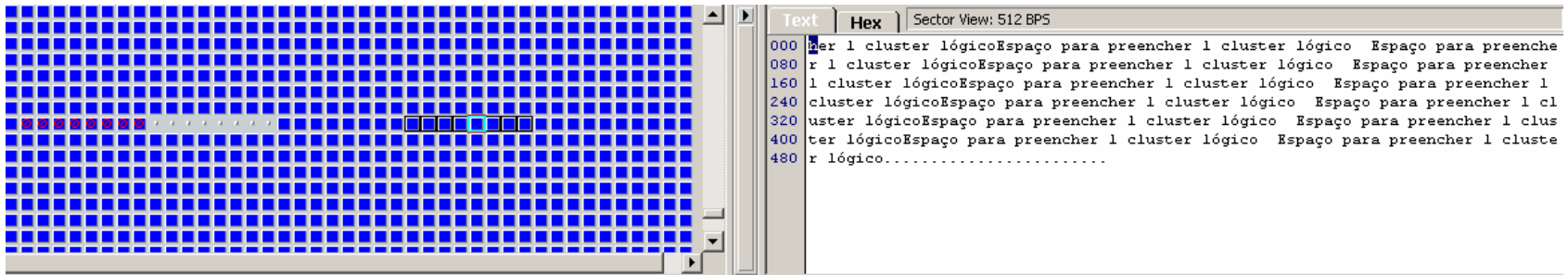
Residuals of overwritten
information on the side of
magnetic disk tracks.
Reproduced with permission
of VEECO

Slack Space

- **NTFS usa cluster lógico de 4kb por padrão**
- **Arquivo menor que 4kb utiliza os 4kb**
- **Ferramenta pode utilizar “Slack Spaces” para armazenar informação**
- **Formas robustas de esteganografia podem ser utilizadas de forma à esconder definitivamente essas informações**

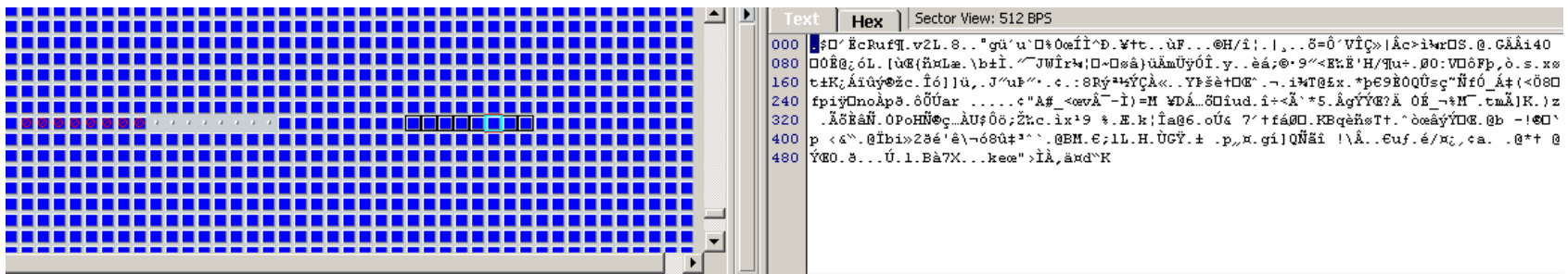


Slack Space



Text Hex Sector View: 512 BPS

```
000 0er 1 cluster lógicoEspaço para preencher 1 cluster lógico Espaço para preenche
080 r 1 cluster lógicoEspaço para preencher 1 cluster lógico Espaço para preencher
160 l cluster lógicoEspaço para preencher 1 cluster lógico Espaço para preencher 1
240 cluster lógicoEspaço para preencher 1 cluster lógico Espaço para preencher 1 cl
320 uster lógicoEspaço para preencher 1 cluster lógico Espaço para preencher 1 clus
400 ter lógicoEspaço para preencher 1 cluster lógico Espaço para preencher 1 cluste
480 r lógico.....
```



Text Hex Sector View: 512 BPS

```
000 [;P' ěcRufq.v2L.8.. "gü'u' 0%0æİİ^D.V+tt.. ùF...@H/i!.. |.. 5=0' VİÇ>|Ăc>i>rDS.@. GĂĂi40
080 00Ē;6L. [ûE{ĥwLæ.\b+i. /JWİr*!0-Dsá)ûĥmÛyóİ.y.. èá;@'9"<EKĒ'H'7tu+.00:VD06P,ò.s.x8
160 t±K;Ăiúy@zç.İó)Û,..J'uf'..c.:8Ry*+YÇĂ«..YFšè+0Q'..-i*İQİx.*pç9E0QŪsq"Ñİó_Ă+(<080
240 fpiy0noăpš.ôŪŭar .....c"A# <œvĂ-İ)=M ŵDĂ.8Diud.i+<Ă*5.ĂgYŶG?Ă OĒ_-M^tmĂ|K.)z
320 ..ĂšăÑ.0PoHŊœç..ĂU;06;Zkc.İx'9 *.E.k;İa@6.oŪ 7'fá00.KBqêñsTt.^òœăyŶDQ.@b -!@0'
400 p <æ^.@İbi>28é'ê\~68Ūt'..@EM.€;İL.H.ŪCŶ.± .p,ŭ.gi|QŊĒi !\Ă..Ēuf.é/mç.ca. .@*+ @
480 YEO.8...Ū.İ.Bà7X...keœ">İĂ,ămd^K
```



Slack Space

19B751940	75 73 74 65 72 20 6C F3	67 69 63 6F 45 73 70 61	uster lógicoEspa
19B751950	E7 6F 20 70 61 72 61 20	70 72 65 65 6E 63 68 65	ço para preenche
19B751960	72 20 31 20 63 6C 75 73	74 65 72 20 6C F3 67 69	r 1 cluster lógico
19B751970	63 6F 0D 0A 45 73 70 61	E7 6F 20 70 61 72 61 20	co..Espaço para
19B751980	70 72 65 65 6E 63 68 65	72 20 31 20 63 6C 75 73	preencher 1 clus
19B751990	74 65 72 20 6C F3 67 69	63 6F 45 73 70 61 E7 6F	ter lógicoEspaço
19B7519A0	20 70 61 72 61 20 70 72	65 65 6E 63 68 65 72 20	para preencher
19B7519B0	31 20 63 6C 75 73 74 65	72 20 6C F3 67 69 63 6F	1 cluster lógico
19B7519C0	0D 0A 45 73 70 61 E7 6F	20 70 61 72 61 20 70 72	..Espaço para pr
19B7519D0	65 65 6E 63 68 65 72 20	31 20 63 6C 75 73 74 65	eencher 1 cluste
19B7519E0	72 20 6C F3 67 69 63 6F	00 00 00 00 00 00 00 00	r lógico.....
19B7519F0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
19B751A00	10 24 8F 92 CB 63 52 75	66 B6 11 76 32 4C 01 38	.\$. 'ÉcRuf%.v2L.8
19B751A10	18 01 B0 67 FC B4 75 60	8D 25 D2 9C CD CC 5E D0	.. ^gu'u` %Ô ÍÍ^Ð
19B751A20	06 A5 86 74 06 12 F9 46	1B 02 17 A9 48 2F EE A6	.% t..ùF...@H/i
19B751A30	10 7C B8 05 18 F5 3D D4	B4 56 CE C7 BB 2A 2A 2Aδ=Ô'VÍÇ>***
19B751A40	2A 54 45 58 54 4F 20 45	53 43 4F 4E 44 49 44 4F	*TEXTO ESCONDIDO
19B751A50	2A 2A 2A 40 BF F3 4C 03	5B F9 8C 7B F1 A4 4C E6	***@óL.[ù {ñLæ
19B751A60	08 5C 62 B1 CC 07 94 AF	4A 57 CE 72 BC A6 9D 7E	.\b±l.. JWÍr% ~
19B751A70	7F F8 E2 7D FC C4 6D DC	FF D3 CE 14 79 1E 18 E8	æâ}üÄmÛýÓí.y..è
19B751A80	E1 3B A9 B7 39 94 3C 45	89 CB 27 48 2F B6 75 F7	á:@.9 <E É'H/¶u+
19B751A90	02 D8 4F 3A 56 8D F4 46	FE 2C F2 0C 73 1A 78 F8	.@:V óFp.ò.s.xø
19B751AA0	74 B1 4B BF C1 EF FB FD	AE 9E 63 07 CE F3 5D 5D	t±K&Áiúý@ c.Íó]]
19B751AB0	FC 2C 0E 4A 94 75 DE 94	B7 0B A2 12 3A 38 52 FD	ü..J ub ..c.:8Rý
19B751AC0	AA BD DD C7 C0 AB 1D 07	59 DE 9A E8 86 81 8C 88	æYÇÀ<<..Yp è lll
19B751AD0	1C AC 04 69 BE 54 40 A3	78 0B 2A FE 80 39 C8 D2	..i%T@fx.*p 9ÈÒ

Esteganografia usando Imagens

- **Arquivos de Imagem seguem layouts (padrões) assim como outros arquivos**
- **Cada padrão tem sua particularidade onde informações podem ser escondidas**
- **Ex: Comentário do GIF89a**
- **Falha: Ferramentas não contém “Analisadores de Padrões” que contemplem análises de discrepâncias**



Esteganografia usando Imagens

- **Técnicas:**
 - ✓ **Color Reduction**
 - ✓ **Comentários**
 - ✓ **Utilização de Espaço Redundante**
 - ✓ **Compressão**
 - ✓ **Criptografia**



Páginas de Memória

- **Examinar uma máquina sem desligá-la pode causar em falhas de análise (falsos negativos)**
- **Diversas ferramentas hoje utilizadas por analisadores em “live systems” são facilmente enganadas por Rootkits que rodam em Kernel Space (Ex: Hacker Defender)**
- **Páginas de memória guardam estruturas que podem revelar todos os processos (inclusive os escondidos) rodando naquele momento, bem como portas tcp e udp abertas, etc.**



Páginas de Memória

- **Falta de Ferramentas para analisar memória**
- **Nas poucas ferramentas que existem (pagas e caras), poucas estruturas são identificadas (processos, portas, etc)**
- **Oportunidade: Identificação de pacotes TCP, UDP, ICMP, Usuários, Atividade de FileSystem (Corroboração com Swap)**



Fontes

- James C. Foster & Vinnie Liu – “Catch Me, If You Can”, TimeStomp
- Data Remanence in Semiconductor Devices - Peter Gutmann
- Digital Archaeology: Rescuing Neglected and Damaged Data - Seamus Ross and Ann Gow
- Secure Deletion of Data from Magnetic and Solid-State Memory - Peter Gutmann
- Memparser - Chris Betz
- Remembrance of Data Passed: Used Disk Drives and Computer Forensics - Simson L. Garfinkel
- Padrão NTFS (Linux-NTFS)



Anti-Forensics - Falhas atuais de perícias técnicas em sistemas de informações

OBRI GADO

Domingo Martin Montanaro Barrales

Perito em TI

h2hc@montanaro.com.br



ADS – Alternate Data Streams

```
C:\ads>echo "Conteudo Normal" > teste.txt
```

```
C:\ads>echo "Conteudo Escondido" > teste.txt:escondido.txt
```

```
C:\ads>dir /a
```

```
O volume na unidade C é Disco local  
O número de série do volume é 5056-0467
```

```
Pasta de C:\ads
```

```
22/11/2004  00:59      <DIR>          .  
22/11/2004  00:59      <DIR>          ..  
22/11/2004  00:59                20 teste.txt  
                1 arquivo(s)                20 bytes  
                2 pasta(s)  1.696.808.960 bytes disponíveis
```

```
C:\ads>type teste.txt  
"Conteudo Normal"
```

```
C:\ads>notepad teste.txt:escondido.txt
```

