Tutorial truecrypt

Atenção! Sempre faça um backup antes de usar a criptografia.

1. TrueCrypt é um aplicativo de código aberto para Linux e Windows que cria volumes criptografados que podem ser montados como unidades virtuais. Esta aplicação tem a capacidade de criptografar uma partição do disco rígido ou *pen drive*.

2. Instalando o truecrypt

baixe o truecrypt no sitio http://www.truecrypt.org/downloads

3. Abra um terminal, vá até a pasta onde foi baixado o TrueCrypt e digite os seguintes comandos:

tar -xzvf truecrypt-6.3a-linux-x86.tar.gz

cd truecrypt-6.3a-setup-x86

./ truecrypt-6.3a-setup-x86

4. Para criar uma pasta criptografada Após instalado o Truecryp, vá no **menu acessórios , depois opção "truecrypt".**

5. Clique no botão **"Create Volume"** para começar a criação do sua pasta criptograda, conforme figura abaixo:

			TrueC	rypt				×
<u>V</u> olume	s <u>K</u> eyfiles	<u>F</u> avorites	T <u>o</u> ols Setting	s <u>H</u> elp				
Slot	Volume			Size	Mount Direct	ory	Туре	
 1 2 3 4 5 6 7 8 9 10 11 		ß						
a 12								▼
Crea	ate Volume		Volume P	roperties		Wip	e Cache	
Volume	✓ <u>N</u> ever	save history	,	Volu	w we <u>T</u> ools	Select	ct <u>F</u> ile D <u>e</u> vice	
	Mount	Auto-M	lount Devices	Di <u>s</u> m	ount All	1	E <u>x</u> it	

6. Selecione "Create an encrypted file container" conforme figura abaixo:



7. Selecione a opção "standard truecrypt volume" conforme figura abaixo:



8. Escolha o nome e o lugar onde o arquivo de senha da pasta criptografada (não apague esse arquivo, pois sem ele é impossível montar a pasta posteriormente). Clique em "Select File..." conforme mostrado na figura abaixo:

•

TrueCr	ypt Volume Creation Wizard
	Volume Location ▼ Select File ▼ Never save history A TrueCrypt volume can reside in a file (called TrueCrypt container), which can reside on a hard disk, on a USB flash drive, etc. A TrueCrypt container is just like any normal file (it can be, for example, moved or deleted as a gy normal file). Click 'Select File' to choose a filename for the container and to select the location where you wish the container to be created. WARNING: If you select an existing file, TrueCrypt will NOT encrypt it; the file will be deleted and replaced with the newly created TrueCrypt container. You will be able to encrypt existing files (later on) by moving them to the TrueCrypt container that you are about to create now.
	Ajuda < Prev Next > Cancelar

9. Selecione o local e digite o nome do arquivo, conforme mostrado na figura abaixo:

Aplicativos	Locais Sistema 🍪 🕐	: <mark>::::::::::::::::::::::::::::::::::::</mark>	ui 17 Jun, 10:0	7 🔲 melo 🕚
		Sem título 1 - OpenOffice.org Writer		
		ão - Shutter		*
<u>A</u> rquivo <u>E</u> ditar	<u>V</u> isualizar Captura de tela	<u>ir Aj</u> uda 📝 🖗	🔶 🖻 👖	Q »
Seleção 🖷		Specify a New TrueCrupt Volume	X	* »
		Specify a new frueerypt volume		· •
<u></u>	Nome: arquivo de s	enha da pasta criptografada	ζ.	18 ▲
	Salvar na pacta	10		
		uh.		
	▼ <u>N</u> avegar em outras pastas			
	home testebackup		riar pasta	
			<u> </u>	
	Locais A Nome	Tamanho Mod	ificado 🔺	
	Q Pesquisar			
	Contraction of the second seco			
	🙍 melo			
	E Desktop			- 15
	adados			
	in usuarios			
	ados			
	间 Consulta			
0 screenshots 0	💾 Unidade de Di			
	20100529_1820			v
	Documentos		T	*
4	<u>Adicionar</u> <u>R</u> emover	All Files		• •
: D / -		Cancelar	Salvar	
Pagina 4 / 11	utadar 🖂 [reat@stirau	Eccesion Chuit III Truc Chunt III Com títule 1		- 🕣 115%

10. Selecione o algoritmo de criptografia que será usado. No caso vamos usar o algoritmo AES e para geração da chave criptográfica (hash) utilizarei o RIPEMD-160 por se tratar de um algoritmo que gera chaves fortes, conforme mostrado na figura abaixo:.

TrueCi	rypt Volume Creation Wizard
	Encryption Options
<u></u>	AES <u>T</u> est
	FIPS-approved cipher (Rijndael, published in 1998) that may be used by U.S. government departments and agencies to protect classified information up to the Top Secret level. 256-bit key, 128- bit block, 14 rounds (AES-256). Mode of operation is XTS.
H	\$
	More information on AES
	Hash Algorithm Information on hash algorithms
	Aj <u>u</u> da < <u>P</u> rev <u>N</u> ext > <u>C</u> ancelar

11. Selecione o tamanho que você deseja que o seu drive (sua pasta) possua.

TrueCr	ypt Volume Creation Wizard
TRUEGBAPT	Volume Size 100 MB Free space available: 33,4 GB Please specify the size of the container to create. If you create a dynamic (sparse-file) container, this parameter will specify its maximum size. Note that the minimum possible size of a FAT volume is 275 KB. The minimum possible size of an NTFS volume is 2829 KB.
	Aj <u>u</u> da < <u>P</u> rev <u>N</u> ext > <u>C</u> ancelar

12. A janela seguinte é a "Volume Password", digite uma senha grande com alguns caracteres especiais tais como: arroba, misturar letras maiúsculas e minusculas, números, pode ser uma frase para facilitar. (Não esqueça essa senha). Depois clique em "Next" conforme figura abaixo:

TrueCr	ypt Volume Creati	on Wizard	
	Volume Pass	word	
	Password:	•••••	
	Confirm password:	••••••	
		<u>D</u> isplay password	
		Use keyfiles	<u>K</u> eyfiles
TRUEO	It is very important avoid choosing one found in a dictionar should not contain a easy to guess. A go and lower case lette ^ = \$ * + etc. We n more than 20 chara possible length is 6	that you choose a good password. that contains only a single word the y (or a combination of 2, 3, or 4 suc- any remes or dates of birth. It shou od password is a random combinat ers, numbers, and special character ecommend choosing a password co cters (the longer, the better). The m 4 characters.	You should at can be h words). It Id not be ion of upper s, such as @ nsisting of naximum
	Aj	<u>u</u> da < <u>P</u> rev <u>N</u> ext >	<u>C</u> ancelar

13. A tela a seguir informa que a senha é pequena, convém mudar para uma senha mais longa e forte, a tela sugere que a senha tenha 20 caracteres, poderá prosseguir mesmo assim se preferir.



14. Selecione o sistema de arquivos "Filesystem type" conforme figura abaixo:

TrueCry	ypt Volume Creation Wizard
TRUECAPT	Format Options Filesystem Options Filesystem type: Linux Ext3 Volume Format Options Quick format In order to enable your operating system to mount your new volume, it has to be formatted with a filesystem. Please select a filesystem type. If your volume is going to be hosted on a device or partition, you can use 'Quick format' to skip encryption of free space of the volume.
	Aj <u>u</u> da < <u>P</u> rev <u>N</u> ext > <u>C</u> ancelar

15. Selecione a opção **"I will mount the volume only on linux"** para usar somente no sistemas linux, conforme figura abaixo:

TrueCr	ypt Volume Creation Wizard
	 ypt Volume Creation Wizard Cross-Platform Support I will mount the volume on other platforms Choose this option if you need to use the volume on other platforms. I will mount the volume only on Linux Choose this option if you do not need to use the volume on other platforms.
	Ajuda Prev Next > Cancelar

16. Na próxima tela você deve ficar mexendo o mouse pra lá e pra cá em cima do programa truecrypt, perceba que em quanto você faz isso os dados que aparecem ali vão mudando isso serve para gerar dados aleatórios para aumentar a segurança da chave, quanto mais tempo e mais vezes mexer no mouse, mais forte a chave ficará. Depois clique em format para ``**Format**'' conforme figura abaixo:

TrueCr	ypt Volume Creation Wizard
	Volume Format
	Random Pool: c5B31c83c13cE6BBDB9ccA4A20 Show Header Key: Master Key:
UE C	Abort Done Speed Left IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly
L I	increases the cryptographic strangth of the encryption keys. Then click Format to create the volume.
	Aj <u>u</u> da < <u>P</u> rev <u>F</u> ormat <u>C</u> ancelar

17. O volume começa a formatação, conforme figura abaixo:



18. Será pedido a senha do administrador do linux, conforme figura abaixo:



19. A pasta criptografada foi criada com sucesso, conforme figura abaixo:



20. Clique em "Exit" para sair, conforme figura abaixo:



21. Após a pasta ter sido criada é necessário montar, clique em um dos **slot**, depois em **SelectFile**... conforme figura abaixo:

			ŝ	TrueCr	ypt			_	X
<u>V</u> olume	s <u>K</u> eyfiles	<u>F</u> avorites	T <u>o</u> ols	Setting	s <u>H</u> elp				
Slot	Volume				Size	Mount Direct	vio	Type	
- 1							,		
2									
i 3									
🦦 <u>4</u>									
- 5									
⇔ 6									
- 7									
🥪 9									
🥪 10									
🥪 11									
a 12									∇
Crea	te Volume			olume Pr	operties		<u>W</u> ip	e Cache	
Volume									
						▼	Sele	ct <u>F</u> ile	
	✓ <u>N</u> ever	save histor	y		Volu	me <u>T</u> ools	Select	Device	
	Mount	<u>Auto-I</u>	Mount D	evices	Di <u>s</u> m	ount All	1	E <u>x</u> it	

22. Selecione o arquivo o qual foi salvo anteriormente no item 9 deste tutorial. conforme figura abaixo:

	Select a TrueCrypt Volume				×
🖉 📄 home tes	tebackup				
<u>L</u> ocais	Nome	▼	Tamanho	Modificado	
Q Pesquisar	🔝 arquivo de senha da pasta criptografada		100,0 MB	10:12	
🛞 Usado recentem					
📠 melo					
🛅 Desktop					
Sistema de arqui					
📠 dados					
📠 Consulta					
📠 dados					
🔟 usuarios	n n				
💾 Unidade de Disq					
20100529_1820					
Pocumentos					
Música					
间 Imagens					
I Vídeos					
Download					
🥃 ver dia 17 jun 20					∇
Adicionar Remover		All	Files		▼
			<u>Cancelar</u>	Abrir	

23. Clique em mount, conforme figura abaixo:

.

	Volume			Size	Mount Directory	Type
- 1				0.20		.,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
2						
. 3						
. 4						
> 5						
6						
» 7						
» 8						
9						
» 10						
» 11						
» 12						
Crea	te Volume		Volume F	properties	<u>v</u>	Vipe Cache
olume	-					
	/home/tes	stebackup/ar	quivo de senl	na da pasta	criptograt 🔻 Se	elect <u>F</u> ile
	Never a	save history		Volu		act Device
	I INCOCI 3					

24. Para proceder a montagem do driver criptografado (pasta criptografada), deverá surgir a janela solicitando a senha de acesso gerada no processo de criação pasta (ítem 9 deste tutorial) e a senha do administrador linux, conforme figura abaixo:

	Administrator privileges required 🛛 🗙
Enter	r your user password 🕃 administrator password:
	<u>C</u> ancelar <u>O</u> K

25. Finalmente, poderá acessar a pasta protegida como qualquer outro HD, adicionando arquivos que serão protegidos no drive truecrypt1, conforme mostrado na figura abaixo:

Aplicativos Locais Siste	ema 🙋 🕐		ः 🛙 🎸 🎸 🖨	🖣 🖂 Qui 17 Jun, 10:20 🔵 melo 🖒
I	truec	rypt1 - Navegador d	e Arquivos	- <u>×</u> ×
<u>A</u> rquivo <u>E</u> ditar <u>V</u> er <u>I</u> r <u>M</u> a	rcadores Aj <u>u</u> da			
🔶 Voltar 🔻 📦 Avançar	• 숨 🔕 🧲 🙍	💻 Q. 100% Q	Visão em ícones 🔻 🔍	
Locais 🔻 🗱	◄ truecrypt1			
📷 melo				
Area de trabalho	Δ.			
Sistema de arquivos	lost+found	pasta sem título	pasta sem título 2	
Rede		•		
Consulta				
🔄 dados 🛛 🚔				
floppy				
floppy0				
pendrive				
🔄 usuarios 🛛 🛔				
🔄 truecrypt1 🛛 📥				
🗒 Lixeira				
Documentos	•			
🔏 Música				
Imagens				
Vídeos				
Download				
🥃 ver dia 17 jun 2010				
				N
				M2
	3 itens, espaço livre: 86,1	MB		
📰 👔 truecrypt1 - Nave	root@stiraux2: /h	TrueCrypt	📸 Sem titulo 1.odt 📃	Sessão - Shutter

26. Para desmontar é necessário estar como root. Use somente o software truecrypt para desmontar, caso contrário aparecerá a mensagem conforme figura abaixo:



27.Agora vamos desmontar o drive criptogrado (considere essa ação obrigatório para evitar perder dados). Clique em ``Dismount'' conforme figura abaixo:

	🖀 TrueCrypt 📃 🗙				
<u>V</u> olume	s <u>K</u> eyfiles <u>F</u> avorites T <u>o</u> ols	Setting	s <u>H</u> elp		
Slot	Volume		Size	Mount Directory	Type
- 1	/dev/sdb1		1.9 GB	/media/truecrypt1	Normal A
	,,		-,	,,,,,,	
🥪 3					
🥪 <mark>4</mark>					
i 🕹 🕹					
 					
- 7					
8					
9					
See 10					
- 11 - 12					~
Crea	ate Volume	lume Pr	operties	W	ipe Cache
Volume					
	/dev/sdb1				
	Volume Tools Select Device				
-					
D	Dismount All Exit				

Obs: Do item 1 ao 27 foi mostrado como criar uma pasta criptografada. Daqui em diante será mostrado como criptografar um pendrive ou partição do disco, pois os procedimentos para os dois casos são os mesmos.

28 Para criar uma pasta criptografada Após instalado o Truecryp, vá no menu acessórios, depois opção "truecrypt".

29. Clique no botão **"Create Volume"** para um pendrive ou partição criptograda, conforme figura abaixo:

	👔 TrueCrypt 📃 🗙								
<u>V</u> olume	es <u>K</u> eyfiles	<u>F</u> avorites	T <u>o</u> ols	Setting	s <u>H</u> elp				
Slot	Volume				Size	Mount Direct	vio	Type	
- 1							,	.76-	
🧼 2									
🥪 3									
🥪 4									
🥯 5									
 ✓ 6 									
~ 7									
8		3							
- 10									
- 10									
- 12									~
Crea	ate Volume]	V	olume P	roperties		Wip	e Cache	
Volume	2	- -							_
	v Select <u>F</u> ile								
	⊻ <u>N</u> ever	save histor	/		Volu	ime <u>T</u> ools	Select	Device	•
	Mount	Auto-1	1ount D	evices	Di <u>s</u> m	ount All		E <u>x</u> it	

30. Clique em ``Create a volume within a partition/drive'', conforme figura abaixo:



31. Selecione opção ``Stardard TrueCrypt volume'' conforme figura abaixo:.



32. Clique em ``Select Device...'' conforme figura abaixo:



33.. Selecione o pendrive conforme figura abaixo:

Device		Size	Mount Directory
🧼 /dev/sda:		74,5 GB	
/dev/sda1		71,5 GB	1
/dev/sda5	3	3,1 GB	
🧼 /dev/sdb:		1,9 GB	
/dev/sdb1		1,9 GB	/media/pendrive

34. Clique em ``**Next**'' conforme figura abaixo:

TrueCr	ypt Volume Creation Wizard	
	Volume Location	
	/dev/sdb1	▼ Select Device
	✓ Never save history	
<u>n a se a s</u>	A device-hosted TrueCrypt volume can b disk partition, solid-state drive, USB mer storage devices	e created within a hard mory stick, and other
	WARNING: Note that the partition/device	will be formatted and all
	data currently stored on it will be lost.	
н		
	₽	
	Aj <u>u</u> da < <u>P</u> rev	<u>N</u> ext > <u>C</u> ancelar

35. Clique em Sim, conforme figura abaixo:

	TrueCrypt
?	IMPORTANT: We strongly recommend that inexperienced users create a TrueCrypt file container on the selected device/ partition, instead of attempting to encrypt the entire device/ partition.
	When you create a TrueCrypt file convainer (as opposed to encrypting a device or partition) there is, for example, no risk of destroying a large number of files. Note that a TrueCrypt file container (even though it contains a virtual encrypted disk) is actually just like any normal file. For more information, see the chapter Beginner's Tutorial in the TrueCrypt User Guide.
	Are you sure you want to encrypt the entire device/partition?
	<u>N</u> ão <u>S</u> im

36. g. coloque a senha do administrador (senha de root) conforme figura abaixo:

	Administrator privileges required 🛛 🗙
E	inter your user password or administrator password:
	••••••
	<u>C</u> ancelar <u>O</u> K

37. Clique em **Sim** para formatar, conforme figura abaixo: (certifique-se de ter feito backup dos dados antes).



38. Escolha o algoritmo de encriptação e o algorimo de hash logo abaixo (se preferir, deixe o padrão) coforme figura abaixo:

TrueCr	ypt Volume Creation Wizard	
	Encryption Options	
	AES	↓ <u>T</u> est
ECBY	FIPS-approved cipher (Rijndael used by U.S. government depa classified information up to the bit block, 14 rounds (AES-256).	l, published in 1998) that may be intments and agencies to protect e Top Secret level. 256-bit key, 128- . Mode of operation is XTS.
	More information on AES	
TF	Hash Algorithm	Information on hash algorithms
	Aj <u>u</u> da	< <u>P</u> rev <u>N</u> ext > <u>C</u> ancelar

39. Digite a senha para criptografar o pendrive, a qual será usada para montá-lo posteriormente.

TrueCrypt Volume Creation Wizard		
	Volume Password	
	Password:	
	Confirm password:	
	Display password	
	Use keyfiles	
TRUEO	It is very important that you choose a good password. You should avoid choosing one that contains only a single word that can be found in a dictionary (or a combination of 2, 3, or 4 such words). It should not contain any names or dates of birth. It should not be easy to guess. A good password is a random combination of upper and lower case letters, numbers, and special characters, such as @ $^ = \$ * + $ etc. We recommend choosing a password consisting of more than 20 characters (the longer, the better). The maximum possible length is 64 characters.	
	Ajuda < <u>P</u> rev <u>N</u> ext > <u>C</u> ancelar	

40. A tela a seguir informa que a senha é pequena, convém mudar para uma senha mais longa e forte, a tela sugere que a senha tenha 20 caracteres, poderá prosseguir mesmo assim se preferir.



41. Agora vamos 'formatar' nossa pendrive/partição, escolhendo o sistema de arquivos (**Filesystem type**). Pode optar pela formatação rápida (Quick format) conforme figura abaixo:

TrueCry	ypt Volume Creation Wizard
TRUECBAPT	Format Options Filesystem Options Filesystem type: FAT Volume Format Options Quick format In order to enable your operating system to mount your new volume, it has to be formatted with a filesystem. Please select a filesystem type. If your volume is going to be hosted on a device or partition, you can use 'Quick format' to skip encryption of free space of the volume.
	Aj <u>u</u> da < <u>P</u> rev <u>N</u> ext > <u>C</u> ancelar

42. Clique em ``**Format**´´ para iniciar a formatação, conforme figura abaixo:

TrueCr	ypt Volume Creation Wizard
	Volume Format
	Random Pool: 07EDA3EE274EAA15F513E64236 Show Header Key: Master Key:
0	Abort
TRUE	Done Speed Left IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.
	Ajuda < <u>P</u> rev <u>F</u> ormat <u>C</u> ancelar

43. A seguir é informado que o dados do pendrive serão apagados, certifique que fez backup do dados e clique em sim para continuar, conforme figura abaixo:

TrueCrypt ×							
CAUTION: ALL FILES CURRENTLY STORED ON THE SELECTED DEVICE '/dev/sdb1' WILL BE ERASED AND LOST (THEY WILL NOT BE ENCRYPTED)!							
Are you sure you want to proceed with format?							
<u> №ão Sim </u>							

44. Pendrive criado com sucesso, conforme figura abaixo:



45. clique em ``Exit'' para sair, conforme figura abaixo:



46. Montando o pendrive (para montar ou desmontar será sempre usado o truecrypt). Clique no **slot**, depois selecione o dispositivo (**Selecte Device...**), conforme figura abaixo:

				TrueCr	ypt			L	
<u>V</u> olume:	s <u>K</u> eyfiles	<u>F</u> avorites	T <u>o</u> ols	Settin <u>g</u>	s <u>H</u> elp	_	-	-	
Slot	Volume				Size	Mount Direct	ory	Туре	
- 1									
🧼 2									
3									
- 6									
- 7									
ھ 🥪									
🥪 9									
10									
11									_
- IL									V
<u>C</u> rea	te Volume]	V	olume Pi	roperties		Wip	e Cache	
Volume									
	/dev/sdb1					▼	Sele	ct <u>F</u> ile	
	Mevers	ave history	/		Volu	me <u>T</u> ools	Select	D <u>evice</u> .	
	Mount	Auto-N	1ount D	evices	Dism	ount All		E <u>x</u> it	

47. Clique em ``Mo	unt´´, c	conforme	figura	abaixo:
--------------------	----------	----------	--------	---------

			TrueCry	pt			_	×
<u>V</u> olume	s <u>K</u> eyfiles <u>F</u> av	orites T <u>o</u> ols	Settin <u>g</u> s	<u>H</u> elp	_	-		=
Slot	Volume			Size	Mount Direct	ory	Туре	
								Δ
🧼 <mark>2</mark>								
i i i i i i i i i i i i i i i i i i i								
4								
S								
6								
~ ~								
- 9								
- 10								
- 11								
- 12								~
Crea	ate Volume	V	olume Pro	perties		Wip	e Cache	
Volume								
	/dev/sdb1	3			▽	Sele	ct <u>F</u> ile	
	✓ Never save	history		Volu	me <u>T</u> ools	Select	D <u>e</u> vice	
	Mount	<u>A</u> uto-Mount D	evices	Di <u>s</u> m	ount All		E <u>x</u> it	

48. Digite a senha criada anteriormente, conforme figura abaixo:

E	Enter password for "/d	ev/sdb1"	×
Password:	[<u>O</u> K
	 Cache passwords and keyfile Display passwords 	<u>C</u> ancelar	
	Use keyfiles	Keyfiles	Op <u>t</u> ions >

49. O drive criptografado nesse caso ficou montado no caminho /**media/truecrypt1** (veja na figura abaixo), o qual poderá ser acessado diretamente pelo Meu Computador.

. TrueCrypt ficará residente no sistema, bastando um clique no respectivo ícone para surgir novamente e caso seja a intenção, poderá r desmontar o volume clicando no botão ``**Dismount**'' conforme figura abaixo:

			TrueC	rypt			L	×
<u>V</u> olume	s <u>K</u> eyfiles <u>F</u> a	avorites T <u>o</u>	ols Setting	is <u>H</u> elp	_	-	-	
Slot	Volume		-N	Size	Mount Direct	ory	Туре	
- 1	/dev/sdb1			1,9 GB	/media/truecr	ypt1	Normal	
🧼 2								
G 3								
≪ 4								
- 6								
- 7								
🥪 9								
- 10								
11								
Se 12								▼
					1			
<u>C</u> rea	ate Volume		Volume P	roperties		Mik	be Cache	
Volume	2							
	/dev/sdb1					Sele	ct <u>F</u> ile	
	✓ Never say	e history		Volu	ime Tools	Select	Device	
				VOID		Sciect	Device	•
		Υ		γ			A CONTRACTOR	
C	Dismount	<u>A</u> uto-Mou	int Devices	Di <u>s</u> m	ount All		E <u>x</u> it	

50. Não tente montar o pendrive/partição cryptografada sem o truecrypt, caso contrário aparecerá a mensagem de erro conforme figur abaixo:

