## Avvocato Hacker

Strumenti per la cifratura, la cancellazione sicura e il backup dei dati e per la sicurezza degli Smart Phone

## Sicurezza delle informazioni

- La sicurezza delle informazioni è un'esigenza che ha accompagnato la storia dell'uomo fin dalle antiche civiltà
- Il termine Crittografia deriva da Kryptós + gráphein = nascosto + scrivere: l'arte di scrivere messaggi segreti
- Erodoto (440 a.c.) racconta di un nobile persiano che fece tagliare a zero i capelli di uno schiavo fidato al fine di poter tatuare un messaggio sul suo cranio; una volta che i capelli furono ricresciuti, inviò lo schiavo alla sua destinazione, con la sola istruzione di tagliarseli nuovamente

## Sicurezza delle informazioni

- Svetonio racconta che Giulio Cesare cifrava i messaggi sostituendo ogni lettera con quella che nell'alfabeto segue di 3 posizioni
- «Extant et ad Ciceronem, item ad familiares domesticis de rebus, in quibus, si qua occultius perferenda erant, per notas scripsit, id est sic structo litterarum ordine, ut nullum verbum effici posset: quae si qui investigare et persequi velit, quartam elementorum litteram, id est D pro A et perinde reliquas commute» (De vita duodecim Caesarum - Libri VIII)

## Il Cifrario di Giulio Cesare

Testo in chiaro	a	b	с	d	е	f	g	h	i	j	k	I	m	n	o	р	q	r	s	t	u	v	w	x	у	z
Testo cifrato	D	E	F	G	Н	I	J	к	L	М	N	0	Ρ	Q	R	S	Т	U	v	w	х	Y	Z	A	В	С

Lo stesso si può fare con l'alfabeto italiano:

Testo in chiaro	a	b	с	d	е	f	g	h	i	I	m	n	0	р	q	r	s	t	u	v	z
Testo cifrato	D	Ε	F	G	H	I	L	М	N	0	Ρ	Q	R	S	Т	U	V	Z	A	В	С

Per cifrare un messaggio, basta prendere ogni lettera del testo in chiaro e sostituirla con la corrispondente lettera della riga testo cifrato. Per decifrare, viceversa. Ecco un semplice esempio:

Testo in chiaro	attaccare	gli	irriducibili	galli	alla	ora	sesta
Testo crittato	DZZDFFDUH	LON	NUUNGAFNENON	LDOON	DOOD	RUD	VHVZD

## Il Cifrario di Giulio Cesare

- Tutti i cifrari di questo tipo sono divenuti **molto semplici da rompere**: nessuno è adatto per comunicazioni sicure allo stato tecnologico attuale, né lo è stato negli ultimi 1000 anni!!
- Tuttavia....un rudimentale sistema di cifratura basato sul cifrario di Cesare è stato usato anche da Bernardo Provenzano per proteggere le informazioni scritte nei suoi famosi pizzini

## I pizzini di Provenzano

"(...) Per una visita medica: avevo intenzione di contattare, con il tuo permesso, 1012234151512 14819647415218. Acquisto terreni: sono stato un po' disubbidiente su questo argomento in quanto sotto le feste mi sono visto con la persona interessata 512151522 191212154 e siamo rimasti che dopo le feste ci dovevamo vedere per discutere [...] "

• Le sequenze numeriche si ottengono rappresentando le lettère con dei numeri, in base all'ordine alfabetico (quindi A=1, B=2, ecc.) e poi sommando un valore prefissato – in questo caso 3

4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
А	В	С	D	Ш	F	G	Η		L	Μ	Ζ	0	Ρ	Ø	R	S	Т	U	$\mathbf{<}$	Ζ

• Quindi

- "10 12 23 4 15 15 12"
- "14819647415218"

• "5 12 15 15 22"

• "19 12 12 15 4"

- = "Givanni"
- = "Mercadante"
  - = "Binnu"
  - = "**Riina**"

## La sicurezza delle informazioni «moderna»

- Oggi buona parte del pianeta vive nella società dell'informazione, basata cioè sull'uso delle informazioni come parte integrante delle attività umane
- Qualunque programma che si occupi di preservare la sicurezza delle informazioni, persegue, in qualche misura, tre obiettivi fondamentali:
  - o Disponibilità
  - o Integrità
  - o Riservatezza

## Disponibilità

- La disponibilità è il grado in cui le informazioni e le risorse informatiche sono accessibili agli utenti che ne hanno diritto, nel momento in cui servono
- Per esempio:
  - Sistemi di backup locale e remoto
  - o Firewall e Intrusion Detection System
  - o Gruppi di continuità

## Integrità

 L'integrità è il grado di correttezza, coerenza e affidabilità delle informazioni e il grado di completezza, coerenza e condizioni di funzionamento delle risorse informatiche

- Per esempio:
  - Procedure di manutenzione e aggiornamenti del sistema operativo e dei programmi applicativi
  - Antimalware (Virus, Trojan, Spyware, Worm,..)

## Riservatezza

- La riservatezza consiste nel limitare l'accesso alle informazioni e alle risorse informatiche alle sole persone autorizzate
- Per esempio:
  - Cifratura dei dati e delle comunicazioni
  - o Cancellazione sicura dei dati digitali
- Ma anche il fattore umano gioca il suo ruolo
  - Scegliere in modo adeguato una password e tenerla segreta
  - **Rifiutare informazioni a sconosciuti** (anche quando affermano di essere tecnici della manutenzione!!)

## L'avvocato hacker

• Vediamo 4 possibili scenari reali:

- 1. Utilizzo una chiavetta USB per conservare i dati di un cliente e la perdo...
- 2. Devo cancellare un file che ho sul computer e non voglio che si possa recuperare...
- 3. Devo dismettere il vecchio computer dello studio per regalarlo all'associazione cui sono iscritto e non voglio che i dati presenti siano recuperabili...
- 4. Ho tutti i dati dello studio su un solo computer e si rompe in modo irrecuperabile l'hard disk...

## Esempio 1: Cifratura di una chiavetta USB

- La cifratura della chiavetta USB è una possibile soluzione, a patto che:
  - Si utilizzino **tecniche consolidate e sicure** (ovvero algoritmi di cifratura affidabili e senza falle riconosciute, es. AES, Serpent, Twofish)
  - Si scelga una password adeguata (no parole di un dizionario, nomi propri, date di nascita, troppo corte, si frasi lunghe, ma per voi facili da ricordare con maiuscole, minuscole, numeri e simboli es.
     @GenovaCiSono2Squadre (21 caratteri)
  - Potete utilizzare un calcolatore per il tempo di violazione della password disponibile online http://lastbit.com/pswcalc.asp

## Passo 1: Scarico TrueCrypt

#### • Sito web: <u>www.truecrypt.org</u>

• Disponibile per Windows, Mac OS X e Linux

<b>*</b>	🕆 www.truecrypt.	org						
т	RUECF							
FR	EE OPEN-	SOURCE	O N	- T H E - F	LYEN	ІСКҮРТІ	O N	
Home	Documentation	Downloads	News	Future	History	Screenshots	Donations	FAQ

#### TrueCrypt

Free open-source disk encryption software for Windows 7/Vista/XP, Mac OS X, and Linux

## Passo 2: Eseguo il software

TrueCi	ypt								x
Volumes	System	Favorites	Tools	Settings	Help			Hon	nepage
Drive	Volume					Size	Encryption algorit	hm Type	
≪G: ≪H: ≪T:									
<ul> <li>⇒ J:</li> <li>⇒ K:</li> </ul>									E
≪L: ≪M: ≪N:									
©0: ©P: ©0:									
@R: @S:									-
	<u>Preate Volur</u>	ne		⊻olume	Propertie	s,		<u>W</u> ipe Cache	
Volume							<b>•</b>	Select <u>F</u> ile	
		ever save his	tory		Vo	lume <u>T</u> ool	s Se	ect D <u>e</u> vice	
	Mount	A	uto-Moun	t Devices		Di <u>s</u> mour	nt All	E <u>x</u> it	

## Passo 3: Creo il volume

TrueC	rypt									x
Volumes	System	Favorites	Tools	Settings	Help				Home	page
Drive G: G: H: J: K: L: M: N: O: Q: R: S:	Volume					Size	Encryption	algorithm	Туре	
Volume	<u>Create Volur</u>	ne		Volume	Propertie	es		<u>W</u> ipe	Cache	
1		ever save his	tory		Vo	olume <u>T</u> ool	▼ s	Select Select D	File	
	<u>M</u> ount	<u>A</u> u	uto-Moun	t Devices		Di <u>s</u> mour	nt All		E <u>x</u> it	

## Passo 4: Seleziono il tipo



## Passo 5: Seleziono il tipo



## Passo 6: Scelgo la modalità



## Passo 7: Scelgo l'algoritmo

TrueCrypt Volume Creation Wizard		x
Encryption Options         AES         FIPS-approved cipher (Rijndael, published in 1998) to used by U.S. government departments and agencies classified information up to the Top Secret level. 256 128-bit block, 14 rounds (AES-256). Mode of operation More information on AES         Bene         Hash Algorithm         RIPEMD-160       Information on hash algorithm	Test that may be to protect 6-bit key, tion is XTS. nchmark	
Help < Back Next >	Cancel	

## Passo 8: Scelgo la dimensione



## Passo 9: Scelgo la password

TrueCrypt Volume Creation Wizard	
TBUEGBAPT	Volume Password         Password:       ************************************
	Help < Back Next > Cancel

## Passo 10: Scelgo il FileSystem

TrueCrypt Volume Creation Wizard	
Vo Fil R R I I I I I I I I I I I I I I I I I	Iume Format         Dotions         lesystem       FAT         Cluster       Default         Quick Format         Random Pool:       DAEB63F1F7B138DDEC839677C1BFA8D0         Random Pool:       DAEB63F1F7B138DDEC839677C1BFA8D0         Header Key:       Master Key:         Master Key:       Abort         Done       Speed         Left       ORTANT: Move your mouse as randomly as possible within this dow. The longer you move it, the better. This significantly eases the cryptographic strength of the encryption keys. Then cromat to create the volume.
	Help < Back Format Cancel

## Passo 11: Formatto

	TrueCrypt Volume Creation Wizard	
	Volume Format Options Filesystem FAT  Cluster Default  Quick Format	
TrueCrypt Vo	B138DDEC839677C1BFA8D0	
<b>A</b>	CAUTION: ALL FILES CURRENTLY STORED ON THE SELECTED PARTITION '\Device\Harddisk1\Partition1' (I:) WILL BE ERASED AND LOST (THEY WILL NOT BE ENCRYPTED)! Are you sure you want to proceed with format? Are you sure you want to proceed with format?	
	Sì No ngth of the encryption keys. Then	
	Help < Back Format Cancel	

## Passo 12: Attendo...

TrueCrypt Volume Creation Wizard	
	Options         Filesystem       FAT ▼ Cluster       □ Quick Format         Random Pool:       B83EB9136DDA4BA4E40F7B7C30631710       ✓         Header Key:       2EBAA7BD2A65B3422595752A1C4EE3BF         Master Key:       95F0FF3C2F558831B69633F8B26C3995         Import for the longer you 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.
	Help < Back Format Cancel

## Passo 13: Leggo...

TrueCrypt Volume Creation Wizard

×

IMPORTANT: Please keep in mind that this volume can NOT be mounted/accessed using the drive letter I:, which is currently assigned to it!

To mount this volume, click 'Auto-Mount Devices' in the main TrueCrypt window (alternatively, in the main TrueCrypt window, click 'Select Device', then select this partition/device, and click 'Mount'). The volume will be mounted to a different drive letter, which you select from the list in the main TrueCrypt window.

The original drive letter I: should be used only in case you need to remove encryption from the partition/device (e.g., if you no longer need encryption). In such a case, right-click the drive letter I: in the 'Computer' (or 'My Computer') list and select 'Format'. Otherwise, the drive letter I: should never be used (unless you remove it, as described e.g. in the TrueCrypt FAQ, and assign it to another partition/device).

OK

## Come accedo al volume?

			23
Computer >	- 🔀 Cerca Computer		٩
Organizza 🔻 Espelli Proprietà Proprietà del sistema Disinst	alla o modifica programma 🛛 » 📓	•	0
<ul> <li>Preferiti</li> <li>Desktop</li> <li>Download</li> <li>Dropbox</li> <li>R Microsoft Windows</li> <li>È necessario formattare il disco nell'unità I: per poterlo utilizzare.</li> <li>Formattarlo?</li> </ul>	Unità BD-ROM (E:) ElcomSoft 0 byte disponibile su 282 MB CDFS Disco rimovibile (I:) FAT		
Formatta disco Annulla			
Disco rimovibile			

## Passo 1: Monto la chiavetta

TrueCr	ypt									x
Volumes	System	Favorites	Tools	Settings	Help				Home	page
Drive G: H: J: K: L: M: N: O: P: Q: R: S: T: U:	Volume					Size	Encryption	n algorithm	Туре	
C	reate Volun	ne		Volume	Propertie	es		<u>W</u> ipe	Cache	
	▼ №	ever save his	tory		Vc	olume <u>T</u> ool	▼ s	Select Select [	: <u>F</u> ile D <u>e</u> vice	
	<u>M</u> ount	A	ito-Moun	t Devices		Di <u>s</u> mour	nt All		E <u>x</u> it	

## Passo 2: Inserisco la password

Enter TrueCrypt Volume Password					
Password:	*****		ОК		
	Cache passwords and	Cancel			
	Display password				
	Use keyfiles	Keyfiles	Mount Options		

## Passo 3: Visualizzo...

TrueCr	ypt									×
Volumes	System	Favorites	Tools	Settings	Help				Homep	age
Drive	Volume					Size	Encryptio	n algorithm	Туре	<b>A</b>
Sin G:	Device Ha	rddisk1\Parti	tion 1			957 MB	AES		Normal	
₩H:										
🥯 ]:										
≪K:										
See La										=
- M: ≪≫N:										
See 0:										
Sep:										
<b>O:</b>										
≪≫R:										
S:										
≪≥т:										
<b>⊚</b> ∪:										Ŧ
<u>c</u>	reate Volur	me		<u>V</u> olume	Properti	es		Wipe	Cache	
Volume										
							•	Select	t <u>F</u> ile	
		ever save his	tory		V	olume <u>T</u> ool	s	Select [	D <u>e</u> vice	
	<u>)</u> ismount		uto-Moun	t Devices		Dismour	nt All		E <u>x</u> it	

## Passo 4: Accedo...



# Esempio 2: Cancellazione sicura di un file

- La cancellazione di un file attraverso la funzione «Elimina» di un sistema operativo non cancella in modo definitivo il file
- E' come cancellare da un libro i riferimenti a un capitolo dell'indice e sperare che qualcuno che lo sfoglia tutto non si accorga del capitolo in più...
- Esistono diversi software di **data recovery** anche gratuiti per recuperare i file cancellati attraverso Windows (e in molti casi possono essere utilissimi...es. Recuva - <u>http://www.piriform.com/</u>)
- Per garantire una cancellazione sicura di un file devo sovrascriverlo con sequenze di zeri oppure dati casuali

## Passo 1: Scarico Eraser

### • Sito web: <u>http://eraser.heidi.ie/</u>

• Disponibile per Windows

eraser.heidi.ie/download.php	9	☆ ▽ C <sup>e</sup> ) 🚼 ▼ e	raser	۹ م	
Eraser Downloads	Home	Downloads	Forum	Trac	
Thank for you having interest in Eraser. Eraser is available in a few flavours, the					

stable, the beta as well as the nightly builds.

Stable builds of Eraser are builds in which few, if any, bugs remain in the code and is suitable for use in all environments. If in doubt, choose the Stable version. The beta and nightly builds cater to a slightly different audience. Beta and nightly builds are built on the previous stable version released, but may contain new



Posted by: Joel, 6<sup>th</sup> November 2011, 1:30 pm +800GMT

# Passo 2: Cancello in modo sicuro il file

### • Click con il tasto destro sul file

• Scelgo la voce **Erase** 



## Passo 3: Scelgo le opzioni

- Nella schermata che compare faccio click sul tasto «Options»
- Scelgo l'algoritmo di cancellazione sicura
  - Dati casuali (1 passaggio)
  - US DoD 5220.22-M (3 passaggi)
  - US DoD 5220.22-M (7 passaggi)
  - Gutmann (35 passaggi)

Confirm	Erasing
	Are you sure you want to erase 'C:\Users\MATTIA\Desktop\Documento da cancellare.docx'?
Optio	Ons Yes No

Prefe	rence	s: Erasing		<b>—</b> X		
File	Files Unused Disk Space					
E	rase w	ith				
	#	Description	Passes	New		
	1	Gutmann	35	Edit		
	2	US DoD 5220.22-M (8-306. / E, C and E)	7			
	3	US DoD 5220.22-M (8-306. / E)	3	Delete		
	4	Pseudorandom Data	1			
	5	Only first and last 2KB	1			
	6	Schneier's 7 pass	7			
Selected: Gutmann (35 passes) Overwrite Cluster Tip Area File Names (File Names will always be cleared on NT/XP and above) Alternate Data Streams						

Annulla

## Passo 4: Attendo...

Eraser		
Erasing:	Files Overwriting	
Item: Pass:	C:\Users\MATTIA\Downloads\Eraser 6.0.9.2343.exe 6 of 35	
		14%
Total:		14%
Show 1	results Stop	

rasing Report		23
Task completed.		
Information:		
Statistics:		
Erased area	= 8892 kB	
Cluster tips	= 7766 bytes	
Data written	= 311220 kB	
Write time	= 6.33 s	
Write speed	= 49143 kB/s	-
4		•
Failures:		
# Item		
	Save As Clo	se )

# Esempio 3: Cancellazione sicura di hard disk

- Il principio è analogo a prima: cancellazione mediante sovrascrittura
- In questo caso non cancello un singolo file ma l'intero contenuto di un hard disk
- Diverse soluzioni gratuite per raggiungere il risultato:
  - Active Kill Disk for Windows (<u>http://www.killdisk.com/</u>)
  - DBAN (Darik's Boot and Nuke) (<u>http://www.dban.org/</u>)
  - DiskWipe (<u>http://www.diskwipe.org/</u>)

## Passo 1: Scarico DBAN

### • Sito web: <u>http://www.dban.org/</u>

• CD di avvio del computer per la cancellazione sicura



#### About DBAN

Darik's Boot and Nuke ("DBAN") is a self-contained boot disk that securely wipes the hard disks of most computers. DBAN will automatically and completely delete the contents of any hard disk that it can detect, which makes it an appropriate utility for bulk or emergency data destruction. DBAN is a means of ensuring due diligence in computer recycling, a way of preventing identity theft if you want to sell a computer, and a good way to totally clean a Microsoft Windows installation of viruses and spyware.

## Passo 2: Masterizzo su CD

 Utilizzo p.es. CD Burner XP (<u>http://cdburnerxp.se/</u>) e scelgo l'opzione «Masterizza immagine ISO»



## Passo 2: Avvio il computer da CD

## • Avvio il computer da cancellare con il CD appena creato

Darik's Boot and Nuke

Marning: This software irrecoverably destroys data.

This software is provided without any warranty; without even the implied warranty of merchantability or fitness for a particular purpose. In no event shall the software authors or contributors be liable for any damages arising from the use of this software. This software is provided "as is".

http://www.dban.org/

- \* Press the F2 key to learn about DBAN.
- \* Press the F3 key for a list of quick commands.
- \* Press the F4 key to read the RAID disclaimer.
- \* Press the ENTER key to start DBAN in interactive mode.
- \* Enter autonuke at this prompt to start DBAN in automatic mode.

boot:

## Passo 3: Scelgo il metodo

• Al termine del caricamento premo il tasto «M» per scegliere il metodo di cancellazione sicura

Darik's Boot and Nuke	e 2.2.6 (beta)			
Options — Entropy: Linux Kernel (urandom) PRNG: Mersenne Twister (mt19937ar-cok) Method: DoD Short Verify: Last Pass Rounds: 1	Statistics — Runtime: Remaining: Load Averages: Throughput: Errors:			
Quick Erase       syslinux.cfg: nuke="dwipemethod dodshort"         RCMP TSSIT OPS-II       Security Level: Medium (3 passes)         ▶ DoD Short       DoD 5220.22-M         Gutmann Wipe       PRNG Stream				
The American Department of Defense 5220.22-M short wipe. This method is composed of passes 1,2,7 from the standard wipe.				

## Passo 4: Scelgo il disco

• Dalla schermata principale scelgo l'hard disk da cancellare e premo «spazio» per selezionarlo

Darik's Boot and Nuke	e 2.2.6 (beta)
Options — Entropy: Linux Kernel (urandom) PRNG: Mersenne Twister (mt19937ar-cok) Method: DoD Short Verify: Last Pass Rounds: 1	Runtime: Remaining: Load Averages: Throughput: Errors:
► [ ] ATA Disk VMware Virtual I 0000 40	GB 000000000000000000000000000000000000

P=PRNG M=Method V=Verify R=Rounds, J=Up K=Down Space=Select, F10=Start

## Passo 5: Avvio la procedura

## • Per avviare la procedura premo il tasto «F10» e attendo il completamento

	Darik's Boot and Nuke 2.2.6 (beta)				
	Options	Statistics			
Entropy:	Linux Kernel (urandom)	Runtime: 00:01:16			
PRNG:	Mersenne Twister (mt19937ar-cok)	Remaining: 08:56:49			
Method:	DoD Short	Load Averages: 1.08 0.46 0.19			
Verify:	Last Pass	Throughput: 6650 KB/s			
Rounds:	1	Errors: 0			

ATA Disk VMware Virtual I 0000 40GB 000000000000000000 [00.24%, round 1 of 1, pass 1 of 3] [writing] [6650 KB/s]

## Esempio 4: Backup dei dati

- Un backup consiste nella copia dei dati personali di un utente
- Richiede un supporto di storage diverso rispetto a quello che contiene i dati originali (p.es. CD/DVD, Chiavetta USB, Hard Disk esterno, NAS Server)
- E' inoltre necessario un software che **a intervalli predefiniti** copi il contenuto dell'origine sulla destinazione
- Diverse soluzioni gratuite:
  - Cobian Backup (<u>http://www.cobiansoft.com/</u>)
  - Uranium Backup (<u>http://www.uraniumbackup.com</u>)

## Passo 1: Scarico Cobian

#### • Sito web: <u>http://www.cobiansoft.com/</u>

> www.cobiansoft.com	🏫 🔻 😋 🚼 र cobian backu	p 🔑 🏦
(5) -	Translate-	
		Home   Contact
Copia	nSoft	

1	5	7	
	9	Į	)
	-	-	5

Navigation	- F
Home	١
News	5
About Personal	F
Pictures <b>Software</b> Cobian Backup Cobian Poirot	s r t
Other software Obsolete	ŀ
Forum Guest book	6

#### Hello and welcome to Cobian's site!

Welcome to Cobian's site, the home of Cobian Backup. This is both a personal site and site about software development.

Please feel free to walk around my site and download any of my programs. Because of the popularity of Cobian Backup, which now is in its 9th version, I am actively supporting only that product. If you have some questions about Cobian Backup, please read the Help file and the FAQ first, and if you don't find the answer to your question there, post it to the support forum and I or other users will gladly try to help you.

Here you can download some other programs developed by me as well. Some useful utilities like Cobian Herald (a mailing list server), CobView (a multipurpose Windows Shell extension) and CobDDNS (a client updater for EditZone dynamic DNS) can be downloaded from Other software.

## Passo 2: Configuro il backup

### • Avvio il programma e seleziono la voce «New Task»

📆 Cobian Backup Boletus		
List Task History Log <u>Tools</u> Help		
Properties S History	Log	
Property	Value	
Number of selected tasks	0	
MainList.lst (Files: 0, Size: 0 bytes)		

## Passo 3: Scelgo file e cartelle

 Seleziono i file e le cartelle di cui effettuare il backup e la destinazione (es. hard disk esterno)

🔅 General		
Files	Source	
💮 Schedule		
📁 Archive		
real Exclusions		
🔔 Events		
움 Advanced		
	Add 🖺 Edit 🖉 Delete	+
	Destination	
	Add	4
	OK Cance	

## Passo 4: Scelgo lo scheduling

 Scelgo ogni quanto effettuare il backup (giornaliero, settimanale, mensile, annuale, manuale)

j Files	Schedule type	1
🕗 Schedule	Once	
🗊 Archive	Daily	
Exclusions	Weekly	
	Yearly	Tuesday
Advanced	Timer Manually	Thursday
	Friday	Saturday
	Sunday	
	Date/Time	
	Date	Time
	14/03/2012	16:26:45
	Days of the month	Month
		lanuary
		Jandary
	Timer (minutes)	From: To:
	180	00:00:00 🔶 23:59:59 🍨

## Passo 5: Scelgo lo cifratura

 Cifrare l'hard disk e poi avere un backup in chiaro non è molto intelligente

• Conviene quindi cifrare anche il backup

, General	Compression	
🔊 Files	Compression type	Split options
🕗 Schedule	No compression	No split 👻
刘 Archive		
Exclusions	Compress individually	Custom size (bytes)
Events	Password protect	430000000
Advanced	Password	Password (retype)
	Archive comment	
	Archive created by Cobian Backup	10
	Strong encryption	
	Strong encryption Encryption type No encryption	Passphrase quality
	Strong encryption Encryption type No encryption RSA-Rijndael (1024-256 bits) Blowfish (128 bits) Rijndael (128 bits) DES (64 bits)	Passphrase quality Passphrase (retype)
	Strong encryption Encryption type No encryption RSA-Rijndael (1024-256 bits) Blowfish (128 bits) Rijndael (128 bits) DES (64 bits)	Passphrase quality Passphrase (retype)
	Strong encryption Encryption type No encryption RSA-Rijndael (1024-256 bits) Blowfish (128 bits) Rijndael (128 bits) DES (64 bits)	Passphrase quality Passphrase (retype)

## E se utilizzo Mac?

• Cifratura:

TrueCrypt

- FileVault (integrato in Mac OS X)
- Backup
  - iBackup
  - TimeMachine (integrato in Mac OS X)

• Wiping

- Permanent Eraser for Mac
- Disk Utility (integrato in Mac OS X)

## Le 7 regole d'oro per gli Smart Phone

- Non perdere il telefono...
- Limitare la conservazione di dati sensibili
- Impostare un **passcode di accesso complesso** (non i semplici 4 numeri...)
- Attivare le procedure di cancellazione sicura dopo un certo numero di tentativi di inserimento di passcode errato
- Aggiornare il sistema operativo
- Disattivare bluetooth e wifi quando non necessari
- Attenzione alle applicazioni che si installano

## DFA (Digital Forensics Alumni)

- DFA è un'associazione nata nel **dicembre** 2009
- Idea di alcuni corsisti della prima e seconda edizione del Corso di Perfezionamento in Computer Forensics e Investigazioni Digitali presso l'Università degli Studi di Milano
- Obiettivo è la creazione di un network tra gli ex alunni del corso e offrire strumenti per la collaborazione e il confronto tra le figure con una formazione tecnica (periti e consulenti) e quelle con formazione giuridica (giudici, pubblici ministeri, avvocati, P.G.)

## DFA (Digital Forensics Alumni)

- Newsletter mensile con aggiornamenti tecnici e legali in materia di Digital Forensics
- Per iscriversi
  - Visitare il nostro sito web <u>www.perfezionisti.it</u> oppure
  - o Inviare una mail a info@perfezionisti.it

## DFA (Digital Forensics Alumni)



#### Digital Forensics Alumni

Via Spallanzani, 16 20129 Milano Fax.: +39 178 6071697

www.perfezionisti.it info@perfezionisti.it



## Mattia Epifani

Mail: mattia.epifani@digital-forensics.it Web: http://www.digital-forensics.it - http://blog.digital-forensics.it Linkedin: http://www.linkedin.com/in/mattiaepifani