



# Mahremiyet Ekseninde Özgür Yazılımlar

Fatih Özavcı  
Bilgi Güvenliği Danışmanı  
[fatih.ozavci@gamasec.net](mailto:fatih.ozavci@gamasec.net)



Büyük Birader seni izliyor....

1984, George Orwell

# Mahremiyet



- Mahremiyet
  - TDK : Kişisel Gizlilik
- Değişen dünyada, bireyin sahip olduğu hakların ve bilgilerin, daha güçlü olan devlete karşı korunması gerekliliği oluşmuştur.
  - Devletin Kendini Korumak İstemesi
  - Sahip Olmanın Dayanılmaz Hafifliği
  - Demokratik Haklar ↔ Söзде Özgürleştirilmiş Yasalar

# Mahremiyet İhlalleri



- Olağan İhlaller
  - Siyasi Fişleme
  - Polis Devleti
  - Korku İmparatorluğu
  
- Terörizmin Etkisi
  - Ülkelerin Havalimanı Kurallarının Değişmesi
  - İstihbarat İmkanlarının Arttırılması
  - Kişisel Mahremiyetin Azaltılmasını Destekleyen Kanunlar
  - Gözaltı, Sorgulama ve Ceza Kavramlarının Evrimi

# Mahremiyet İhlalleri



## ➤ Dolaylı İhlaller

- Cep/Sabit Telefon Dinleme
- Cep Telefonundan Yer Saptama
- Kameralarla Sürekli İzleme
- Parmak İzi Temelli Doğrulama
- E-Postaların Takibi
- Facebook/Myspace/Twitter Etkisi
- Skype/VoIP Görüşmelerinin Kaydı

## ➤ Doğrudan İhlaller

- Havalimanında Taşınabilir Bilgisayarın Analizi
- Servis Sağlayıcı Üzerinden İletişimin Kaydedilmesi
- İnternet İçeriğine Erişim Kısıtlaması



Kahrolsun Büyük Birader !

1984, George Orwell



## ➤ Veri Depolama Gizlilik Gereksinimi

- Havalimanı Geçiřlerinde Tařınabilir Bilgisayar/Disk/Kart
- Olası Gzaltında Kiřisel Verilerinizin İfřası
- Tařınabilir Bilgisayar/Disk/Kart'ın Kaybolması veya alınması
- Bir Diskin/Kartın Satılması, El Deđiřtirmesi

## ➤ Disk Kriptolama

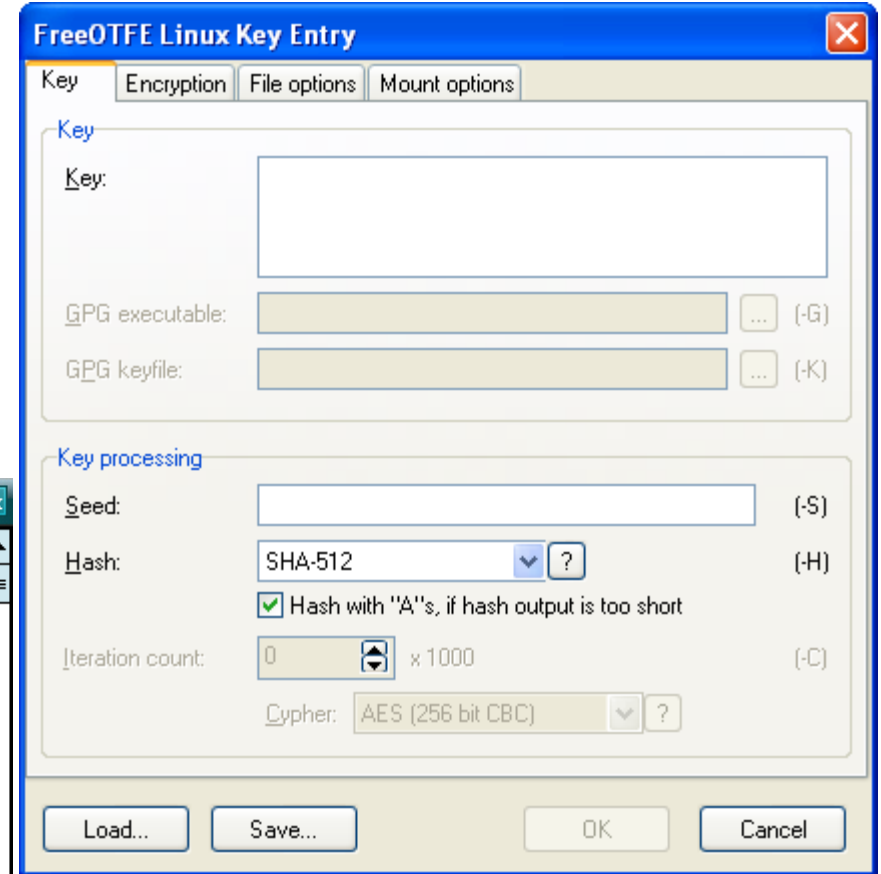
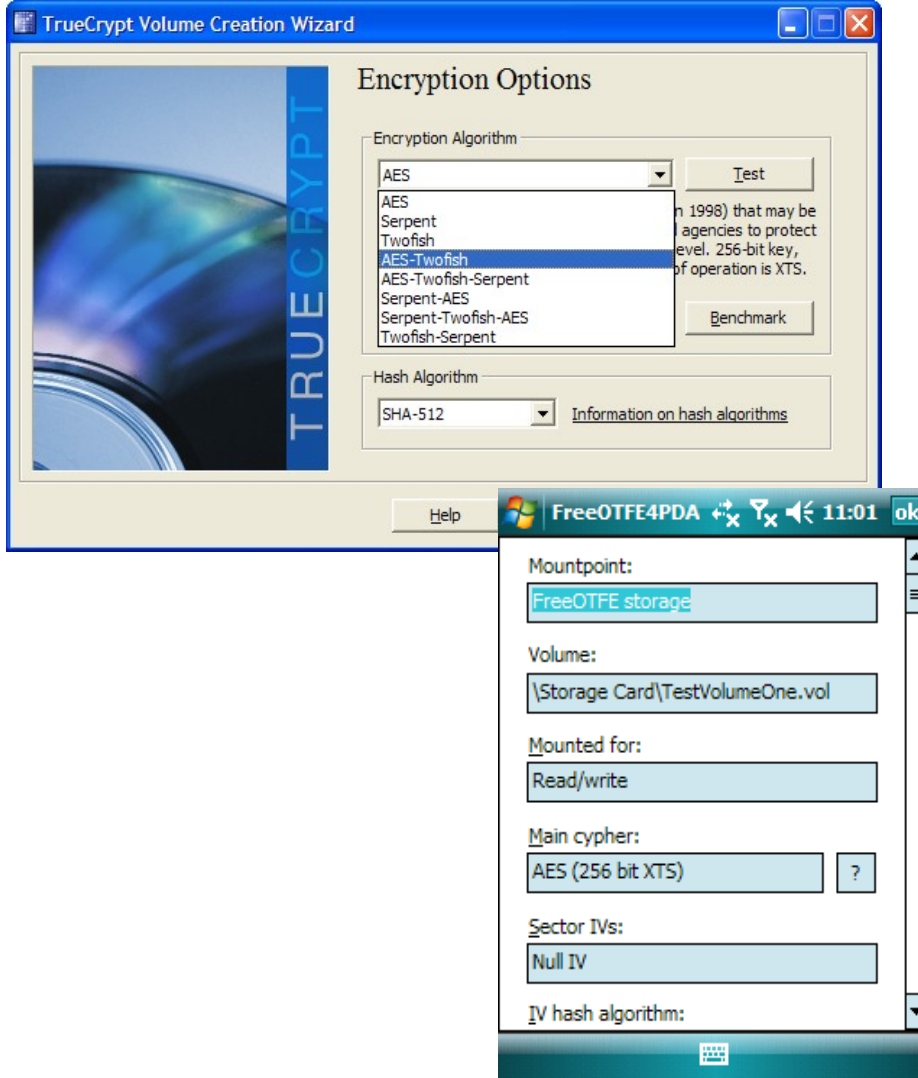
- Bir Diskin/Kartın Kriptolanması
- zel Bir Dosyanın Kriptolanarak Disk Biiminde Kullanılması
- Kripto özme Anahtarının Saklanması
- Plausible Deniability

# Disk Kriptolama Yazılımları



- Truecrypt - [www.truecrypt.org](http://www.truecrypt.org)
  - Sabit Disk, Sanal Bir Disk Dosyası, Kart Kriptolama
  - AES, Serpent, Twofish Algoritma Desteği
  - Windows, Mac, Linux Desteği
  - Kriptolama ve Yasal Nedenlerle Özel Bir Lisans Kullanmaktadır
  
- FreeOTFE - [www.freeotfe.org](http://www.freeotfe.org)
  - Sabit Disk, Sanal Bir Disk Dosyası, Kart Kriptolama
  - AES, Serpent, Twofish Algoritma Desteği
  - Windows, Windows Mobile, Mac, Linux Desteği
  
- Cryptoloop, dm-crypt, LUKS

# Ekran Görüntüleri





- Kriptolama Destekli Yedekleme ve Arşivleme
  - Areca – [www.areca-backup.org](http://www.areca-backup.org)
    - Arşiv (ZIP, ZIP64), AES, Ağ Sürücüsü, FTP/SSL Destekleri
    - Windows, Linux
  - PeaZip – [peazip.sourceforge.net](http://peazip.sourceforge.net)
    - Winzip, 7z Uyumlu AES 256 Bit Kriptolama
    - ZIP, DMG, RAR, 7Z, BZIP2 vb.
  - KGB Archiver - [kgbarchiver.net](http://kgbarchiver.net)
    - AES 256 Bit Desteği
  
- Güvenli Silme
  - Wipe – [wipe.sourceforge.net](http://wipe.sourceforge.net) / Linux
  - Eraser – [eraser.heidi.ie](http://eraser.heidi.ie) / Windows

# Ekran Görüntüleri



The screenshot displays the Areca application interface. The main window is titled "Areca - Target edition [Modified]". It features a sidebar on the left with a menu containing: Main, Sources, Compression, **Advanced** (highlighted), Filters, Pre-processing, Post-processing, and Description. The main area is divided into three sections: "Files management" with checkboxes for "Track directories", "Store permissions", "Follow subdirectories", and "Follow symbolic links"; "Encryption" with a checked "Encryption" checkbox, a dropdown menu set to "AES 128 - Passphrase", and a "Key" input field with the example "MyPassphrase123!"; and "Configuration" with a checkbox for "Disable target configuration bar".

Overlaid on the bottom right is a "Computer's root" file explorer window. It shows a tree view of the filesystem and a table of drives:

Name	Type	Size	Free	Filesystem
(C:) DATA	Local disk	69.6 GB	54.3 GB	NTFS, 78% free
(D:) ACER	Local disk	34.8 GB	6.4 GB	NTFS, 18% free
(F:) Optical drive	Optical drive	0 B	0 B	0 B

A "Done: Create PeaZip.zip" dialog box is also visible, showing a green checkmark and the message "Job successfully completed". It includes a progress bar and statistics: Input: 9.2 MB @ 8.8 MB/s, Output: 6.4 MB (69%) @ 6.1 MB/s, Time: 1045 ms. The dialog has "Ok" and "Explore" buttons.



## ➤ Mahremiyet Sorunları

- Ziyaret Edilen Sayfaların Proxy'lerde, Yazışmaların E-Posta Sunucularında, VoIP Görüşmelerinin Servislerde Kaydedilmesi
- Ziyaret Edilecek Sayfalara Kısıtlama veya Engelleme
- Sadece Belirli Uygulamaların Kullanımına Zorlanma

## ➤ Anonim Proxy Kullanımları

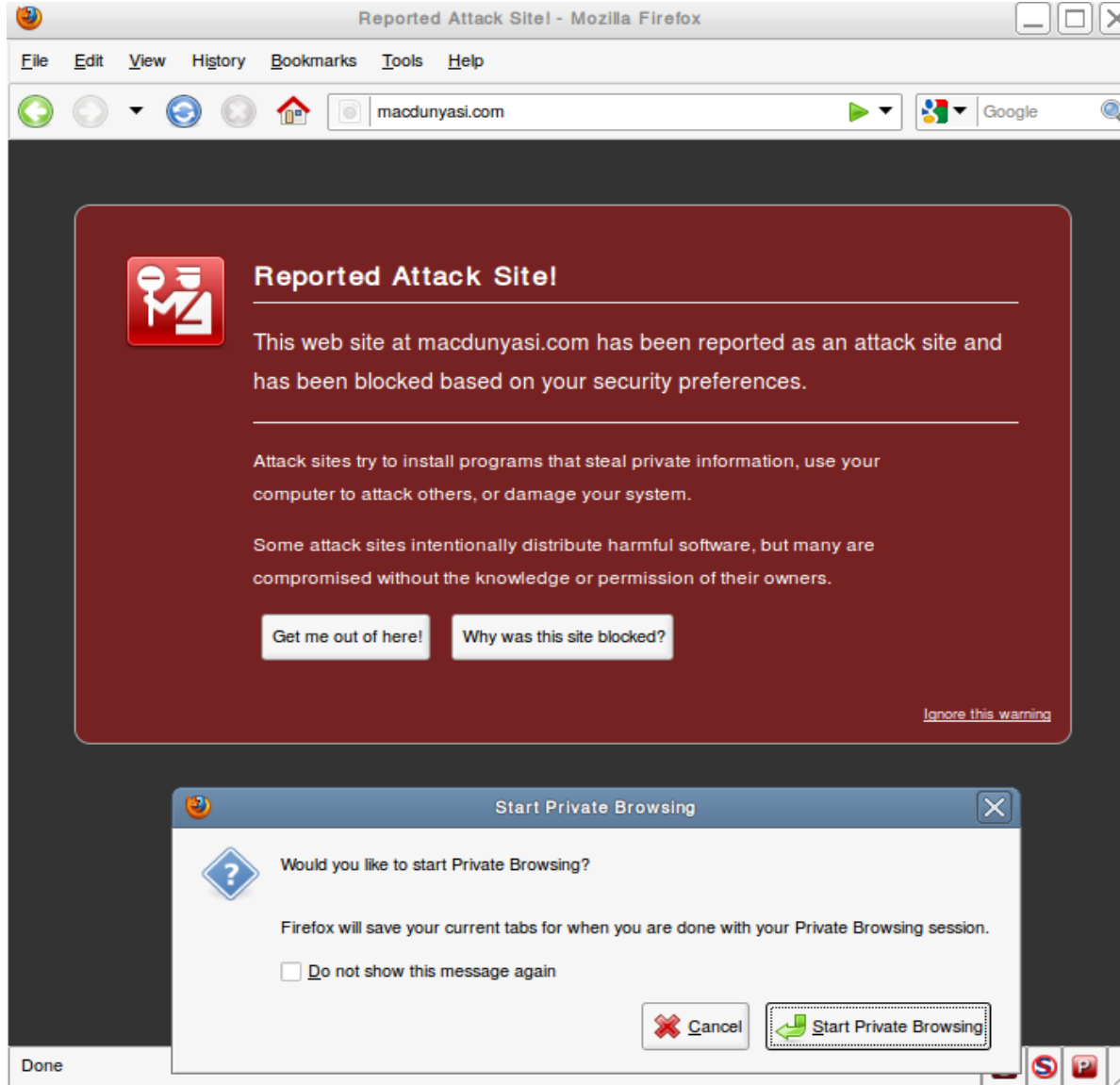
- Tor Projesi – [www.torproject.org](http://www.torproject.org)
  - Dağıtılmış, Anonim Bir Ağ
  - Devlet Kuruluşları İstihbarat Amaçlı, Farklı Ülkelerden Geliyormuş Gibi Kullanılmaktalar
  - Tor'da Olan, Tor'da Kalır
  - Windows, Mac, Linux Desteği
  - Harici Proxy'ler ile Desteklenmeyen Uygulamalara Arayüz
- Sınırlandırmaların Aşılması, Takibin Zorlaşması

# İnternette Güvenli Gezmek



- Mozilla Firefox – [firefox.org](http://firefox.org)
  - Açık Kaynaklı İçi Biliniyor; Kayıt, Kopyalama, İstatistik
  - Geçmiş ve Geçici Depolama Yönetimi İçin Özel Seçenekler
  - Özel Gezme için Ayarlar
  - Eklenti Desteği
    - NoScript
    - Privacy+
    - ViewCookies
  - Ortalama Saldırılarına Koruma
  - Hızlı Güncelleme Yönetimi
  
- Privoxy – [www.privoxy.org](http://www.privoxy.org)
  - Tor için Proxy Desteği

# Ekran Görüntüleri



# E-Posta Kriptolanması



- Mozilla Thunderbird - [www.mozillamessaging.com/en-US/thunderbird](http://www.mozillamessaging.com/en-US/thunderbird)
  - Açık Kaynak, Spam/Oltalama Koruması, Eklenti Desteği
  - E-Posta Resmi Göstermeme, Otomatik Güncelleme, Okuma Bilgisi
- GPG – [gnupg.org](http://gnupg.org)
  - Açık Anahtarlı Kriptolama Altyapısı
  - Simetrik, Asimetrik Kriptolama, Sayısal İmzalama
  - Açık Anahtar Yönetme Sunucuları, Bireysel Güven Yönetimi
  - Windows, Mac, Linux
  - Yaygın E-Posta, Yazışma, Depolama ve İletişim Yazılımlarının 3. Parti Eklentiler/Yazılımlar ile Entegrasyonu
  - GPG Arayüzleri - [gnupg.org/related\\_software/frontends.en.html](http://gnupg.org/related_software/frontends.en.html)
- E-Posta Yazılımları Entegrasyonu
  - Mozilla Thunderbird, Enigmail
  - Evolution
  - MS Outlook Eklentisi, GPGol, GPGOE

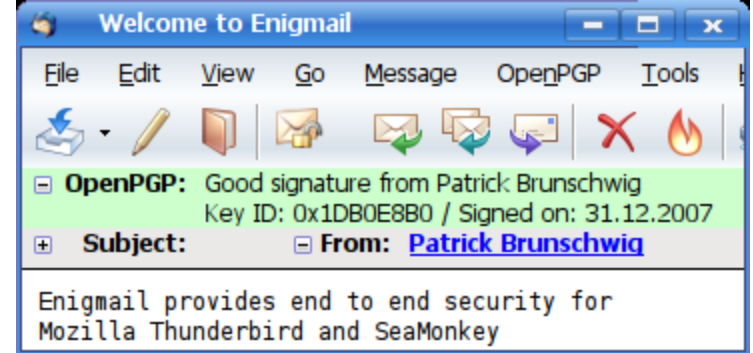
# Ekran Görüntüleri



-----BEGIN PGP MESSAGE-----  
Version: GnuPG v1.0.4 (GNU/Linux)

Comment: Gnome PGP version 0.4

hQIOA7HMZGc8Py7SEAf/eWVrPAF/k75uWRthVdsQcy7e725F2cl5kQDIDI44/KdP  
vyaCEMd+4eVqEh3Ao3PmdGzAc31KGLA56sWPYySk4f7YlbyRF8bLL1odZNa3Mbwu  
B0mH6vsUDmgMAoSSvTn3ckWNaDaVjXMn1RFD+1yzrs/hCoBzTMx12aH628JE+qeg  
KG9fRununsabmV3a29uaZKSaxyXIBMvms7E377SEuiDj+Q4+xjqVL49v8u9nWci  
EaUovJECrJVDBEFp/575jc6DJZZ9I448nK5IHHpV68O8s+xwZ7GESGHfLUcoBPcn  
HOuUc7I9o2dry+zFDT9alsWGtPL9nSMJ1fSGNbpkLQf9Hybi96v8QE8F+8bomHs  
qEfsuMxWRsMtNNj3gc3YAZquiUGDqcUD58uOssUqe/vdE6LaTV99rPThI2zf3r0  
sMe7U9CmvFa6h0YkkAt6hoLdkDKM+IXzVNuyibvsWSOez3fko9BJ+YUOLNvTgWwO  
rTIX6c+f2tObTk9P3jzZu9qy2GVgV8zajd23Bh12JTLyGhBhOa4WivYibVvCNHu3n  
DdpgQ9WaSVWSSkyE9wLYxM90Wz3cVjFeNd2ZQslxoxZv+1yTyyIR1nOpz5MjuGrZ  
WPLVTjhfUUEAbOsqF2MhIEW0XH+j25DWgUrjnK0CxPKC1TR3hX8yHhGPGlow+MFH  
LNKRAdJ5uOqgd3ET6NfV5x2gFaW2Bn/fta024Z1P4IEQ/dis3M8QW/71Z5CZ7/8w  
MUREmJiEaWc6YOxahWO/2D3i5DfIM2dArDRu4c9hXIA5+dwyxewEKERGUvb1X5X0  
9ZFgULUtWKXC7ZzoODxvIQvCUBO+nMUD/lo4OAPDxWrHKHE7IDhpCBGxa/ja/9fD  
XtrvA===nDBS  
-----END PGP MESSAGE-----

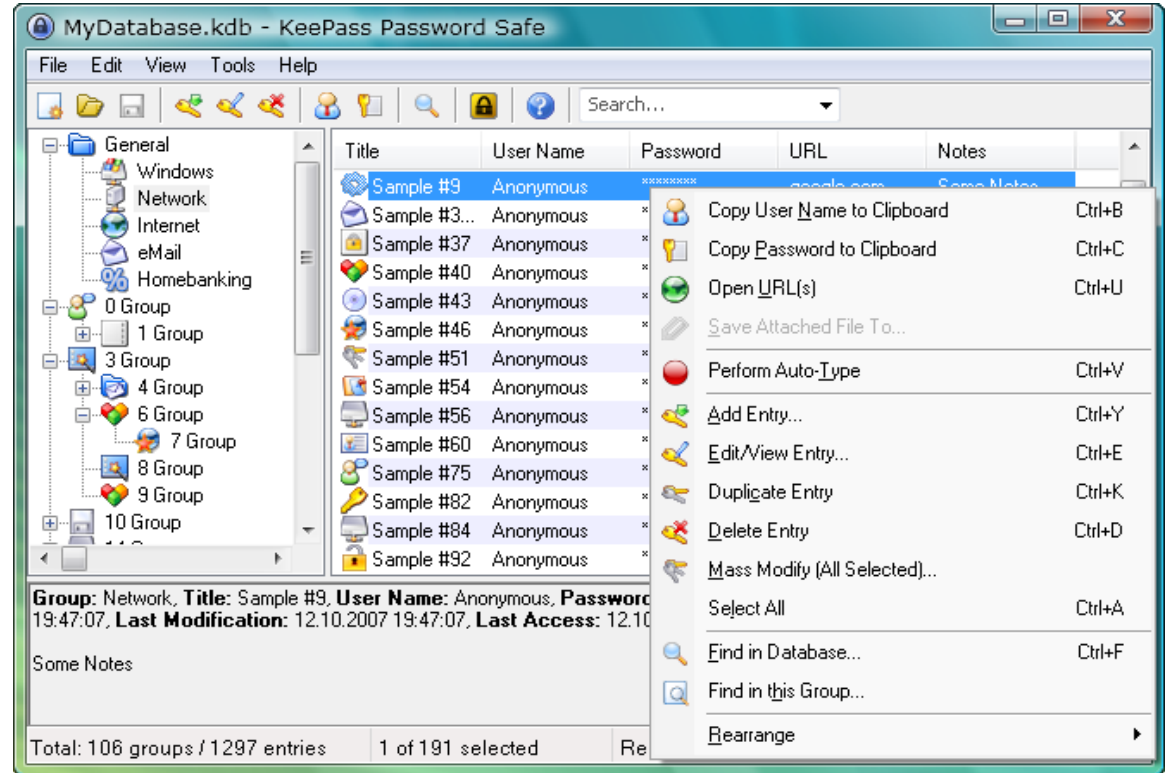


# Kişisel Şifrelerin Güvenli Depolanması



- Keepass – [keepass.info](http://keepass.info)
  - AES-256 Bit Kriptolama ile Verilen Saklanması
  - Windows, Mac, Linux Desteği
  - Şifre Üretme, Dışarıya Aktarma, Eklenti ve Dil Destekleri
  
- Password Safe – [passwordsafe.sourceforge.net](http://passwordsafe.sourceforge.net)
  - Bruce Schneier Tarafından Geliştirildi
  - Şifre Üretme, Dışarıya Aktarma Destekleri

# Ekran Görüntüleri



# Bağlantılar ve Referanslar



- Taking your laptop into the US? Be sure to hide all your data first  
[www.guardian.co.uk/technology/2008/may/15/computing.security](http://www.guardian.co.uk/technology/2008/may/15/computing.security)
- Osalt - Security & Privacy  
[www.osalt.com/security-and-privacy](http://www.osalt.com/security-and-privacy)
- 40 Open Source Tools for Protecting Your Privacy  
[www.esecurityplanet.com/features/article.php/3788181/40-Open-Source-Tools-for-Protecting-Your-Privacy.htm](http://www.esecurityplanet.com/features/article.php/3788181/40-Open-Source-Tools-for-Protecting-Your-Privacy.htm)
- Plausible Deniability  
[http://en.wikipedia.org/wiki/Plausible\\_deniability](http://en.wikipedia.org/wiki/Plausible_deniability)  
<http://www.truecrypt.org/docs/?s=plausible-deniability>



*Teşekkürler....*