



Test porównawczy narzędzi do szyfrowania zawartości pamięci masowych

0 – 33 34 – 66 67 – 100

Miejsce w teście	Waga	1.	2.	3.	4.	5.	6.
Produkt		TrueCrypt 6.1a	Jetico BestCrypt Volume Encryption v2	FreeOTFE 4.60	SecurStar DriveCrypt PlusPack 3.94	ntldr Disk Cryptor 0.6a	Microsoft BitLocker Vista Edition
Cena/licencja		darmowy/open source	475 zł	darmowy/open source	600 zł	darmowy/open source	darmowy
Adres WWW		truecrypt.org	jetico.com	freeotfe.org	securstar.de	diskcryptor.net	microsoft.com
Ocena końcowa	100	70	59	54	50	48	31
Opłacalność		nie dotyczy	59	nie dotyczy	44	nie dotyczy	nie dotyczy
Funkcjonalność	47	72	49	45	44	34	15
Szyfrowanie	36	60	59	59	46	51	38
Wydajność	17	77	74	62	67	73	56
Wyniki							
Obsługiwane systemy plików	4,00	dowolne	FAT, NTFS	dowolne	FAT, NTFS	FAT, NTFS	NTFS
Obsługiwane systemy operacyjne	3,00	Linux, XP, Vista, 2000/03/08, OS X	XP, 2000/03/08, Vista	XP, Vista, 2000	XP, Vista, 2000, 2003	XP, Vista, 2000, 2003, 2008	Vista Ultimate, 2008
Współpraca z 64-bitowymi OS	1,50	natywna	tak	tak	nie	natywna	natywna
Możliwe użycie przed instal. OS	2,50	nie	nie	nie	nie	nie	nie
Zdalna obsługa	4,00	nie	nie	nie	nie	nie	nie
Automat. odmont. woluminów po określonym czasie	2,00	tak	tak	nie	nie	nie	nie
Wiele kluczy dla woluminu	2,00	tak	tak	tak	tak	nie	tak
Keyfiles	2,00	tak	tak	tak	tak	tak	nie
Zamazywanie wolnego miejsca	2,00	tak	nie	tak	tak	tak	nie
Tworzenie wirtualnych archiwów/folderów	2,50	tak/tak	nie/nie	tak/tak	nie/nie	nie/nie	nie/nie
Ukryte woluminy/systemy operacyjne	5,00	tak/tak	nie/nie	tak/nie	tak/tak	nie/nie	nie/nie
Ustawienia per-user dla niesystemowych woluminów	2,50	nie	tak	nie	nie	nie	nie
Zachowanie w razie uszkodzenia binarnego partycji	4,00	brak kontroli, dekrypcja typu brute-force	brak kontroli, dekrypcja typu brute-force	brak kontroli, dekrypcja typu brute-force	brak kontroli, dekrypcja typu brute-force	brak kontroli, dekrypcja typu brute-force	brak kontroli, dekrypcja typu brute-force
Bootowalny CD ratunkowy	5,00	tak, ISO z kluczami ratunkowymi	tak, ISO z plikiem odzyskującym; plugin BartPE	nie	tak, obraz IMG dla flopa lub ISO dla CD	tak, plugin BartPE	nie
Backup/odtworzenie nagłówków partycji	2,50	tak/tak	tak/tak	tak/tak	nie/nie	tak/tak	nie/nie
Inne możliwości	2,50	reset przez crash systemu, podgląd wybranych sektorów dysku/partycji	reset przez crash systemu, podgląd wybr. sektorów dysku/partycji, anti-keylogger	brak	brak	reset przez crash systemu (BSOD)	brak
Szyfrowanie							
Algorytmy i siła szyfrowania (w bitach)	5,00	AES-256, Serpent-256, Twofish-256, kombinacje w/w, Blowfish	AES-256, RC6-256, Serpent-256, Twofish-256	AES-256, 3DES-256, RC6-256, Serpent-256, Twofish-256, Blowfish, CAST6	AES-256	AES-256, Serpent-256, Twofish-256, kombinacje w/w	AES-128/512
Tryby pracy z woluminami	3,00	XTS	LRW, XTS	CBC (ze znanymi/tajnymi wektorami IV), LRW, XTS	LRW	LRW, XTS	CBC z tajnymi wektorami IV
Możliwości kodowania	3,50	dysk, partycja, klucz USB	partycja, klucz USB	dysk, partycja, klucz USB	partycja, klucz USB	dysk, partycja, klucz USB	partycja
Obsługa konfiguracji dyskowych	3,50	RAID, dysk dynam., LVM	RAID, dysk dynamiczny	tylko zwykłe napędy	tylko zwykłe napędy	dysk dynamiczny	dysk dynamiczny
Kodowanie w miejscu	4,00	tak	tak	tak	tak	tak	tak
Uwierzytelnianie pre-boot	4,00	tak	tak	nie	tak	tak	tak
Utwierdzanie kluczy	2,00	tak	tak	tak	tak	tak	nie
Obsługa TPM	3,00	nie	nie	nie	nie	nie	tak
Obsługa tokenów sprzętowych	4,00	tak	tak, np. Alladin R2/PRO	tak	tak, np. Aladdin R2, Rainbow USB	nie	nie
Inne możliwości	3,00	brak	brak	kompatybilność z linuxowym dmccrypt'em	definiowanie haseł zniszczenia	brak	brak
Wydajność							
Zajmowane zasoby: HDD, RAM	2,00	7 MB, 7 MB	9 MB, 7 MB	6 MB, 7 MB	10 MB, 5 MB	1 MB, 6 MB	niemierzalne
Czas szyfrowania partycji 6 GB/20 GB [min:sek]	5,00	5:52/16:27	4:22/12:53	0:02/0:03	5:42/17:54	4:54/16:03	8:46/22:18
Spadek szybkości odczytu/zapisu	5,00	1,9% / 3,3%	14,7% / 8,4%	12,8 / 10,2%	9,6% / 6,9%	7,1% / 4,0%	16,4% / 8,3%
Spowolnienie startu systemu	5,00	6,72%	21,8%	0%	36,5%	25%	33%
Miejsce w teście	Waga	1.	2.	3.	4.	5.	6.

☐ tylko wspierane natywnie przez system operacyjny ☐ ale sama aplikacja jest 32-bitowa ☐ wolumin szyfrowany tylko jednym kluczem, ale dostęp do niego jest możliwy przez wiele nagłówków kodowanych różnymi kluczami ☐ utworzenie pliku jest obowiązkowe, możliwość steganograficznego ukrycia go w plikach WAV/BMP ☐ nie powiedzie się, jeżeli zamazany będzie nagłówek woluminu ☐ dla woluminu systemowego wymagane stworzenie CD i jej weryfikacja ☐ tylko pod Windows ☐ tylko systemowa (Windows)/z wyjątkiem systemowej (Linux) ☐ z wyjątkiem systemowej ☐ tylko Vista/2008 ☐ przez PIN/klucz USB ☐ przez bibliotekę PKCS #11 ☐ komponent systemowy ☐ brak szyfrowania całej powierzchni woluminu w momencie tworzenia ☐ ze względu na brak możliwości szyfrowania woluminu systemowego