MOUNTING FORENSIC IMAGES FOR SCANNING

Цел: Разгледување на форензичка слика при напад на систем

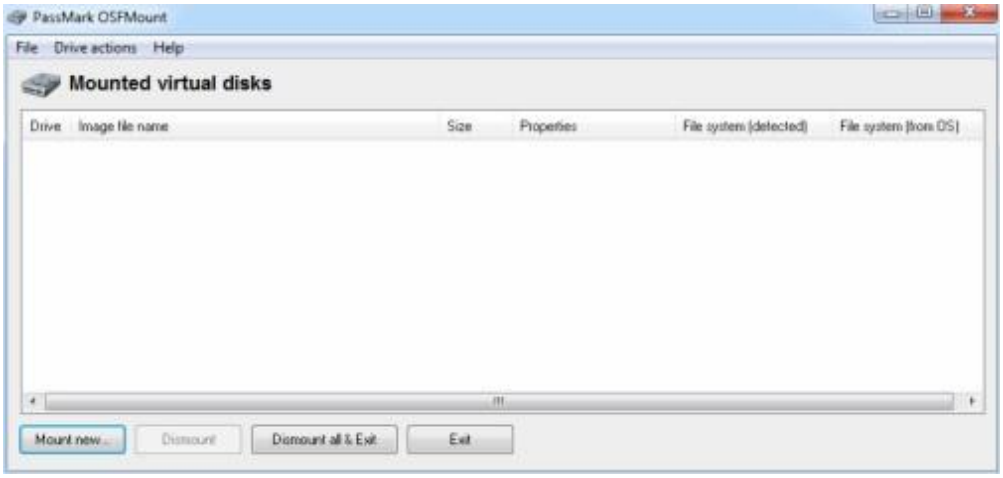
Примена: Разгледување на форензичка слика со OSFmount и скенирање на истата со антивирус софтвер за да се детектира дали содржи познати малициозни датотеки

Дел 1:

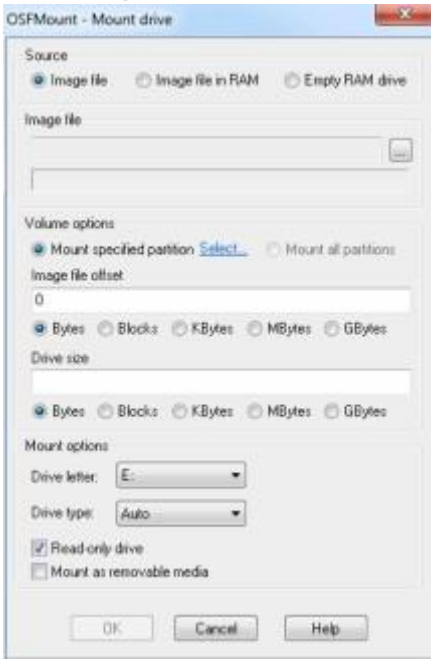
Потребни алатки: OSFMount

Чекори:

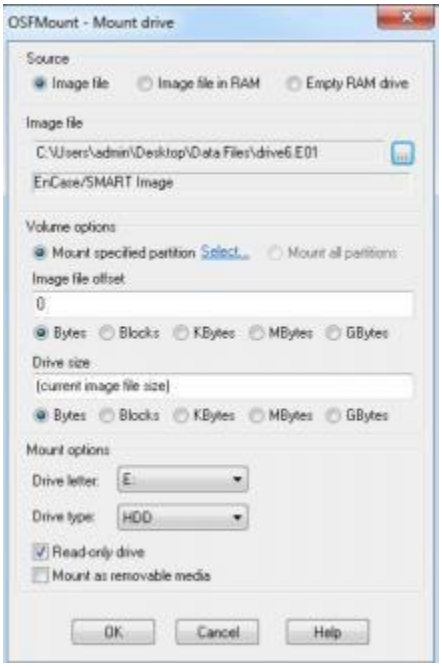
1. Симнете ја алатката и поставете ја на вашиот дектоп.
2. Симнете ја форензичката слика drive06.E01 од дадениот линк и поставете ја во фолдерот *Forensic_Images*
3. Отворете ја OSFMount алатката, прозорецот на алатката треба да ви изгледа како на сликата.



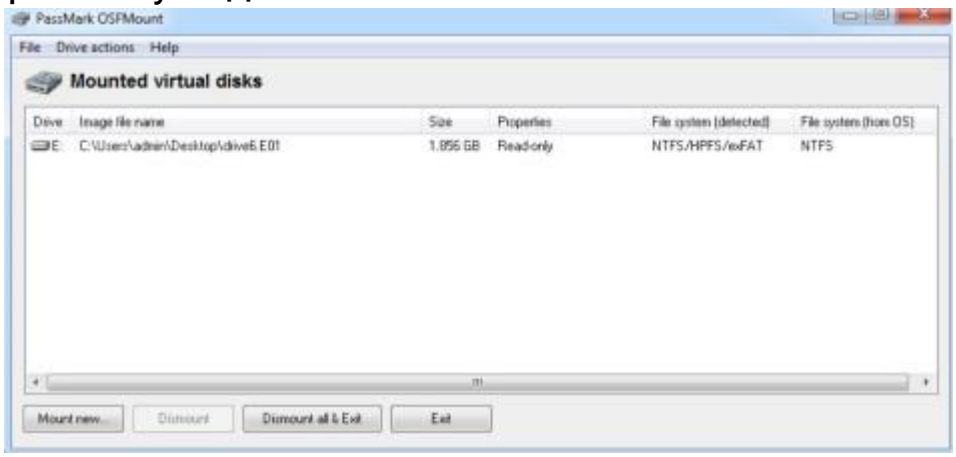
4. Кликнете на “*Mount new virtual disk…”,* прозорецот кој ќе ви се отвори за *Mount drive* треба да изгледа како на сликата.



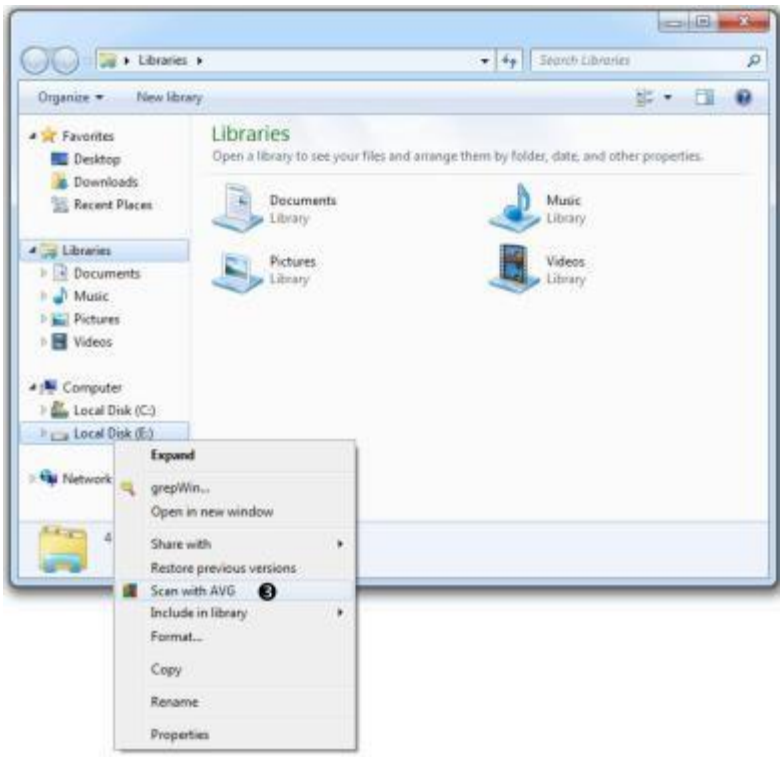
5. Kaj *Source* заокружете *Image file.*
6. Kaj *Image file* навигирајте се до форензичката слика
7. Откако ќе ја прикачите сликата прозорецот ќе го има следниот облик како на сликата.



8. Клик на “*OK*” копчето и со тоа треба да ви се креира фајлот што претставува доказ.



9. Отворете File Explorer и на левата страна кај Local Disk (E:) притиснете десен клик. Од тука изберете Scan with антивирусот кој го имате на вашиот компјутер.



10. Резултатите од скенирањето треба да ви прикажат дека станува збор за тројански коњ.