

# Анализа на File System

**Цел:** Анализа на хардверските компоненти и меморијата

**Примена:** Анализа на форензичка слика при напад на систем

**Потребни алатки:** [The Sleuth Kit](#)

**Чекори:**

1. Симнете ја алатката и поставете ја на вашиот дектоп.
2. Симнете ги од [линкот](#) фајловите од Chapter 4: drive1.E01, drive2.E01, drive4.E01 и зачувајте ги во фолдер *Forensic\_Images*.
3. Поставете го фолдерот на десктоп.
4. Отворете command prompt.
5. Внесете ја следната команда  
`cd C:\Users\username\Desktop\sleuthkit-4.2.0-win32\bin`
6. Напишете ја следната команда на cmd со цел преглед на табелата на партиција за форензичката слика drive.E01  
`fsstat -i ewf C:\Users\<username>\Desktop\Forensic_Images\drive1.E01`