

# CHFI 實作



# Module – 02

## R-Drive Image的實作



先把R-Drive Image安裝好（我使用6.3版，30天試用）

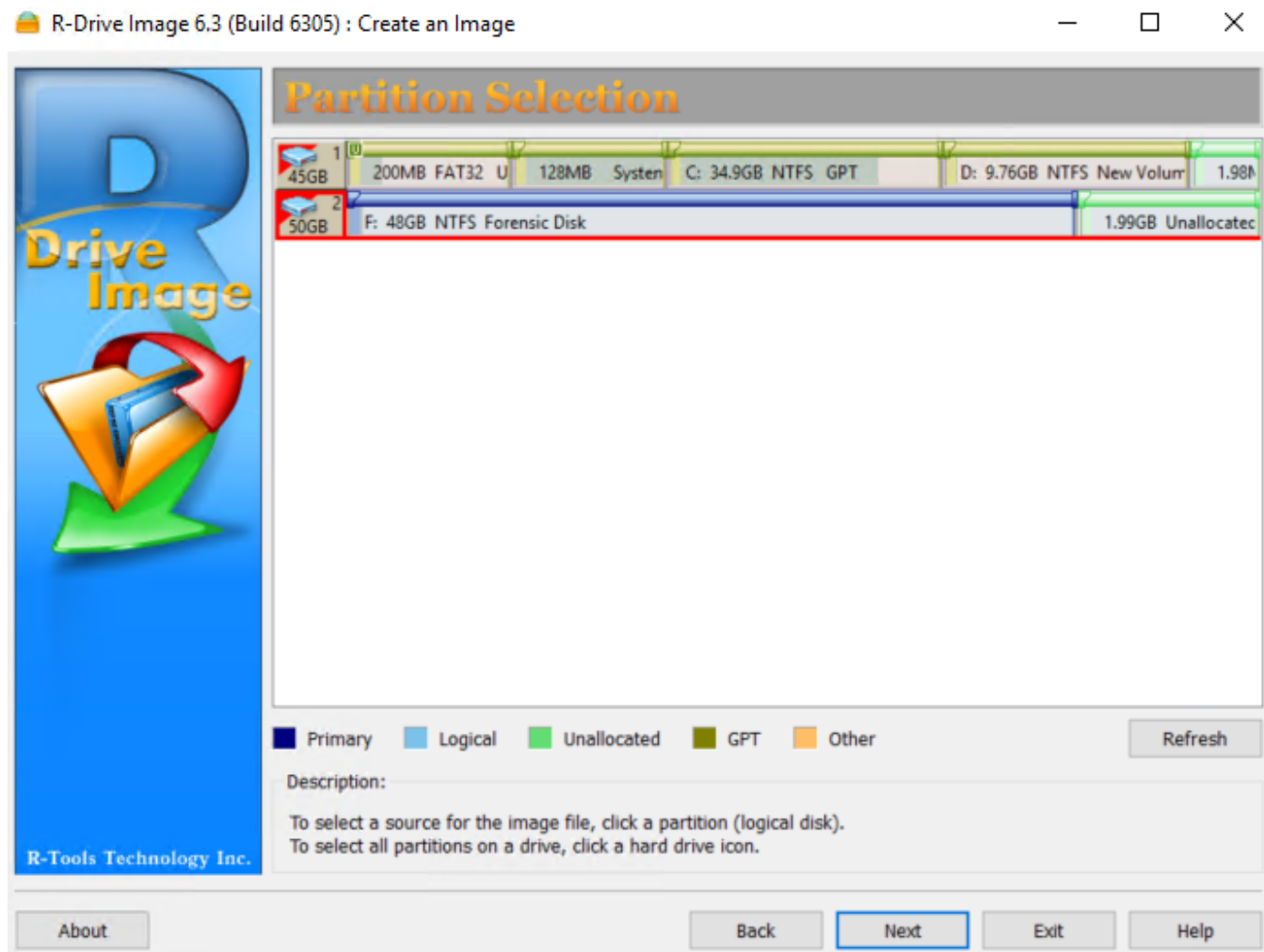
R-Drive Image會產出rdr副檔名，該副檔名為廠商的專屬格式，但R-Drive Image有過CFTT，所以可以在各個工具做轉換，但無法使用該廠商提供的特殊功能





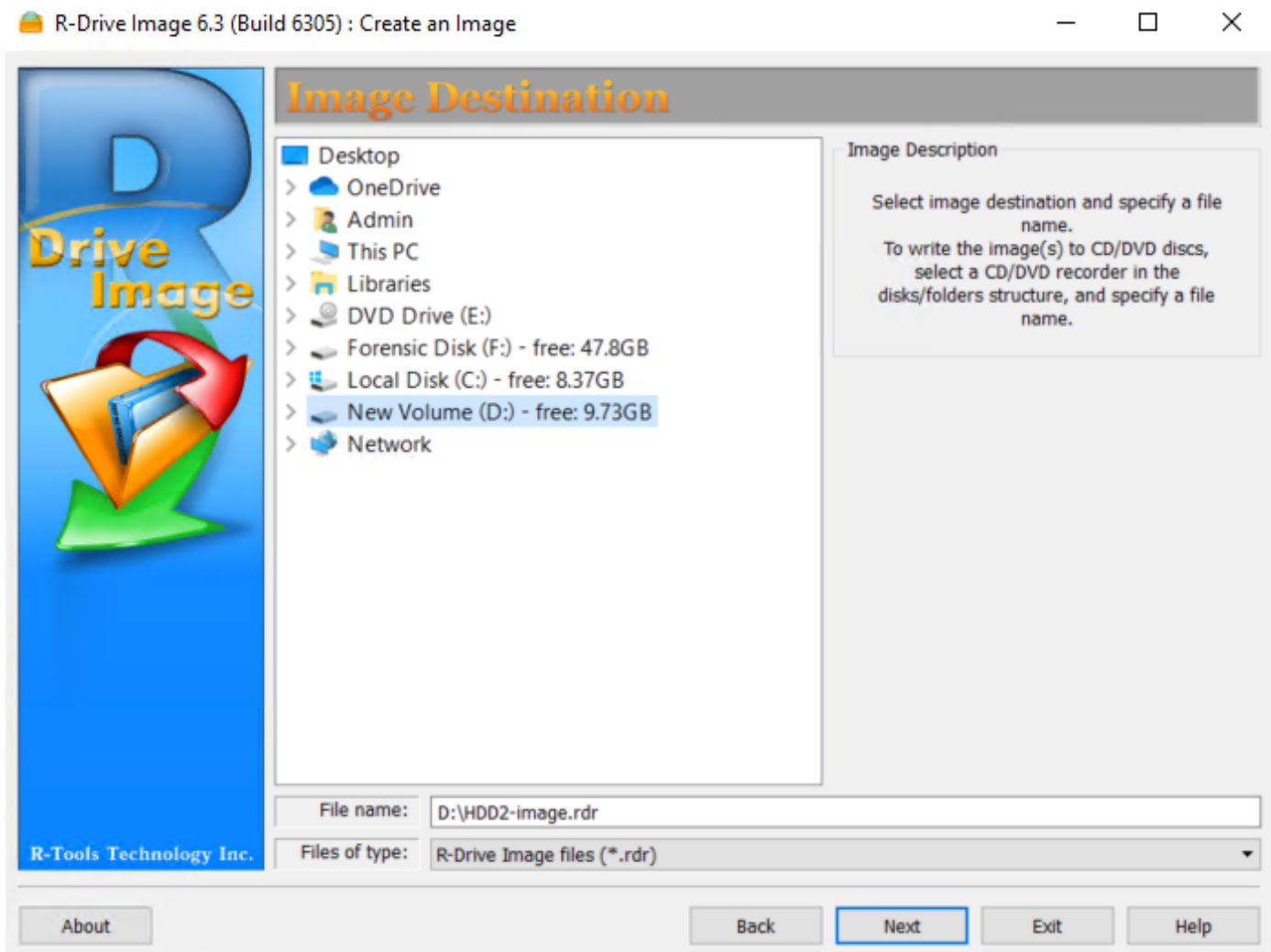
先製作一個映像檔





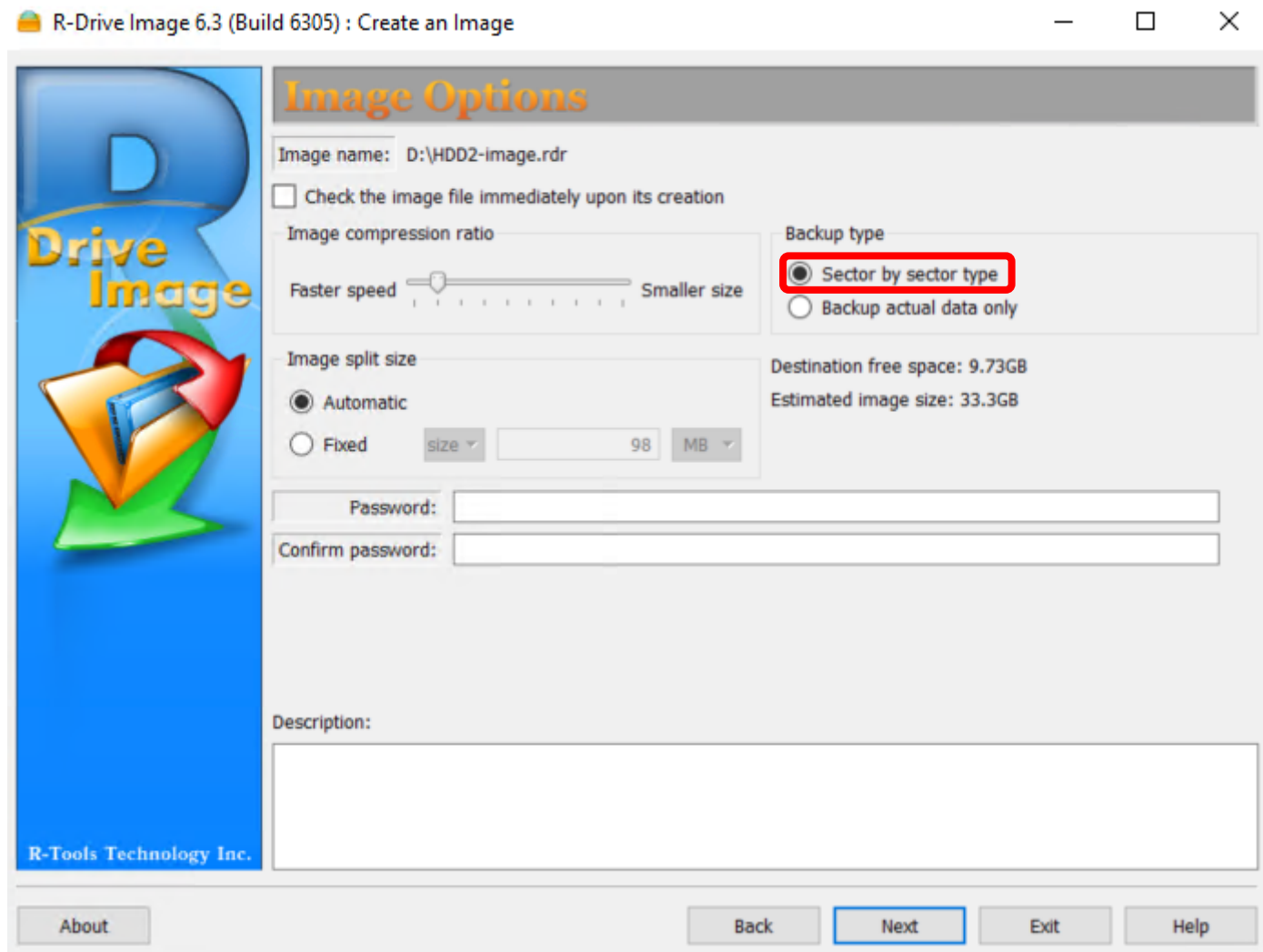
選擇要製作成映像檔的磁碟，切記要選擇到整個硬碟（注意紅框框）  
因為我們要做的是Forensic copy






選擇要存放映像檔的位置，盡量不要放在要製作映像檔的那個硬碟中





注意備份種類要選擇Sector by sector，因為我們要做的是Forensic copy，其他都可以選擇預設值





## Backup Options

**Snapshot providers**

- ☒ Windows Volume Snapshot Service
- ☒ R-TT Volume Snapshot Service

**Process priority**

Backup Process Priority: Normal

Use CPU Cores: Unlimited

☐ Notify system applications

**Backup AUX applications**

Before:  ...

After:  ...

**Snapshot AUX applications**

Before:  ...

After:  ...

☐ Ignore disk read errors (bad sectors)

皆為預設值即可







確定沒問題，就可以開始製作了  
製作完成後，即可按關閉，拿這個映像檔去做分析

