Ch. 4
Acquiring Digital Evidence

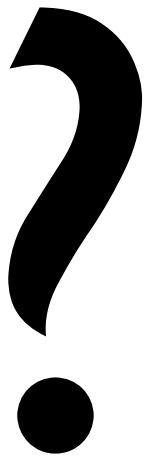
Översikt

- DOS-boot-diskar
- Drive-till-drive
- Nätverksutvinning
- Fastblock LE
- Fastblock SE
- LinEn
- Enterprise/FIM

DOS-boot-disk

- Nackdelar
  - Filsystem
  - Support för hårdvara
  - Måste ”fixas”
- Fördelar
  - ?

Att boota från en okänd maskin



Nätverksutvinning

- Korskabel/ switch
- Bootdisk
- IP
- Brandvägg
- Koppla upp EnCase
- Utvinn

Write-blockers

- SE
- LE
- Block
- Protect

- TEST!!!

LinEn

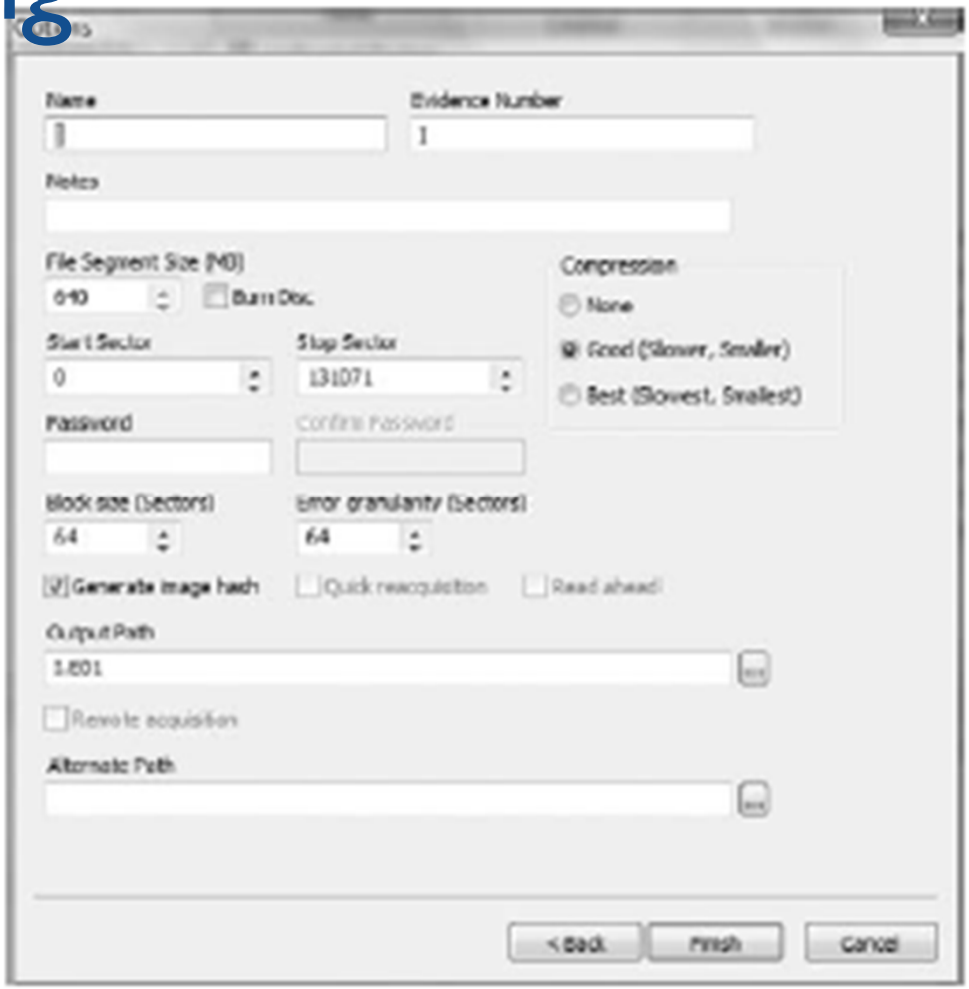
- Knoppix
- Nätverksutvinning
- Direktutvinning
- Många filsystem
- Stöd för hårdvara (delvis)

EE/FIM

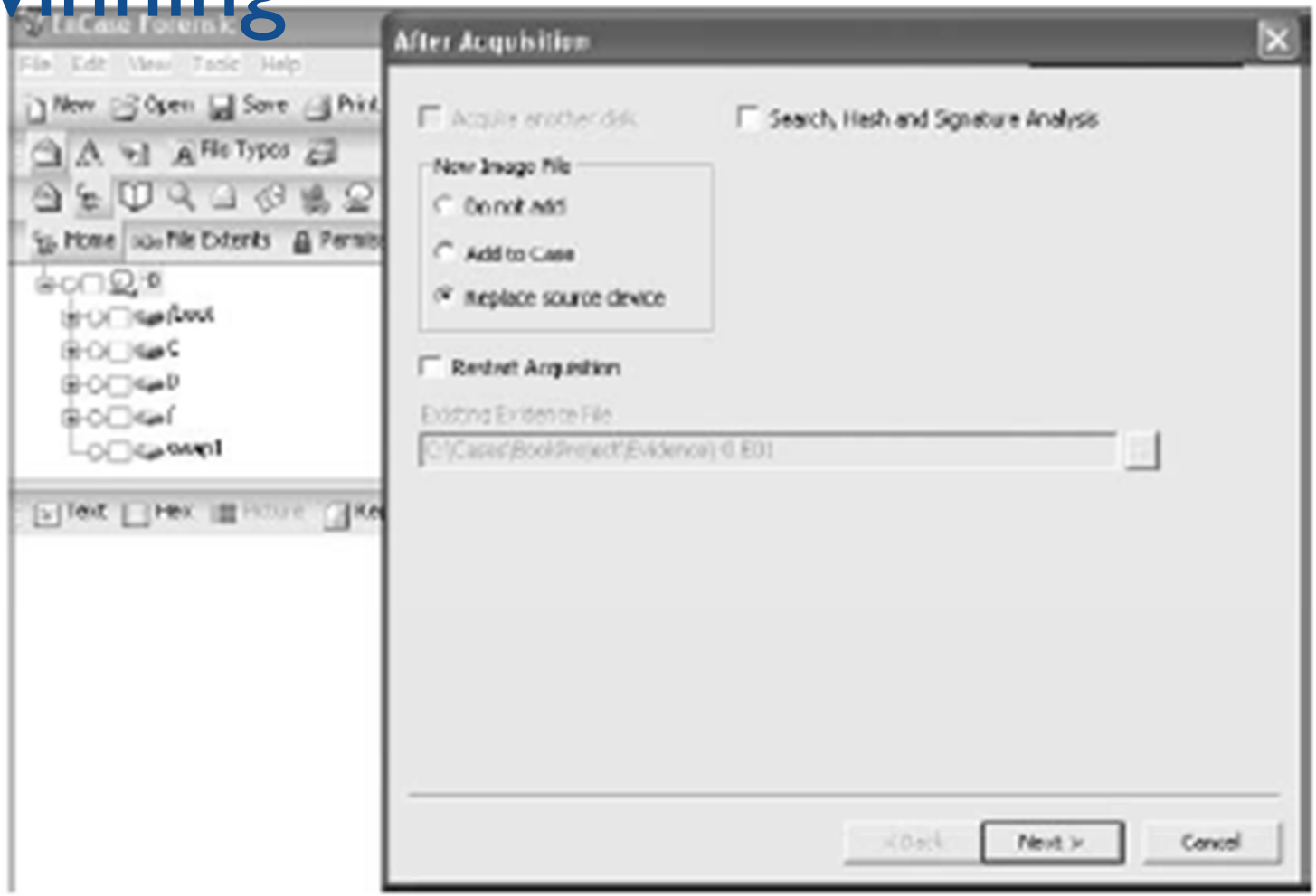
Är hårddisken död?

- Vad är felet?
  - Koppling
  - Kontrollerkort
  - Mekanik

Utvinning


Name
Evidence Number
1
Notes
File Segment Size (MB)
Burn Disc
Start Sector
Stop Sector
0
131071
Password
Confirm Password
Compression
None
Good (Slower, Smaller)
Best (Slowest, Smallest)
Block size (sectors)
Error granularity (sectors)
64
64
Generate image hash
Quick reacquisition
Read ahead
Output Path
Remote acquisition
Alternate Path
< Back
Finish
Cancel

Utvinning


After Acquisition
Search, Hash and Signature Analysis
New Image File
Add to Case
Replace source device
Next >
Cancel