

# **EXHIBIT I**

## **Volume 7**

# Downgrades

- Sony fixed the exploit
- Service mode triggered by USB “JIG”
  - HMAC authenticated, keys dumped
- Leaked service app used to enable downgrades



You have earned a trophy.  
🏆 More Piracy

- Sony fixed the exploit
- Service mode triggered by USB “JIG”
  - HMAC authenticated, keys dumped
- Leaked service app used to enable downgrades

# AsbestOS

# AsbestOS

- Replace LV2/GameOS in memory

# AsbestOS

- Replace LV2/GameOS in memory
- OtherOS mode and GameOS mode are virtually identical
- Except GameOS can do more stuff, e.g. 3D

# AsbestOS

- Replace LV2/GameOS in memory
- OtherOS mode and GameOS mode are virtually identical
  - Except GameOS can do more stuff, e.g. 3D
- Run Linux again (even on the Slim!)

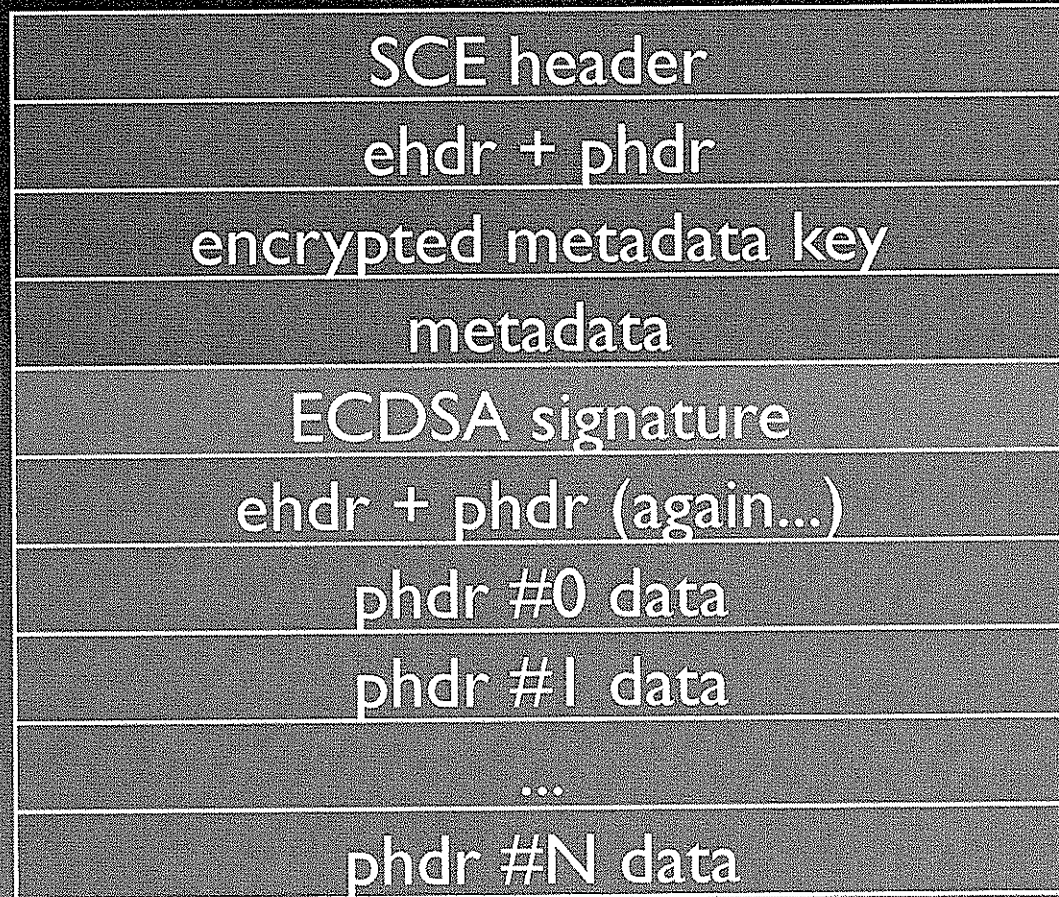
# AsbestOS

- Replace LV2/GameOS in memory
- OtherOS mode and GameOS mode are virtually identical
  - Except GameOS can do more stuff, e.g. 3D
- Run Linux again (even on the Slim!)
- Use NetRPC to remote-control the PS3 and experiment...

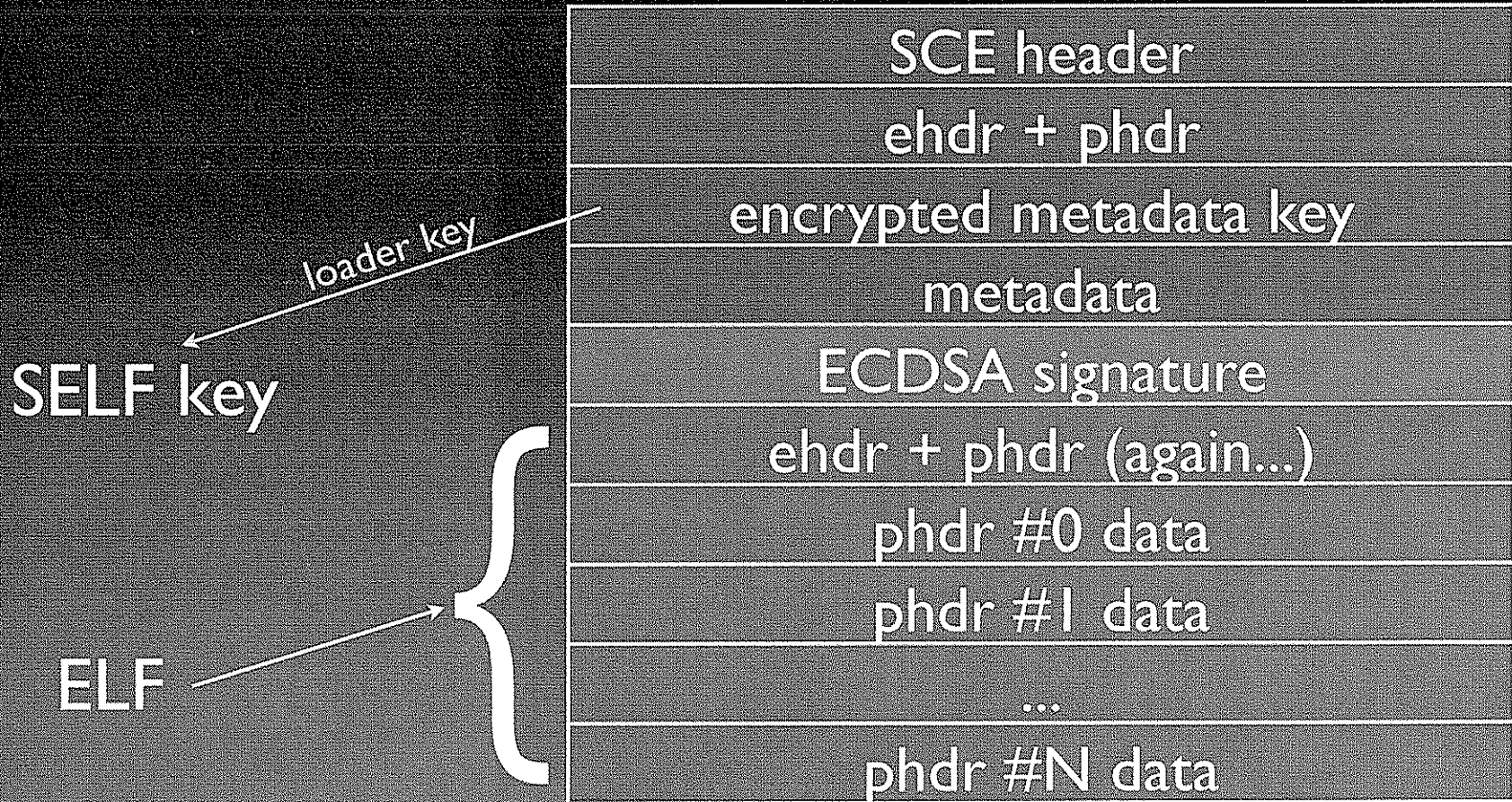


# SELFs

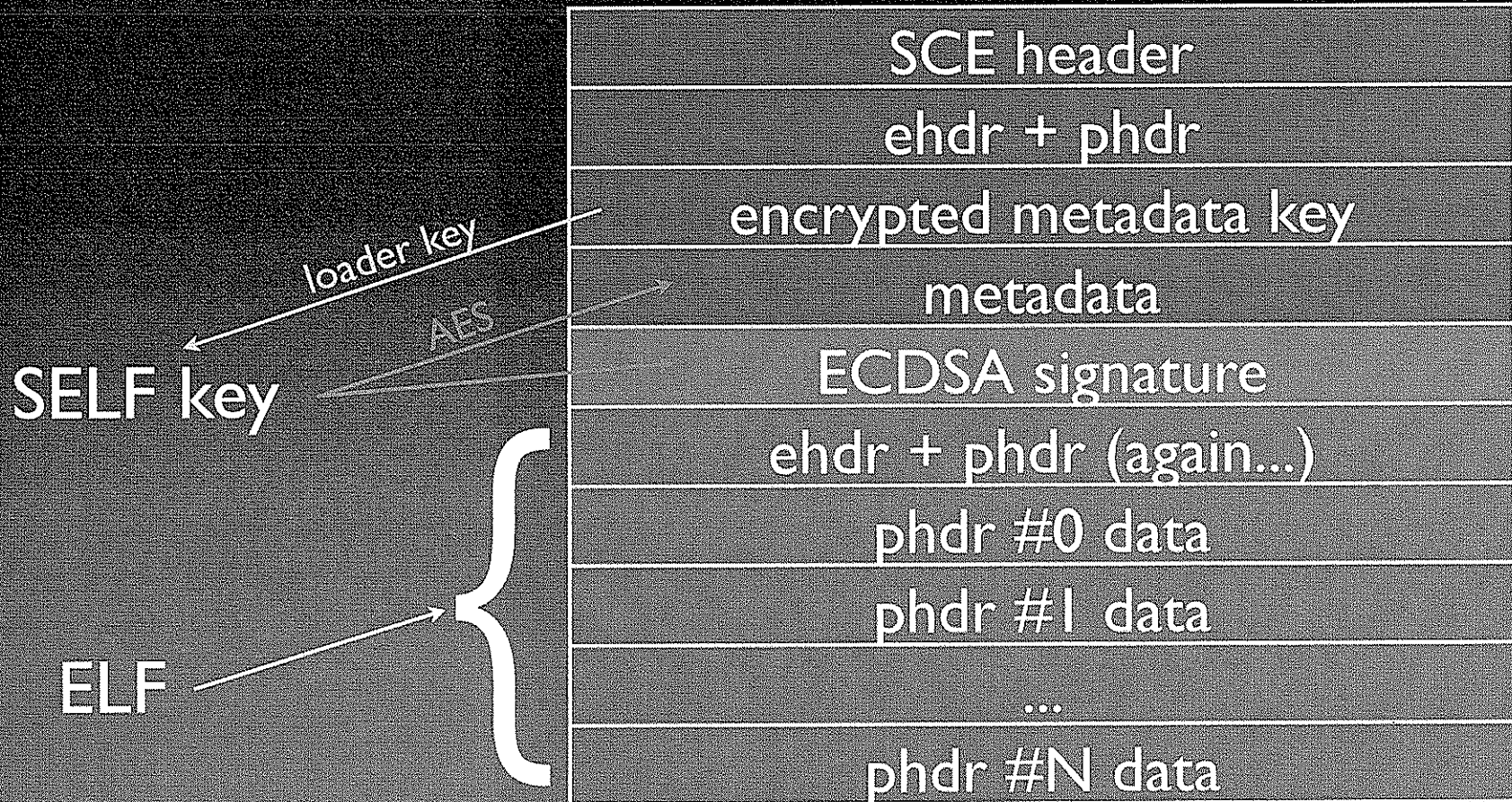
ELF



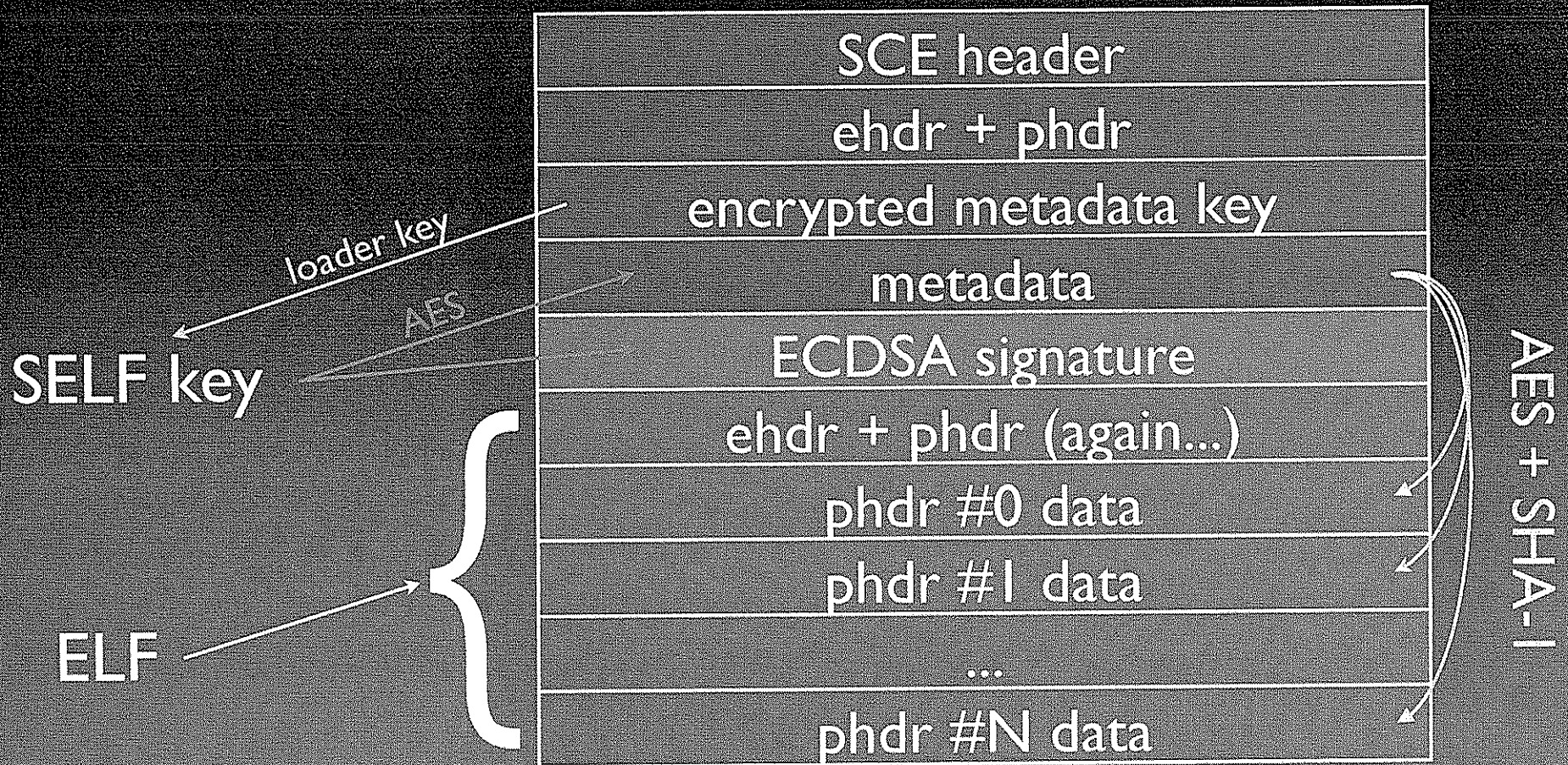
# SELFs



# SELFs



# SELFs



# The Oracle

- Sony's idea: "No one can see our code!"
- ... unless the PPE is compromised
- Decrypting all code possible from GameOS
  - security coprocessor pointless!
- But we want keys!