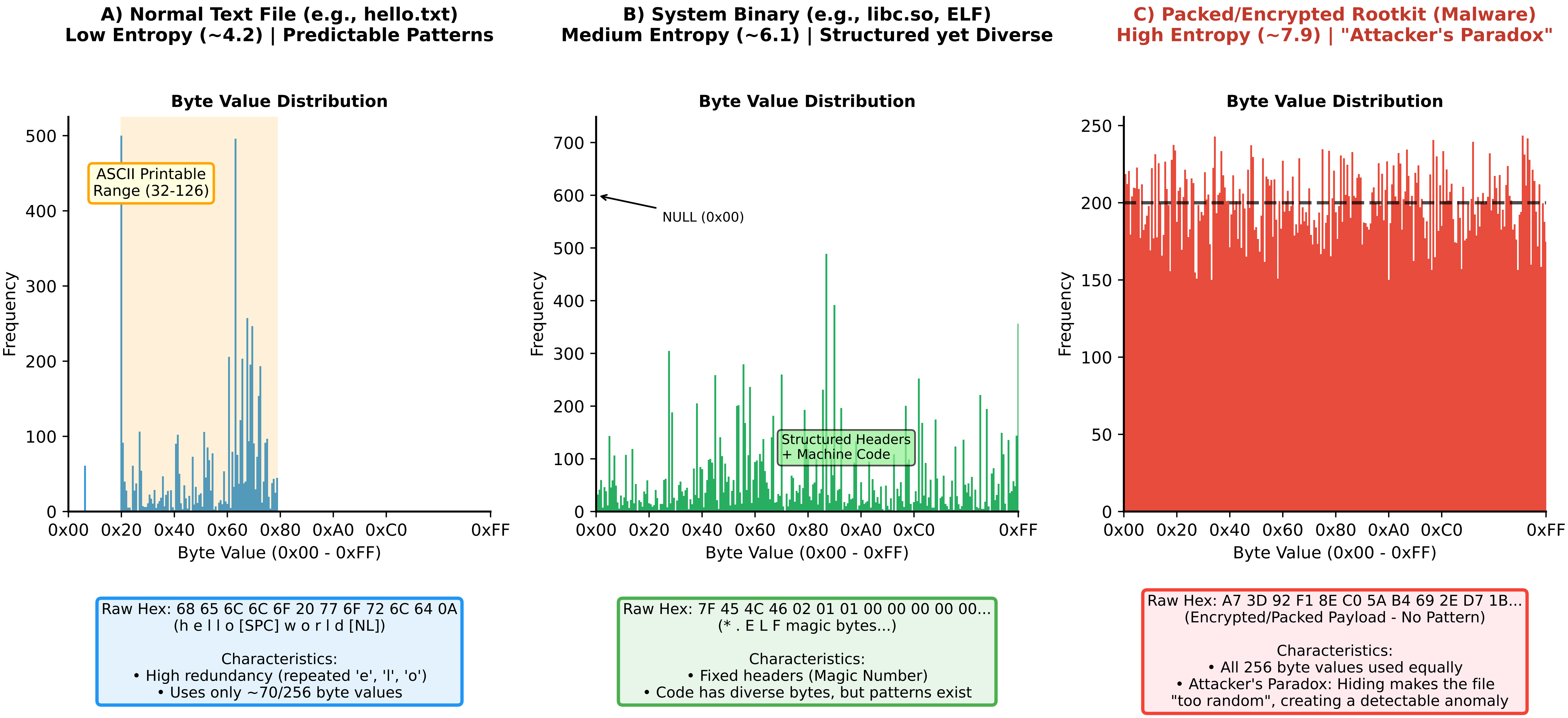
Figure: Entropy-based Analysis and Byte Patterns of Different File Types



A) Normal Text File (e.g., hello.txt)
Low Entropy (~4.2) | Predictable Patterns

B) System Binary (e.g., libc.so, ELF)
Medium Entropy (~6.1) | Structured yet Diverse

C) Packed/Encrypted Rootkit (Malware)
High Entropy (~7.9) | "Attacker's Paradox"

Raw Hex: 68 65 6C 6C 6F 20 77 6F 72 6C 64 0A
(h e l l o [SPC] w o r l d [NL])

Characteristics:
• High redundancy (repeated 'e', 'l', 'o')
• Uses only ~70/256 byte values

Raw Hex: 7F 45 4C 46 02 01 01 00 00 00 00 00...
(* . E L F magic bytes...)

Characteristics:
• Fixed headers (Magic Number)
• Code has diverse bytes, but patterns exist

Raw Hex: A7 3D 92 F1 8E C0 5A B4 69 2E D7 1B...
(Encrypted/Packed Payload - No Pattern)

Characteristics:
• All 256 byte values used equally
• Attacker's Paradox: Hiding makes the file
"too random", creating a detectable anomaly