PROJECT 2 BINWALK analysis

8 File types included in project 2. MPG, PDF, BMP, GIF, ~~ZIP~~, JPG, DOCX, AVI, PNG

File signatures obtained from https://www.garykessler.net/library/file\_sigs.html

**BINWALK ANALYSIS RESULTS**

**Binwalk on 6 out of 8 resulted in reliable matches.   
MPG & BIMP signatures are too short and result in thousands of false positives.**

1. MPG

Sigs 4

FF Ex small sig too many false positives

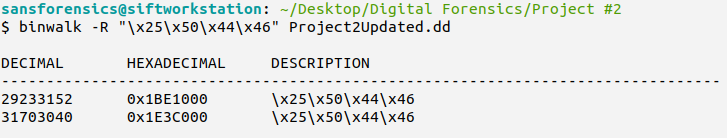
FF Fx small sig too many false positives

00 00 01 Bx

~~00 00 01 BA~~ 0 hits

2. PDF

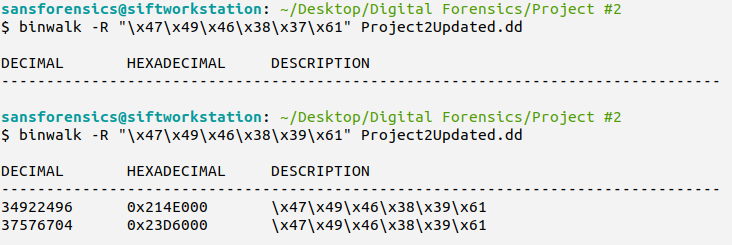
25 50 44 46 2 hits



3. BMP

42 4D small sig too many false positives (~2044)

4. GIF  
2 sigs  
~~47 49 46 38 37 61~~ 0 binwalk hits  
47 49 46 38 39 61 2 bw hits



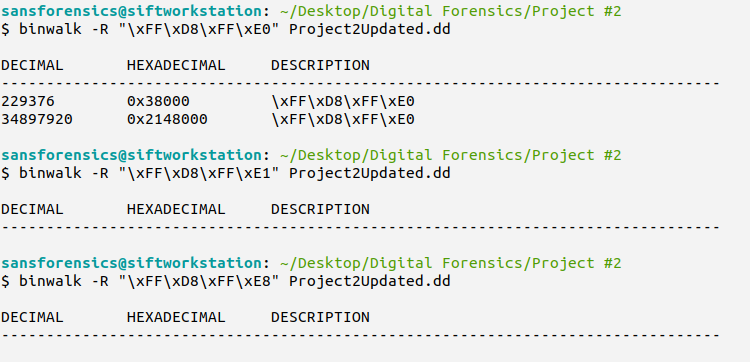
5. JPG

3 sigs

FF D8 FF E0 xx xx 4A 46 49 46 00 2 BW HITS

~~FF D8 FF E1 xx xx 45 78 69 66 00~~  0 BW HITS

~~FF D8 FF E8 xx xx 53 50 49 46 46 00~~ 0 BW HITS

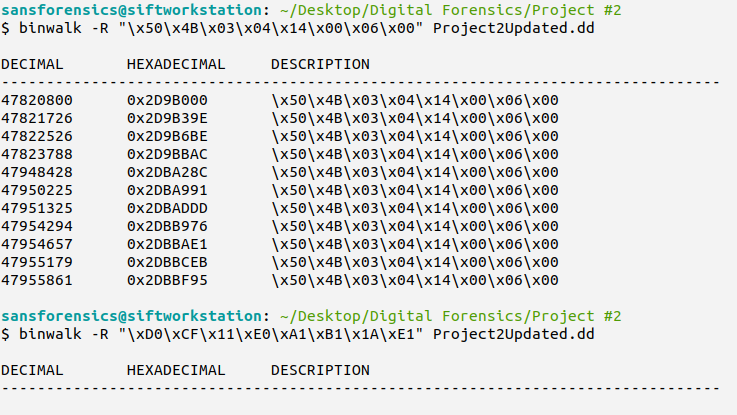


6. DOCX

2 sigs

50 4B 03 04 14 00 06 00 11 HITS

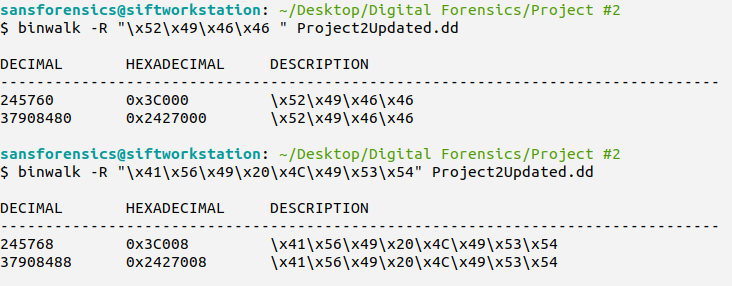
~~D0 CF 11 E0 A1 B1 1A E1~~  0 HITS



7. AVI

1 sig (two lines belong to the same sig)

52 49 46 46 xx xx xx xx (*xx xx xx xx* is the file size (little endian))  
41 56 49 20 4C 49 53 54 2 hits



8. PNG

89 50 4E 47 0D 0A 1A 0A

