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

```
sansforensics@siftworkstation: ~/Desktop/Digital Forensics/Project #2
$ binwalk -R "\x25\x50\x44\x46" Project2Updated.dd

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
29233152      0x1BE1000       \x25\x50\x44\x46
31703040      0x1E3C000       \x25\x50\x44\x46
```

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

```
sansforensics@siftworkstation: ~/Desktop/Digital Forensics/Project #2
$ binwalk -R "\x47\x49\x46\x38\x37\x61" Project2Updated.dd

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------

sansforensics@siftworkstation: ~/Desktop/Digital Forensics/Project #2
$ binwalk -R "\x47\x49\x46\x38\x39\x61" Project2Updated.dd

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
34922496      0x214E000       \x47\x49\x46\x38\x39\x61
37576704      0x23D6000       \x47\x49\x46\x38\x39\x61
```

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

```
sansforensics@siftworkstation: ~/Desktop/Digital Forensics/Project #2
$ binwalk -R "\xFF\xD8\xFF\xE0" Project2Updated.dd

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
229376        0x38000         \xFF\xD8\xFF\xE0
34897920      0x2148000       \xFF\xD8\xFF\xE0

sansforensics@siftworkstation: ~/Desktop/Digital Forensics/Project #2
$ binwalk -R "\xFF\xD8\xFF\xE1" Project2Updated.dd

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------

sansforensics@siftworkstation: ~/Desktop/Digital Forensics/Project #2
$ binwalk -R "\xFF\xD8\xFF\xE8" Project2Updated.dd

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
```

6. DOCX
2 sigs
50 4B 03 04 14 00 06 00 11 HITS
~~D0 CF 11 E0 A1 B1 1A E1~~ 0 HITS

```
sansforensics@siftworkstation: ~/Desktop/Digital Forensics/Project #2
$ binwalk -R "\x50\x4B\x03\x04\x14\x00\x06\x00" Project2Updated.dd

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
47820800      0x2D9B000       \x50\x4B\x03\x04\x14\x00\x06\x00
47821726      0x2D9B39E       \x50\x4B\x03\x04\x14\x00\x06\x00
47822526      0x2D9B6BE       \x50\x4B\x03\x04\x14\x00\x06\x00
47823788      0x2D9BBAC       \x50\x4B\x03\x04\x14\x00\x06\x00
47948428      0x2DBA28C       \x50\x4B\x03\x04\x14\x00\x06\x00
47950225      0x2DBA991       \x50\x4B\x03\x04\x14\x00\x06\x00
47951325      0x2DBADDD       \x50\x4B\x03\x04\x14\x00\x06\x00
47954294      0x2DBB976       \x50\x4B\x03\x04\x14\x00\x06\x00
47954657      0x2DBBAE1       \x50\x4B\x03\x04\x14\x00\x06\x00
47955179      0x2DBBCEB       \x50\x4B\x03\x04\x14\x00\x06\x00
47955861      0x2DBBF95       \x50\x4B\x03\x04\x14\x00\x06\x00

sansforensics@siftworkstation: ~/Desktop/Digital Forensics/Project #2
$ binwalk -R "\xD0\xCF\x11\xE0\xA1\xB1\x1A\xE1" Project2Updated.dd

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
```

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

```
sansforensics@siftworkstation: ~/Desktop/Digital Forensics/Project #2
$ binwalk -R "\x52\x49\x46\x46 " Project2Updated.dd

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
245760        0x3C000         \x52\x49\x46\x46
37908480      0x2427000       \x52\x49\x46\x46

sansforensics@siftworkstation: ~/Desktop/Digital Forensics/Project #2
$ binwalk -R "\x41\x56\x49\x20\x4C\x49\x53\x54" Project2Updated.dd

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
245768        0x3C008         \x41\x56\x49\x20\x4C\x49\x53\x54
37908488      0x2427008       \x41\x56\x49\x20\x4C\x49\x53\x54
```

8. PNG

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

```
sansforensics@siftworkstation: ~/Desktop/Digital Forensics/Project #2
$ binwalk -R "\x89\x50\x4E\x47\x0D\x0A\x1A\x0A" Project2Updated.dd

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
31297536      0x1DD9000       \x89\x50\x4E\x47\x0D\x0A\x1A\x0A
47824425      0x2D9BE29       \x89\x50\x4E\x47\x0D\x0A\x1A\x0A
```