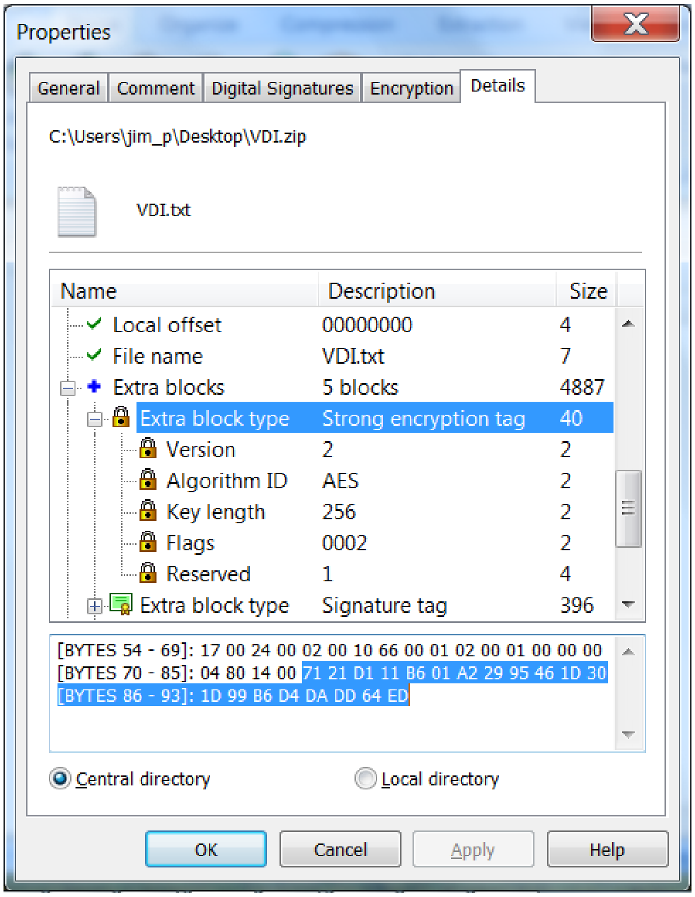
1. Within a certificate encrypted .ZIP file, locate the “strong encryption tag” block (0x0017) in Details.



C:\Users\jim_p\Desktop\VDI.zip

VDI.txt

Name	Description	Size
✓ Local offset	00000000	4
✓ File name	VDI.txt	7
⊟ ✚ Extra blocks	5 blocks	4887
⊟ 🔒 Extra block type	Strong encryption tag	40
🔒 Version	2	2
🔒 Algorithm ID	AES	2
🔒 Key length	256	2
🔒 Flags	0002	2
🔒 Reserved	1	4
⊞ Extra block type	Signature tag	396

```
[BYTES 54 - 69]: 17 00 24 00 02 00 10 66 00 01 02 00 01 00 00 00
[BYTES 70 - 85]: 04 80 14 00 71 21 D1 11 B6 01 A2 29 95 46 1D 30
[BYTES 86 - 93]: 1D 99 B6 D4 DA DD 64 ED
```

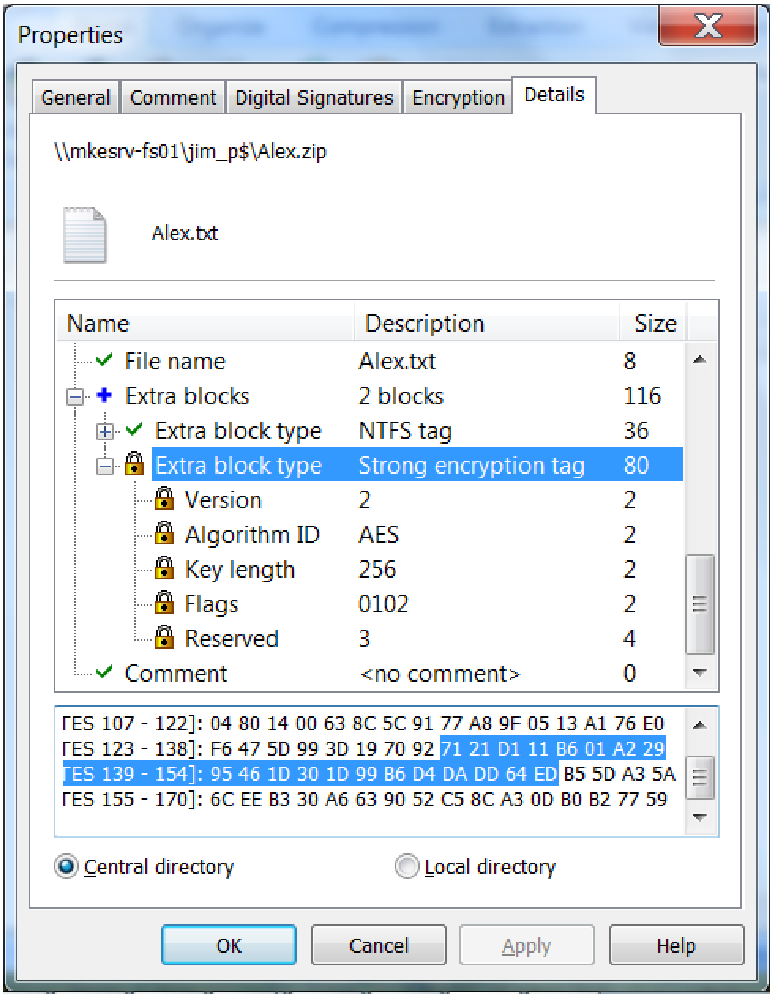
● Central directory ○ Local directory

2. Match the public key hash value for the certificate using the “Key Id Hash(sha1)” value from “`certutil -v -store -user My > mystore.txt`

```
  00d0  0b c0 93 6b ca 10 a2 ff  b5 52 ab b1 89 07 81 4e
  00e0  1b 25 6d 1d 73 12 eb 4b  3f b3 83 01 7d be 8b e1
  00f0  7f c0 a6 17 8e db 6b fc  40 72 4f 43 8e ab 2a c1
Non-root Certificate
Key Id Hash(rfc-sha1): 17 e9 34 87 02 08 f3 98 04 e4 6b fb 9d c3 90 0e 7a 57 65 d5
Key Id Hash(sha1): 71 21 d1 11 b6 01 a2 29 95 46 1d 30 1d 99 b6 d4 da dd 64 ed
Cert Hash(md5): d0 a5 c5 7b 56 42 20 37 45 ba fe 4e b9 ab 24 71
Cert Hash(sha1): e3 01 56 96 3d fd e1 b8 d3 d9 1b b0 dd 08 9c 16 cf 58 d8 b9

 CERT_REQUEST_ORIGINATOR_PROP_ID(71):
  mkelap-jimp7.pkware.com
```

3. When multiple public keys have been used during encryption (which is likely when contingency keys are used), you will need to search through the strong encryption tag data looking for the 20 byte match to the public key you seek.



\\mkesrv-fs01\jim_p$\Alex.zip

Alex.txt

Name	Description	Size
✓ File name	Alex.txt	8
Extra blocks	2 blocks	116
✓ Extra block type	NTFS tag	36
Extra block type	Strong encryption tag	80
Version	2	2
Algorithm ID	AES	2
Key length	256	2
Flags	0102	2
Reserved	3	4
✓ Comment	<no comment>	0

```
ΓES 107 - 122]: 04 80 14 00 63 8C 5C 91 77 A8 9F 05 13 A1 76 E0
ΓES 123 - 138]: F6 47 5D 99 3D 19 70 92 71 21 D1 11 B6 01 A2 29
ΓES 139 - 154]: 95 46 1D 30 1D 99 B6 D4 DA DD 64 ED B5 5D A3 5A
ΓES 155 - 170]: 6C EE B3 30 A6 63 90 52 C5 8C A3 0D B0 B2 77 59
```

● Central directory ○ Local directory