Excel 4 macro code obfuscation

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

View all posts by pcsxcetrasupport3 \rightarrow

November 16, 2021

This sample comes from a Twitter thread located <u>Here</u> by Frost @fr0s7_ and appears to be "BazarLoader"

Since this is a XIsb file I usually just open it up in my Office 2010 Pro sandbox and then convert to XIsm 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.

5cd1c8b742	5fcfd	1d23	acb	30562	26220	368	6174	d87d	6b8f	eb20	8779	0694	ea48	b5			
Offset(h)	00	01	02	03	04	05	06	07	08	09	OA	0B	oc	OD	0E	OF	
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	./•ὑ[C
00000020	6F	6E	74	65	6E	74	5F	54	79	70	65	73	5D	2E	78	6D	ontent Types].xm
0000030	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	èè¥TÉ
00000050	6E	DB	30	10	BD	07	E8	ЗF	08	BC	06	22	ED	1E	82	A2	nÛ0.%.è?.%."í.,¢
00000060	B0	9C	43	16	AO	87	Α6	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.ùï;'œ£XñE.
00000080	F9	16	BE	21	39	8B	F3	B6	71	C5	13	26	B2	C1	57	62	ù.¾!9<ó¶qÅ.&°ÁWb
00000090	2E	67	A2	40	AF	83	B1	7E	53	89	5F	B7	D7	E5	17	51	.go@_f±~St×å.Q
0A00000	50	06	6F	C0	05	8F	95	D8	22	89	F3	E5	A7	93	C5	ED	P.oÅ•Ø"‰óå§``Åí
000000B0	36	22	15	CC	F6	54	89	3A	E7	F8	55	29	D2	35	36	40	6".İöT‰:çøU)Ò560
00000000	32	44	F4	3C	B3	0E	A9	81	CC	BF	69	A3	22	E8	07	D8	2Dô<'.©.Ì¿i£"è.Ø
00000D0	AO	FA	3C	9B	9D	29	1D	7C	46	9F	CB	DC	69	88	E5	E2	ú<>.). FŸËÜi^åâ
000000E0	12	D7	FO	E8	72	71	D5	F2	FO	BO	92	7B	EB	45	71	31	.×ðèrqÕòð°' {ëEq1
000000F0	EO	ЗA	AB	4A	40	8C	CE	6A	C8	зc	AD	9E	BC	91	OD	95	à:«J@ŒĨjĒ<.ž¼`.•
00000100	D8	6A	74	92	6A	C4	2C	99	00	69	2B	1B	DO	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	.wÉ.`.µW.å7¯ômÓ.
00000120	2F	F2	F8	7E	46	42	47	EF	2C	E9	FF	DC	E5	2E	B3	64	/òø~FBGï,éÿÜå.³d
00000130	66	8F	A1	DA	46	ЗA	65	C0	1B	0E	DD	CC	DB	06	3B	DE	f.;ÚF:eÀÝÍŨ.;Þ
00000140	OF	DE	AC	64	OD	16	2B	48	F9	06	1A	46	A9	D6	A9	E7	.Þ¬d+HùF©Ö©ç
00000150	90	1E	FA	42	90	EA	5F	73	39	A1	82	7F	C8	87	19	0C	úB.ê_s9;,.E‡
00000160	A5	FE	E6	OD	B6	93	6C	18	DA	93	EE	68	C4	A 7	DF	C0	¥þæ.¶"l.U"îhA§ßA
00000170	OF	27	F9	CB	3E	DO	E2	D8	2C	DF	C7	B2	64	BE	0E	38	.'ùE>ĐâØ,BÇ*d¾.8
00000180	3C	E7	72	7C	77	F7	1C	9F	BO	5E	5B	8D	26	E8	C7	86	<çr w÷.Y°^[.&èdž
00000190	29	B2	97	39	1D	ЗF	05	94	B7	0E	69	4A	8E	81	31	26)*-9.?.".iJ2.1&
000001A0	59	43	42	F3	33	27	EE	08	D3	94	FF	25	8E	18	98	04	YCB63'1.0″ÿ%Z.~.
000001B0	CF	1D	E4	E5	E3	F8	4A	ED	84	C6	6A	C5	D8	55	0A	91	I.äáāøJi"ÆjAØU.`
000001C0	B8	15	25	9C	6E	F8	72	B3	3B	76	19	59	08	53	B6	48	,.%œnør';v.Y.S¶H
000001D0	07	39	B2	F4	D1	09	B1	6B	1A	06	CD	1E	6F	D5	37	E6	.9*öN.±kI.007æ
000001E0	E5	6F	50	4B	03	04	AO	00	00	00	00	00	BD	80	69	53	áoPK₩€iS
000001F0	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/UTeœSae
00000210	9C	8A	61	75	78	0B	00	01	04	E8	03	00	00	04	E8	03	œSauxèè.
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	OB	00	10	00	C, āAīL
00000240	5F	72	65	6C	73	2F	2E	72	65	6C	73	55	54	09	00	03	_rels/.relsUT
00000250	00	<u>A6</u>	CE	12	66	9C	8A	61	75	78	0B	00	01	04	E8	03	.!I.fœSauxè.

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".

lame	Date modified	Туре	Size
_rels	11/9/2021 10:05 AM	File folder	
drawings	11/9/2021 10:05 AM	File folder	
acrosheets	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

Scd1c8b7425fcfd1d23acb3056262203b86174d87d6b8feb2087790694ea48b5 Image: SharedStrings.bin Offset (h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 0000000000 0F 01 08 22 00 00 02 13 05 0C 0D 20 V "	
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	
00000000 WE 01 08 22 00 00 00 22 00 00 00 18 CK 0C 00 20 Y " " A	
00000010 03 00 00 63 00 6F 00 6E 00 66 00 65 00 72 00 65C.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.sw.e.r	
00000030 00 65 00 20 00 73 00 6F 00 75 00 67 00 68 00 74 .es.o.u.g.n.t	
00000040 00 20 00 61 00 /3 00 20 00 6D 00 /5 00 63 00 68a.sm.u.c.n	
00000050 00 20 00 66 00 67 00 72 00 20 00 68 00 69 00 73F.O.Fh.1.8	
00000000 00 20 00 70 00 60 00 65 00 61 00 73 00 75 00 72p.i.e.a.s.u.r	
00000070 00 65 00 20 00 61 00 73 00 20 00 66 00 67 00 72 .ea.si.o.r	
00000080 00 20 00 6D 00 79 00 20 00 62 00 65 00 65 00 65m.yb.e.n.e	
00000000 00 66 00 69 00 74 00 22 00 49 00 20 00 20 00 69 .I.I.t	
000000A0 00 6E 00 69 00 65 00 64 00 20 00 74 .n.d.e.e.d., .t	
000000B0 00 61 00 60 00 68 00 69 00 20 00 63 00 67 .a.i.k.e.ac.o	
00000000 00 6D 00 70 00 61 00 72 00 61 00 74 00 69 00 76 .m.p.a.r.a.t.i.v	
00000000 00 65 00 60 00 79 00 20 00 60 00 69 00 74 00 74 .e.i.yi.i.t.	
000000E0 00 60 00 65 00 20 00 62 00 75 00 74 00 20 .1.e., .b.u.t.	
00000000 00 49 00 20 00 68 00 65 00 61 00 72 00 64 00 20 .1n.e.a.r.d.	
00000100 00 68 00 69 00 60 00 20 00 74 00 61 00 60 00 68 .n.i.mt.a.i.k	
00000110 00 20 00 77 00 69 00 74 00 68 00 72 00 65 00 6Cw.i.t.n.r.e.i	
00000120 00 69 00 /3 00 68 00 22 00 20 00 49 00 /4 00 20 .1.3.h1.t.	
00000130 00 // 00 61 00 /3 00 20 00 68 00 69 00 /3 00 20 .w.a.sh.i.s.	
00000140 00 6E 00 61 00 74 00 75 00 72 00 65 00 20 00 74 .n.a.t.u.r.et	
00000150 00 6F 00 20 00 62 00 65 00 20 00 63 00 6F 00 6D .ob.ec.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.; .n.e1	
00000180 00 69 00 68 00 65 00 64 00 20 00 74 00 6F 00 20 .1.K.e.dt.o.	
00000190 00 6F 00 70 00 65 00 6E 00 20 00 74 00 6F 00 20 .o.p.e.nt.o.	
000001A0 00 61 00 60 00 69 00 6E 00 64 00 20 00 75 00 6E .a.m.1.n.du.n	
000001B0 00 61 00 63 00 /1 00 /5 00 61 00 69 00 6E 00 /4 .a.c.g.u.a.1.n.t	
000001C0 00 65 00 64 00 20 00 77 00 69 00 74 00 68 00 20 .e.dw.i.t.n.	
000001D0 00 74 00 68 00 65 00 20 00 77 00 6F 00 72 00 6C .t.n.ew.o.r.1	
000001E0 00 64 00 20 00 67 00 6C 00 69 00 6D 00 70 00 73 .ag.1.1.m.p.s	
00000110 00 65 00 73 00 20 00 67 00 66 00 20 00 69 00 74 .e.s6.f1.t	
00000200 00 /3 00 20 00 /3 00 63 00 65 00 65 00 65 00 73 .s. s.c.e.n.e.s	
00000210 00 20 00 61 00 62 00 64 00 20 00 77 00 61 00 79a.n.dW.a.Y	
00000220 00 /3 00 20 00 28 00 49 00 20 00 64 00 6F 00 6E .s(.1d.o.n	
00000230 00 6F 00 74 00 20 00 6D 00 65 00 61 00 6E 00 20 .0.tm.e.a.n.	
00000240 00 09 00 /4 00 /3 00 20 00 03 00 61 00 /2 00 72 .1.t.sC.O.r.r	
00000250 00 /5 00 /0 00 /4 00 20 00 /3 00 63 00 65 00 65 .u.p.ts.C.e.n	
00000200 00 05 00 /3 00 20 00 01 00 02 00 04 00 20 00 // .e.sa.n.dW	
00000270 00 00 00 00 00 00 00 00 00 00 00 20 00 77 00 01 .1.C.K.e.dW.a	
00000200 00 /9 00 /3 00 20 00 20 00 62 00 /5 00 /4 00 20 .y.s., .b.u.t.	
00000230 00 /3 00 /5 00 63 00 60 00 20 00 61 00 /3 00 20 .s.u.c.na.s.	
000002R0 00 04 00 05 00 /2 00 09 00 /0 00 05 00 04 00 20 .d.e.r.1.V.e.d.	
00000200 00 /4 00 08 00 05 00 09 00 /2 00 69 00 65 00 79 .t.n.e.1.r.1.n.t	
00000200 00 65 00 72 00 65 00 73 00 74 00 20 00 66 00 72 .e.r.e.s.tr.	
00000250 00 07 00 00 00 20 00 /4 00 00 00 05 00 20 00 07 .0.mC.n.eg	

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.

5cd1c8b742	5fcfd	1d23	Bacb	30562	26220)3b8	6174	d87d	6b8f	eb20	8779	0694	ea48	b5	8	share	edStrings.bin 📓 sheet1.bin	
Offset(h)	00	01	02	03	04	05	06	07	08	09	OA	0B	oc	OD	0E	OF		
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	.00000000	
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	00	26	00		
00000050	89	01	1E	9E	03	00	00	00	00	17	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	ЗA	00	00	00	02	00	00	00	.~.\$	
00000080	00	00	00	00	01	00	00	00	ЗA	00	00	00	ЗA	00	00	00		
00000090	02	00	00	00	02	00	00	00	8A	01	00	86	01	00	E5	03	štå.	
0A000000	0C	FF	FF	FF	FF	08	00	2C	01	00	00	00	00	86	03	00	·ÿÿÿÿ,t	
00000B0	3C	12	03	00	00	00	03	00	00	00	B6	08	00	00	00	00	<¶	
00000000	00	00	02	00	зc	12	04	00	00	00	04	00	00	00	00	0A	<	
00000D0	00	00	00	00	00	00	02	00	зc	12	05	00	00	00	05	00		
000000E0	00	00	DB	0A	00	00	00	00	00	00	02	00	3C	12	07	00		
000000F0	00	00	07	00	00	00	B6	09	00	00	00	00	00	00	02	00	¶	
00000100	87	03	00	91	01	00	00	19	00	00	00	00	00	00	00	00	ŧ`	
00000110	2C	01	00	10	00	01	00	00	00	00	00	00	00	07	00	00	,	
00000120	00	07	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
00000130	19	01	00	00	00	00	00	00	00	20	01	00	10	00	01	00		
00000140	00	00	00	00	00	00	00	00	00	10	02	00	00	00	00	00		
00000150	00	00	20	01	00	10	00	01	00	00	02	00	00	00	00	07		
00000170	00	00	00	07	00	00	00	00	00	00	00	00	00	02	00	00	,	
00000180	00	00	19	03	00	00	00	00	00	00	00	20	01	00	10	00		
00000190	01	00	00	00	00	00	00	00	07	00	00	00	07	oc	00	00		
000001A0	00	00	00	00	00	00	03	00	00	00	00	19	04	00	00	00		
000001B0	00	00	00	00	2C	01	00	10	00	01	00	00	00	00	00	00		
000001C0	00	07	00	00	00	07	oc	00	00	00	00	00	00	00	00	04		
000001D0	00	00	00	07	0C	01	00	00	00	00	00	00	00	05	00	00		
000001E0	00	00	19	05	00	00	00	00	00	00	00	2C	01	00	10	00		
000001F0	01	00	00	00	00	00	00	00	07	00	00	00	07	0C	00	00		
00000200	00	00	00	00	00	00	06	00	00	00	0A	91	07	05	00	00	·····	
00000210	00	00	00	00	00	01	00	00	7E	03	00	00	1E	53	00	41	S.A	
00000220	6F	00	44	0A	00	00	00	04	C0	1E	0C	00	1E	01	00	41	o.DAA	
00000230	1F	00	08	44	0A	00	00	00	04	C0	1E	03	00	1E	01	00	DA	
00000240	41	1F	00	08	44	OA	00	00	00	04	C0	1E	04	00	1E	01	ADA	
00000250	00	41	11	00	80	44	0A	00	00	00	04	CO	1E	12	00	1E	.ADA	
00000260	01	00	41	11	100	63	1E	33	00	41	10	00	08	1E	32	00		
00000270	41	10	40	08	12	53	00	41	10	00	44	44	00	00	00	01	AO5.AO.D	
00000280	01	20	15	23	100	15	01	41	41	15	00	11	44	00	00	00	λ # λ D	
00000230	00	01	C0	15	00	00	15	01	00	41	15	00	0.8	44	00	00	à a D	
00000280	00	00	01	co	1E	09	00	1E	01	00	41	1 5	00	08	1E	45	à à F	
00000200	00	41	6F	00	08	1E	78	00	41	6F	00	08	44	OD	00	00	. AO X . AO D	
000002D0	00	01	CO	1E	23	00	1E	01	00	41	1F	00	08	44	0D	00	À.#AD	
000002E0	00	00	01	CO	1E	4E	00	1E	01	00	41	1F	00	08	44	OD	À.NAD.	
000002F0	00	00	00	01	CO	1E	2B	00	1E	01	00	41	1F	00	08	44	À.+AD	
00000300	OD	00	00	00	01	CO	1E	2E	00	1E	01	00	41	1F	00	08	ÀA	
00000310	44	0D	00	00	00	01	C0	1E	23	00	1E	01	00	41	1F	00	DÀ.#A	
00000320	08	44	OD	00	00	00	01	C0	1E	5F	00	1E	01	00	41	1F	.DÀA.	
00000330	00	08	1E	4A	00	41	6F	00	1E	4A	00	41	6F	00	08	1E	J.AoJ.Ao	
00000340	43	00	41	6F	00	08	1E	43	00	41	6F	00	08	1E	43	00	C.AoC.AoC.	
00000350	41	6F	00	08	1E	43	00	41	6F	00	08	1E	4A	00	41	6F	AoC.AoJ.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_XIsm.xls	sm																
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	oc	OD	0E	OF	
00000000	60	4B	03	04	14	00	06	00	08	00	00	00	21	00	A5	22	ÊK!.¥"
00000010	90	41	99	01	00	00	8B	05	00	00	13	00	08	02	5B	43	œA™<[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	AO	00	02	00	00	00	00	00	00	00	1
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	
00000B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000000	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000D0	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	AC	54	4B	4F	1B	31	10	TKO.1.
00000240	BE	57	E2	ЗF	AC	7C	45	BB	0E	1C	AA	AA	CA	86	43	4B	Wa?¬ E»*E†CK
00000250	8F	25	52	E9	OF	18	EC	49	D6	8A	5F	F2	18	48	FE	7D	.%Ré1IOS_0.Hp}
00000260	C7	4E	48	21	4A	B 3	8D	EO	B2	EB	D7	F7	98	B1	67	A6	ÇNH!J³.à*ë×÷~±g¦
00000270	37	6B	67	9B	27	4C	64	82	EF	C5	55	37	11	OD	7A	15	7kg>'Ld, ïÁU7z.
00000280	B4	F1	CB	5E	FC	BE	FF	D1	7E	11	OD	65	FO	1A	6C	FO	'ñE^u%ÿN~eð.lð
00000290	D8	8B	OD	92	B8	99	5D	7C	9A	DE	6F	22	52	C3	68	4F	Ø<.',™] ŠÞo"RAhO
000002A0	BD	18	72	8E	5F	A5	24	35	AO	03	EA	42	44	CF	3B	8B	H.r2_W\$5 .eBDI;<
000002B0	90	10	64	9E	A6	A 5	8C	AO	56	BO	44	79	ЗD	99	7C	96	dž¦¥Œ V°Dy=™ -
000002C0	2A	F8	8C	3E	B7	B9	70	88	D9	F4	3B	2E	E0	D1	E6	E6	*øŒ> ``p^Uô; àNææ
000002D0	76	CD	CB	5B	27	73	BF	14	CD	B7	ED	B9	22	D5	OB	E3	VIE['s¿.I.i'"O.ā
000002E0	OA	3E	F2	BA	3C	8A	48	68	E9	00	02	31	5A	A3	20	73	.>o° <shhé1z£ s<="" td=""></shhé1z£>
000002F0	6C	F2	C9	EB	03	5F	ED	CE	53	C7	C8	7A	86	06	13	E9	loreliscezte
00000300	92	8D	FF	43	A1	EC	BC	F5	F4	5A	60	87	BB	E3	64	26	.yC;1400Z ***********************************
00000310	A3	81	99	43	CA	3F	C1	81	73	89	86	F2	39	A4	D5	43	LICE?AIS'NO9HOC
00000320	08	AB	EE	34	49	71	E9	A8	C5	85	42	DB	D1	80	98	3B	.«14Ide AµBUN€";
00000330	07	2A	85	5B	OF	OF	16	79	OF	8C	7F	71	78	42	A9	22	."[y.@.qxB©"
00000340	49	D6	DF	D5	71	48	BE	вD	в0	36	20	16	46	A1	0E	EA	1080 H995 6, F; e

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	Туре	Size
鷆 _rels	11/10/2021 5:25 PM	File folder	
鷆 drawings	11/10/2021 5:25 PM	File folder	
鷆 macrosheets	11/10/2021 5:25 PM	File folder	
鷆 media	11/10/2021 5:25 PM	File folder	
鷆 theme	11/10/2021 5:25 PM	File folder	
鷆 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.

crast vertices.10* excellent.10* excellent.10* is users 11* using our 11* is used to be invested to the south a much for his passes as formy basels.1. For a basel of the south is reaching the invested of the south 11* using our 11* is the south is

<?xml version="1.0" encoding="UTF-8" standalone="yes"?)</pre>

<sst xmlns="http://schemas.openxmlformats.org/spreadsheetml/2006/main" count="34" uniqueCount="34"><si><t>conferences were indeed, talked comparatively little, but I heard him talk withrelish. It was his nature to be communicative; he liked to o scenes and ways (I donot mean its corrupt scenes and wicked ways, but such as derived theirinterest from the great scale o were characterised); and I had a keen delight inreceiving the new ideas he offered, in imagining the new pictures heportra hedisclosed, never startled or troubled by one noxious allusion.The ease of his manner freed me from painful restraint: th treated me,</t>treated me,troubled or troubled by one noxious allusion.The ease of his manner freed me from painful restraint: th treated me,treated me,troubled or troubled by one noxious allusion.The ease of his manner freed me from painful restraint: th treated me,treated me,troubled or troubled by one noxious allusion.The ease of his manner freed me from painful restraint: th treated me,neat yellow sheaf of rye laid on thethreshing floor for seed.Floodor came from a village at some distance from the one in w association. Now ithad been let to the innkeeper.Levin talked to Floodor about this land and asked whether Platon, awell-to village,would not take the land for the coming year.clear, notfeverish; but their expression was stern.SThank God15 she said. STou5re not in pain755A little here,5 he pointed silence, stiffening his broad jaws, he looked at her while shebandaged him up. When she had finished he said:515m not deli shot myself on purpose.5

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.

| eacher m manage aller ar m manage and and m acco | |
|---|--|
| <pre><?xml version="1.0" encoding="UTF-8" st</pre></pre> | andalone="yes"?> |
| <sst count="34" uniquecount="34" xmlns="http://schemas.openxmlforma</td><td>ats.org/spreadsheetml/2006/main"><si><t>conferences were sought at</t></si></sst> | |
| indeed, talked comparatively little, but | It I heard him talk withrelish. It was his nature to be communicative; he liked to open to am |
| scenes and ways (I donot mean its corru | upt scenes and wicked ways, but such as derived theirinterest from the great scale on which t |
| were characterised); and I had a keen | the second |
| hedisclosed, never startled or trouble | Parse_Excel4_SharedStrings 10.0.3 |
| treated me, <si><t>Working on</t></si> | |
| neat yellow sheaf of rye laid on theth | Select Fie |
| association. Now ithad been let to the | SelectedFile |
| village, would not take the land for the | \Sample_2021-11-10_doc\File_Xlam\w\aharedSkings.xml |
| clear, notfeverish; but their expressi | Daut |
| silence, stiffening his broad jaws, he | Lecose |
| shot myself on purpose.5 | Output |
| anunamiable-looking man, he repelled m | count="34" uniqueCount="34" |
| there was no thought on thelow, even 1 | |
| beaming full over him- for heoccupied | index. U contenences were sought as much for his preasure as for my benefit, indeed, tarked comparatively little, but heard him talk writeriash, it was his had
amind uncompared with the world dimension of the sense and uncomparatively little, but heard him talk writeriash |
| deference be it spoken) the contrast of | amount of several ways were worked grimpses on as several and ways proving and an account of the several and were characterised; and had a keen delicht interceiving the several and worked ways, but so it as derived a seminetest norm |
| ever, for everyone availed them-selves | regions hedisclosed, never startled or troubled by one noxicus allusion. The ease of his manner freed me from painful restraint, thefriendly trankness, as com- |
| fell upon her in the hall, crying with | Index:1 Working on till the peasants5 dinner hour, which was not long incoming, he went out of the barn with Flodor and fell into talk withhim, stopping beside |
| that, and said something brilliant,or | foor for seed Fieldor came from a village at some distance from the one in which Levin had once allotted land to his co-operative association. Now thad bee |
| ashamed of the great tear that dropped | about his land and asked whether Platon, awell-to-do peasant of good character belonging to the same village, would not take the land for the coming year. |
| selfish girl! But I511 truly try to 1 | not in nair 9556 little here 5 te notied to his hread 57 here let ne chance vur bance anielence stillence types were level, notevensit, but there expression not in nair 100 here the termine to here the here 5 here honder at the here the |
| more, if I can help it.55I511 try and | said SISm not delirious. Please manage that there may be no talk of myhaving shot myself on purpose 5 |
| thinking that keeping her temper | Index:3 and had no meaning in its wandering; this gave him an odd look, suchas I never remembered to have seen. For a handsome and not anunamiable |
| him aman unlikely to be influenced by | there was nopower in that smooth-skinned face of a full oval shape: no firmness inthat aquiline nose and small cherry mouth; there was no thought on thelow, e |
| justified in judging and blamingeither | brown eye As I sat in my usual nook, and looked at him with the light of the grandoles on the mantelpiece beaming full over him-for beoccupied an arm-chair |
| these principles: I supposed, then, the | samparer, as in the were coupling to make init with the rooms in the same or a spoken) the contrast coupling the more greater
lader 4 area built har had not a bar inc. During the satt files an initiation frame like a room for supervised and supervised and their noise
the second |
| <si><t>was beginning with fla</t></si> | old Hannah who, adorned with a headdeess fearfully and wonderfully made, fell upon her in the hall, crying with a sob and achuckle. Silless you, deary, a hu |
| wasleft alone. He had eaten scarcely a | everything looks lovely. 5Everybody cleared up after that, and said something brilliant or tried to, which did just as well, for laughter is ready whenhearts are lived to a solution of the s |
| but was incapable of thinking of sleep | w010 |
| open panes. Over the snow-covered root | Index 5 ashamed of the greatear that dropped off the end of her nose, and Amy never minded the rumping of her curls as she hid her face on her mother 5a |
| her that she could not make it fit to | but toi ruly try to be ceter, so ne maynot be disappointed in me dy-an-dy-sive all wills ched Meg. Si think too much of my looks andhate to work, but wonst
he lowest to call me i all fai women fand each he nowh and wild het de nu dete hans instead of diversitient he somewhere also 5 said. In this think to some the |
| grove of lettuce leaves. The potatoes | Index 6 conject of manying for interest and connections. Its surprised meshafts discovered that such was his interface. That Bought him ama unitable to |
| as they looked, having been skilfully | hischoice of a write; but the longer I considered the position, education.etc., of the parties, the less I feit justified in judging and blamingeither him or Miss Ingra |
| | |

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.

<pre>Image: Second Seco</pre>	Intellec	and the C Shared St dates to C Stocoded to C			1
<pre> the state of the stat</pre>	1	simi version=1.0: encoding	PUTT-R' standalonas'us'		-
<pre> thtp://telmane.squexel.rul</pre> thtp://telmane.squexel.rul thtp://telmane.squexel.rul thtp:/telmane.squexel.rul thtp:/telmane.squexel	2	(xm:macrosheet xmlns="http://	/schemas.openxxlformats.org/spreadsheetml/2006/main* xmlns:xm**http://schemas.microsoft.com/office/excel/2006/main* xmlns:r=		
thy in the intervent is a function of the intervent is		"http://schemas.openmilform/	A Development And Market And 1991	0 8 3	Deer
		"http://schemas.microsoft.or			and 1
<pre> Pipe Cost comfittee * 1/2 * Cost comfittee * 1/2 * Cost comfittee * Cost compares * 1 = mark * 1 = m</pre>		activeCell="C59" scref="C59"	(hout)	Cear input	8-
Mit Mit Mit Mit Mit Mit Mit Mit Mit Mit Mit Mit Mit Mit		"10" custosWidth="1"/> <col m<="" td=""/> <td>- Million</td> <td>(D-0-0-1</td> <td>a ca</td>	- Million	(D-0-0-1	a ca
<pre>r = spatial="1"" https://www.net.inter.com/inter.co</pre>		="1"> <c r="A1" t="s"><v>0<td>ipd.</td><td>Cearculus</td><td>K/C</td></v></c>	ipd.	Cearculus	K/C
		⁻¹ + ⁻¹ galax ⁻¹ ² h ² deg ⁻¹ ² h ²	Inter States 1000014 (1990) Automatic Trans T	* 00 w0460.75 (54wep.MO) 18 * 00 18 * 00 18 * 00 18 * 00 18 * 00 18 * 00 19 * 00 19 * 00 19 * 00 19 * 00 10 br>10 * 00 10 * 00	6), 0 (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)
		<v>1</v> <row< td=""><td>- getCuth*100002 afeet* Tridgede* Tridgede* Tridgede* Tridgede* 0.7 faite* 0.7 faite* 0.7 feater* 0.7 feater* 0.7 feater* 0.7 for 0.7 for 0.7 feater* 0.7 feate</td><td></td><td>15-</td></row<>	- getCuth*100002 afeet* Tridgede* Tridgede* Tridgede* Tridgede* 0.7 faite* 0.7 faite* 0.7 feater* 0.7 feater* 0.7 feater* 0.7 for 0.7 for 0.7 feater* 0.7 feate		15-
c/v>c/c>c/cov/crow17#17# Technik am DistCell P x=#18# x=bb>c/c>c/call (CHAR) Technik am DistCell P Remaining Functions P P CHAR (74) 4 ange (2MAR) (75) 4 ange (<e r="H15" t="s"><v3< td=""><td>OVER .</td><td></td><td>645</td></v3<></e>	OVER .		645
remaining Functions Braining Functions RED (014, 9, 1) Samp, ADD (014, 9, 1) Remaining Functions RED (012, 90, 1) Samp, ADD (014, 9, 1) Remaining Functions RED (012, 90, 1) Samp, ADD (014, 9, 1) Remaining Functions RED (012, 90, 1) Samp, ADD (014, 9, 1) Remaining Functions RED (012, 90, 1) Samp, ADD (015, 9) Remaining Functions RED (015, 739, 1) Samp, ADD (015, 10, 1) Remaining Functions RED (015, 739, 1) Samp, ADD (015, 10, 1) Remaining Functions RED (015, 739, 1) Samp, ADD (015, 10, 1) Remaining Functions RED (015, 739, 1) Samp, ADD (015, 10, 1) Remaining Functions RED (015, 739, 1) Samp, ADD (015, 10, 1) Remaining Functions REM (011, 2) Samp, ADD (015, 10, 1) Remaining Functions REM (011, 2) Samp, ADD (015, 10, 1) Remaining Functions REM (011, 2) Samp, ADD (015, 10, 1) Remaining Functions REM (011, 2) Samp, ADD (015, 10, 1) Remaining Functions REM (011, 2) Samp, ADD (012, 1) Samp, ADD (011, 2) Samp, ADD (011, 2) Samp, ADD (011, 2) Samp, ADD (014, 2) Samp, ADD		<row r='17"' st<="" td=""><td>Functions with Get Cell</td><td>- A</td><td>**</td></row>	Functions with Get Cell	- A	**
MDD (014,4,7,1) 4 samp 2MD (014,5) Rev Value EIR CHAR (714) samp 2MD (012, 5) Rev Value Rev Value CHAR (714) samp 2MD (012, 5) CIAR (714) samp 2MD (012, 5) Rev Value Rev Value CHAR (714) samp 2MD (012, 5) CIAR (714) samp 2MD (012, 5) CIAR (714) samp 2MD (012, 5) Rev Value CHAR (715) samp 2MD (012, 5) CIAR (714) samp 2MD (012, 5) CIAR (714) samp 2MD (012, 5) Rev Value CHAR (715) samp 2MD (015, 1, 1) samp 2MD (015, 1, 6) CIAR (714) samp 2MD (015, 1, 6) CIAR (714) samp 2MD (015, 1, 6) CIAR (714) samp 2MD (015, 1, 6) MD (015, 787, 1) samp 2MD (015, 5), 61, 10 CIAR (714) samp 2MD (015, 1, 6) CIAR (714) samp 2MD (015, 1, 6) CIAR (714) samp 2MD (015, 1, 6) C/200 (200 (200 (200 (200 (200 (200 (200		r="E18" t="b"> <f>CALL(CHAR(6</f>	Remaining Functions		35,
CHAR (74) samp/CHAR (67) sam		MID (814,9,1) 4amp;MID (814,9,1	- Hermanney - Ernary		CILL
MD (012, 49, 1) & amp; MD (012, 3) cm ² /M ² /H		CHAR(74) samp/CHAR(67) samp/CE	Row Value		234
CHAR (51) samp /CHAR (50) samp /CHAR (5		MID(C12,60,1) samp;MID(C12,31	et in WL in day on define (its		D (B
6 amp,MID (BS, 1, 1) 6 amp,MID (BS, 1, 6) 9 amp,MID (BS, 2) 9 am		CHAR(51) samp; CHAR(50) samp; HI	 A setting in the production of the set of		2 6.0
MDD (05, 281, 1) 4 amp;MDD (05, 1, 6) GridW = V ² to v		samp;MID(85,1,1) samp;MID(85,	Set that is a strategic property of the s		260
HDL0(b);77,13 44mp/MDU(b);14;14 Gen/SP +**/sock@idealp P2 C(V>C(V)C(V)C(V)CVC(V)CVC(V) Gen/SP +**/sock@idealp P2 gen/SP +**/sock@idealp Gen/SP +**/sock@idealp P2		MID (85, 201, 1) samp; MID (85, 9, 1	<pre><pre><pre>%AC</pre><pre>b*</pre><pre><pre><pre><pre><pre><pre><pre><</pre></pre></pre></pre></pre></pre></pre></pre></pre>		D (B
CVP>C/2>C/2D0PCEOVIE CVP>C/2>C/2D0PCEOVIE CVP>C/2>C/2D0PCEOVIE CVP>C/2>C/2D0PCEOVIE CVP>C/2>C/2D0PCEOVIE CVP>C/2D0PCEOVIE <		MID (85,79,1) 4amp;MID (85,16,1	<10-m3/2/mm2/2/m3/2/m3/2/m3/2/m3/2/m3/2/m3/		P28
		<pre></pre>	Sig PAGE PSY-tox-delytor/clip cits PPE PSY-tox-delytor/clip cits	(14.3.1) (24AR 21.17.1) AR(37)	0.3

This tool is designed to extract values to aid in better viewing what is happening without all of the xml tags. In this case some are left.



Here we see what the values are.

10		
1.1		
12		
10		
1.5	CC F=-P6- E=-D-SCISCALL (CHAR(03) s	mp;MiD(kin ,12,1) samp;MiD(kin ,3,1) samp;MiD(kin ,4,1) samp;MiD(kin ,4,1) samp;CRAR(51) samp;CRAR(50),CRAR(53) samp;MiD(bi
	MID(B14,9,1) samp/MID(B14,9,1) samp	2008 (69) samp /CHUR (120) samp /MLD (B14, 35, 1) samp /MLD (B14, 76, 1) samp /MLD (B14, 45, 1) samp /MLD (B14, 35, 1) samp /MLD (B14, 35
	CHAR(74) samp; CHAR(67) samp; CHAR(67	samp;CHAR(67) samp;CHAR(67) samp;CHAR(74) samp;CHAR(74),0,MID(H15,35,1) samp;MID(H15,4,1) samp;MID(H15,2,1) samp;MID(H1
	MID(C12,60,1) & amp,MID(C12,31,1),C	AR(47) samp/MID(F21,19,1) samp/MID(F21,8,1) samp/MID(F21,99,1) samp/MID(F21,416,1) samp/MID(F21,24,1) samp/MID(F21,2,1)
	MID(F21,8,1) samp; CHAR(37) samp; MID	F21, 17, 1) & amp;MID (F21, 14, 1) & amp;MID (F21, 5, 1) & amp;MID (F21, 39, 1) & amp;MID (F21, 14, 1) & amp;MID (F21, 22, 1) & amp;MID (F21, 99)
	MID(F21,22,1) samp;MID(F21,3,1) sam	MID (P21,22,1) samp;CHAR (37) samp;CHAR (92) samp;MID (P21,1,1) samp;MID (P21,5,1) samp;MID (P21,4,1) samp;CHAR (106) samp;CHA
14	<pre><c r="A7" t="s"><v>7</v></c></pre>	
15	<c r="B7" t="s"><v>8</v></c>	BtractedSharedStrings-Correct.td - Notepad
16	<pre><c r="A8" t="s"><v>9</v></c></pre>	File Edit Format View Help
17	<c r="H8" t="s"><v>10</v></c>	would not nermit her to su # Extent Sub Str From Str Type21002
18	<pre><c r="A9" t="s"><v>11</v></c></pre>	you tall me that for? with
19	<pre><c r="D9" t="b"><f>WAIT(NOW() + ")</f></c></pre>	you cert me chac for in the Get Sub Sing Stat Point End point / Length
20	<pre><c r="A10" t="s"><v>12</v></c></pre>	Taday 15 Ideal and your 12
21	<pre><c r="C10" t="s"><v>13</v></c></pre>	There are the cost 25 th cost of the the strength the
22	<pre><c r="A11" t="s"><v>14</v></c></pre>	and an analysis of the second and the presentation from at Sub Str From Str Type2 1002
23	<pre><c r="E11" t="s"><v>15</v></c></pre>	and astramed, a didn's tremen bengkind to Lave because hefe inch and e
24	<pre><c r="A12" t="s"><v>16</v></c></pre>	Get Sub String Start Fort End point / Length
25	<pre><c r="C12" t="s"><v>17</v></c></pre>	and the state of t
26	<pre><c r="A13" t="s"><v>18</v></c></pre>	Index : 10 to be billined T
27	<pre><c r="F13" t="b"><f>CALL (MID (B7, 1))</f></c></pre>	now, don't lay it all on y and shamed. I don't was so anyy and shamed. I don't was so anyy and shamed. I don't was so anyy in a shamed. I don't was so any 55,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5
	MID (H8, 16, 1) 6amp; MID (H8, 41, 1) 6amp	amazingly. SNEVER mind what bees shy things to be provide the should be shou
	MID (H8, 68, 1) 4amp (MID (H8, 3, 1) 4amp (Pickwick. SButon my honor
	MID (G19, 129, 1) 64mp (CHAR (58) 64mp (CHAR (58)	club.ssHear! Hear!s cried
	MTD (G19, 72, 1) 4 amp (CHAR (49) 4 amp (CH	Index :1/ once glancing
	MTD (E20, 21, 1) 64mp (MTD (E20, 141, 1) 6	indicating Levin.Sconstant
	CHAR (106) 4 amp (CHAR (120) 4 amp (CHAR (Levin, shook hands withhim
	MTD (#20 6 1) 0 0) -#16() (/f2(*))	Sbut you had unexpectedly
2.0		Countess Nordstone
20		Index :18 my children I Own
30		enough_to have teachers-th
34		what ISm reading5- he point
32		explain to me Here he
30	S0 1- 010 - 0- 5-257235/925/02	but Lvov would not agree w
24	<pre>cc r==hio= c==b=3cr3wAir(NOW() + // // // // // // // // // /</pre>	ISm Codout
26		Index :19 5Ah, let me al
35	<pre><c r="n1/=" t="n="><v>25</v></c></pre>	occupied when talkingto he
36	<pre><c r="A18" t="s"><v>26</v></c></pre>	

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 to letter is "e" and then the next 2 are at the same index and is "I".

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 .



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.

Byter	esearc	n be g	a 🗖	Shared	ISC-BY	tes.bd	ta je	new	16																													1
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	Α7	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	в3	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	8B	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	9B	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	89	02	00	00	73	00	74	00	61	00	79	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	в9	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	В9	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 e
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	6В	00	69	00	6E	00 0
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 3
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	17	00	69	00	6C	00 E

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

By	teRe	search	hbe E	3	Shared	19t-By	tes bd	8	new	1 23																													
1	1	9F	01	08																																			
3	2	48	00	00	00																																		- 1
	5	2C	00	00	00																																		- 1
	5	13	07	00	01	00	00	00	65	00																													- 1
(5	13	07	00	01	00	00	00	6C	00																													- 1
1	7	13	07	00	01	00	00	00	41	00																													- 1
8	3	13	07	00	01	00	00	00	69	00																													- 1
1	2	13	07	00	01	00	00	00	79	00																													- 1
11	1	13	07	00	01	00	00	00	72	00																													- 1
12	2	13	07	00	01	00	00	00	6F	00																													
13	3	13	07	00	01	00	00	00	54	00																													
14	1	13	07	00	01	00	00	00	74	00																													- 1
15	5	13	07	00	01	00	00	00	64	00																													- 1
11	7	13	07	00	01	00	00	00	61	00																													- 1
18	3	13	07	00	01	00	00	00	6E	00																													- 1
19		13	07	00	01	00	00	00	44	00																													- 1
20	0	13	07	00	01	00	00	00	77	00																													- 1
21	1	13	07	00	01	00	00	00	4C	00																													- 1
22	2	13	07	00	01	00	00	00	52	00	40	~~	<i>c</i> n	~~	c.n	0.0																							- 1
20	5	13	02	00	01	00	00	00	40	00	40	00	01	00	0E	00																							- 1
25	5	13	07	00	01	00	00	00	43	00																													- 1
26	6	13	07	00	01	00	00	00	4B	00																													- 1
27	7	13	11	00	06	00	00	00	4A	00	4A	00	43	00	43	00	42	00	42	00																			- 1
28	З	13	15	00	08	00	00	00	4B	00	65	00	72	00	6E	00	65	00	6C	00	33	00	32	00															- 1
29	2	13	OD	00	04	00	00	00	66	00	6C	00	61	00	74	00	~ ~		~ ~	~ •	~ ~	-	~ ~	~ *	~ ~		~ ~	~ ~	~ ~	CD	~ ~	C D	~~	~~	~~		~~		
30		13	B7	2E 0P	00	99	08	00	00	97	00	6F	00	6F	00	24	00	20	00	20	00	72 6D	00	61 70	00	20	00	20	00	68	00	6E	00	65	00	20	00	20	00
32	2	13	07	00	01	00	00	00	73	00	00	51	00	05	00	/4	00	00	00	20	00	60	00	19	00	20	00	/ 1	00	00	00	03	00	60	00	20	00	0.9	~~
33	3	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	5	13	09	00	02	00	00	00	55	00	44	00																											
30	5	13	FB	3D	00	7B	0F	00	00	53	00	75	00	73	00	70	00	65	00	63 6 D	00	74	00	65	00	64	00	20	00	6A	00	6F	00	69	00	6E	00	74	00
38	2	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	6E	00	6E	00	73	00
39	5	13	A5	03	00	DO	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	0	13	в5	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	L	13	в5	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	2	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
93	5	13	07	00	01	00	00	00	95	00		00																											- 1
4		13	09	00	02	00	00	00	52	00	45	00																											- 1
40	6	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	- 1
41	7	13	в3	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	3	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
<		_	_	_	_	_	_	_			_					_			_		_	_	_									_	_		_	_		_	
		<u> </u> 1	ther	me												7/6	/20	21 6	i:06	PM		F	ile	fold	er														- 1
		1	wor	ksh	eet	s										7/6	/20	21 6	5:06	PM		F	ilef	fold	er														
			qut.	xm	L											1/1	/19	80 1	:00	AN	1	>	ML	Do	cur	nen	t				34	KB							
		2	styl	es.b	in											1/1	/19	80 1	:00	AN	1	E	BIN	File							3	KB							
		1	wor	kbo	ook.	bin										1/1	/19	80 1	:00	AN	1	E	BIN	File							2	KB							
																																							- 1

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	OA	0B	0C	0D	0E	OF	
00000000	ÐF	01	08	48	00	00	00	2C	00	00	00	13	07	00	01	00	Щн,
00000010	00	00	65	00	13	07	00	01	00	00	00	6C	00	13	07	00	el
00000020	01	00	00	00	41	00	13	07	00	01	00	00	00	69	00	13	Ai
00000030	07	00	01	00	00	00	79	00	13	07	00	01	00	00	00	46	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	.oT
00000060	00	00	00	74	00	13	07	00	01	00	00	00	64	00	13	07	td
00000070	00	01	00	00	00	63	00	13	07	00	01	00	00	00	61	00	Ca.
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	Dw
000000A0	00	00	4C	00	13	07	00	01	00	00	00	52	00	13	OD	00	LR
000000B0	04	00	00	00	4C	00	4D	00	6F	00	6E	00	13	07	00	01	L.M.o.n
00000000	00	00	00	55	00	13	07	00	01	00	00	00	43	00	13	07	UC
00000D0	00	01	00	00	00	4B	00	13	11	00	06	00	00	00	4A	00	KJ.
000000E0	4A	00	43	00	43	00	42	00	42	00	13	15	00	80	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.1.3.2
00000100	00	13	OD	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.wk.n.
00000130	65	00	77	00	20	00	62	00	72	00	65	00	64	00	20	00	e.wb.r.e.d
00000140	68	00	61	00	6D	00	20	00	62	00	75	00	73	00	79	00	h.a.mb.u.s.y.
00000150	20	00	68	00	69	00	73	00	20	00	68	00	61	00	75	00	.n.1.sn.o.u.
00000160	72	00	28	00	20	00	41	00	73	00	68	00	20	00	61	00	rA.s.ka.
00000170	67	00	72	00	65	00	65	00	64	00	20	00	61	00	6E	00	g.r.e.e.da.n.
00000180	13	00	65	00	00	00	20	00	20	00	12	00	20	00	20	00	s.w.e.rr.a.t.
00000130	60	00	63	00	74	00	20	00	72	00	65	00	20	00	20	00	n.e.rj.o.y
000001R0	64	00	601	00	60	00	72	00	65	00	20	00	20	00	60	00	dmire wi
00000120	73	00	64	00	65	00	60	00	25	00	20	00	40	00	65	00	adom Mo
00000100	6F	00	6F	00	60	00	69	00	67	00	68	00	74	00	20	00	o.p.l.i.g.b.t.
000001E0	61	00	67	00	65	00	20	00	64	00	65	00	70	00	65	00	age dene
000001E0	6E	00	64	00	69	00	6F	00	67	00	20	00	62	00	65	00	nding. he
00000200	64	00	20	00	60	00	65	00	64	00	20	00	74	00	68	00	d. l.e.dt.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	sp.r.e.s.e.r.
00000240	76	00	65	00	64	00	20	00	65	00	78	00	71	00	75	00	v.e.de.x.g.u.
00000250	69	00	73	00	69	00	74	00	65	00	20	00	73	00	68	00	i.s.i.t.es.h.
00000260	65	00	2E	00	20	00	41	00	6E	00	20	00	66	00	61	00	eA.nf.a.

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

imx.tup 📓		Higher Person of the Company Strategy Co	Churs and Estant Event December Chursel Onione 100.11
		1 97 01 08	Cear(wd)(watched)(her(oncos)(hared)(high 100.01)
OCCARC(II)	00 01 02 03 04 05 04 07 08 09 0A 08 0C 00 0E 0F	2 48 00 00 00	
00000000	9F 01 08 48 00 00 00 2C 00 00 03 07 00 01 00 Y	3 37 00 00 00	Decode
00000030	00 00 65 00 13 07 00 01 00 00 00 6C 00 13 07 00e1	3 20 00 00 00	head .
00000020	01 00 00 00 41 00 13 07 00 01 00 00 00 49 00 13	4	
00000030	07 00 01 00 00 00 79 00 13 07 00 01 00 00 00 46yF	5 13 07 00 01 00 00 00 65 00	2020年0年0月0月0月0日に22日年の月の22日時の7月0日の10月0日
00000040	00 13 07 00 01 00 00 00 72 00 13 07 00 01 00 00	6 13 07 00 01 00 00 00 6C 00	
00000050	00 4F 00 13 07 00 01 00 00 00 54 00 13 07 00 01 .cT	7 13 07 00 01 00 00 00 41 00	64 00 6F 00 77 00 20 00 70 00 75 00 9C 00 9C 00 65 00 64 00 20 00 61 00 68 00 79 00 26 00 20 00 4F
00000060	00 00 00 74 00 13 07 00 01 00 00 00 64 00 13 07td	13 07 00 01 00 00 69 00	64 00 4C 00 6F 00 72 00 64 00 20 00 74 00 6F 00 20 00 73 00 70 00 65 00 61 00 68 00 65 00 6F
00000070	00 01 00 00 00 43 00 13 07 00 01 00 00 00 41 00e		○ 時間 14 回 75回 72回時間 25回4 回時間 73回1 回移 四月回 73回 73回5 回去。
00000080	13 07 00 01 00 00 00 4£ 00 13 07 00 01 00 00 00	9 13 07 00 01 00 00 79 00	
00000090	44 00 13 07 00 01 00 00 07 00 13 07 00 01 00 D	10 13 07 00 01 00 00 00 46 00	69 00 73 00 20 00 72 00 6F 00 75 00 6E 00 64 00 20 00 74 00 6F 00 20 00 68 00 6E 00 20 00 48 00 74
000000A0	00 00 4C 00 13 07 00 01 00 00 00 52 00 13 0D 00LR	11 13 07 00 01 00 00 072 00	6E 00 20 00 61 00 64 00 64 00 72 00 65 00 73 00 20 00 67 00 72 00 65 00 73 00 75 00 72 00 65 00 61 00 74 00 6C 00 79
00000080	04 00 00 00 4C 00 4D 00 4F 00 4E 00 13 07 00 01L.N.O.B	12 13 07 00 01 00 00 00 6F 00	· · · · · · · · · · · · · · · · · · ·
000000000	00 00 00 55 00 13 07 00 01 00 00 03 00 13 070G	13 13 07 00 01 00 00 54 00	4E 00 73 00 20 00 73 00 77 00 EF 00 70 00 73 00 E5 00 77 00 74 00 79 00 20 00 74 00 E8 00 73 00 73
00000000	00 01 00 00 00 45 00 13 11 00 06 00 00 00 4A 00Rd.	14 13 07 00 01 00 00 74 00	20 00 74 00 6F 00 6C 00 65 00 72 00 61 00 62 00 6C 00 79 00 20 00 6D 00 79 00 20 00 62 00 68 00 68
00000020	4A 00 43 00 43 00 42 00 42 00 13 15 00 05 00 00 0.c.c.8.8		(b) 00 (iii) 00 (i7 00 2i) 00 2i0 00 (iii) 00 (iii) 00 74 00 (iii) 00 (iii) 00 20 10 (iii) 00 20 10 (iii) 00 74 00 20
000000000	00 40 00 45 00 72 00 46 00 45 00 40 00 33 00 32	15 13 07 00 01 00 00 00 64 00	
00000100	00 13 0D 00 04 00 00 00 08 00 00 00 00 00 00 00 00 00	16 13 07 00 01 00 00 00 63 00	00 49 00 42 00 44 00 49 00 77 00 20 00 70 00 75 00 45 00 46
00000110		17 13 07 00 01 00 00 00 61 00	00 61 00 68 00 64 00 60 00 67 00 72 00 64 00 20 00 74 00 67 00 20 00 73 00 68 00 61 00 68 00
00000120	20 00 64 00 72 00 61 00 77 00 20 00 68 00 68 00 10.1.8.W. 18.H.	18 13 07 00 01 00 00 68 00	75 00 72 00 61 00 69 00 74 00 75 00 72 00 65 00 20 00 64 00 69 00 73 00 63 00 67 00 75 00 72 00 73
00000140	48 00 41 00 40 00 10 00 42 00 12 00 80 00 80 00 20 00 8.4	19 13 07 00 01 00 00 00 44 00	D 5 2 5 5 7 2 5 7 2 5 6 2 7 2 5 6 2 7 2 5 6 2 7 2 5 7 2 7 2
00000180	20 00 48 00 49 00 75 00 20 00 48 00 4F 00 75 00	20 13 07 00 01 00 00 77 00	004500200490073002007200#00750042004002007400#00200690420
00000140	72 00 2E 00 20 00 41 00 73 00 48 00 20 00 41 00 E		74 00 65 00 68 00 20 00 61 00 64 00 64 00 72 00 65 00 73 00 73 00 20 00 67 00 72 00 65 00 61 00 74
00000170	#7 00 72 00 #5 00 #5 00 #4 00 20 00 #1 00 #E 00 m.v.e.e.de.e.		00 75 00 69 00 74 00 20 00 67 00 72 00 20 00 62 00 75 00 74 00 20 00 62 00 73 00 74 00 20 00 4C 00 61 00 73 00
00000180	75 00 77 00 45 00 72 00 20 00 72 00 41 00 74 00 8.9.8.7	22 13 07 00 01 00 00 52 00	Key stor Key do Key do 22 do Key do Tel do Tel do 72 do Key do Key do Key do Key do Key do Key do Tel do Key do
00000190	48 00 45 00 72 00 20 00 45 00 4F 00 79 00 20 00 h.e.F1.0.V.	23 13 0D 00 04 00 00 00 4C 00 4D 00 6F 00 6E 00	
00000120	6E 00 61 00 74 00 75 00 72 00 65 00 20 00 61 00 n.a.t.u.r.ea.	24 13 07 00 01 00 00 05 00	Output
00000130	64 00 6D 00 69 00 72 00 65 00 20 00 77 00 69 00 d.m.1.r.ew.1.	25 13 07 00 01 00 00 00 43 00	Header Bytes: 0x9F0108
00000100	73 00 64 00 67 00 6D 00 2E 00 20 00 4D 00 67 00 s.d.e.mN.e.	26 13 07 00 01 00 00 00 48 00	
00000120	4F 00 4E 00 4C 00 69 00 47 00 48 00 74 00 20 00 o.m.l.i.g.h.t	27 13 11 00 06 00 00 43 00 43 00 43 00 43 00 43 00 42 00 4	count = 72
00000120	61 00 67 00 65 00 20 00 64 00 65 00 70 00 65 00 a.g.ed.e.p.e.		uniqueCount = 44
000001F0	4E 00 64 00 69 00 6E 00 67 00 20 00 62 00 65 00 n.d.i.n.gb.e.		
00000200	44 00 20 00 4C 00 45 00 44 00 20 00 74 00 48 00 dl.e.dt.h.	29 13 0D 00 04 00 00 00 66 00 6C 00 61 00 74 00	
00000210	45 00 72 00 65 00 66 00 6F 00 72 00 65 00 20 00 e.r.e.f.o.r.e	1.0	Extracted Strings:
00000220	73 00 4F 00 4D 00 45 00 74 00 49 00 4D 00 45 00 s.o.m.e.t.i.m.e.	Normal text file length : 204,128 lines: 48 Ln : 12 Col : 28 Sel : 0 0	index 0 e
00000230	73 00 20 00 70 00 72 00 65 00 73 00 65 00 72 00 sp.z.e.s.e.z.		Index 1
00000240	76 00 65 00 64 00 20 00 65 00 78 00 71 00 75 00 v.e.se.x.q.u.		Index 2 A
00000250	49 00 73 00 49 00 74 00 45 00 20 00 73 00 48 00 i.s.i.t.es.h.		Pidex 3 i
00000260	65 00 2E 00 20 00 41 00 4E 00 20 00 66 00 41 00 e A.sf.a.		Index 4 y
00000270	49 00 60 00 20 00 75 00 70 00 20 00 73 00 68 00 1.1. u.ps.c.		index o P
00000280	20 00 73 00 68 00 67 00 74 00 20 00 60 00 65 00 .#.h.o.tl.e.		Index 0 r
00000290	61 00 66 00 20 00 77 00 69 00 73 00 65 00 20 00 A.EW.L.B.C		Index / O
00000280	es co es co ze co zo co es co es co es co 1.n.,		Index 0 1
00000280	74 00 68 00 72 00 20 00 68 00 69 00 67 00 68 00 5.4.FB.1.g.B.		index 10 d
000000000	40 00 10 00 10 00 40 00 00 00 00 00 73 00 20 00 8.8.5		index 11 c
00000200	44 00 4F 05 72 05 20 05 70 05 75 05 74 05 20 05 F.o. =		Index 12 a
00000280	41 00 4E 00 64 00 2E 00 20 00 48 00 4F 00 70 00 a.m.d		Index 13 n
00000300	45 00 73 00 20 00 60 00 69 00 76 00 65 00 64 00 8.81.1.9.8.4.		Index 14 D
00000310	20 00 62 00 79 00 20 00 72 00 6F 00 6F 00 6D 00 .B.V. F.O.O.B.		Index 15 w
00000320	73 00 20 00 4F 00 48 00 20 00 49 00 4E 00 20 00 so.hi.m		Index 16 L
00000330	4E 00 4F 00 20 00 64 00 65 00 61 00 74 00 68 00 m.od.e.a.t.h.		
00000340	20 00 68 00 6F 00 75 00 73 00 65 00 2E 00 20 00 .h.e.u.s.e		
00000350	43 00 4F 00 4E 00 74 00 45 00 4E 00 74 00 45 00 C.o.n.t.e.n.t.e.		



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.

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 6 13 DB 08 00 2B 02 00 00 57 00 6F 00 72 00 6B 00 69 00 6E 00 66 00 65 7 13 DB 07 00 EB 01 00 00 57 00 69 00 74 00 68 00 6F 00 75 00 74 8 13 A7 0B 00 D1 02 00 00 61 00 6E 00 64 00 20 00 68 00 61 00 64 9 13 D9 09 00 6A 02 00 00 61 00 61 00 76 00 65 00 20 00 69 00 74 10 13 FD 08 00 3C 02 00 00 61 00 73 00 68 00 61 00 65 00 20 00 69 00 74 10 13 FD 08 00 3C 02 00 00 70 00 72 00 6F 00 6A 00 65 00 63 00 74 11 13 B3 0A 00 97 02 00 00 70 00 72 00 6F 00 6A 00 65 00 63 00 74 13 E9 09 00 72 02 00 00 74 00 68 00 65 00 20 00 65 00 63 00 74 13 B3 0A 00 97 02 00 00 77 00 61 00 73 00 20 00 62 00 65 00 67 13 B3 0A 00 97 02 00 00 77 00 61 00 73 00 20 00 62 00 72 00 65 14 13 8B 10 00 03 04 00 00 61 00 6E 00 64 00 20 00 77 00 65 00 20 14 13 BF 0A 00 9D 02 00 00 54 00 68 00 65 00 62 00 77 00 65 00 20	0 6 0 2 0 2 0 2 0 2 0 2 0 2 0 2 0 6 0 6
2 22 00 00 00 3 22 00 00 00 4 5 13 C5 0C 00 20 03 00 00 65 00 65 00 72 00 65 6 13 DB 08 00 2B 02 00 00 57 00 6F 00 68 00 69 00 6E 00 68 00 6E 00 67 7 13 DB 07 00 EB 01 00 00 57 00 69 00 74 00 68 00 6E 00 64 13 DF 07 00 EB 01 00 00 67 00 64 00 20 00 68 00 61 00 64 00 20 00 69 00 74 10 13 FD 08 00 3C 02 00 06 <t< td=""><td>0 6 0 2 0 2 0 2 0 2 0 2 0 2 0 2 0 2 0 6 0 6</td></t<>	0 6 0 2 0 2 0 2 0 2 0 2 0 2 0 2 0 2 0 6 0 6
3 22 00 00 00 4 5 13 C5 0C 00 20 03 00 06 6F 00 6E 00 65 00 72 00 65 6 13 DB 08 00 2B 02 00 057 00 6F 00 72 00 6B 00 69 00 6E 00 6F 00 74 00 68 00 6F 00 74 00 68 00 6F 00 74 00 68 00 6F 00 74 13 DB 07 00 EB 01 00 00 57 00 6F 00 74 00 68 00 6F 00 74 13 DF 07 00 6A 02 00 06 67 00 61 00 74 00 68 00 61 00 65 00 20 00 74 <	0 6 0 2 0 2 0 2 0 2 0 2 0 2 0 2 0 6
4 5 13 C5 0C 00 20 03 00 06 6F 00 6E 00 66 00 65 00 72 00 65 6 13 DB 08 00 2B 02 00 00 57 00 6F 00 72 00 6B 00 69 00 6E 00 67 7 13 DB 07 00 EB 01 00 00 57 00 69 00 74 00 68 00 6F 00 74 8 13 A7 0B 00 D1 02 00 00 61 00 64 00 20 00 68 00 61 00 64 00 20 00 68 00 61 00 74 00 68 00 61 00 74 10 13 FD 08 00 3C 02 00 61 00 73	0 6 0 2 0 2 0 2 0 2 0 2 0 2 0 6
5 13 C5 0C 00 20 03 00 06 6F 00 6E 00 65 00 72 00 65 13 DB 08 00 2B 02 00 00 57 00 6F 00 72 00 6B 00 69 00 6E 00 67 7 13 DB 07 00 EB 01 00 00 57 00 69 00 74 00 68 00 6F 00 74 8 13 A7 0B 00 D1 02 00 00 61 00 64 00 20 00 68 00 61 00 64 00 20 00 69 00 74 10 13 FD 08 00 3C 02 00 06 70 61 00 76 00 6A 00 65 00 63 00 74 10 13 <t< td=""><td>0 6 0 2 0 2 0 2 0 2 0 2 0 2 0 2 0 2 0 6 0 6</td></t<>	0 6 0 2 0 2 0 2 0 2 0 2 0 2 0 2 0 2 0 6 0 6
6 13 DB 08 00 2B 02 00 00 57 00 6F 00 72 00 6B 00 69 00 6E 00 67 13 DB 07 00 EB 01 00 00 57 00 69 00 74 00 68 00 6F 00 74 13 DB 07 00 EB 01 00 00 57 00 69 00 74 00 68 00 6F 00 74 13 DP 09 00 6A 02 00 06 6E 00 64 00 20 00 69 00 74 10 13 FD 08 00 3C 02 00 06 61 00 76 00 6A 00 66 00 61 00 66 00 6A 00 65 00 64 00 66 00 65 00	0 2 0 2 0 2 0 2 0 2 0 2 0 2 0 6 0 6
7 13 DB 07 00 EB 01 00 00 57 00 69 00 74 00 68 00 6F 00 75 00 74 8 13 A7 0B 00 D1 02 00 00 61 00 64 00 20 00 68 00 61 00 64 00 20 00 68 00 61 00 64 00 20 00 68 00 61 00 64 00 20 00 68 00 61 00 64 00 20 00 69 00 74 10 13 FD 08 00 3C 02 00 61 00 73 00 68 00 61 00 65 00 63 00 74 10 13 FD 08 00 97 02 00 00 70 00 72 00 64 00 65 <t< td=""><td>0 2 0 2 0 2 0 2 0 2 0 2 0 6 0 6</td></t<>	0 2 0 2 0 2 0 2 0 2 0 2 0 6 0 6
8 13 A7 0B 00 D1 02 00 61 00 64 00 20 00 68 00 61 00 64 00 20 00 68 00 61 00 64 9 13 D9 09 00 6A 02 00 06 67 00 61 00 76 00 65 00 20 00 69 00 74 10 13 FD 08 00 3C 02 00 00 61 00 73 00 68 00 61 00 65 00 65 00 64 11 13 B3 0A 00 97 02 00 00 72 00 6F 00 6A 00 65 00 63 00 74 12 13 E9 09 00 72 02 00 077 00 61 00 73 00 20 00 65	0 2 0 2 0 2 0 2 0 6 0 6
9 13 D9 09 00 6A 02 00 67 00 61 00 76 00 65 00 20 00 69 00 74 10 13 FD 08 00 3C 02 00 00 61 00 73 00 68 00 61 00 6D 00 65 00 64 11 13 B3 0A 00 97 02 00 00 72 00 6F 00 6A 00 65 00 63 00 74 12 13 E9 09 00 72 00 61 00 73 00 6A 00 65 00 67 13 A9 0A 00 92 02 00 00 54 00 68 00 65 00 62 00 72 00 65 00 65 00 65 00 65 00 65 00 65	0 2 0 2 0 2 0 6 0 6
10 13 FD 08 00 3C 02 00 00 61 00 63 00 61 00 6D 00 65 00 64 11 13 B3 0A 00 97 02 00 00 72 00 6F 00 6A 00 65 00 63 00 74 12 13 E9 09 00 72 02 00 07 70 61 00 73 00 6A 00 65 00 63 00 74 12 13 E9 09 00 72 02 00 07 70 61 00 73 00 20 00 65 00 67 13 A9 0A 00 92 02 00 05 54 00 68 00 65 00 62 00 72 00 65 00 20 00 77 00 65 00 20 00	02 02 06 06
11 13 B3 0A 00 97 02 00 00 70 00 72 00 6F 00 6A 00 65 00 63 00 74 12 13 E9 09 00 72 02 00 07 00 61 00 73 00 20 00 65 00 67 13 A9 0A 00 92 02 00 00 54 00 68 00 65 00 62 00 72 00 65 14 13 8B 10 00 03 04 00 05 64 00 20 00 65 00 20 10 65 00 20 10 65 00 20 10 77 00 65 00 20 00 77 00 65 00 20 00 77 00 65 00 20 00 77 00 65 00 20 00	02 06 06
12 13 E9 09 00 72 02 00 00 77 00 61 00 73 00 20 00 62 00 65 00 67 13 13 A9 0A 00 92 02 00 05 400 68 00 65 00 20 00 62 00 72 00 65 14 13 8B 10 00 03 04 00 06 61 00 64 00 20 00 77 00 65 00 20 00 77 00 65 00 20 00 72 00 65 00 20 00 77 00 65 00 20 00 77 00 65 00 20 00 77 00 65 00 20 00 77 00 65 00 20 00 77 00 65 00 20 00 77 00 65 00	06 06
13 13 A9 0A 00 92 02 00 054 00 68 00 65 00 20 00 62 00 72 00 65 14 13 8B 10 00 03 04 00 06 61 00 64 00 20 00 77 00 65 00 20 15 13 BF 0A 00 9D 02 00 54 00 68 00 65 00 62 00 72 00 65 00 20 00 77 00 65 00 20 00 77 00 65 00 20 00 77 00 65 00 20 00 63 00 61 15 13 BF 0A 00 9D 02 00 54 00 68 00 65 00 62 00 63 00 61 16 13 BF 0A 00	0 6
14 13 8B 10 00 03 04 00 00 61 00 62 00 67 00 65 00 20 15 13 BF 0A 00 9D 02 00 54 00 68 00 65 00 63 00 61 16 13 BF 0A 00 9D 02 00 54 00 68 00 65 00 20 00 63 00 61 16 13 BF 0A 00 9D 02 00 54 00 68 00 65 00 20 00 63 00 61	-
15 13 BF 0A 00 9D 02 00 00 54 00 68 00 65 00 6E 00 20 00 63 00 61	0 7
	0 6
16 13 A7 09 00 51 02 00 00 35 00 4E 00 6F 00 2C 00 20 00 77 00 61	0 6
17 13 B9 0C 00 1A 03 00 00 6C 00 61 00 72 00 67 00 65 00 20 00 68	0 6
18 13 BB 0A 00 9B 02 00 00 61 00 72 00 65 00 20 00 74 00 6F 00 6F	0 2
19 13 97 0A 00 89 02 00 00 73 00 74 00 61 00 79 00 20 00 20 00 61	0 6
	0 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	0 6
25 15 ES 07 00 EF 01 00 00 6F 00 6E 00 6S 00 20 00 67 00 6C	
24 13 B5 05 00 5A 02 00 00 6D 00 79 00 20 00 65 00 68 00 69 00 6C	0 0 7
25 13 B5 0A 00 9A 02 00 00 55 00 41 00 66 00 2C 00 20 00 6C 00 65	0 7
27 13 PD 08 00 1C 02 00 00 73 00 61 00 69 00 64 00 2C 00 20 00 63	0 7
28 13 99 08 00 03 02 00 00 65 00 65 00 65 00 20 00 68 00 69	o é
29 13 F3 08 00 37 02 00 00 67 00 72 00 75 00 66 00 66 00 6C 00 79	
30 13 8F 08 00 05 02 00 00 35 00 4F 00 6F 00 20 00 6F 00 70 00 70	6
31 13 E7 09 00 71 02 00 00 61 00 76 00 6E 00 69 00 64 00 69 00 6E	6
32 13 FF 08 00 3D 02 00 00 41 00 74 00 20 00 74 00 68 00 61 00 74	0 2
33 13 91 08 00 06 02 00 00 35 00 49 00 20 00 68 00 61 00 64 00 20	0 6
34 13 9D 09 00 4C 02 00 00 63 00 6F 00 6E 00 64 00 65 00 73 00 63	0 6
35 13 CF 09 00 65 02 00 00 73 00 61 00 69 00 6E 00 74 00 20 00 6E	0 6
36 13 93 09 00 47 02 00 00 68 00 65 00 72 00 73 00 65 00 6C 00 66	0 2
37 13 E9 09 00 72 02 00 00 52 00 75 00 73 00 73 00 69 00 61 00 6E	0 7
38 13 ED 08 00 34 02 00 00 77 00 69 00 74 00 68 00 6F 00 75 00 74	0 2
39 13 AD 08 00 14 02 00 00 73 00 75 00 72 00 65 00 20 00 6E 00 6F	0 6

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

🔚 Shan	idSir Bytes Int 🔝 🔚 Betracted Shared Strings-Correct Int 🖸 🔚 Shared Sir Bytes Correct Format Int 🔝													
16	16 Index :13 are too impulsive, too vehement; the sovereign hand that createdyour frame, and put													
	life into it, has provided you with otherresources than your feeble self, or than creatures feeble													
as you.Besides this earth, and besides Catulator														
	spirits: that world is round us, for i he would be are													
	commissioned toguard us; and if we were tak View Hep													
	hatred crushed us, angels see our torte 213 as I know													
	you are of this chargewhich Mr. Brockle Bler One Oct Bn @ Qword Oword Word Bte Bhand													
17	Index :14 stay, and I stayed, 5 he say do this?5 he													
	said after a moment5s silence, bending hw hp Backspace CE C he would lay													
	hers in it.She was glad of this appeal and the second seco													
	her give herself up to her feelings, al Sa FE () MC 7 8 9 / Mod And to													
	surrender.50f course you wanted to stat													
	you tell me that for? With what object Are dra bo n MH 4 5 6 2 Kor snyone	al												
	contest your rights?But you want to be Sm m with in MS 1 2 3 Leb Net	ar.												
18	Index :15 5Well, if that isn5t the g	11												
	didn5t you pop out and tell them so on s cos x3 ni M. 0	41												
	couldn5t helphearing at first, and the													
	to go away.55Just wait till I see Annie De ten x2 in p A B C D t F Iculous													
	stuff. The idea of having `plans5 and try us													
	by-and-by! Won5the shout when I tell him what those silly things say about us poor													
19	Index :16 to be blamed for the base stratagem of tonight. I planned it, andshe only gave in													
	after lots of teasing.SSCome now, donst lay it all on yourself. You know I proposed the cupboard, 5													
	broke in Shodgrass, who was enjoying the joke amazingly. Snever mind what she says. Ibm the wretch													
	that did it, sir, ssaid the new member, with a welleresque hod to Mr. Pickwick. SButon my honor, i													
	never will do so again, and nencesorin devote myselito the interest of this immortal club.Schear:													
20	Rearis cried Jo, clashing the 11d of the warming pan													
20	index :1/ once glancing at Levin, who had never taken his eyes orr him.slet me introduce you, s													
	said the Frincess, indicating Levin Sconstantin Emittevich Levin, count Alexel Kirillovich													
1	A substitutionary doe of anot rowards constants as feature show using a result and the state of a second state of the second s	1												
Normal	text file length: 21,387 lines: 38 Ln: 19 Col: 544 Sel: 531 1 Windows (CR LF) UTF-8 INS													
reormal	text tree tength: 22,587 tines: 58 Lh:19 Col:544 Sel:531 1 Windows (CKD) UTI-8 INS													

If we look at the string under index 16 we see it is 531 characters long.

531 = 0x0213 and our value in the data is 0x1302.

						10100	See See		or one to	9.64	-			-		~ ~													_
1	9F	01	08																										
2	22	00	00	00																									I
3	22	00	00	00																									I
4																													I
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
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
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
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
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
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
11	13	B 3	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
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
13	13	29	0 A	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
14	13	88	10	00	03	04	00	00	61	00	65	00	64	00	20	00	77	00	65	00	20	00	73	00	68	00	61	00	60
15	13	BF	02	00	90	02	00	00	54	00	68	00	65	00	6F	00	20	00	63	00	61	00	6D	00	65	00	20	00	74
16	13	37	09	00	51	02	00	00	35	00	45	00	65	00	20	00	20	00	77	00	61	00	69	00	74	00	20	00	61
17	13	BQ	00	00	12	03	00	00	60	00	61	00	72	00	67	00	65	00	20	00	68	00	61	00	75	00	65	00	60
1.9	13	22	02	00	95	02	00	00	61	00	72	00	65	00	20	00	74	00	65	00	65	00	20	00	69	00	60	00	20
10	12	92	02	00	20	02	00	00	72	00	74	00	61	00	20	00	20	00	20	00	61	00	60	00	64	00	20	00	10
20	12	02	00	00	25	02	00	00	25	00	67	00	65	00	60	00	60	00	20	00	20	00	60	00	66	00	20	00	74
21	12	20	00	00	12	02	00	00	74	00	60	00	20	00	62	00	65	00	20	00	62	00	60	00	61	00	60	00	6
22	12	AD F2	00	00	10	02	00	00	62	00	62	00	62	00	62	00	20	00	67	00	60	00	60	00	601	00	62	00	60
22	13	20	00	00	5.3	01	00	00	6D	00	70	00	20	00	63	00	20	00	60	00	60	00	64	00	72	00	65	00	69
23	13	89	09	00	SA	02	00	00	25	00	19	00	20	00	03	00	00	00	69	00	60	00	24	00	12	00	65	00	OE CC
24	13	89	0A	00	9A	02	00	00	35	00	41	00	68	00	20	00	20	00	60	00	05	00	74	00	20	00	60	00	00
25	13	81	09	00	3E	02	00	00	51	00	64	00	61	00	19	00	20	00		00	OF CR	00	72	00	60	00	54	00	20
26	13	BD	08	00	10	02	00	00	13	00	61	00	69	00	69	00	20	00	20	00	6A	00	15	00	/3	00	/ 9	00	20
27	13	99	08	00	0A	02	00	00	68	00	65	00	65	00	70	00	20	00	68	00	69	00	6D	00	ZE	00	35	00	5/
28	13	F3	08	00	37	02	00	00	67	00	12	00	75	00	66	00	66	00	6C	00	79	00	20	00	62	00	65	00	63
29	13	SF.	08	00	05	02	00	00	35	00	45	00	61	00	20	00	6F	00	70	00	70	00	6F	00	12	00	/4	00	/5
30	13	E/	09	00	/1	02	00	00	61	00	76	00	6F.	00	69	00	64	00	69	00	6E	00	67	00	20	00	6C	00	6F
31	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
32	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
33	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
34	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
35	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
36	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
37	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
38	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
																													- 1

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 out 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