Erel Regev

Table of Contents

Intro

Challenge description:

CHALLENGE DESCRIPTION

Another Phishing document. Dig in and see if you can find what it executes.

Received files:

oBfsC4t10n2.xls   oBfsC4t10n2.zip
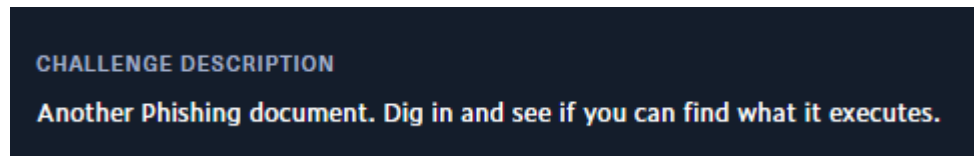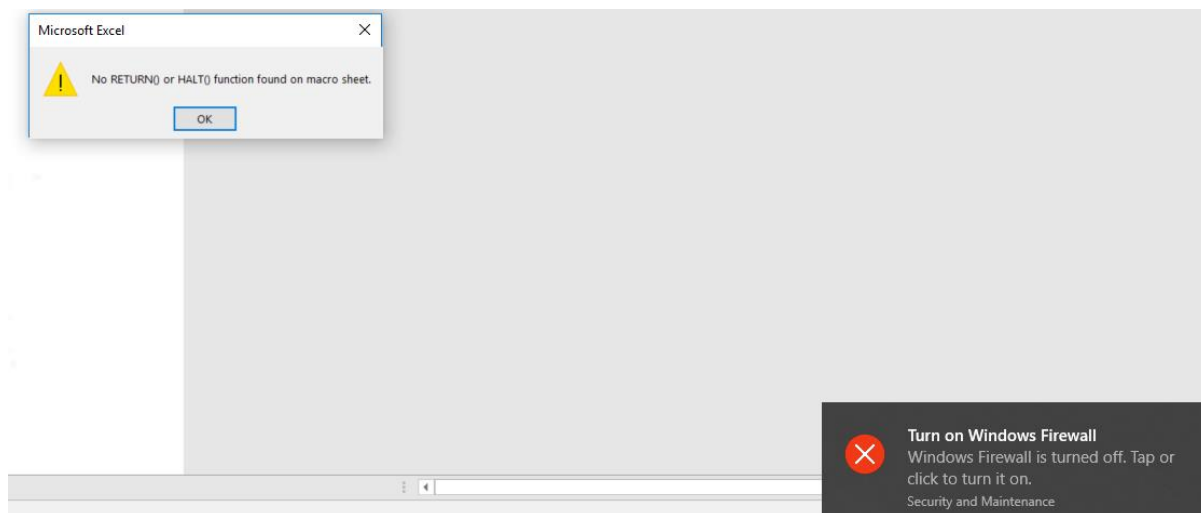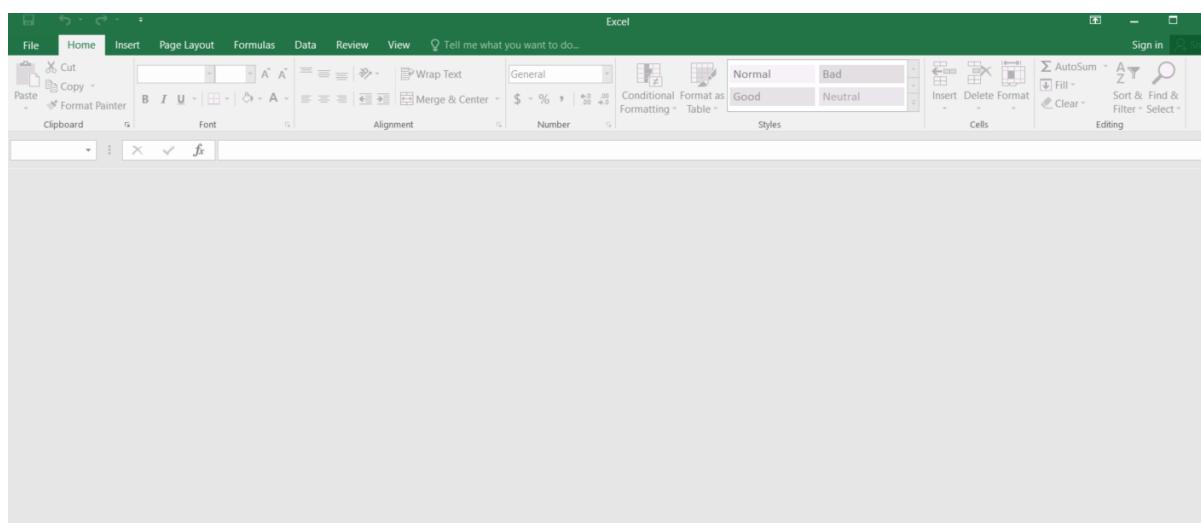
Viewing the xls file:
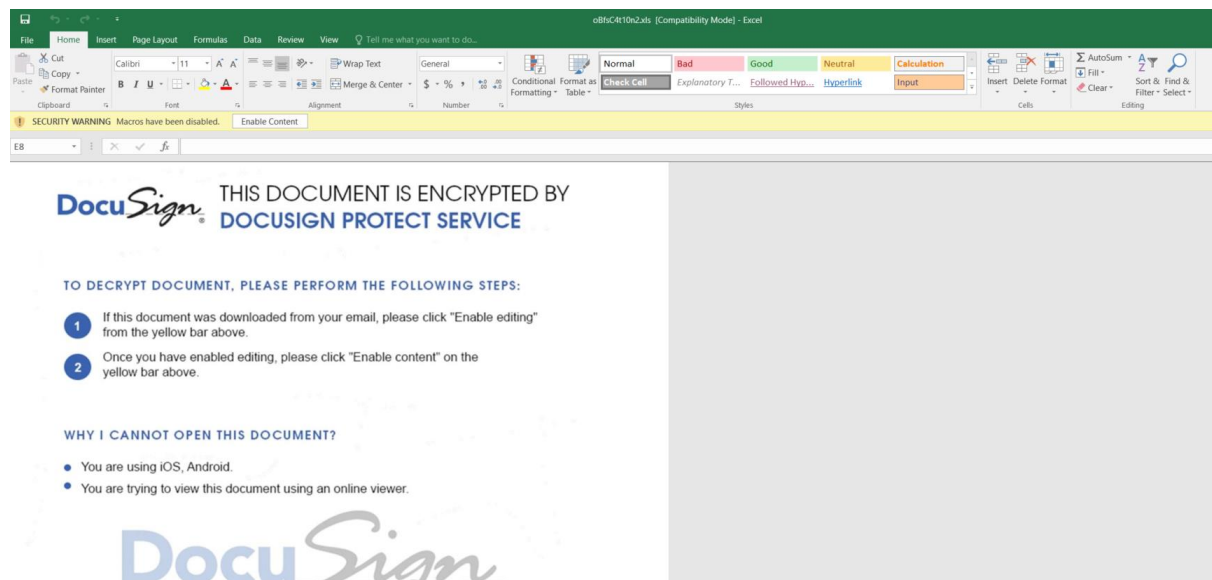
Erel Regev

Analyzing

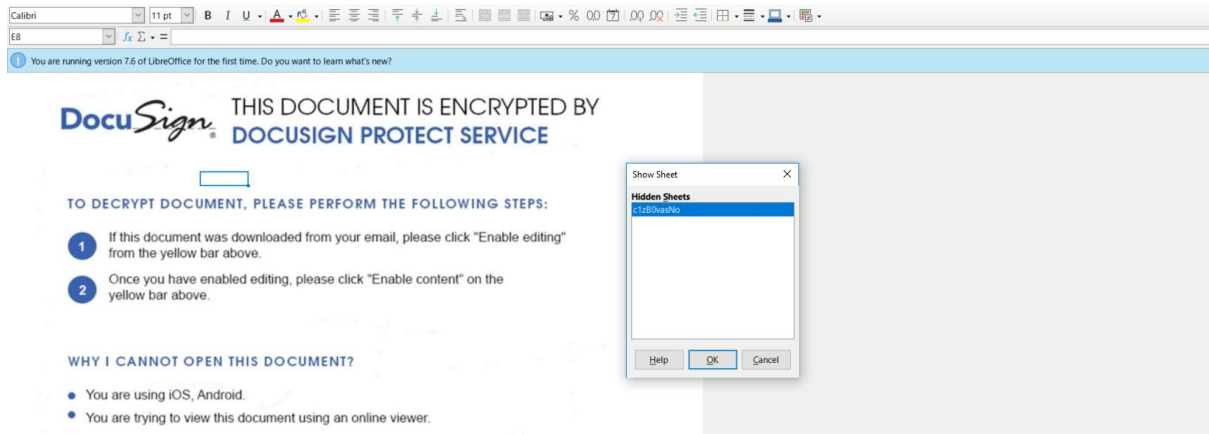I followed the steps and received:

Eventually it ended up like this:

Tried to reveal and hide sheets using libre office:

Erel Regev

There is a hidden sheet.

I got a hidden page, again. But this time I am more suspicious regarding to the fact that I revealed a hidden sheet.
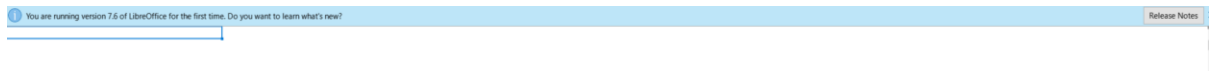
I marked all cells in order to change the font color and see if I can reveal more information,
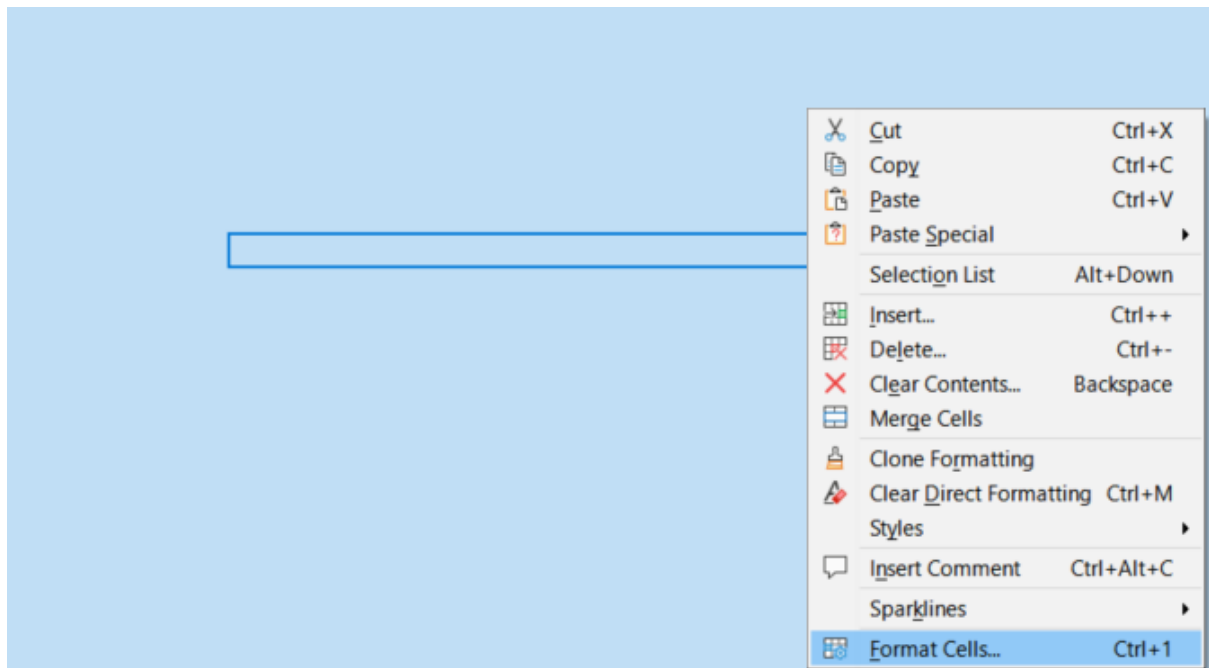
Erel Regev

I changed the color from white to black:

Interesting!

I received the following formula:

=IF(#NAME!(),CONCATENATE(E394,F1194,F549,E635,O697,U208,T458,M868,Z4,U777),CONCATENATE(F394,F1194,E549,O635,U697,D777))

Erel Regev

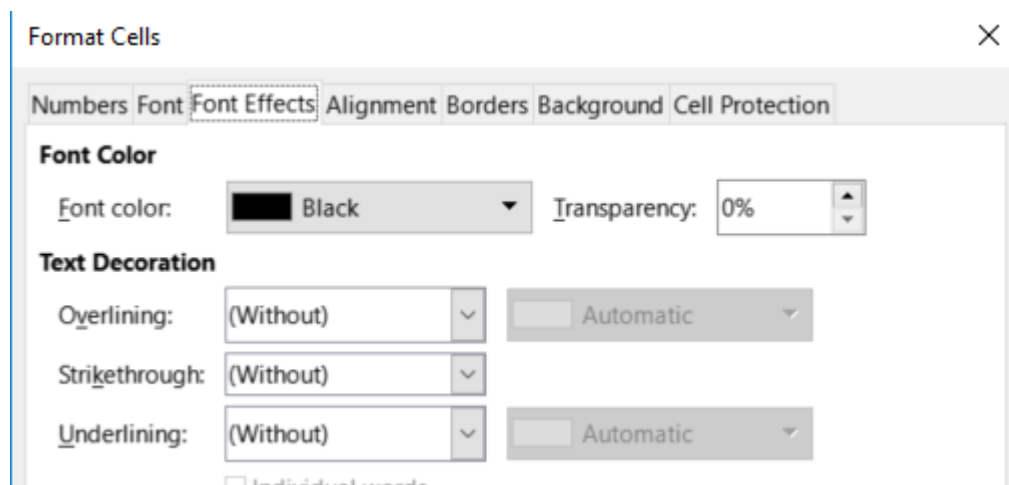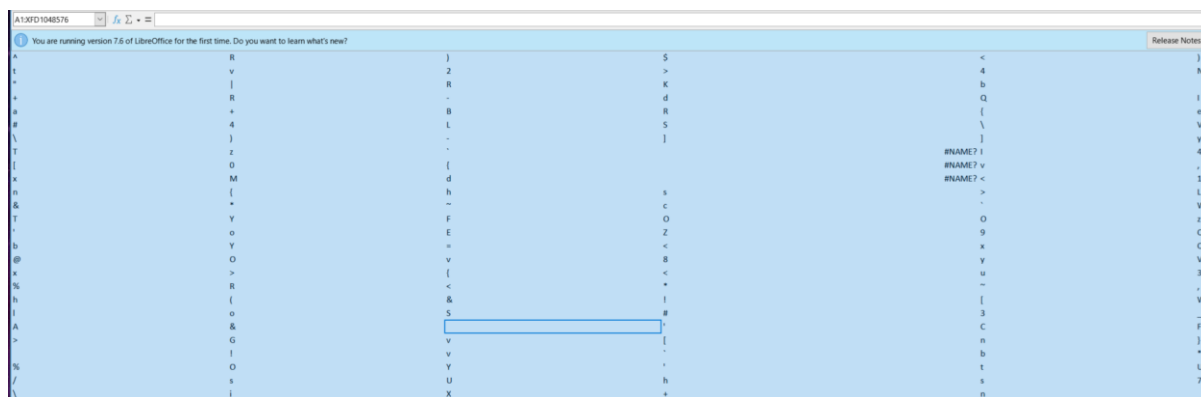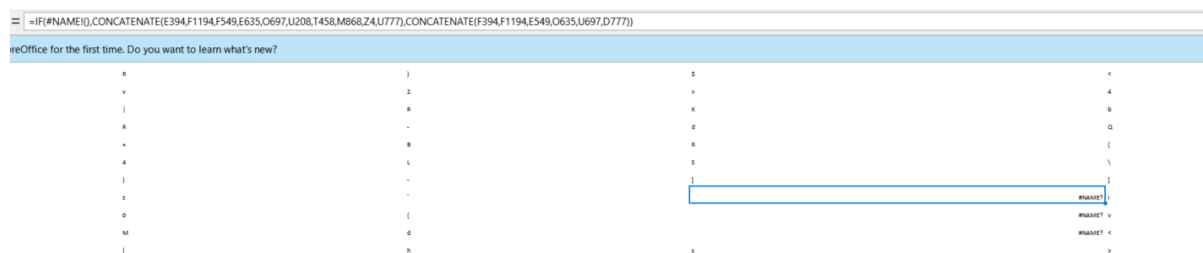CONCATENATE(…): This function is used to concatenate (join together) multiple text strings.

The letter followed by numbers (e.g., E394, F1194) are cell references. They refer to specific cells in the spreadsheet.

Based on the structure of the formula, it seems to be concatenating the contents of various cells based on whether the named range error #NAME! is present or not.

If the #NAME! error is present:

The formula concatenates the contents of cells E394, F1194, F549, E635, O697, U208, T458, M868, Z4, and U777.

If the #NAME! error is not present:

The formula concatenates the contents of cells F394, F1194, E549, O635, U697, and D777.

I started to manually go over the functions. These are part of them:

Eventually I reached an interesting function, that looks more complex than the others.

=IF(ISNUMBER(SEARCH("6.1",N546)),CONCATENATE(Z699,L932,J1190,C574,J644,A718,E813),CONCATENATE(A699,E932,K1190,J574,A644,Z718,W813))

Erel Regev
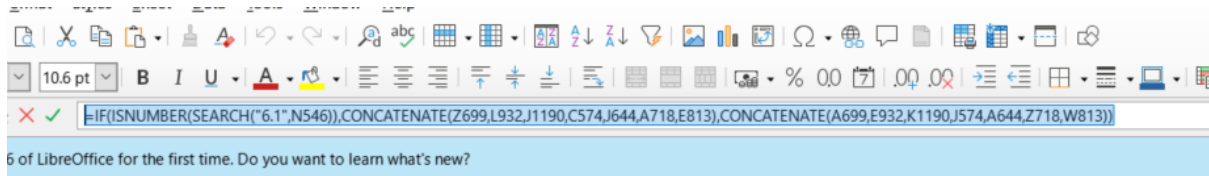
Based on the structure of the formula, it seems to be concatenating the contents of various cells based on whether the text "6.1" is found in cell N546 or not.

If "6.1" is found in cell N546 (resulting in TRUE):

The formula concatenates the contents of cells Z699, L932, J1190, C574, J644, A718, and E813.

If "6.1" is not found in cell N546 (resulting in FALSE):

The formula concatenates the contents of cells A699, E932, K1190, J574, A644, Z718, and W813.

Used the function wizard in libre office:
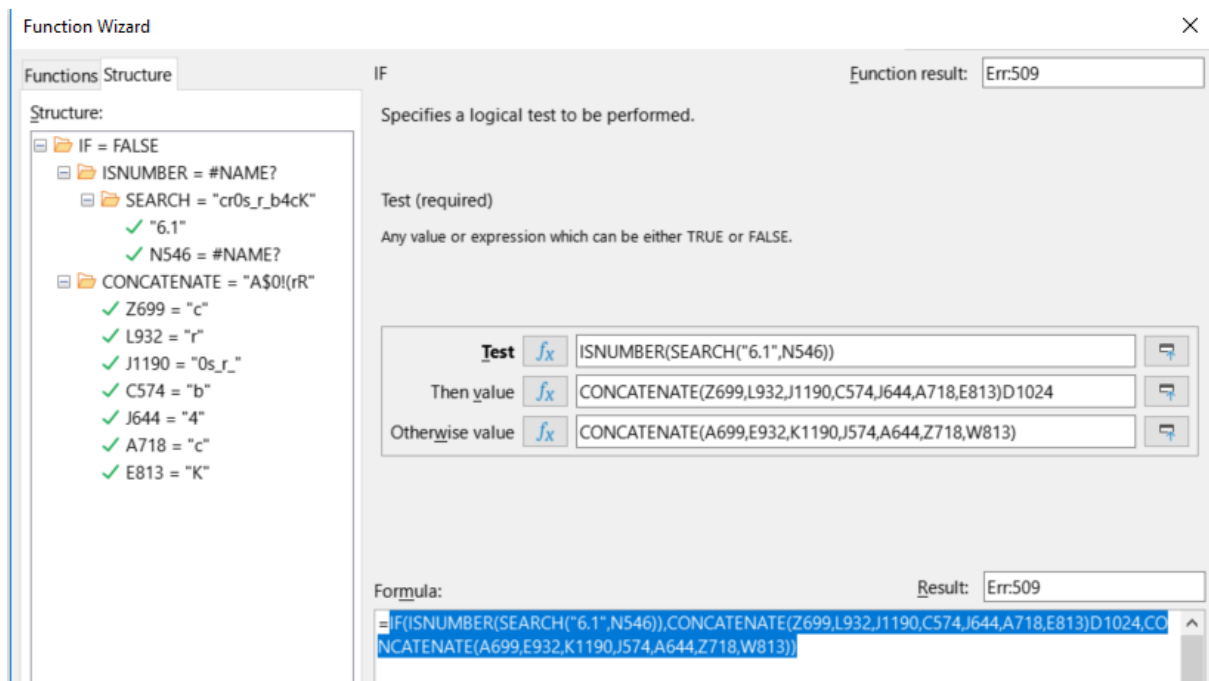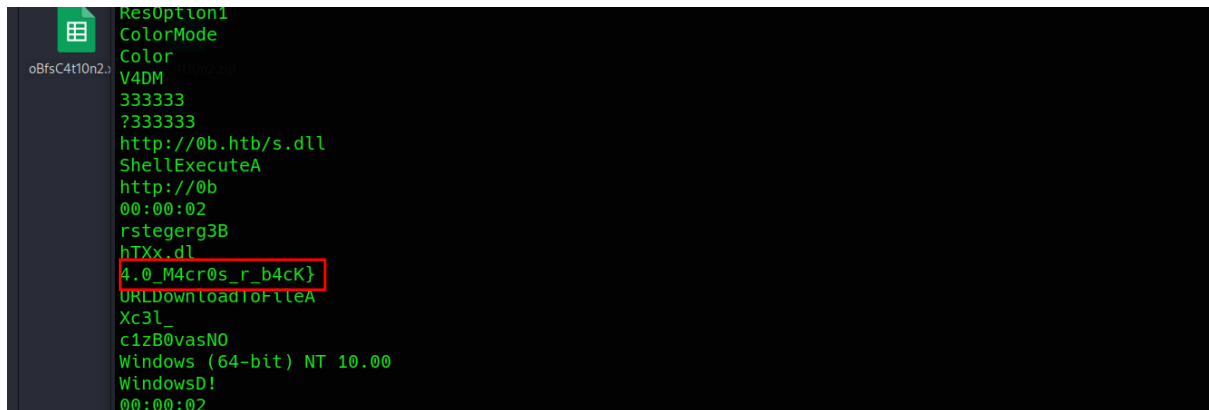
Looks like a part of the flag?

cr0s_r_b4ck

Erel Regev

Can't see anything else there at the moment. Moved on to strings:

When using strings, it seems that part of the flag is there!

It's the same thing I found earlier! Now there are more parts of the flag: 4.0_M4cr0s_r_b4ck}

But some characters are still missing.

Well, I guess I should go back to the same method I used before and try to reveal the beginning of the flag.

Back to the first function I analyzed:

=IF(#NAME!(),CONCATENATE(E394,F1194,F549,E635,O697,U208,T458,M868,Z4,U777),CONCATENATE(F394,F1194,E549,O635,U697,D777))

The formula concatenates the contents of cells F394, F1194, E549, O635, U697, and D777.

I used the navigator in order to check the value of cells that are being concatenates by the function.

Erel Regev

H

```
.              .
+              n
r              b
r              m
p              U
U              e
6              F
T              @
0              ;
F              =
%              W
^              }
[              W
u              u
x              {
4              G
<              u
?              %
s              H
]              i
```

Navigator	
Column:	F
Row:	549

- ⊞ 🏢 Sheets
- ⊞ 🔗 **Range names**
- ▢ Database ranges
- ⚑ Linked areas
- ⊟ 🖼 Images
-     Picture 3
- 📇 OLE objects
- 💬 Comments
- 🗨 Drawing objects

oBfsC4t10n2 (active)

T

```
...            .              .
Y              c              %
W              w              M
n              )              i
}              !              @
Z              d              -
o              "              J
s              q              U
M              '              Q
B              D              ^
+              ;              J
f              b              Z
[              <              r
J              +              q
n              O              U
7              x              _
e              [              Q
{              p              <
<              m              f
Z              Q              5
f              #              d
```

Navigator	
Column:	E
Row:	635

- ⊞ 🏢 Sheets
- ⊞ 🔗 **Range names**
- ▢ Database ranges
- ⚑ Linked areas
- ⊟ 🖼 Images
-     Picture 3
- 📇 OLE objects
- 💬 Comments
- 🗨 Drawing objects

oBfsC4t10n2 (active)

B

Erel Regev

s	t	(
X	C	N
P	M	\
_	]	=
A	Q	g
#	^	j
&	b	0
~	[	!
U	E	P
{	v	)
+	"	)
D	U	L
+	g	<
&	r	\
2	L	!
/	1	8
i	.	0
F	v	U
4	0	u
o	M	4
\	%	F

Navigator

Column: O   Row: 697

Sheets
Range names
Database ranges
Linked areas
Images
   Picture 3
OLE objects
Comments
Drawing objects

oBfsC4t10n2 (active)

{

P	+
s	N
)	Z
L	:
5	t
}	%
N	/
n	+
f	h
c	d
%	F
z	f
=	:
.	C
[	r
K	C
x	p
I	Z
7	7

Navigator

Column: U   Row: 208

Sheets
Range names
Database ranges
Linked areas
Images
   Picture 3
OLE objects
Comments
Drawing objects

oBfsC4t10n2 (active)

n

Erel Regev

Z	t
_	;
T	y
?	z
T	a
9	\
0	{
%	R
t	}
D	&
?	q
N	m
v	\
?	[
u	Q
7	}
?	$

Navigator

Column: T   Row: 458

Sheets
Range names
  Database ranges
  Linked areas
Images
  Picture 3
  OLE objects
  Comments
  Drawing objects

oBfsC4t10n2 (active)

u
w
t
F
Y
J
0
z
n
?
V
'
P
j
"
1
?

0
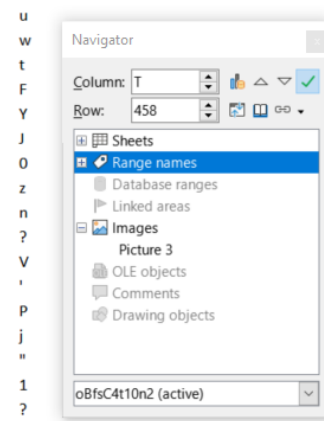
$	0
"	r
U	Y
o	o
a	?
K	A
*	g
F	*
w	b
J	+
6	4
T	*
t	T
A	I
@	^
'	'
C	y
k	/
7	U
H	Z

Navigator

Column: M   Row: 868

Sheets
Range names
  Database ranges
  Linked areas
Images
  Picture 3
  OLE objects
  Comments
  Drawing objects

oBfsC4t10n2 (active)
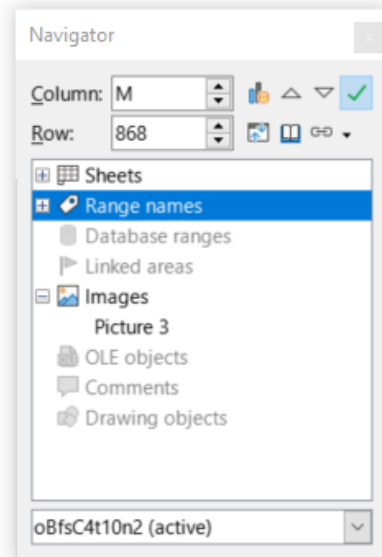
w

Erel Regev

;
F

_

w
i
/
M
{
p
,
9
K
%
E
A
M

_
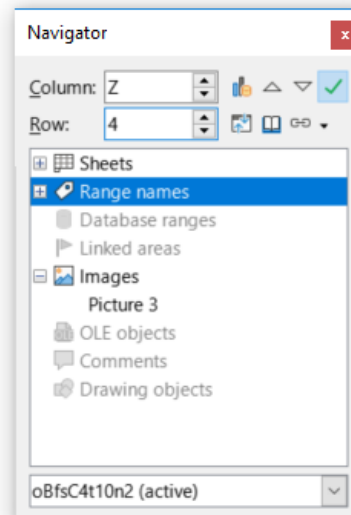
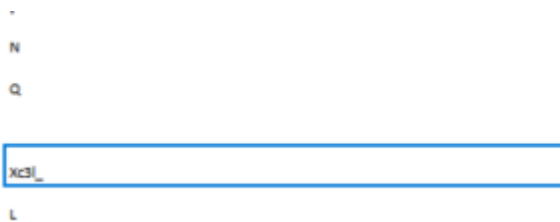| -	-
^	n
=	.
]	K
q	)
w	O
:	;
`	h
b	]
R	l
f	7
6	K
e	c
n	u
*	2
,	[
w	0
/	e
q	Q
'	p
a	m
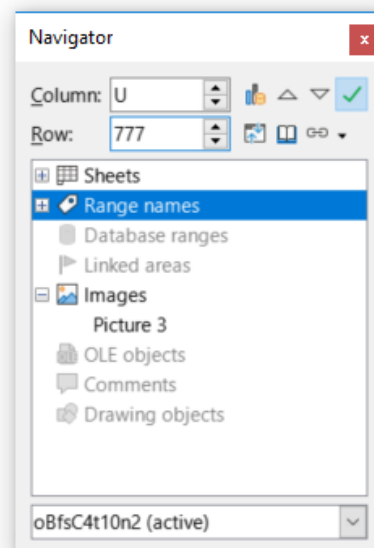
E

I received: HTB{n0w_e

Erel Regev

Combining both parts is not enough. But I got remembered on the following finding from earlier:

N

Q

xc3l_

L

Therefore, when combining all of the parts:

HTB{n0w_eXc3l_4.0_M4cr0s_r_b4ck}