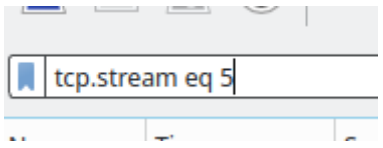
[FORENSIC]

Investiga II

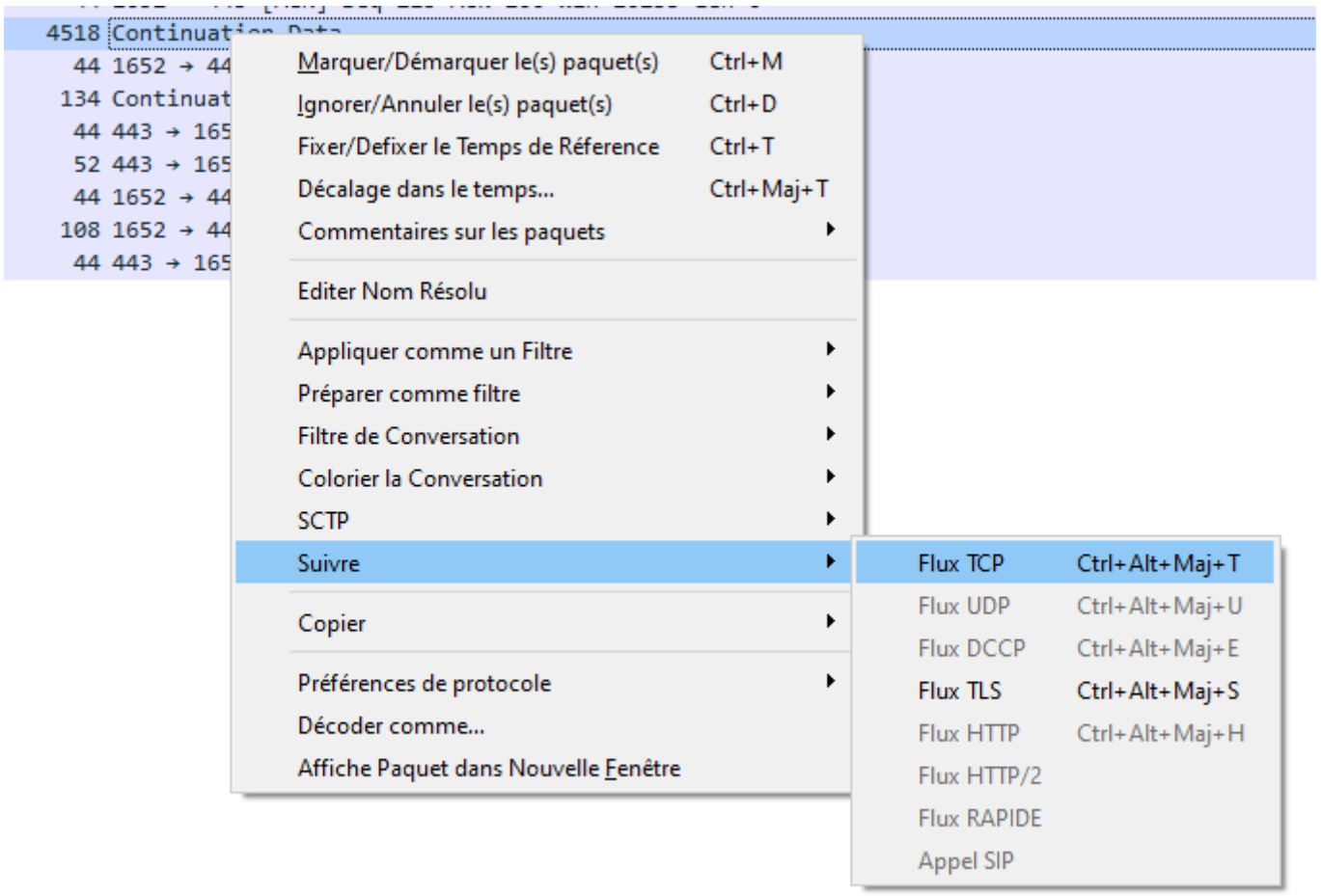
Upload d'un fichier ODT avec le flag à l'intérieur du RAT

Filtre :

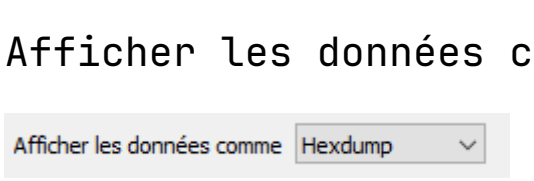
```
tcp.stream eq 5
```



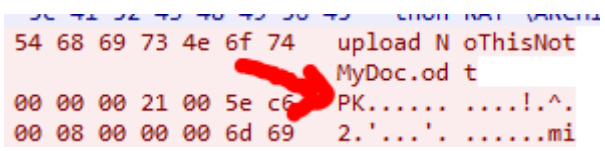
Click droit :



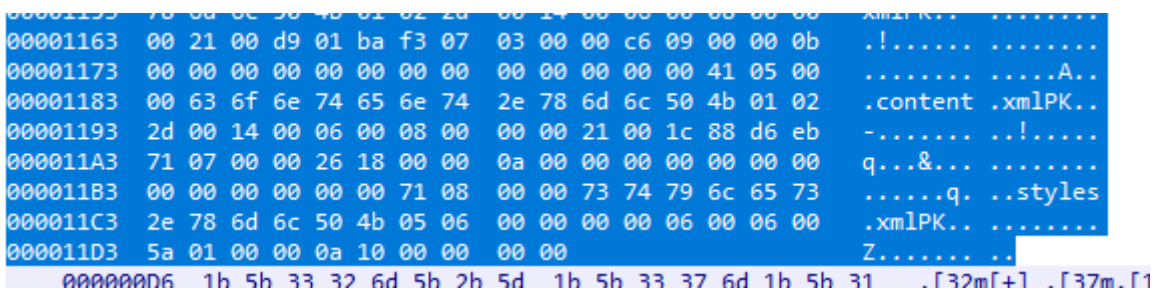
Afficher les données comme hexdump :



Repérer le début de la structure du document odt :



Copier toute la structure du document :



Coller tout ça dans cyberchef :

Input length: 22113 lines: 280

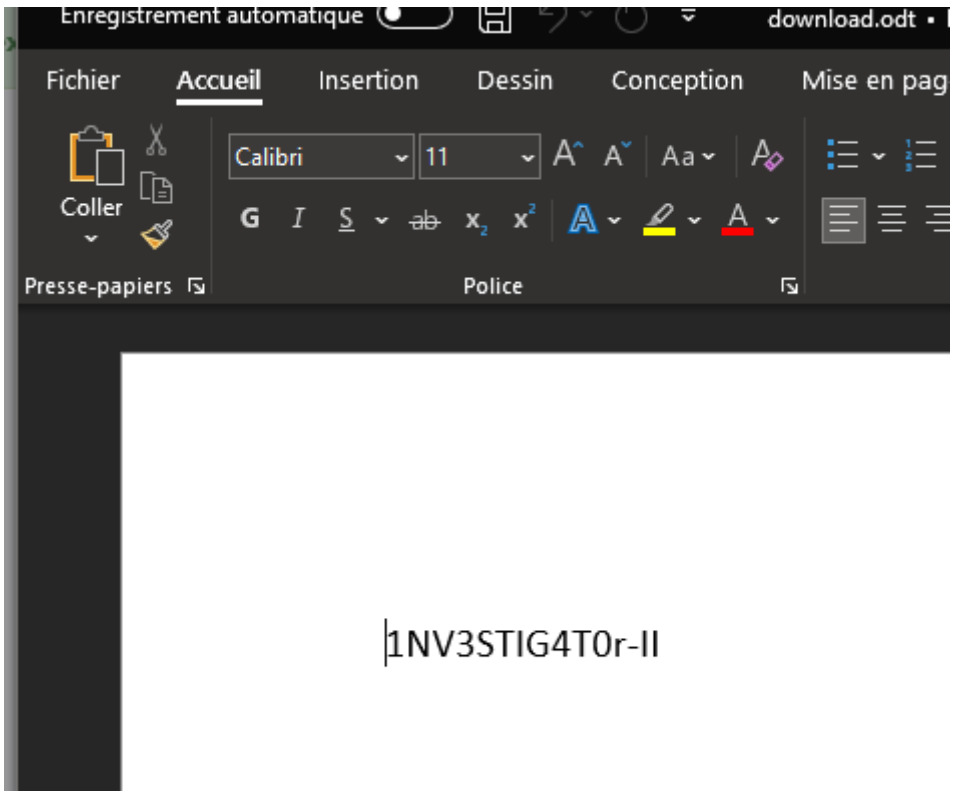
```
00000063  50 4b 03 04 0a 00 00 00  00 00 00 00 21 00 5e c6   PK...... ....!.^.
00000073  32 0c 27 00 00 00 27 00  00 00 08 00 00 00 6d 69   2.'...'. ......mi
00000083  6d 65 74 79 70 65 61 70  70 6c 69 63 61 74 69 6f   metypeap plicatio
00000093  6e 2f 76 6e 64 2e 6f 61  73 69 73 2e 6f 70 65 6e   n/vnd.oa sis.open
000000A3  64 6f 63 75 6d 65 6e 74  2e 74 65 78 74 50 4b 03   document .textPK.
000000B3  04 14 00 06 00 08 00 00  00 21 00 00 f8 9f 93 a8   ........ .!......
000000C3  01 00 00 04 06 00 00 0c  00 00 00 73 65 74 74 69   ........ ...setti
000000D3  6e 67 73 2e 78 6d 6c 8c  54 cb 4e c3 30 10 bc 23   ngs.xml. T.N.0..#
000000E3  f1 0f 91 39 a7 6e e9 85  5a 0d dc 38 c1 0d 3e c0   ...9.n.. Z..8..>.
000000F3  b5 9d d6 c2 8f c8 eb 36  e1 ef d9 38 6d 71 50 91   .......6 ...8mqP.
00000103  7c c9 21 3b b3 8f d9 1d  6f 5f 06 6b aa 93 0a a0   |.!;.... o_.k....
00000113  bd 6b c8 6a b1 24 95 72  c2 4b ed f6 0d f9 fc 78   .k.j.$.r .K.....x
00000123  ad 9f 48 05 91 3b c9 8d  77 aa 21 df 0a c8 cb f3   ..H..;.. w.!.....
00000133  fd dd d6 b7 ad 16 8a 49  2f 8e 56 b9 58 83 8a 11   .......I /.V.X...
00000143  49 50 61 42 07 8c 3b 6d  1b 72 0c 8e 79 0e 1a 98   IPaB..;m .r..y...
00000153  e3 56 01 8b 82 f9 4e b9  0b 89 fd 62 79 c4 06 58   .V....N. ...by..X
00000163  aa 3f fd 14 07 1e 62 69  86 04 9e b1 bd 6b 35 4e   .?....bi .....k5N
00000173  50 d6 80 48 e8 9c 2f 77  a5 5c c9 23 df 71 50 33   P..H../w .\.#.qP3
00000183  b6 68 c8 21 c6 8e 51 da  1d 83 59 f8 b0 a7 52 50   .h.!..Q. ..Y...RP
00000193  65 d4 28 15 d0 d5 62 45  c9 59 28 19 d6 b2 b8 16   e.(...bE .Y(.....
000001A3  62 67 75 02 ef cb b9 bc  c7 fd e4 f4 d6 97 92 07   bgu..... ........
000001B3  30 75 eb 6b e1 6d 87 8b  da 99 d9 b4 ad 0f c5 ab   0u.k.m.. ........
000001C3  1e b1 79 0b fb 20 a5 b9  8a d5 f7 fd a2 5f 27 b9   ..y.. .. ..... '.
```

Output time: 11ms length: 4474 lines: 19

```
PK..
.......!.^Æ2.'...'.......mimetypeapplication/vnd.oasis.opendocument.textPK..........!..ø..¨..........settings.xml.T
ËNÃ0.¾#ñ..9§né.Z
Ü8Á
>Àµ.ÖÂ.Èë6áïÙ8mqP.|É!;³.Ù.o_.kª.
 ¼kÈj±$.rÂKíö
ùüx..H..;É.wª!ß
ÈËóýÝÖ·...I/.V¹X...IPaB..;m.r..y...ãV...ùN¹..ýbyÄ.Xª?ý...bi...±¼k5NPÖ.Hè.
/w¥\É#ßqP3¶hÈ!Æ.QÚ..Yøº§RPeÔ(.ÐÕbEÉY(.Ö².bgu.ïË¹¼Çýäôö...0uëkám..Ú.Ù´..Å«.±y.û
¥¹.Õ÷ý¢_'¹..Ë5EÕPÝú¤UÿpÑËòx¸EXm6Oô..éóþvÅ«ÈKÇ´.Í»sG»S¡.=ö
ñ{.Îd.Ò.gSe6è..¾.d.Ò,9'..DÐ]±§&ô.o5îªÌR.Ø.î%iT.ç¯ p*¶5Bÿi.-kð1+.%.s.¢..U.±9w...·../þ.NáËí..hoº..}CSô
5Ú}ÝJ;AÇ(©Îç.=÷kB.....ÿÿ..PK..........!.Î2./Ù...d.......META-INF/manifest.xml¬.ÁjÃ0..ï.¾.ñ=öv.¦No{.í...l.
[6.R.·.3H»...ô&Éâû?£Ãñ\²:áÌ©.xÏæI+¤Pc¢.¯ßß^...X."äJèõ.¬.ããÃ¡.¥  YÜ^¨N"¾´^/3¹
.Ø..d'ÁÕ..kX
.¸ßûnË.¯Ø)e.úÚ¾ª=ÁMKÎC.ùôÚêë¸`L0ÈÚº.´.S.éß±'.æ[ÀüÌ5.gÑöö¨PIº.é¾..nD»=ÿ.Ê²fä{CQ¤_îÞØ..7.ÚË±öbü...ÿÿ..PK..........!.VØ
ævð...5.......meta.xml.SM.Óð.¾#ñ."ß.'Ý-ÚZIö.¸ð!Q.ÄÍØÓÔ.Ø.=![Nû.àOî/Áq.Ð.
.ä.ýÞ¾.ñ<»¾.èÚä.X§.®H.å$.-.Tº©È.ýËô.$.¹.¼5.*r.GîëçÏJs8(.L.1t 1í.yâ.iÇfª".ÕÌp§.Ó¾.ÇP0Ó.^$ì<..Ò32¥úWõ.
{®.¢"GÄ.QÚ.¶Í.m¨..Z.ºt´È
Jb...Ò_×ðq.³ñ&..ÝnG.K.xÏ³.Ý.z¹ýT¼.C.
hº..._+a.3.|.FD.m.'+øÑXYÒ+I).C.-Ô¥ïvÙú..'¬êÑ»3S...pÃç/ p&×CH¯´BÅÛTX.}¾âÝw.<=þ¸\?..ã.m]ë¦æþ#ÇYô<. õ.H%G¨7ùf..~Ýîó;
VlY..../.§².Q,ì\.¡ë[.>  ®±£.CEÞ.Ûñ6..;oùd6ÃSï.±S>...Ö.ô.ÒM*N¢.Wob;Wõ\h.åàÍ.\y·..¿¿R¬ä¬Y.|ê?.*.J$Á .7.
3hô?.,.å.åýñ..ý»Yº M..Gn¹@º.Ql#cÍ¸b.ÒÞ.ñ¨.\Ï.¯û.öv...ï}jð÷i¼A.....ÿÿ..PK..........!.Ù.ºó....Æ
      content.xml Vlo.0.} ´ÿ`yÏ  Ò0E|\ ´0R[M[¶w  X  Ù&$ÿ«x¤»KWk D +ÜëãsÏ5ìîÏU NT*&x  Õ #ÊS 1^ÃØxáœw  Ò gπ  ÆœB ¾R ü°
```

Cliquer sur save output file

- Choisir un nom de fichier + .odt
- Ouvrir le fichier



flag : 1NV3STIG4T0r-II

Challenge setup

Investiga II - Eazy
Forensic - Facile

Un attaquant s'est introduit dans notre réseau, voici la trace PCAP.

NHM2I{1NV3STIG4T0r-II}