CA SENT LE SAPIN !

VOYAGE DANS LE MONDE DE LA RECHERCHE EN SÉCURITÉ SAP

Yvan GENUER, Alexandre BOLLE REDDAT

devoteam onapsis

SOMMAIRE

- SAP ?
- SAP IGS ?
- Protocole IGS
- Outils
- ADM:INSTALL
- Vulnérabilités
- Conclusion

SOMMAIRE

- SAP ?
- SAP IGS ?
- Protocole IGS
- Outils
- ADM:INSTALL
- Vulnérabilités
- Conclusion

SAP ?

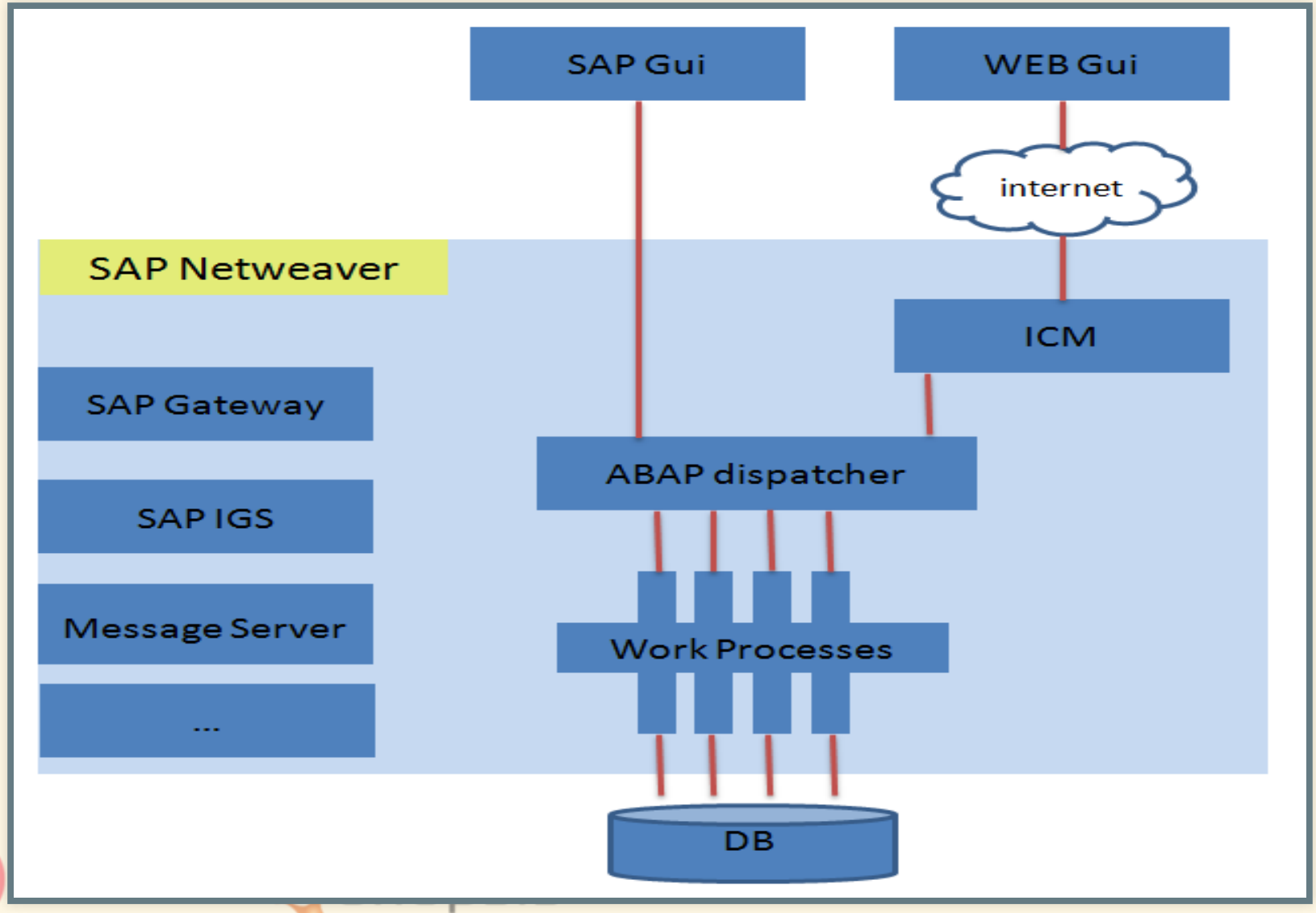

Financial management
Business Analytics
CRM
ERP
E-Mails
Sales
Projects
Purchasing

SAP ?

https://www.sap.com/corporate/en/company.html

SAP ?

ARCHITECTURE D'UN SYSTÈME SAP



VOCABULAIRE SAP

SID	SAP système identifiant (3 char)
<sid>adm	Utilisateur administrateur (bobadm, prdadm, d01adm, etc)
Numéro de system SAP	Un identifiant sur deux chiffres. SN = 05, port = 3205, 3305, 3605, etc.

VOCABULAIRE SAP

ABAP	Advanced Business Application Programing
Report	Programme ABAP
Module fonction	Fonction ABAP
Transaction	Alias permettant de lancer une séquence de report (SU01, SM21, SIGS, etc)

LES CONCEPTS WTF...

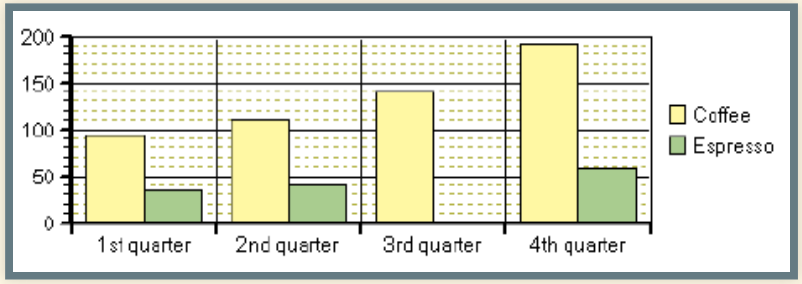
- Les services SAP tournent sur sidadm
- Le kernel SAP = ensemble de binaires sur l'OS
- Code source ABAP = dans la base de données
  - compatibilité...
  - ... du coup accessible!
- Tout système SAP possède un environnement de développement

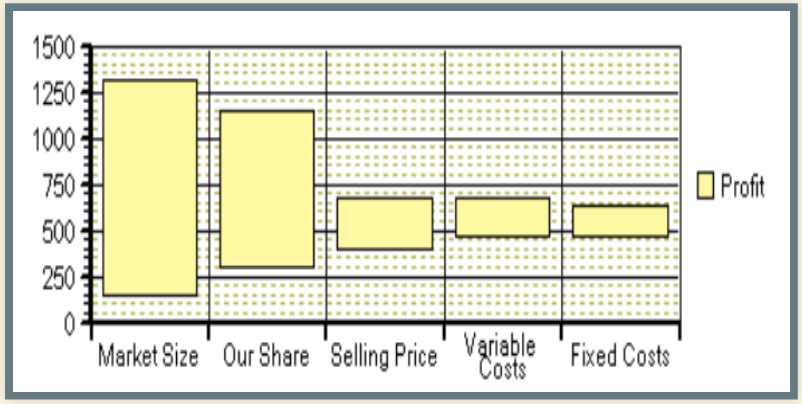
SOMMAIRE

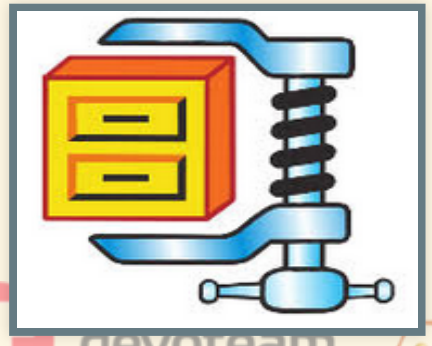
- SAP ?
- SAP IGS ?
- Protocole IGS
- Outils
- ADM:INSTALL
- Vulnérabilités
- Conclusion

A QUOI IL SERT ?

SAP Internet Graphics Services

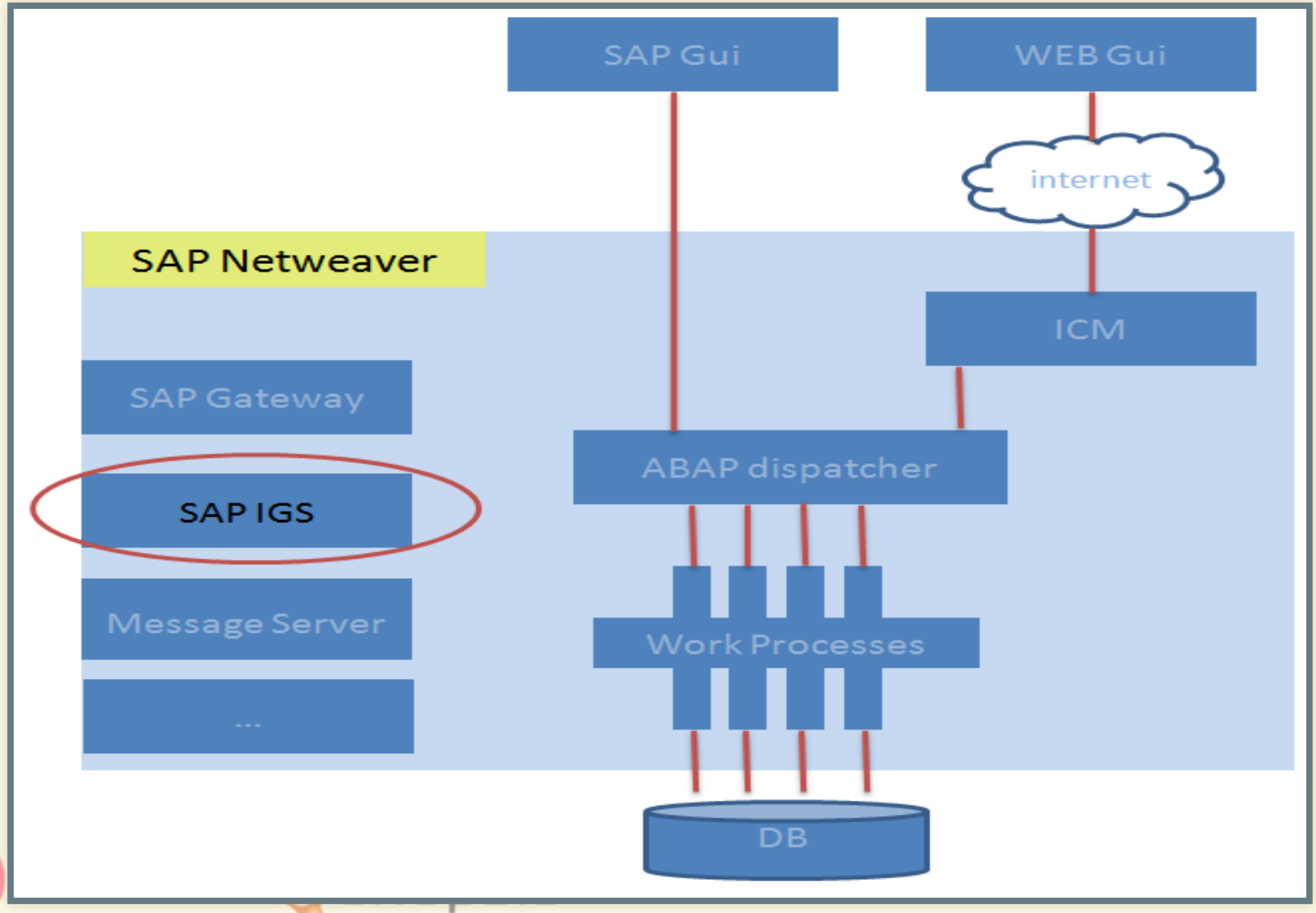




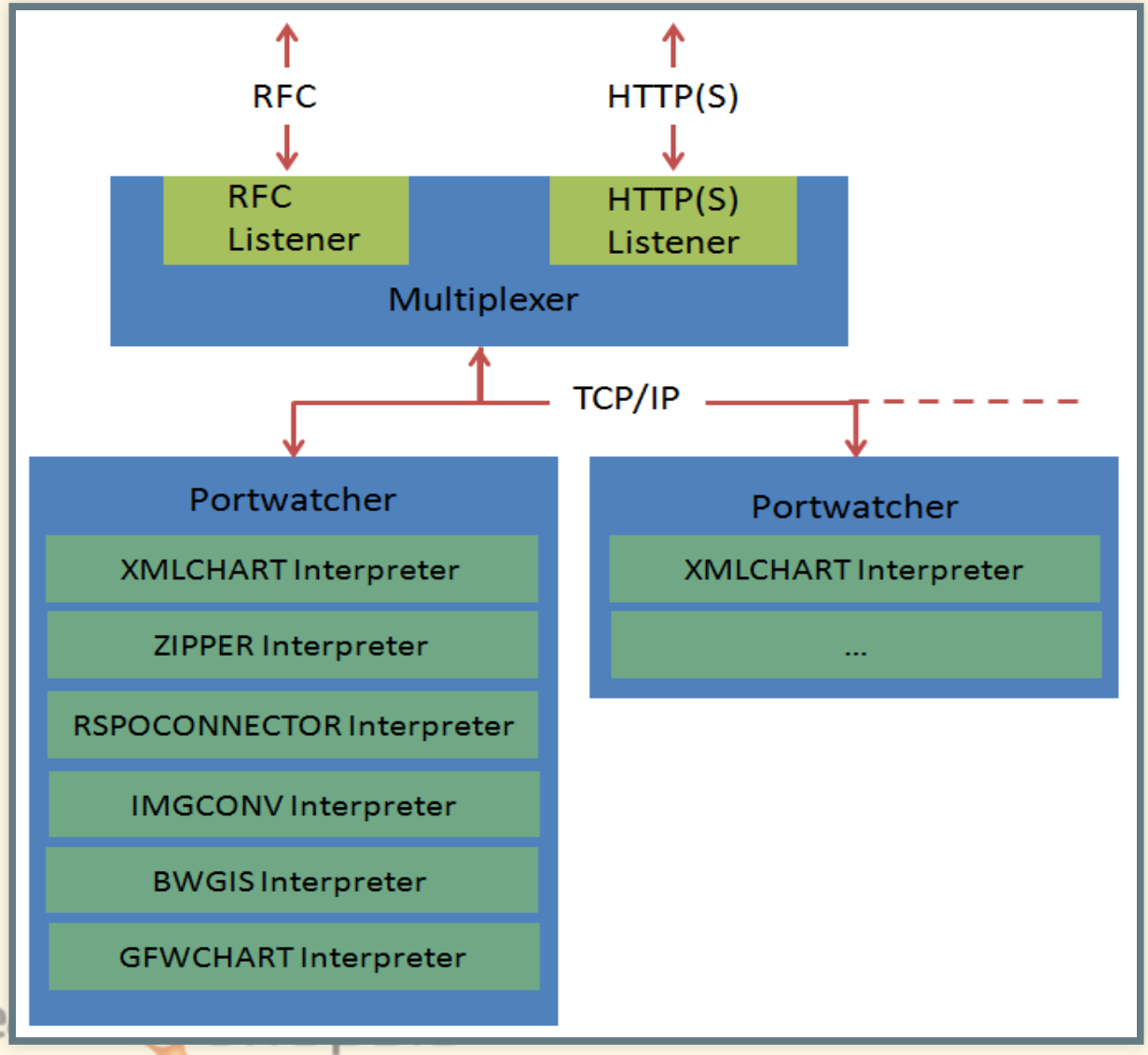


devoteam onapsis

ARCHITECTURE DU SERVICE SAP IGS



ARCHITECTURE DU SERVICE SAP IGS



ARCHITECTURE DU SERVICE SAP IGS

```
bobadm@sapbob:~# ss -lntp | grep igs
LISTEN   0   128   *:40000    *:*   users:(("igsmux_mt",pid=42225,fd=9)
LISTEN   0   20    *:40001    *:*   users:(("igspw_mt",pid=42226,fd=7))
LISTEN   0   20    *:40002    *:*   users:(("igspw_mt",pid=42227,fd=7))
LISTEN   0   128   *:40080    *:*   users:(("igsmux_mt",pid=42225,fd=6)
```

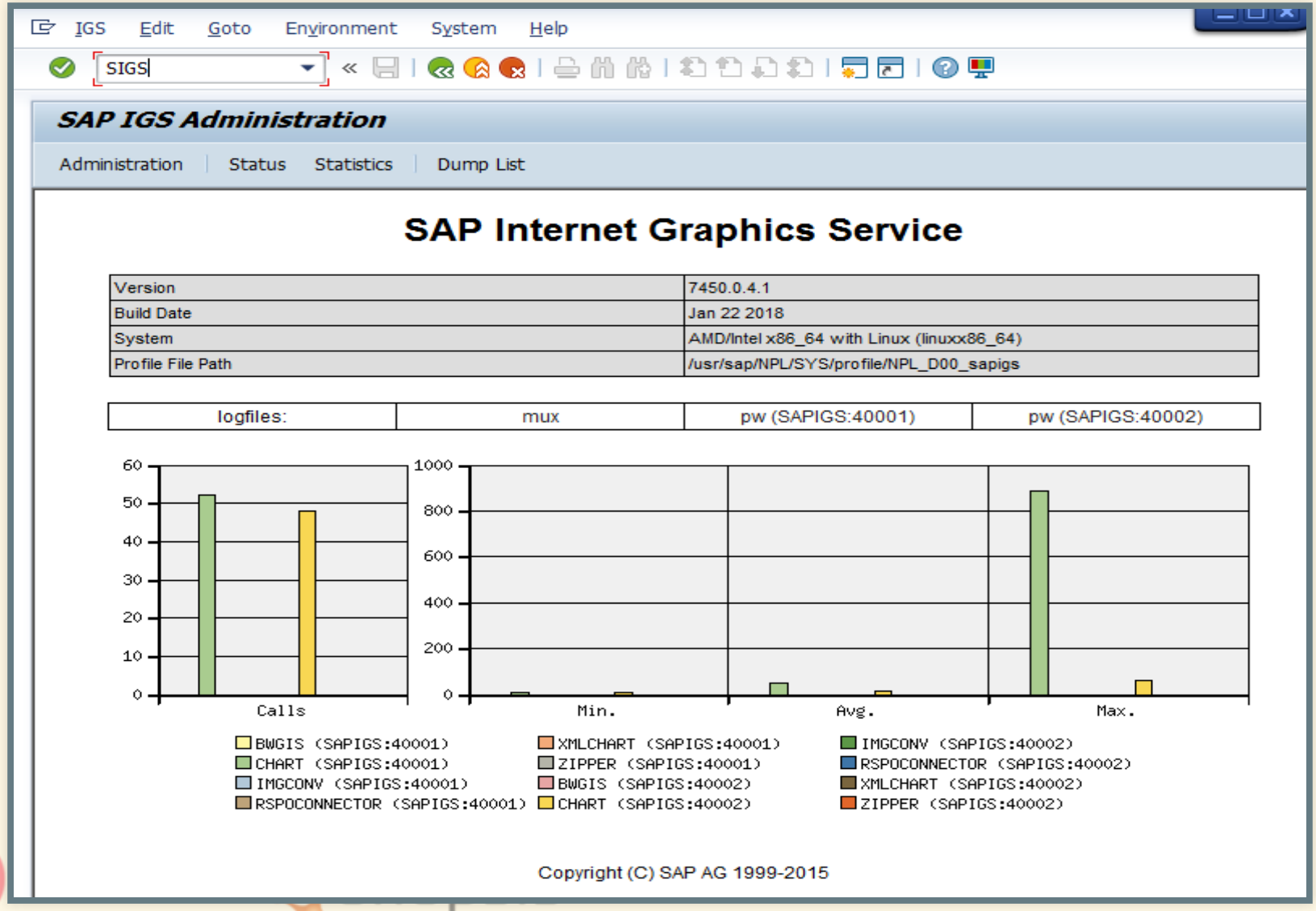
4<SN>00	RFC Listener
4<SN>80	HTTP Listener
4<SN>01	Portwatcher 1
4<SN>02	Portwatcher 2

ARCHITECTURE DU SERVICE SAP IGS

```
root@sapbob:~# pstree -a
...
  ├─sapstart pf=/usr/sap/BOB/SYS/profile/BOB_D00_sapbob
  │    ├─BOB_00_DP pf=/usr/sap/BOB/SYS/profile/BOB_D00_sapbob
  │    │    ├─BOB_00_BTC_W5 pf=/usr/sap/BOB/SYS/profile/BOB_D00_sapb
  │    │    ...
  │    │    └─{BOB_00_DP}
  │    └─ig.sapBOB_D00 -mode=profile pf=/usr/sap/BOB/SYS/profile/BO
  │         ├─igsmux_mt -mode=profile -restartcount=0 -wdpid=40722 p
  │         │    └─19*[{igsmux_mt}]
  │         ├─igspw_mt -mode=profile -no=0 -restartcount=0 -wdpid=40
  │         │    └─15*[{igspw_mt}]
  │         └─igspw_mt -mode=profile -no=1 -restartcount=0 -wdpid=30
  │              └─15*[{igspw_mt}]
```

devoteam onapsis

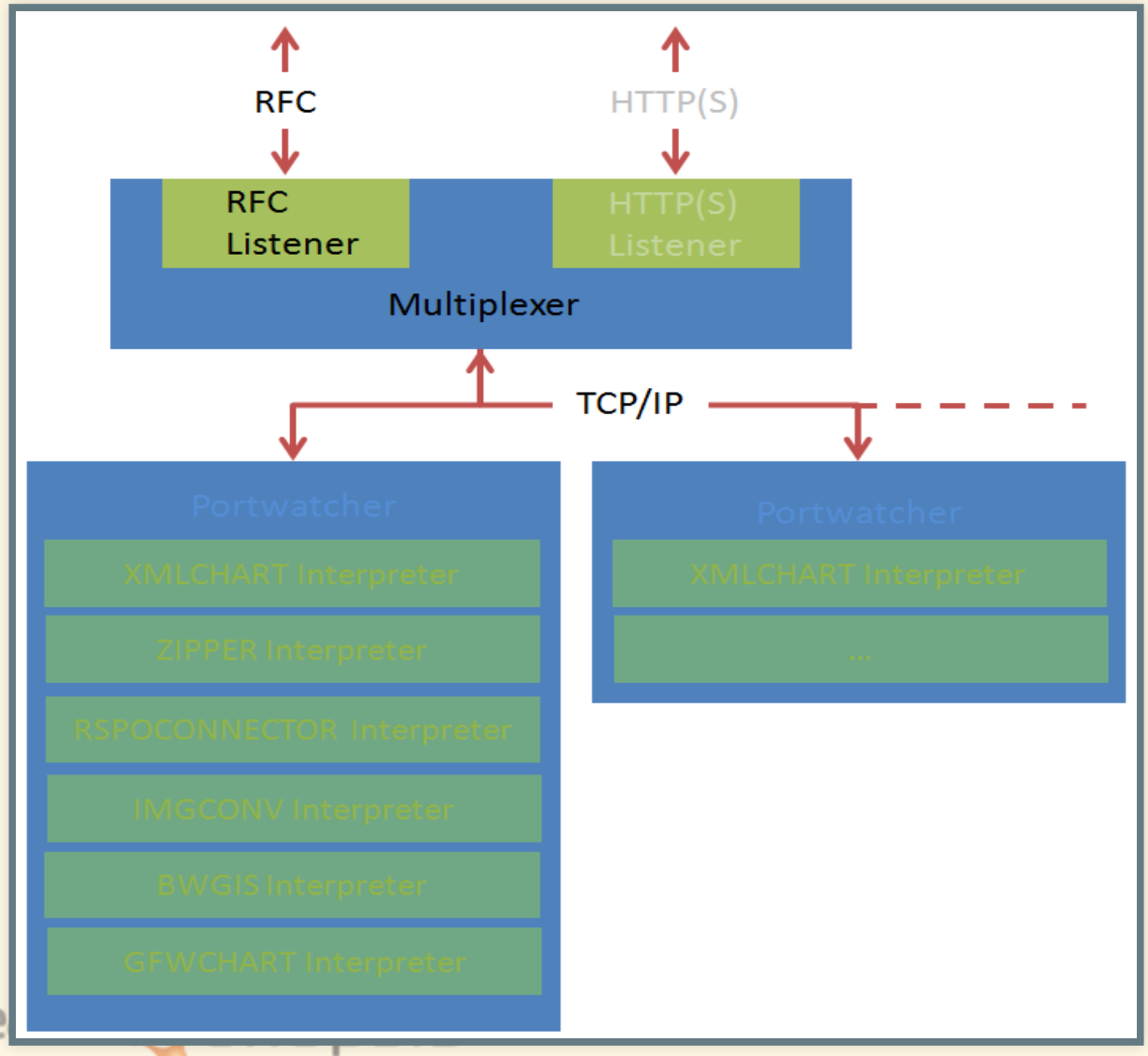
ARCHITECTURE DU SERVICE SAP IGS



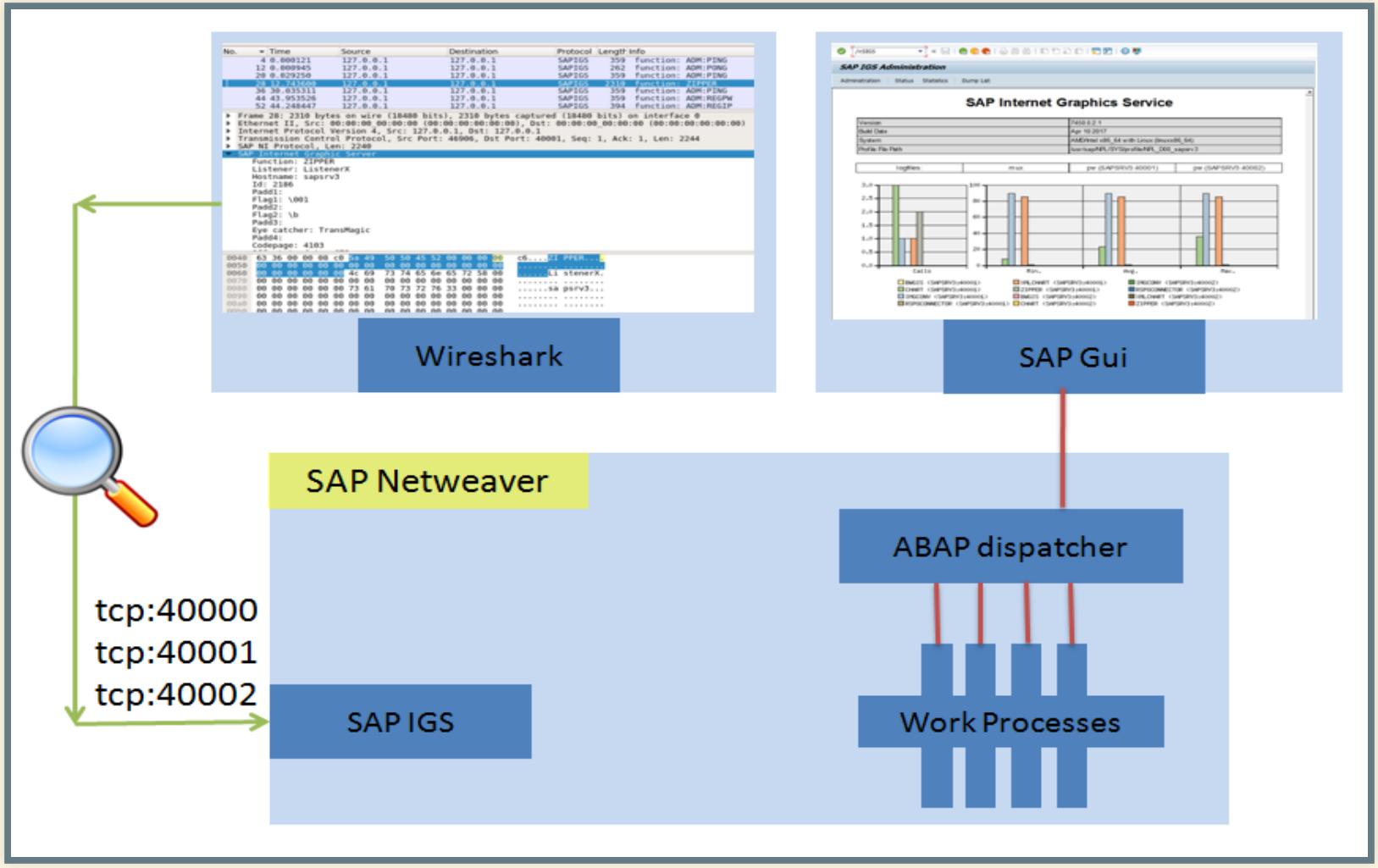
SOMMAIRE

- SAP ?
- SAP IGS ?
- Protocole IGS
- Outils
- ADM:INSTALL
- Vulnérabilités
- Conclusion

PROTOCOLE IGS : TEST

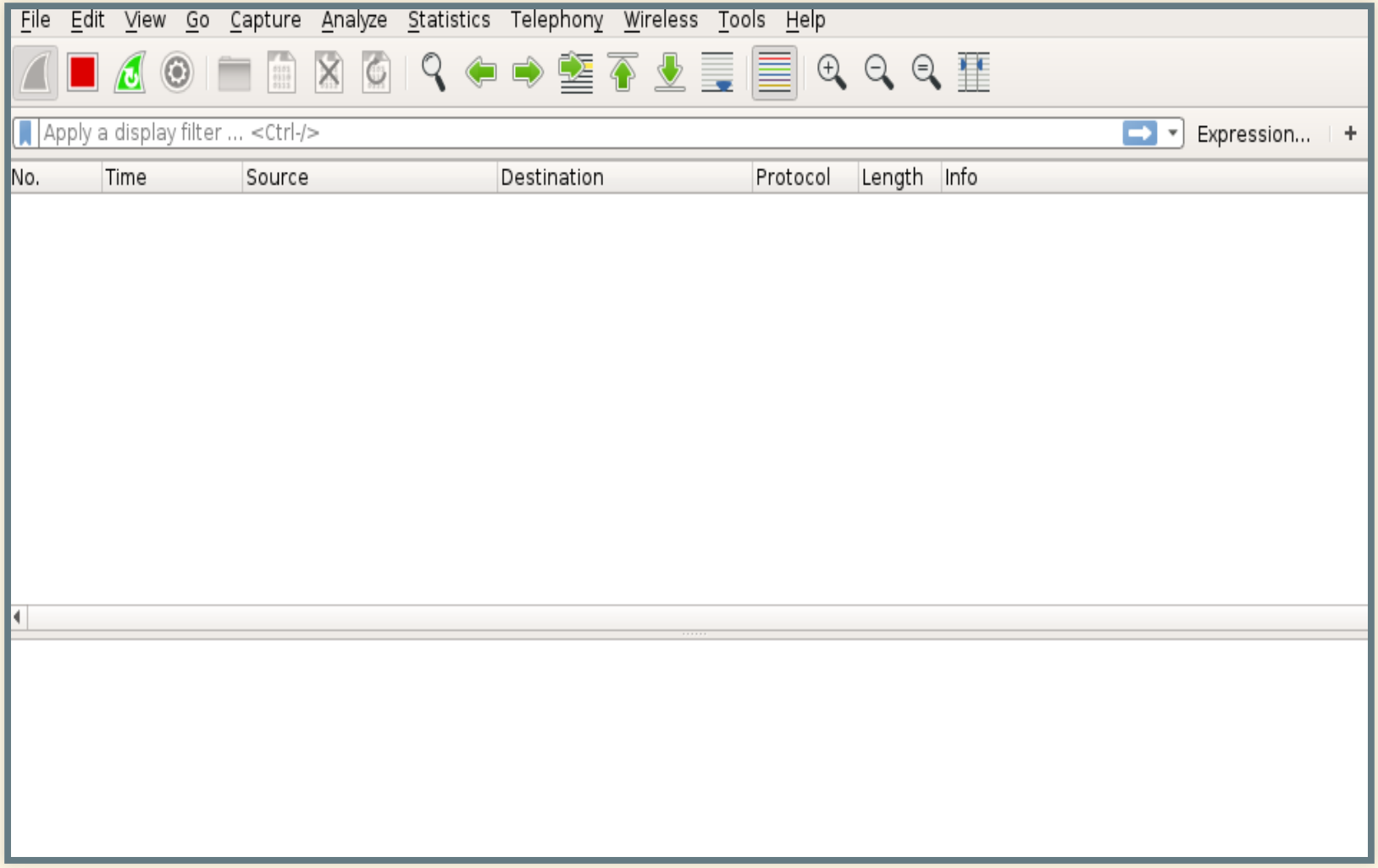


PROTOCOLE IGS : TEST



devoteam onapsis

PROTOCOLE IGS : TEST



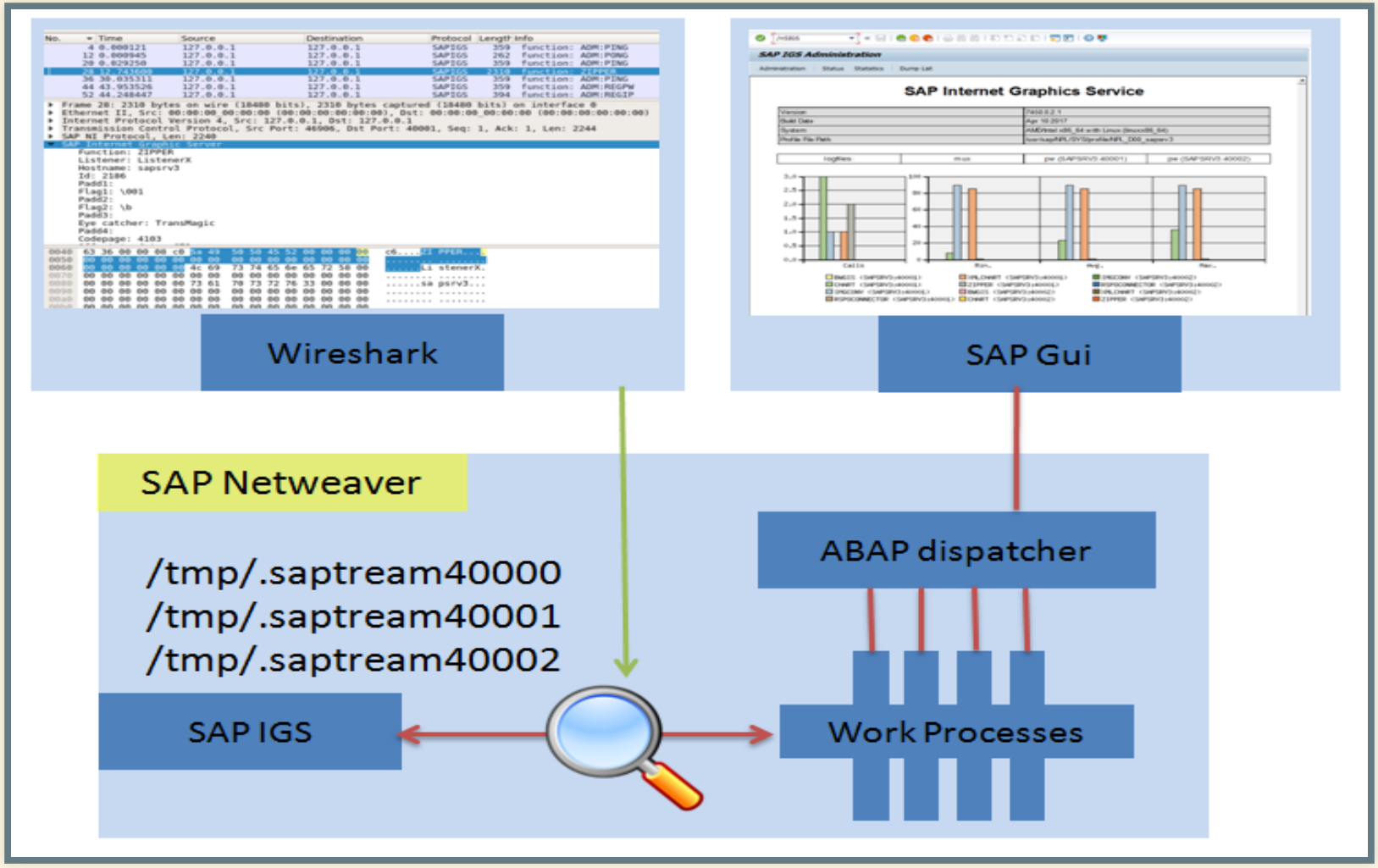
devoteam onapsis

PROTOCOLE IGS : TEST

- Découverte des sockets internes

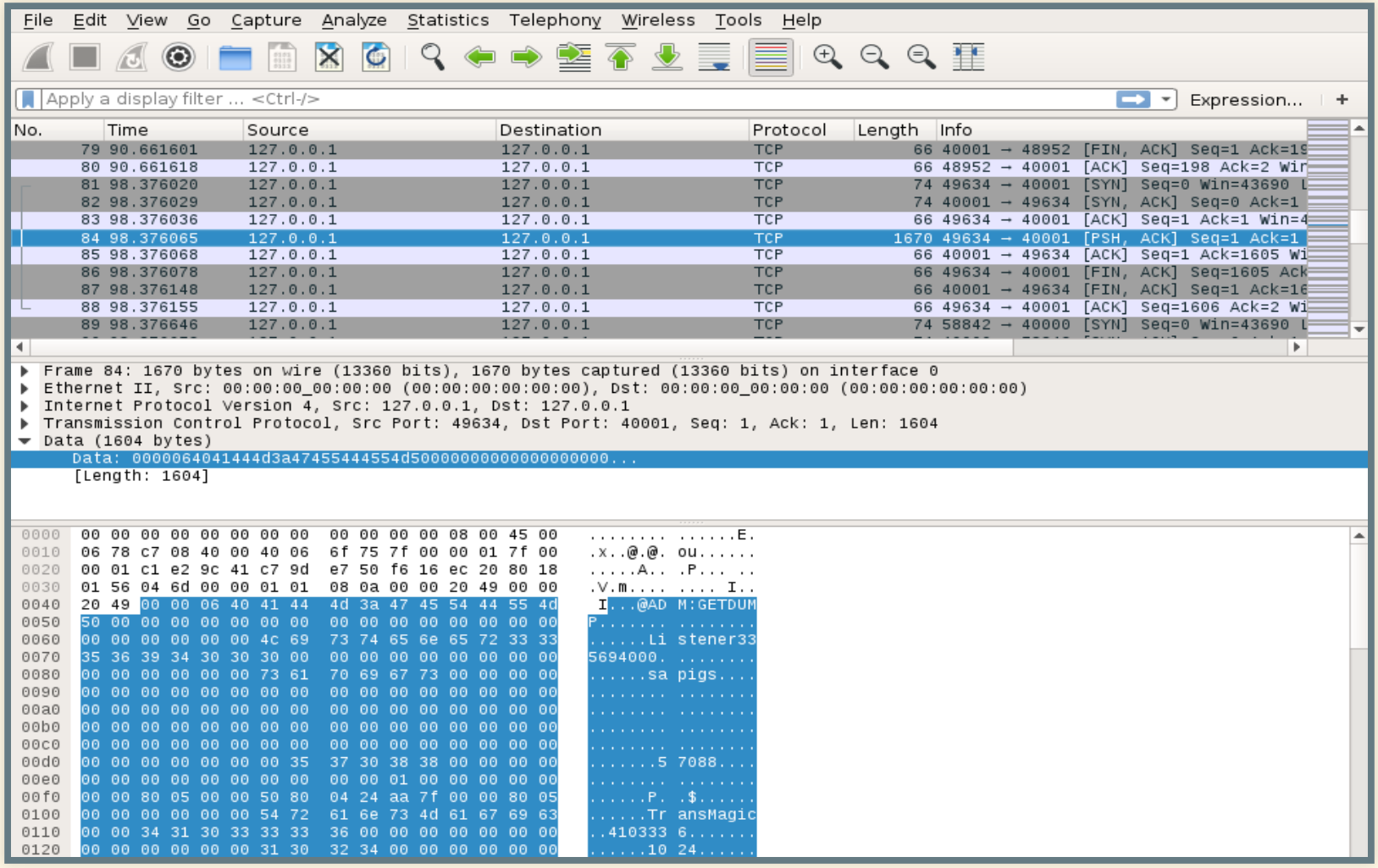
```
/tmp/.sapstream40000
/tmp/.sapstream40001
/tmp/.sapstream40002
```

PROTOCOLE IGS : TEST



devoteam onapsis

PROTOCOLE IGS : TEST



devoteam onapsis

PROTOCOLE IGS : BINAIRES

Binaires du kernel SAP associés à l'IGS

```
igsmux_mt                Multiplexer
igspw_mt                 Portwatcher
bwgis.so                 Library for BWGIS interpreter
bwgis_c.so               Library for BWGIS interpreter
gfwchart.so              Library for CHART interpreter
gfwchart_c.so            Library for CHART interpreter
imgconv.so               Library for IMGCONV interpreter
rspoconnector.so         Library for RSPOCONNECTOR interpreter
sgxgis.so                Library for SAPIGSXML interpreter
xmlchart.so              Library for XMLCHART interpreter
xmlchart_c.so            Library for XMLCHART interpreter
zipper.so                Library for ZIPPER interpreter
```

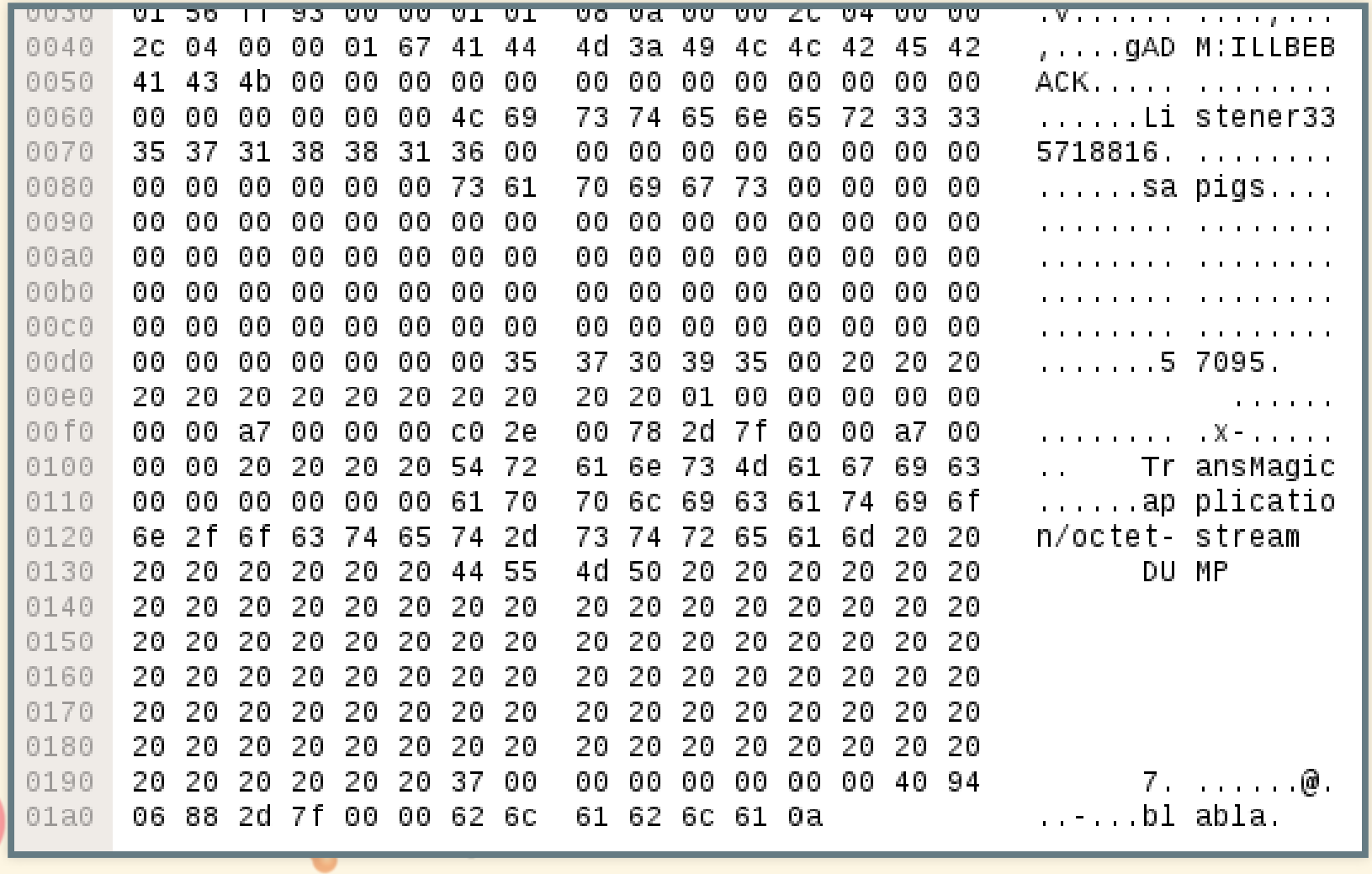
PROTOCOLE IGS : BINAIRES

```
root@sapbob:/sapmnt/BOB/exe/uc/linuxx86_64# file igsmux_mt
igsmux_mt: ELF 64-bit LSB executable, x86-64, version 1 (SYSV),
dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2,
for GNU/Linux 2.6.4, BuildID[sha1]=d800fb09cf0729672a6993557126871
not stripped
```

PROTOCOLE IGS : RÉSULTATS

PROTOCOLE IGS : RÉSULTATS

- Tout est en clair



```
0030  01 56 11 93 00 00 01 01   08 0a 00 00 2c 04 00 00   .V...... ....,...
0040  2c 04 00 00 01 67 41 44   4d 3a 49 4c 4c 42 45 42   ,....gAD M:ILLBEB
0050  41 43 4b 00 00 00 00 00   00 00 00 00 00 00 00 00   ACK..... ........
0060  00 00 00 00 00 00 4c 69   73 74 65 6e 65 72 33 33   ......Li stener33
0070  35 37 31 38 38 31 36 00   00 00 00 00 00 00 00 00   5718816. ........
0080  00 00 00 00 00 00 73 61   70 69 67 73 00 00 00 00   ......sa pigs....
0090  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ........ ........
00a0  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ........ ........
00b0  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ........ ........
00c0  00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ........ ........
00d0  00 00 00 00 00 00 00 35   37 30 39 35 00 20 20 20   .......5 7095.
00e0  20 20 20 20 20 20 20 20   20 20 01 00 00 00 00 00                ......
00f0  00 00 a7 00 00 00 c0 2e   00 78 2d 7f 00 00 a7 00   ........ .x-.....
0100  00 00 20 20 20 20 54 72   61 6e 73 4d 61 67 69 63   ..    Tr ansMagic
0110  00 00 00 00 00 00 61 70   70 6c 69 63 61 74 69 6f   ......ap plicatio
0120  6e 2f 6f 63 74 65 74 2d   73 74 72 65 61 6d 20 20   n/octet- stream
0130  20 20 20 20 20 20 44 55   4d 50 20 20 20 20 20 20         DU MP
0140  20 20 20 20 20 20 20 20   20 20 20 20 20 20 20 20
0150  20 20 20 20 20 20 20 20   20 20 20 20 20 20 20 20
0160  20 20 20 20 20 20 20 20   20 20 20 20 20 20 20 20
0170  20 20 20 20 20 20 20 20   20 20 20 20 20 20 20 20
0180  20 20 20 20 20 20 20 20   20 20 20 20 20 20 20 20
0190  20 20 20 20 20 20 37 00   00 00 00 00 00 00 40 94         7. ......@.
01a0  06 88 2d 7f 00 00 62 6c   61 62 6c 61 0a              ..-...bl abla.
```


devoteam
onapsis

PROTOCOLE IGS : RÉSULTATS

Récupération des noms des fonctions d'administration

```
1: "ADM:REGPW",            # Register a PortWatcher
2: "ADM:UNREGPW",          # Unregsiter a PortWatcher
3: "ADM:REGIP",            # Register an Interpreter
4: "ADM:UNREGIP",          # Unregsiter an Interpreter
5: "ADM:FREEIP",           # Inform than Interpreter is free
6: "ADM:ILLBEBACK",        # Call back function
7: "ADM:ABORT",            # Abort Interpreter work
8: "ADM:PING",             # Ping receive
9: "ADM:PONG",             # Ping send
10: "ADM:SHUTDOWNIGS",     # Shutdown IGS
11: "ADM:SHUTDOWNPW",      # Shutdown PortWatcher
12: "ADM:CHECKCONSUMER", # Check Portwatcher status
```

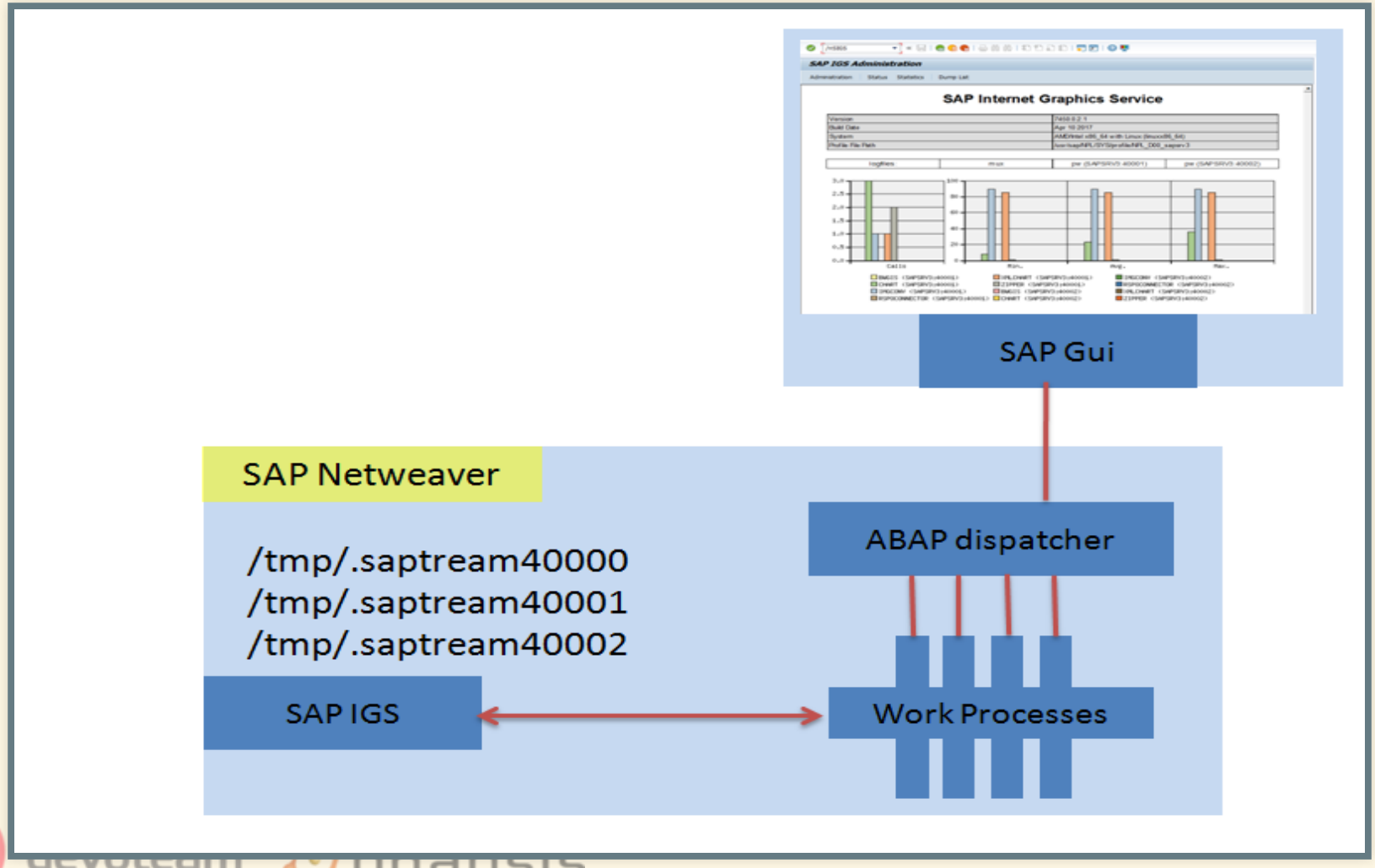
PROTOCOLE IGS : RÉSULTATS

Récupération des noms des fonctions d'administration

```
13: "ADM:FREECONSUMER",   # Inform than portwather is free
14: "ADM:GETLOGFILE",     # Display log file
15: "ADM:GETCONFIGFILE", # Display configfile
16: "ADM:GETDUMP",        # Display dump file
17: "ADM:DELETEDUMP",     # Delete dump file
18: "ADM:INSTALL",        # ???
19: "ADM:SWITCH",         # Switch trace log level
20: "ADM:GETVERSION",     # Get IGS Version
21: "ADM:STATUS",         # Display IGS Status
22: "ADM:STATISTIC",      # old Display IGS Statistic
23: "ADM:STATISTICNEW",   # Display IGS Statistic
24: "ADM:GETSTATCHART",   # Get IGS Statistic chart
25: "ADM:SIM",            # Simulation function
```

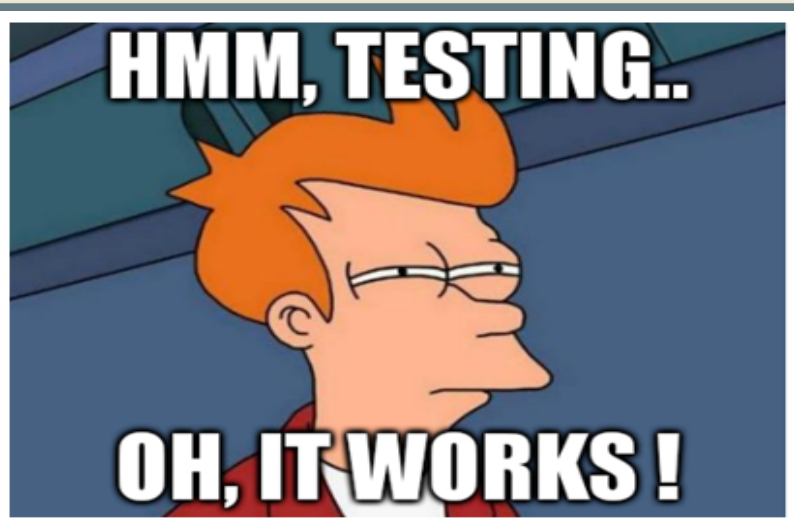
PROTOCOLE IGS : RÉSULTATS

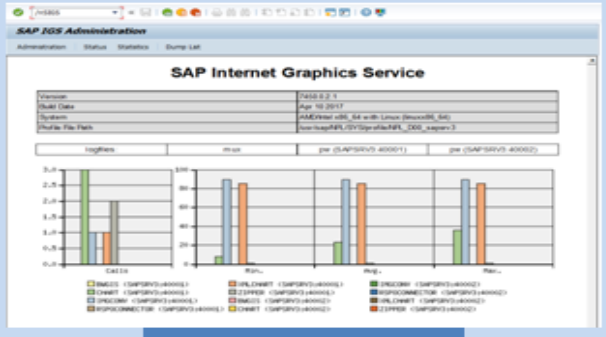
- Pas de mécanisme d'authentification...



PROTOCOLE IGS : RÉSULTATS

- Pas de mécanisme d'authentification...





SAP Gui

SAP Netweaver

ABAP dispatcher

tcp:40000
tcp:40001
tcp:40002

SAP IGS

Work Processes

SOMMAIRE

- SAP ?
- SAP IGS ?
- Protocole IGS
- Outils
- ADM:INSTALL
- Vulnérabilités
- Conclusion

OUTILS : PYSAP

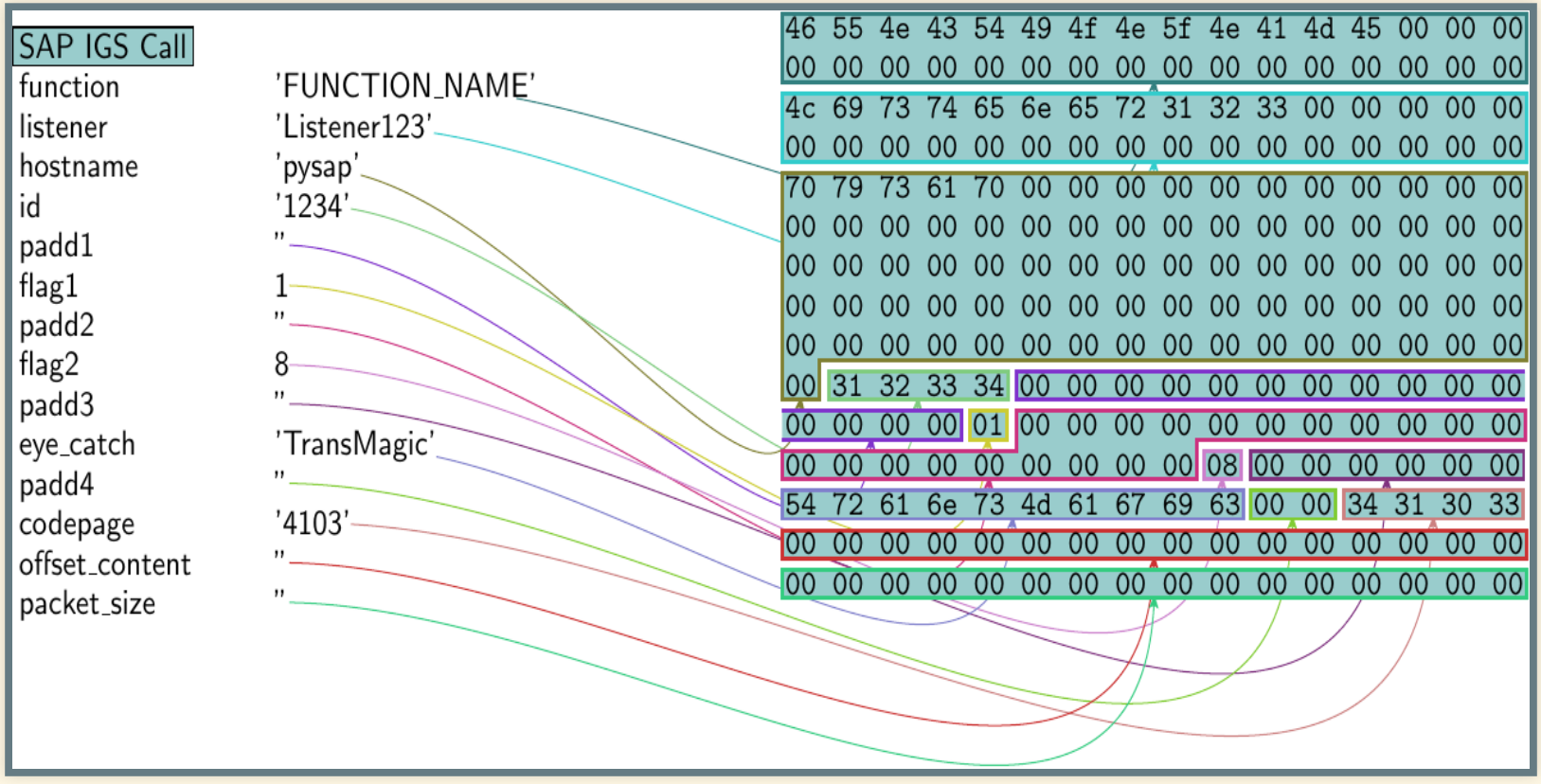
Librairie python

Utilisant scapy

SAP NI, SAP MS, SAP ENQ, ...

... SAP IGS

OUTILS : PYSAP



devoteam onapsis

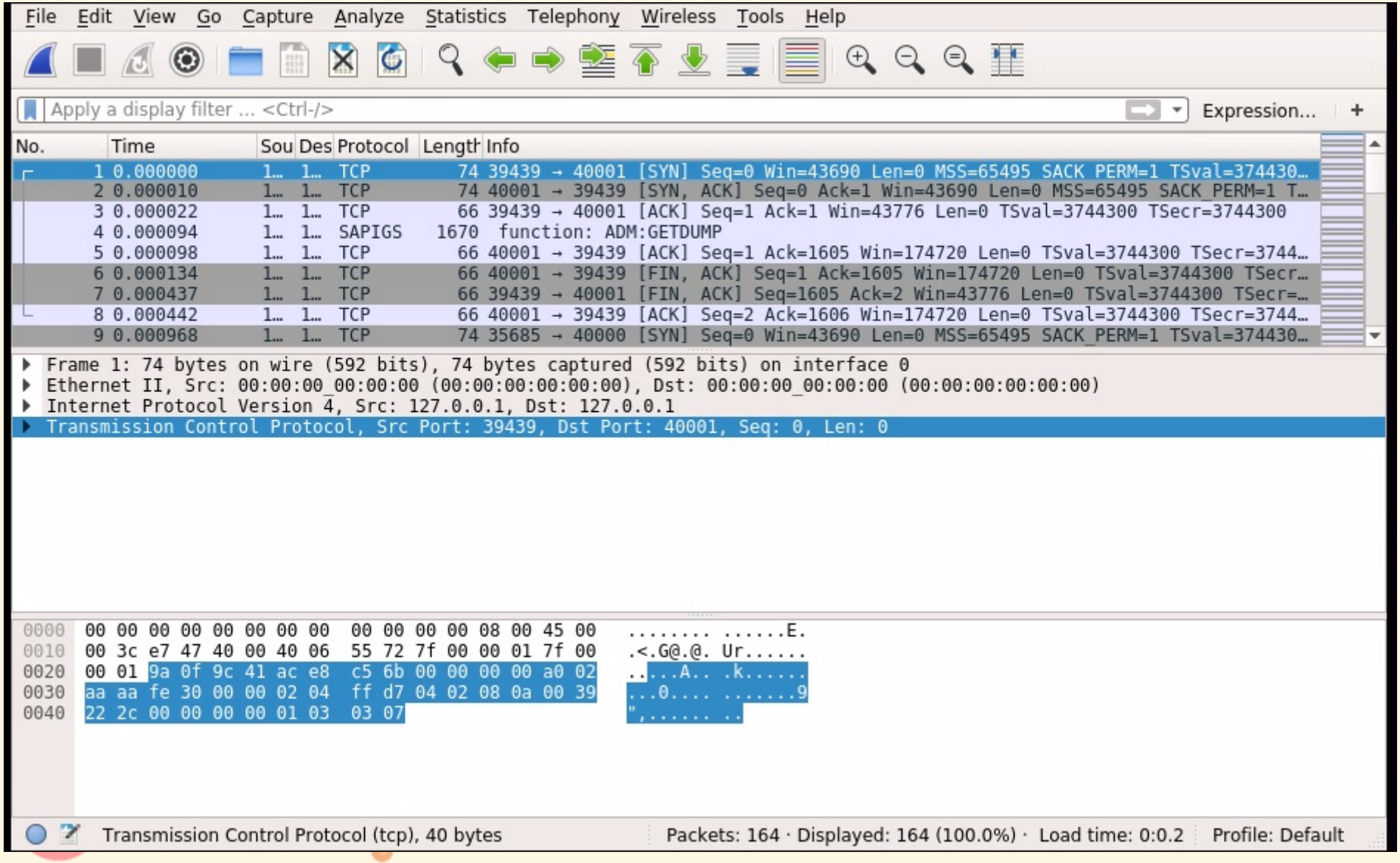
OUTILS : SAP-DISSECTION

Plugin wireshark

SAP NI, SAP MS, SAP ENQ, ...

... SAP IGS

OUTILS : SAP-DISSECTION



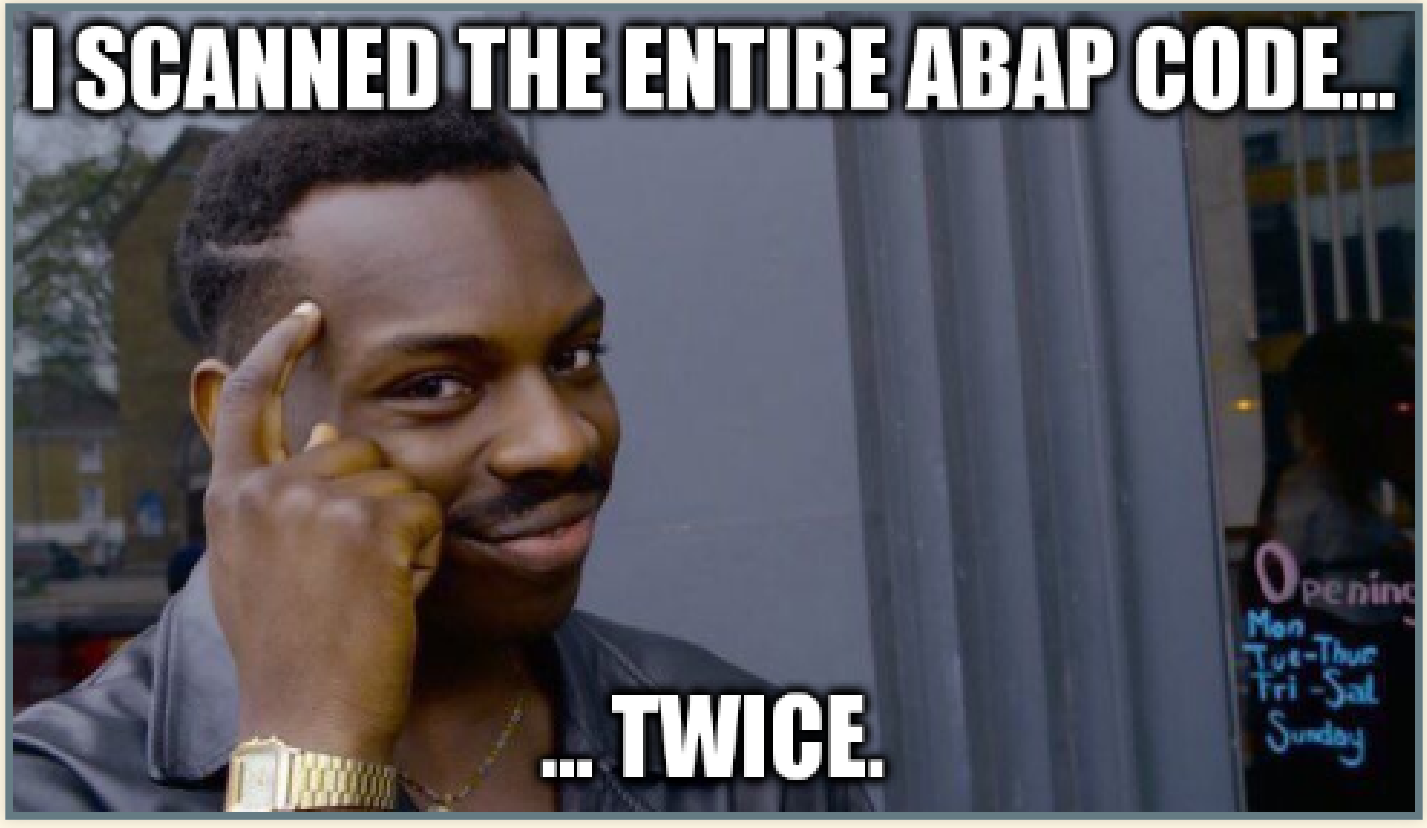
SOMMAIRE

- SAP ?
- SAP IGS ?
- Protocole IGS
- Outils
- ADM:INSTALL
- Vulnérabilités
- Conclusion

ADM:INSTALL : POURQUOI ?

- A cause de son nom...
- Trouvé dans le binaire, mais n'apparait jamais dans nos captures réseaux

ADM:INSTALL : RECHERCHE D'INFORMATION

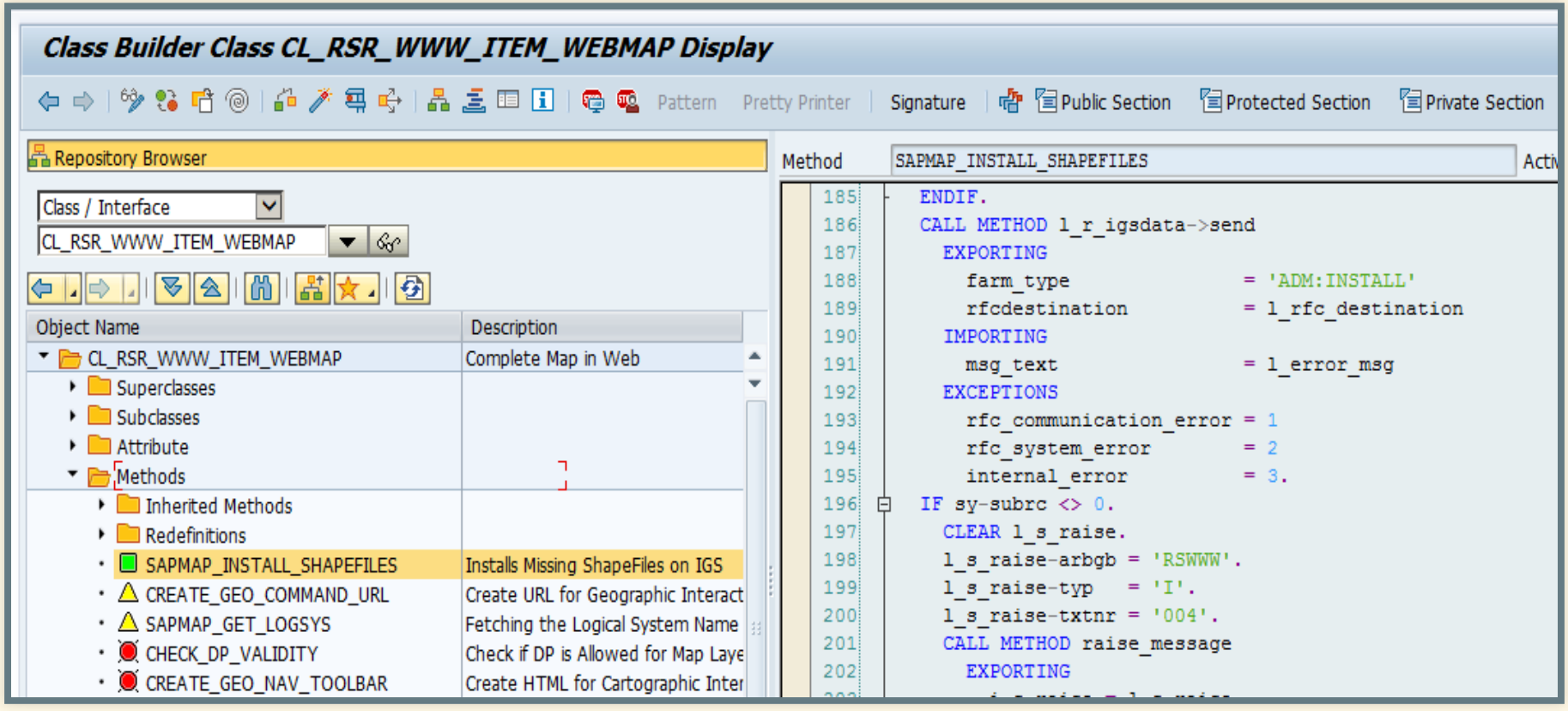


devoteam onapsis

ADM:INSTALL : RECHERCHE D'INFORMATION

- Recherche du pattern "ADM:INSTALL" dans tout le code ABAP
- 30.000 programmes... 1 occurence !

ADM:INSTALL : SAPMAP_INSTALL_SHAPEFILES



devoteam onapsis

ADM:INSTALL : SAPMAP_INSTALL_SHAPEFILES

- Vérifie s'il y a des shapefiles manquants sur l'IGS
- Si oui il upload les shapefiles via la fonction nommée adm:install
- ADM:INSTALL = installation de nouveaux shapefiles

ADM:INSTALL : SAPMAP_INSTALL_SHAPEFILES

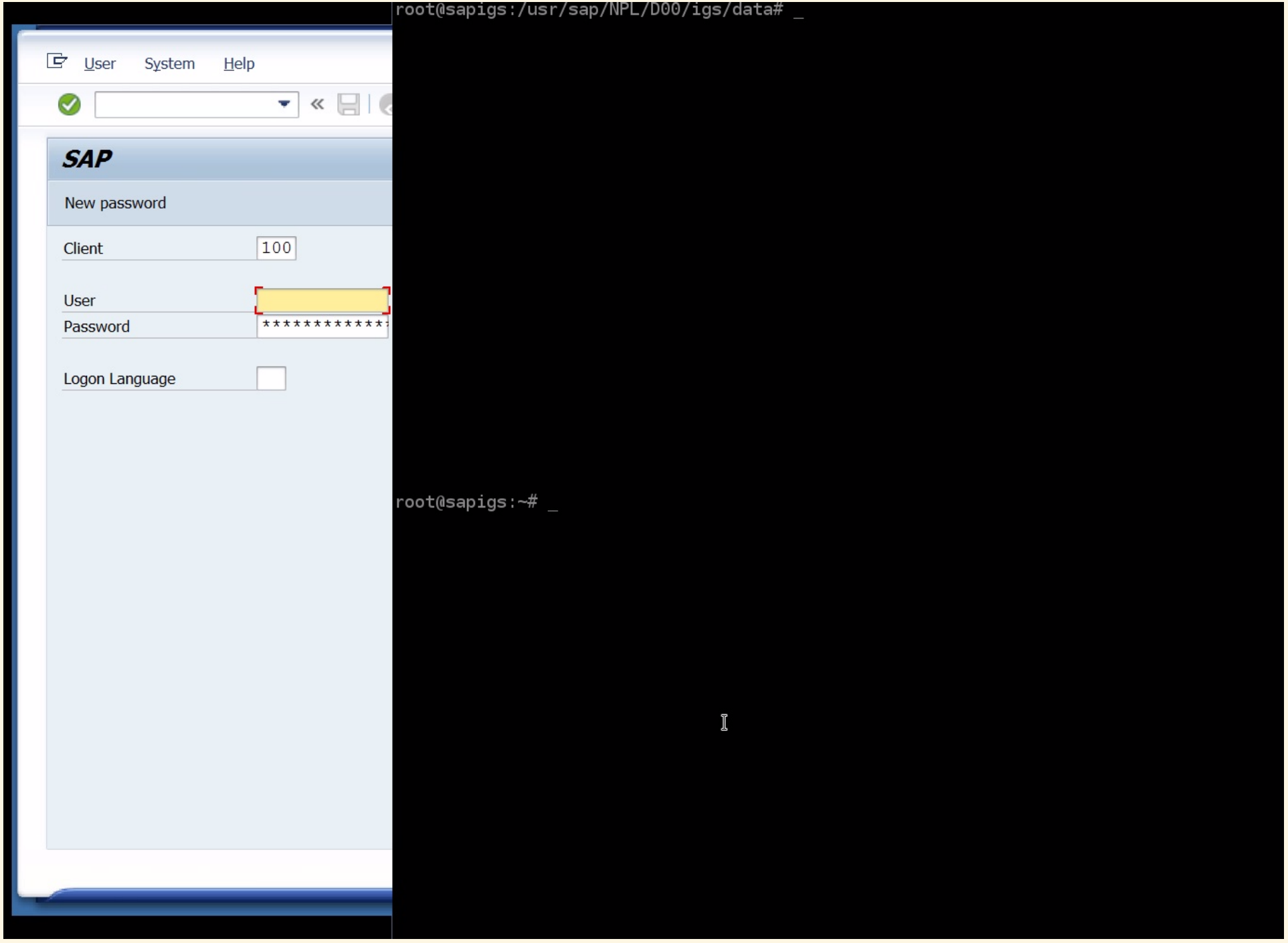
"On peut peut-être envoyer autre chose qu'un shapefile ?"

ADM:INSTALL : SAPMAP_INSTALL_SHAPEFILES

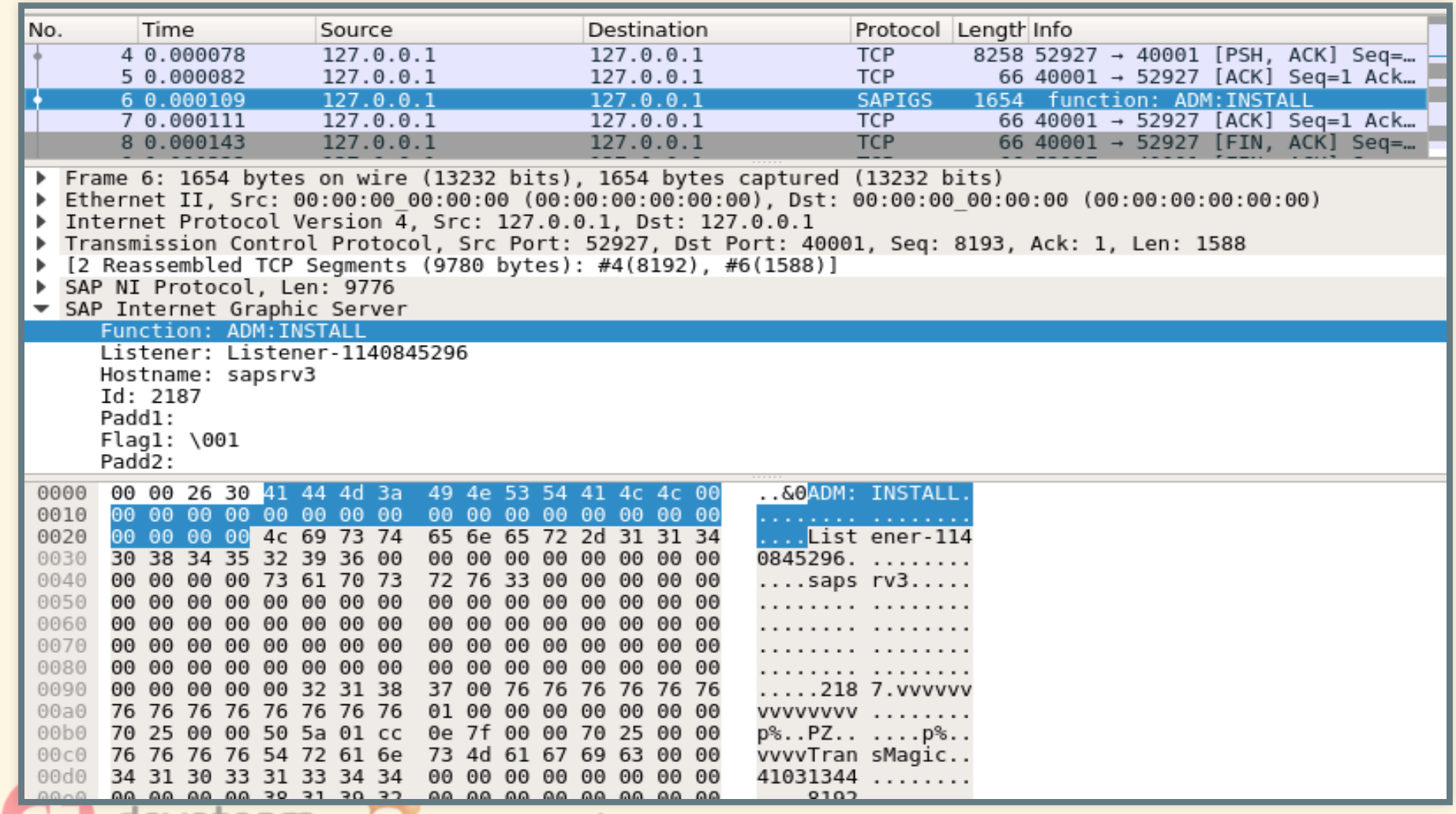
- Code un peu compliqué
- Beaucoup d'appels à d'autres fonctions
- Failed si on essaye de l'exécuter...

ADM:INSTALL : DEBUGGER ABAP

- Un système SAP fourni en standard un environnement de développement
- Donc avec un debugger...


root@sapigs:/usr/sap/NPL/D00/igs/data# _
User
System
Help
SAP
New password
Client
100
User
Password
Logon Language
root@sapigs:~# _

ADM:INSTALL : PACKET IGS



No.	Time	Source	Destination	Protocol	Length	Info
4	0.000078	127.0.0.1	127.0.0.1	TCP	8258	52927 → 40001 [PSH, ACK] Seq=…
5	0.000082	127.0.0.1	127.0.0.1	TCP	66	40001 → 52927 [ACK] Seq=1 Ack…
6	0.000109	127.0.0.1	127.0.0.1	SAPIGS	1654	function: ADM:INSTALL
7	0.000111	127.0.0.1	127.0.0.1	TCP	66	40001 → 52927 [ACK] Seq=1 Ack…
8	0.000143	127.0.0.1	127.0.0.1	TCP	66	40001 → 52927 [FIN, ACK] Seq=…

```
▸ Frame 6: 1654 bytes on wire (13232 bits), 1654 bytes captured (13232 bits)
▸ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
▸ Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
▸ Transmission Control Protocol, Src Port: 52927, Dst Port: 40001, Seq: 8193, Ack: 1, Len: 1588
▸ [2 Reassembled TCP Segments (9780 bytes): #4(8192), #6(1588)]
▸ SAP NI Protocol, Len: 9776
▾ SAP Internet Graphic Server
    Function: ADM:INSTALL
    Listener: Listener-1140845296
    Hostname: sapsrv3
    Id: 2187
    Padd1:
    Flag1: \001
    Padd2:
```

```
0000  00 00 26 30 41 44 4d 3a  49 4e 53 54 41 4c 4c 00   ..&0ADM: INSTALL.
0010  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0020  00 00 00 00 4c 69 73 74  65 6e 65 72 2d 31 31 34   ....List ener-114
0030  30 38 34 35 32 39 36 00  00 00 00 00 00 00 00 00   0845296. ........
0040  00 00 00 00 73 61 70 73  72 76 33 00 00 00 00 00   ....saps rv3.....
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0090  00 00 00 00 00 32 31 38  37 00 76 76 76 76 76 76   .....218 7.vvvvvv
00a0  76 76 76 76 76 76 76 76  01 00 00 00 00 00 00 00   vvvvvvvv ........
00b0  70 25 00 00 50 5a 01 cc  0e 7f 00 00 70 25 00 00   p%..PZ.. ....p%..
00c0  76 76 76 76 54 72 61 6e  73 4d 61 67 69 63 00 00   vvvvTran sMagic..
00d0  34 31 30 33 31 33 34 34  00 00 00 00 00 00 00 00   41031344 ........
00e0  00 00 00 00 38 31 39 32  00 00 00 00 00 00 00 00       8192 ........
```

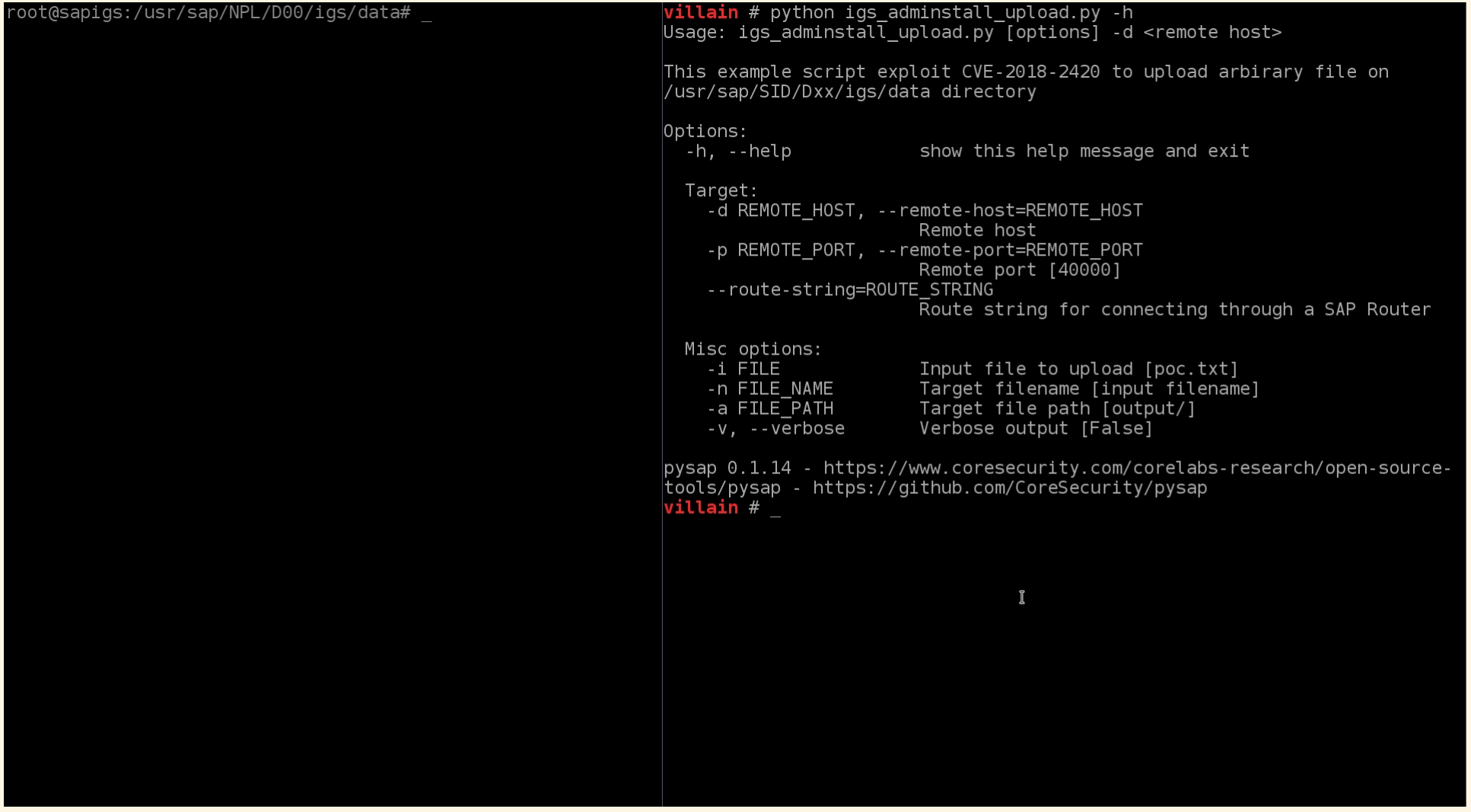
devoteam onapsis

ADM:INSTALL : PACKET IGS

- Si nous renvoyons ce packet sur le port 40000
- Les fichiers shapefiles sont aussi créés...
- ... a distance, sans être authentifié sur SAP

SOMMAIRE

- SAP ?
- SAP IGS ?
- Protocole IGS
- Outils
- ADM:INSTALL
- Vulnérabilités
- Conclusion

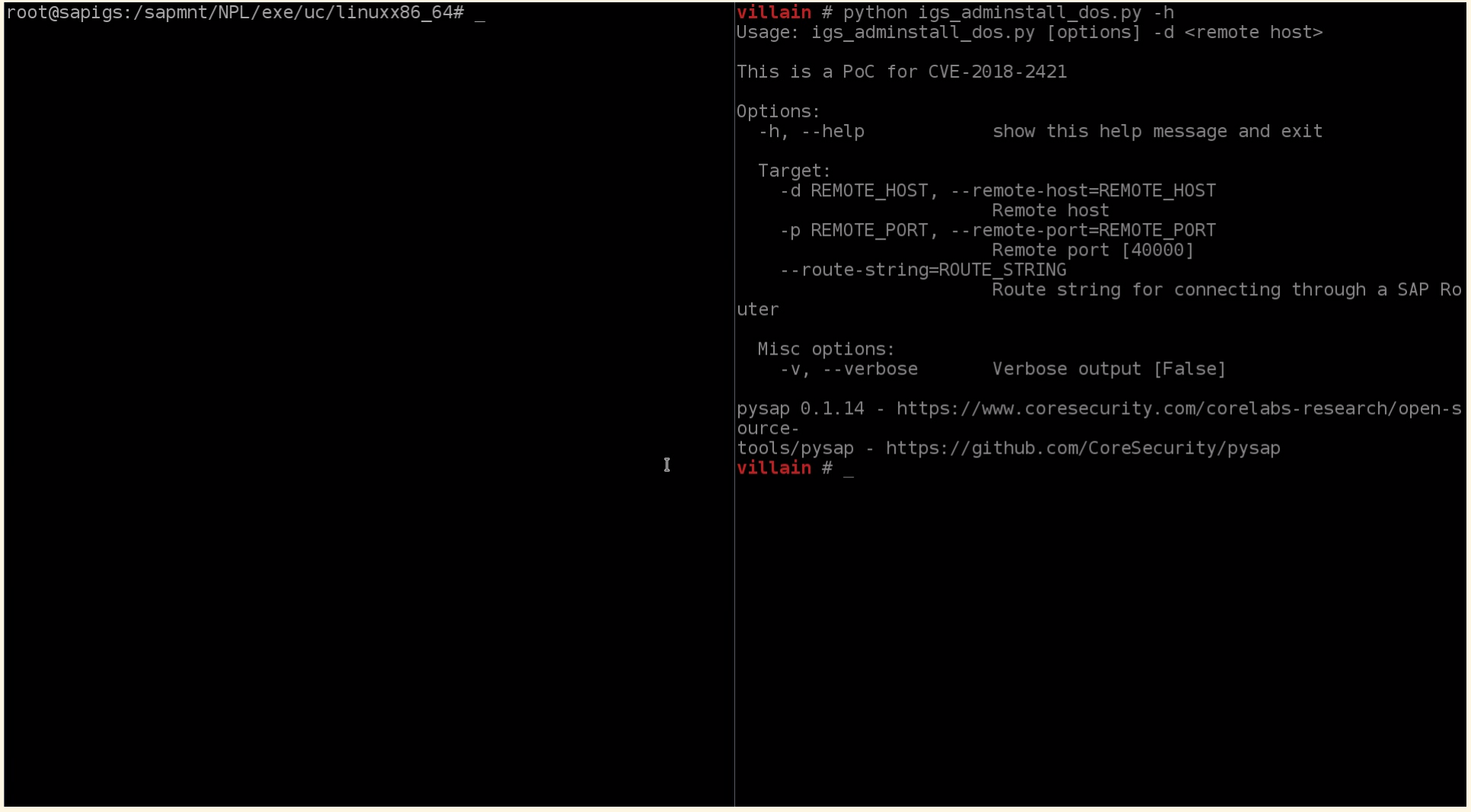


devoteam onapsis

VULNÉRABILITÉS : TÉLÉDÉCHARGEMENT DE FICHIERS

2615635 - [CVE-2018-2420] Unrestricted File Upload in SAP Internet Graphics Server (IGS)

igs/pw/install = disable



devoteam onapsis

VULNÉRABILITÉS : DÉNI DE SERVICE

2616599 - [CVE-2018-2421] Denial of Service in SAP Internet Graphics Server (IGS) Portwatcher

SOMMAIRE

- SAP ?
- SAP IGS ?
- Protocole IGS
- Outils
- ADM:INSTALL
- Vulnérabilités
- Conclusion

CONCLUSION

- Propriétaire != sécurisé
- Pas si compliqué que ça
- Reverse, network, ABAP, python, web...

- SAP https://www.sap.com/corporate/en/company.html
- SAP IGS online help IGS SAP Help
- SAP Security notes 2525222, 2538829, 2615635, 2616599
- gdb peda https://github.com/longld/peda
- PySAP https://github.com/CoreSecurity/pysap
- SAP-Dissection https://github.com/CoreSecurity/SAP-Dissection-plug-in-for-Wireshark
- Devoteam https://www.cert-devoteam.fr/
- Onapsis https://www.onapsis.com

MERCI !

ygenuer [\x40] onapsis.com

alexandre.bolle.reddat [\x40] devoteam.com