

Sprint 2

TREMOULET BRETON Loan

JACQUEMIN Paul

SALA-MOCHIZUKI Yûki

VACHALDE Rémi

AUXILIEN Katia

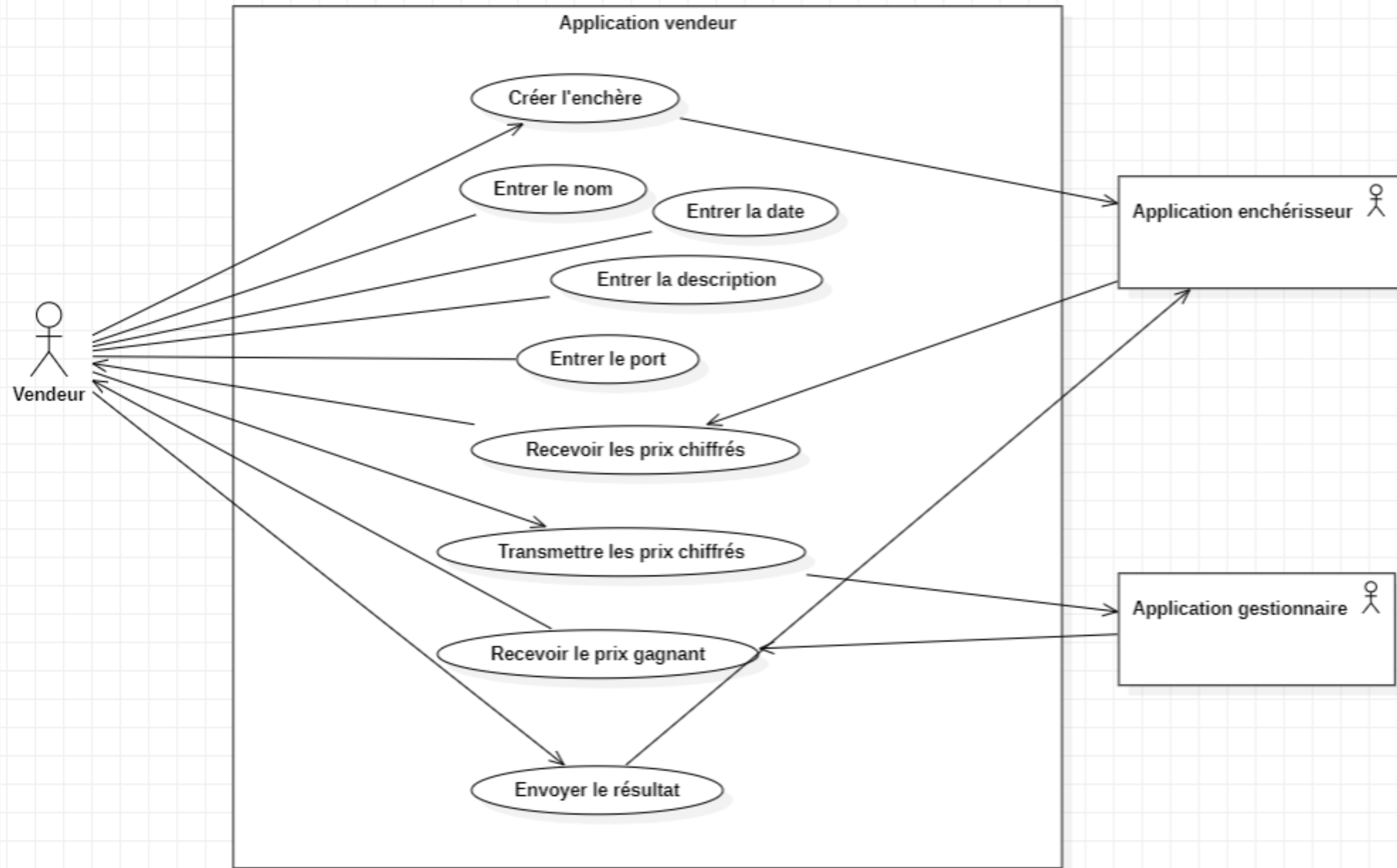
Mise en contexte

Pour le Sprint 2, nous devions :

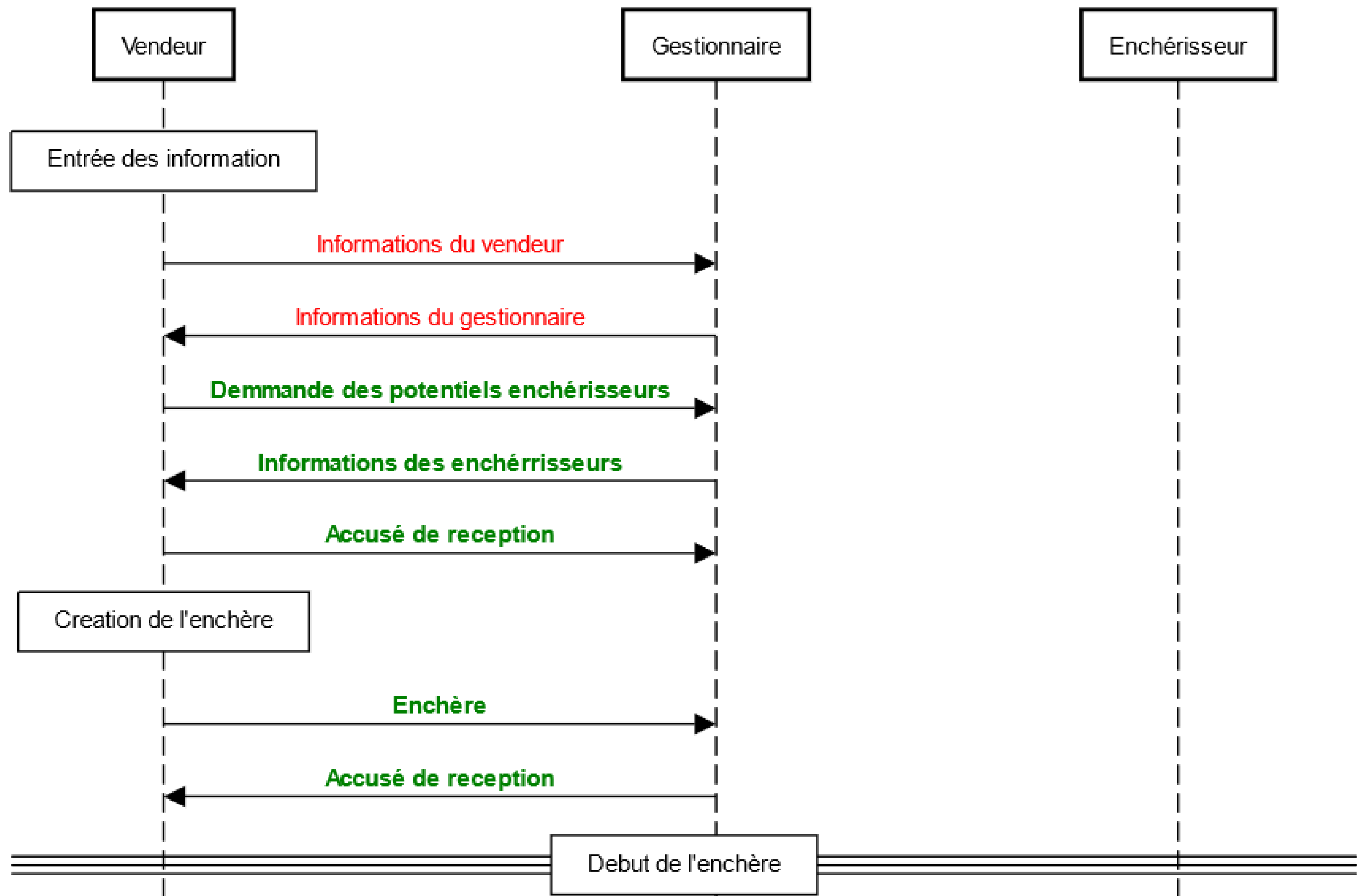
- Intégrer les signatures cryptographiques.
- Trouver une faille de la version sprint 1.
- *Éventuellement, intégrer des sockets sécurisés.*

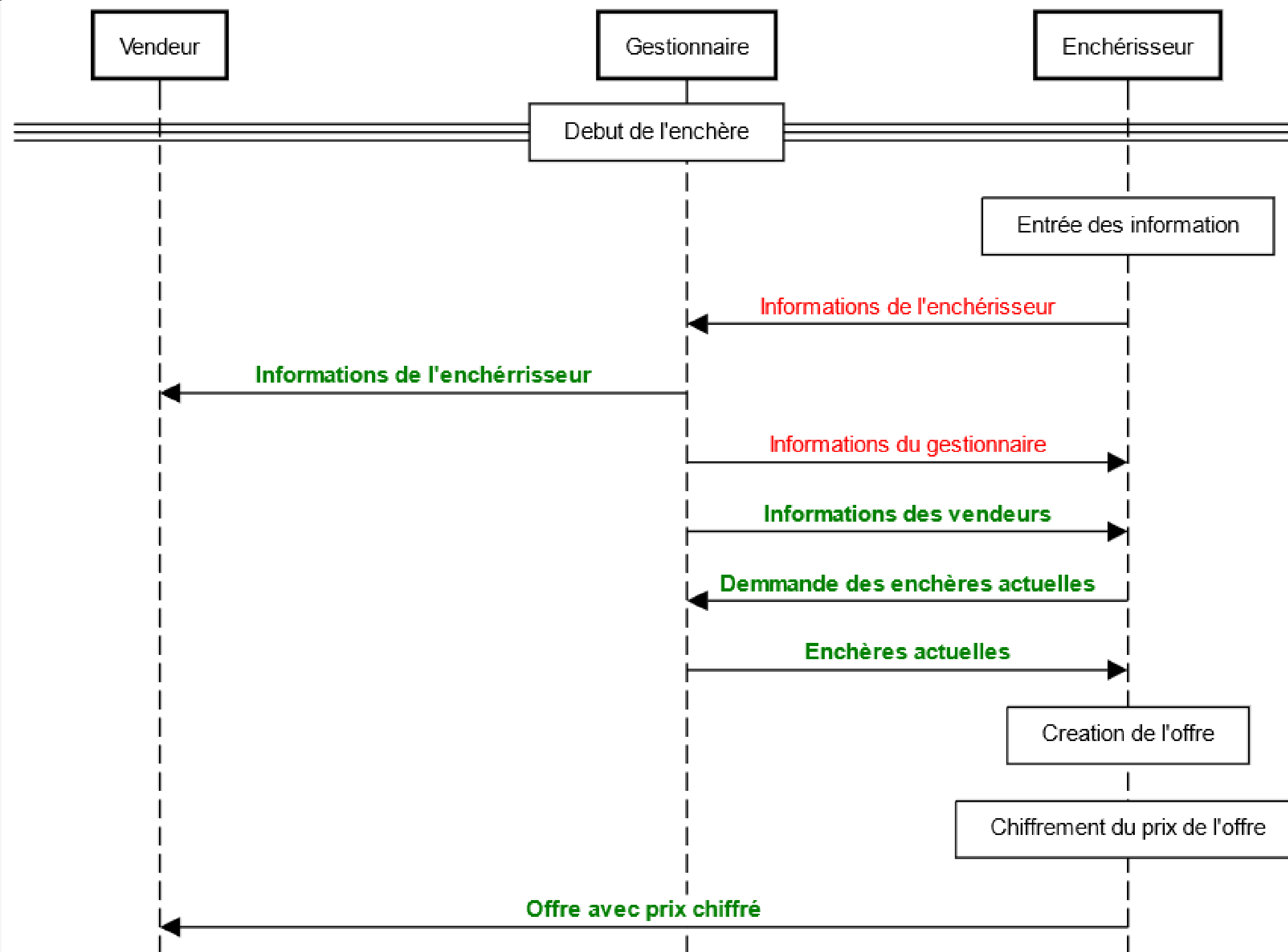
Proposition de nom

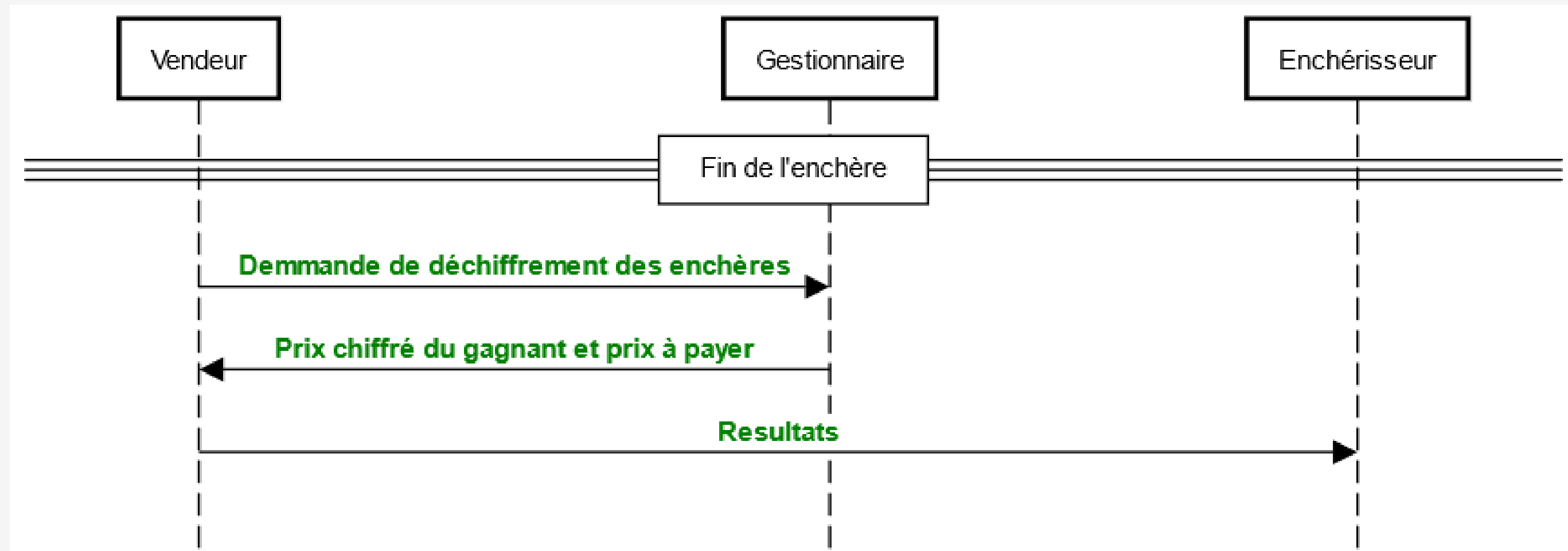
SecureWin



Échanges







Démo. Intrusion (Wireshark)

```
Paul
Quel port voulez-vous utiliser ? (49152 à 65535)
50000
Bienvenue!
Enchère Actuelle :
Nom : Test
Date de création : 2023-11-22
Description : Test.
Date de fin : 2023-11-22T23:05.

Quel est votre prix ?
1
```

```
Jacques
Quel port voulez-vous utiliser ? (49152 à 65535)
500001
Port invalide, entrez un port valide (entre 49152 et 65535) :
50001
Bienvenue!
Enchère Actuelle :
Nom : Test
Date de création : 2023-11-22
Description : Test.
Date de fin : 2023-11-22T23:05.

Quel est votre prix ?
2
```

```
Lancement de l'enchère ...
Reception des prix ...
Traitement des prix :
[1.0, 2.0]
1.0
```



tcp.port == 50001 || tcp.port == 50000 || tcp.port == 24682

No.	Time	Source	Destination	Protocol	Length	Info
7959	110.844398627	192.168.145.91	192.168.145.91	TCP	68	46964 → 50000 [PSH, ACK] Seq=587 Ack=1 Win=33280 Len=2 TSval=4029849783 TSecr=4029849783
7960	110.844400047	192.168.145.91	192.168.145.91	TCP	66	50000 → 46964 [ACK] Seq=1 Ack=589 Win=33024 Len=0 TSval=4029849783 TSecr=4029849783
7961	110.844409597	192.168.145.91	192.168.145.91	TCP	68	46964 → 50000 [PSH, ACK] Seq=589 Ack=1 Win=33280 Len=2 TSval=4029849783 TSecr=4029849783
7962	110.844411137	192.168.145.91	192.168.145.91	TCP	66	50000 → 46964 [ACK] Seq=1 Ack=591 Win=33024 Len=0 TSval=4029849783 TSecr=4029849783
7963	110.844418517	192.168.145.91	192.168.145.91	TCP	73	46964 → 50000 [PSH, ACK] Seq=591 Ack=1 Win=33280 Len=7 TSval=4029849783 TSecr=4029849783
7964	110.844419967	192.168.145.91	192.168.145.91	TCP	66	50000 → 46964 [ACK] Seq=1 Ack=598 Win=33024 Len=0 TSval=4029849783 TSecr=4029849783
7965	110.844434477	192.168.145.91	192.168.145.91	TCP	73	46964 → 50000 [PSH, ACK] Seq=598 Ack=1 Win=33280 Len=7 TSval=4029849783 TSecr=4029849783
7966	110.844435927	192.168.145.91	192.168.145.91	TCP	66	50000 → 46964 [ACK] Seq=1 Ack=605 Win=33024 Len=0 TSval=4029849783 TSecr=4029849783
7967	110.844445327	192.168.145.91	192.168.145.91	TCP	68	46964 → 50000 [PSH, ACK] Seq=605 Ack=1 Win=33280 Len=2 TSval=4029849783 TSecr=4029849783
7968	110.844446777	192.168.145.91	192.168.145.91	TCP	66	50000 → 46964 [ACK] Seq=1 Ack=607 Win=33024 Len=0 TSval=4029849783 TSecr=4029849783
7969	110.844454267	192.168.145.91	192.168.145.91	TCP	75	46964 → 50000 [PSH, ACK] Seq=607 Ack=1 Win=33280 Len=9 TSval=4029849783 TSecr=4029849783
7970	110.844455707	192.168.145.91	192.168.145.91	TCP	66	50000 → 46964 [ACK] Seq=1 Ack=616 Win=33024 Len=0 TSval=4029849783 TSecr=4029849783
7971	110.845223373	192.168.145.91	192.168.145.91	TCP	185	46964 → 50000 [PSH, ACK] Seq=616 Ack=1 Win=33280 Len=119 TSval=4029849784 TSecr=4029849783
7972	110.845225973	192.168.145.91	192.168.145.91	TCP	66	50000 → 46964 [ACK] Seq=1 Ack=735 Win=33024 Len=0 TSval=4029849784 TSecr=4029849784
7973	110.845317472	192.168.145.91	192.168.145.91	TCP	91	46964 → 50000 [PSH, ACK] Seq=735 Ack=1 Win=33280 Len=25 TSval=4029849784 TSecr=4029849784
7974	110.845319692	192.168.145.91	192.168.145.91	TCP	66	50000 → 46964 [ACK] Seq=1 Ack=760 Win=33024 Len=0 TSval=4029849784 TSecr=4029849784
7975	110.845373592	192.168.145.91	192.168.145.91	TCP	414	46964 → 50000 [PSH, ACK] Seq=760 Ack=1 Win=33280 Len=348 TSval=4029849784 TSecr=4029849784
7976	110.845375182	192.168.145.91	192.168.145.91	TCP	66	50000 → 46964 [ACK] Seq=1 Ack=1108 Win=32896 Len=0 TSval=4029849784 TSecr=4029849784
7977	110.845388082	192.168.145.91	192.168.145.91	TCP	95	46964 → 50000 [PSH, ACK] Seq=1108 Ack=1 Win=33280 Len=29 TSval=4029849784 TSecr=4029849784
7978	110.845418372	192.168.145.91	192.168.145.91	TCP	95	46964 → 50000 [FIN, PSH, ACK] Seq=1137 Ack=1 Win=33280 Len=29 TSval=4029849784 TSecr=4029849784
7979	110.849068673	192.168.145.91	192.168.145.91	TCP	95	[TCP Retransmission] 46964 → 50000 [FIN, PSH, ACK] Seq=1137 Ack=1 Win=33280 Len=29 TSval=4029849788 TSecr=4029849784
7980	110.849072943	192.168.145.91	192.168.145.91	TCP	78	50000 → 46964 [ACK] Seq=1 Ack=1167 Win=33152 Len=0 TSval=4029849788 TSecr=4029849784 SLE=1137 SRE=1167
7982	110.857162060	192.168.145.91	192.168.145.91	TCP	66	50000 → 46964 [FIN, ACK] Seq=1 Ack=1167 Win=33280 Len=0 TSval=4029849796 TSecr=4029849784
7983	110.857166540	192.168.145.91	192.168.145.91	TCP	66	46964 → 50000 [ACK] Seq=1167 Ack=2 Win=33280 Len=0 TSval=4029849796 TSecr=4029849796
8307	115.622884849	127.0.0.1	127.0.0.1	TCP	74	38320 → 24682 [SYN] Seq=0 Win=33280 Len=0 MSS=65495 SACK_PERM TSval=4265635723 TSecr=0 WS=128
8308	115.622890749	127.0.0.1	127.0.0.1	TCP	74	24682 → 38320 [SYN, ACK] Seq=0 Ack=1 Win=33280 Len=0 MSS=65495 SACK_PERM TSval=4265635723 TSecr=4265635723 WS=128
8309	115.622896399	127.0.0.1	127.0.0.1	TCP	66	38320 → 24682 [ACK] Seq=1 Ack=1 Win=33280 Len=0 TSval=4265635723 TSecr=4265635723
8310	115.622930869	127.0.0.1	127.0.0.1	TCP	70	38320 → 24682 [PSH, ACK] Seq=1 Ack=1 Win=33280 Len=4 TSval=4265635723 TSecr=4265635723
8311	115.622932729	127.0.0.1	127.0.0.1	TCP	66	24682 → 38320 [ACK] Seq=1 Ack=5 Win=33280 Len=0 TSval=4265635723 TSecr=4265635723
8312	115.622979748	127.0.0.1	127.0.0.1	TCP	244	38320 → 24682 [PSH, ACK] Seq=5 Ack=1 Win=33280 Len=178 TSval=4265635723 TSecr=4265635723
8313	115.622981608	127.0.0.1	127.0.0.1	TCP	66	24682 → 38320 [ACK] Seq=1 Ack=183 Win=33152 Len=0 TSval=4265635723 TSecr=4265635723
8314	115.622996978	127.0.0.1	127.0.0.1	TCP	68	38320 → 24682 [PSH, ACK] Seq=183 Ack=1 Win=33280 Len=2 TSval=4265635723 TSecr=4265635723
8315	115.622998358	127.0.0.1	127.0.0.1	TCP	66	24682 → 38320 [ACK] Seq=1 Ack=185 Win=33152 Len=0 TSval=4265635723 TSecr=4265635723
8316	115.623005128	127.0.0.1	127.0.0.1	TCP	70	38320 → 24682 [PSH, ACK] Seq=185 Ack=1 Win=33280 Len=4 TSval=4265635723 TSecr=4265635723
8317	115.623006548	127.0.0.1	127.0.0.1	TCP	66	24682 → 38320 [ACK] Seq=1 Ack=189 Win=33152 Len=0 TSval=4265635723 TSecr=4265635723
8318	115.623421716	127.0.0.1	127.0.0.1	TCP	182	38320 → 24682 [PSH, ACK] Seq=189 Ack=1 Win=33280 Len=116 TSval=4265635723 TSecr=4265635723
8319	115.623425196	127.0.0.1	127.0.0.1	TCP	66	24682 → 38320 [ACK] Seq=1 Ack=305 Win=33152 Len=0 TSval=4265635723 TSecr=4265635723
8320	115.623489346	127.0.0.1	127.0.0.1	TCP	92	38320 → 24682 [PSH, ACK] Seq=305 Ack=1 Win=33280 Len=26 TSval=4265635723 TSecr=4265635723
8321	115.623491196	127.0.0.1	127.0.0.1	TCP	66	24682 → 38320 [ACK] Seq=1 Ack=331 Win=33152 Len=0 TSval=4265635723 TSecr=4265635723

▶ Frame 8320: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface lo, id 0
▶ 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: 38320, Dst Port: 24682, Seq: 305, Ack: 1, Len: 26
▼ Data (26 bytes)
Data: 78707400045061756c757200025b42acf317f8060854e0020000
[Length: 26]

0000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00E.
0010 00 4e 9a 78 40 00 40 06 a2 2f 7f 00 00 01 7f 00 .N.x@.@. /.....
0020 00 01 95 b0 60 6a d3 9a e4 89 93 9f 96 6e 80 18`j.. ..n..
0030 01 04 fe 42 00 00 01 01 08 0a fe 40 6f 8b fe 40 ...B.... ..@o..@
0040 6f 8b 78 70 74 00 04 50 61 75 6c 75 72 00 02 5b o.xpt..P aulur.. [
0050 42 ac f3 17 f8 06 08 54 e0 02 00 00 B.....T



tcp.port == 50001 || tcp.port == 50000 || tcp.port == 24682

No.	Time	Source	Destination	Protocol	Length	Info
9972	138.227874278	192.168.145.91	192.168.145.91	TCP	66	50001 → 57002 [ACK] Seq=1 Ack=589 Win=33024 Len=0 TSval=4029877167 TSecr=4029877167
9973	138.227883068	192.168.145.91	192.168.145.91	TCP	68	57002 → 50001 [PSH, ACK] Seq=589 Ack=1 Win=33280 Len=2 TSval=4029877167 TSecr=4029877167
9974	138.227884348	192.168.145.91	192.168.145.91	TCP	66	50001 → 57002 [ACK] Seq=1 Ack=591 Win=33024 Len=0 TSval=4029877167 TSecr=4029877167
9975	138.227890768	192.168.145.91	192.168.145.91	TCP	73	57002 → 50001 [PSH, ACK] Seq=591 Ack=1 Win=33280 Len=7 TSval=4029877167 TSecr=4029877167
9976	138.227892108	192.168.145.91	192.168.145.91	TCP	66	50001 → 57002 [ACK] Seq=1 Ack=598 Win=33024 Len=0 TSval=4029877167 TSecr=4029877167
9977	138.227904498	192.168.145.91	192.168.145.91	TCP	73	57002 → 50001 [PSH, ACK] Seq=598 Ack=1 Win=33280 Len=7 TSval=4029877167 TSecr=4029877167
9978	138.227905818	192.168.145.91	192.168.145.91	TCP	66	50001 → 57002 [ACK] Seq=1 Ack=605 Win=33024 Len=0 TSval=4029877167 TSecr=4029877167
9979	138.227913938	192.168.145.91	192.168.145.91	TCP	68	57002 → 50001 [PSH, ACK] Seq=605 Ack=1 Win=33280 Len=2 TSval=4029877167 TSecr=4029877167
9980	138.227915228	192.168.145.91	192.168.145.91	TCP	66	50001 → 57002 [ACK] Seq=1 Ack=607 Win=33024 Len=0 TSval=4029877167 TSecr=4029877167
9981	138.227921478	192.168.145.91	192.168.145.91	TCP	75	57002 → 50001 [PSH, ACK] Seq=607 Ack=1 Win=33280 Len=9 TSval=4029877167 TSecr=4029877167
9982	138.227922728	192.168.145.91	192.168.145.91	TCP	66	50001 → 57002 [ACK] Seq=1 Ack=616 Win=33024 Len=0 TSval=4029877167 TSecr=4029877167
9983	138.227957238	192.168.145.91	192.168.145.91	TCP	185	57002 → 50001 [PSH, ACK] Seq=616 Ack=1 Win=33280 Len=119 TSval=4029877167 TSecr=4029877167
9984	138.227958538	192.168.145.91	192.168.145.91	TCP	66	50001 → 57002 [ACK] Seq=1 Ack=735 Win=33024 Len=0 TSval=4029877167 TSecr=4029877167
9985	138.227975638	192.168.145.91	192.168.145.91	TCP	91	57002 → 50001 [PSH, ACK] Seq=735 Ack=1 Win=33280 Len=25 TSval=4029877167 TSecr=4029877167
9986	138.227976908	192.168.145.91	192.168.145.91	TCP	66	50001 → 57002 [ACK] Seq=1 Ack=760 Win=33024 Len=0 TSval=4029877167 TSecr=4029877167
9987	138.228007267	192.168.145.91	192.168.145.91	TCP	414	57002 → 50001 [PSH, ACK] Seq=760 Ack=1 Win=33280 Len=348 TSval=4029877167 TSecr=4029877167
9988	138.228008687	192.168.145.91	192.168.145.91	TCP	66	50001 → 57002 [ACK] Seq=1 Ack=1108 Win=32896 Len=0 TSval=4029877167 TSecr=4029877167
9989	138.228021557	192.168.145.91	192.168.145.91	TCP	95	57002 → 50001 [PSH, ACK] Seq=1108 Ack=1 Win=33280 Len=29 TSval=4029877167 TSecr=4029877167
9990	138.228053207	192.168.145.91	192.168.145.91	TCP	95	57002 → 50001 [FIN, PSH, ACK] Seq=1137 Ack=1 Win=33280 Len=29 TSval=4029877167 TSecr=4029877167
9991	138.232399093	192.168.145.91	192.168.145.91	TCP	95	[TCP Retransmission] 57002 → 50001 [FIN, PSH, ACK] Seq=1137 Ack=1 Win=33280 Len=29 TSval=4029877171 TSecr=4029877167
9992	138.232403763	192.168.145.91	192.168.145.91	TCP	78	50001 → 57002 [ACK] Seq=1 Ack=1167 Win=32896 Len=0 TSval=4029877171 TSecr=4029877167 SLE=1137 SRE=1167
9993	138.234605351	192.168.145.91	192.168.145.91	TCP	66	50001 → 57002 [FIN, ACK] Seq=1 Ack=1167 Win=33280 Len=0 TSval=4029877174 TSecr=4029877167
9994	138.234609571	192.168.145.91	192.168.145.91	TCP	66	57002 → 50001 [ACK] Seq=1167 Ack=2 Win=33280 Len=0 TSval=4029877174 TSecr=4029877174
10707	148.334695383	127.0.0.1	127.0.0.1	TCP	74	49640 → 24682 [SYN] Seq=0 Win=33280 Len=0 MSS=65495 SACK_PERM TSval=4265668435 TSecr=0 WS=128
10708	148.334701503	127.0.0.1	127.0.0.1	TCP	74	24682 → 49640 [SYN, ACK] Seq=0 Ack=1 Win=33280 Len=0 MSS=65495 SACK_PERM TSval=4265668435 TSecr=4265668435 WS=128
10709	148.334707553	127.0.0.1	127.0.0.1	TCP	66	49640 → 24682 [ACK] Seq=1 Ack=1 Win=33280 Len=0 TSval=4265668435 TSecr=4265668435
10710	148.334744602	127.0.0.1	127.0.0.1	TCP	70	49640 → 24682 [PSH, ACK] Seq=1 Ack=1 Win=33280 Len=4 TSval=4265668435 TSecr=4265668435
10711	148.334746982	127.0.0.1	127.0.0.1	TCP	66	24682 → 49640 [ACK] Seq=1 Ack=5 Win=33280 Len=0 TSval=4265668435 TSecr=4265668435
10712	148.334795672	127.0.0.1	127.0.0.1	TCP	244	49640 → 24682 [PSH, ACK] Seq=5 Ack=1 Win=33280 Len=178 TSval=4265668435 TSecr=4265668435
10713	148.334797692	127.0.0.1	127.0.0.1	TCP	66	24682 → 49640 [ACK] Seq=1 Ack=183 Win=33152 Len=0 TSval=4265668435 TSecr=4265668435
10714	148.334814302	127.0.0.1	127.0.0.1	TCP	68	49640 → 24682 [PSH, ACK] Seq=183 Ack=1 Win=33280 Len=2 TSval=4265668435 TSecr=4265668435
10715	148.334815792	127.0.0.1	127.0.0.1	TCP	66	24682 → 49640 [ACK] Seq=1 Ack=185 Win=33152 Len=0 TSval=4265668435 TSecr=4265668435
10716	148.334822952	127.0.0.1	127.0.0.1	TCP	70	49640 → 24682 [PSH, ACK] Seq=185 Ack=1 Win=33280 Len=4 TSval=4265668435 TSecr=4265668435
10717	148.334824552	127.0.0.1	127.0.0.1	TCP	66	24682 → 49640 [ACK] Seq=1 Ack=189 Win=33152 Len=0 TSval=4265668435 TSecr=4265668435
10718	148.335251220	127.0.0.1	127.0.0.1	TCP	182	49640 → 24682 [PSH, ACK] Seq=189 Ack=1 Win=33280 Len=116 TSval=4265668435 TSecr=4265668435
10719	148.335254499	127.0.0.1	127.0.0.1	TCP	66	24682 → 49640 [ACK] Seq=1 Ack=305 Win=33152 Len=0 TSval=4265668435 TSecr=4265668435
10720	148.335321339	127.0.0.1	127.0.0.1	TCP	95	49640 → 24682 [PSH, ACK] Seq=305 Ack=1 Win=33280 Len=29 TSval=4265668435 TSecr=4265668435
10721	148.335323279	127.0.0.1	127.0.0.1	TCP	66	24682 → 49640 [ACK] Seq=1 Ack=334 Win=33152 Len=0 TSval=4265668435 TSecr=4265668435
10722	148.335340209	127.0.0.1	127.0.0.1	TCP	334	49640 → 24682 [PSH, ACK] Seq=334 Ack=1 Win=33280 Len=268 TSval=4265668435 TSecr=4265668435

Frame 10720: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interface lo, id 0
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: 49640, Dst Port: 24682, Seq: 305, Ack: 1, Len: 29
Data (29 bytes)

Data: 78707400074a616371756573757200025b42acf317f8060854e0020000
[Length: 29]

```
0000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00  .....E.
0010  00 51 94 e4 40 00 40 06 a7 c0 7f 00 00 01 7f 00  ..Q..@.e. ....
0020  00 01 c1 e8 60 6a a0 37 66 12 2a 51 b4 2e 80 18  ....`j.7 f.*Q...
0030  01 04 fe 45 00 00 01 01 08 0a fe 40 ef 53 fe 40  ...E.....@.S.@
0040  ef 53 78 70 74 00 07 4a 61 63 71 75 65 73 75 72  .Sxpt..J acquesur
0050  00 02 5b 42 ac f3 17 f8 06 08 54 e0 02 00 00  ...[B.....T....
```

Merci de votre attention !