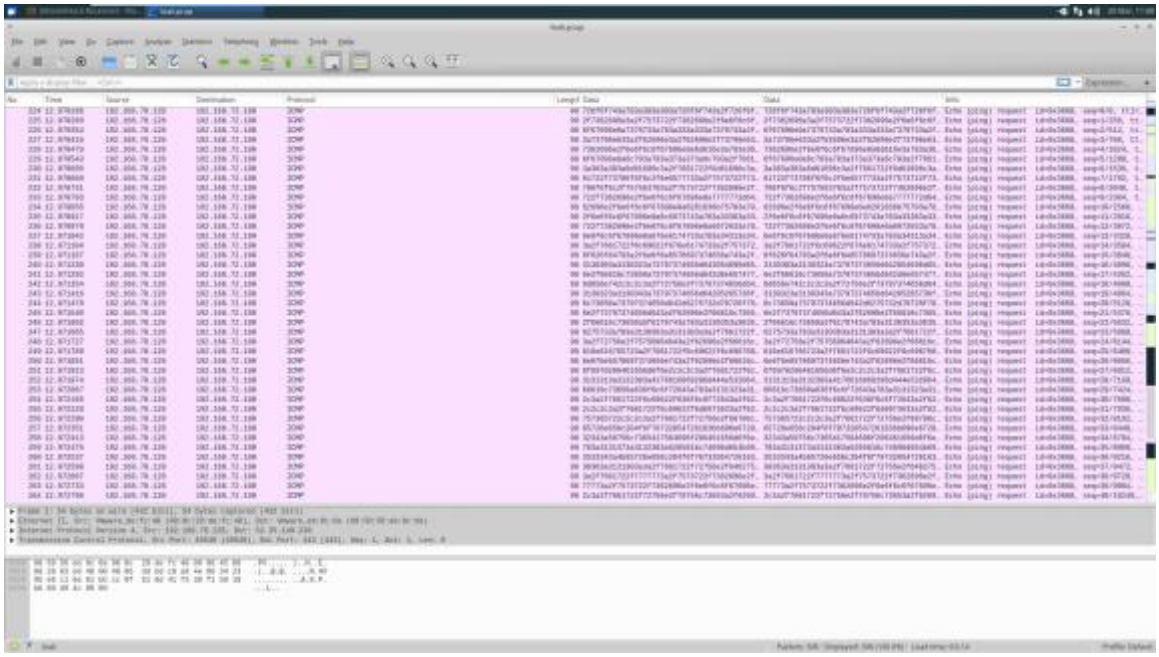
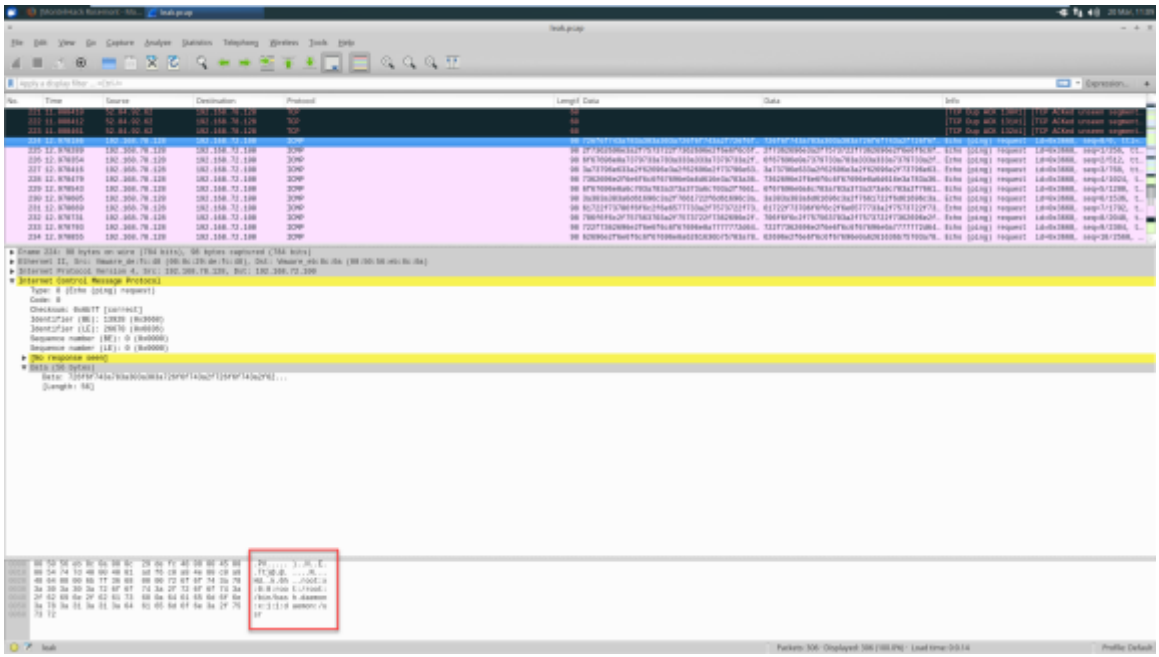
Exfiltration

Nous avons devant nous un pcap contenant un échange particulier

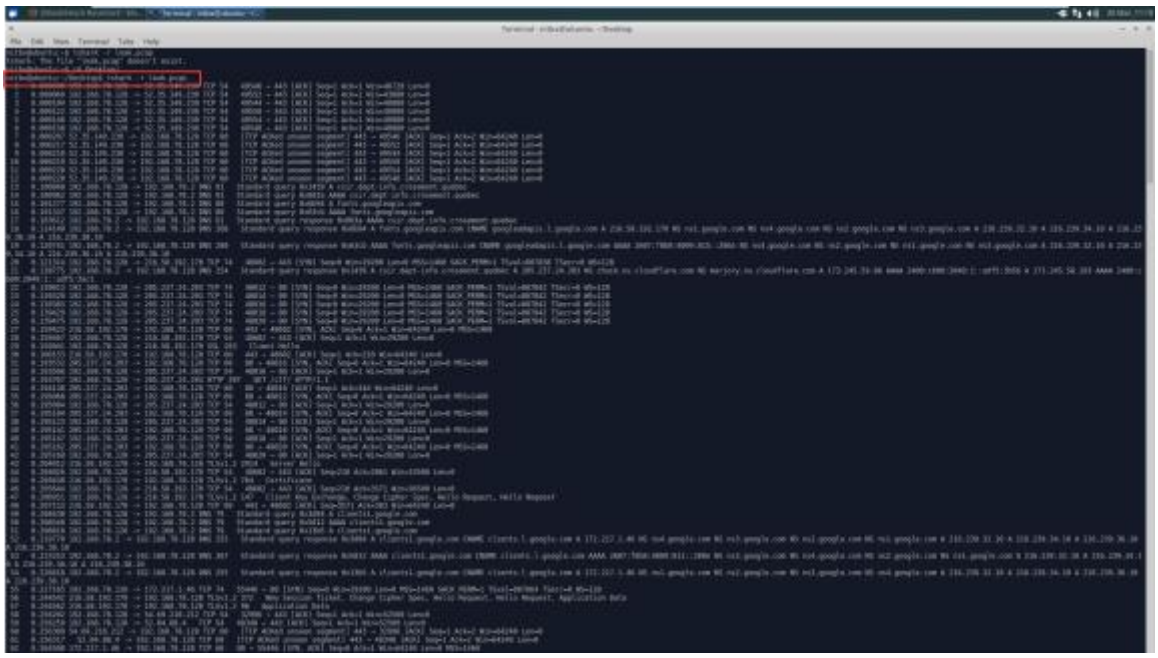




En effet, nous pouvons remarquer plusieurs ping ayant été envoyés à un hôte distant contenant un data inhabituel

Utilisons tshark pour filtrer le tout !

```
~/Desktop$ tshark -r leak.pcap
```



Spécifions le champ data !

```
tshark -r leak.pcap  -T fields -e data
```


```
726f6f743a783a303a303a726f6f743a2f726f6f743a2f62696e2f626173680a6461656d6f6e3a783a313a313a6461656d6f6e3a2f757372
2f7362696e3a2f7573722f7362696e2f6e6f6c6f67696e0a62696e3a783a323a323a62696e3a2f62696e3a2f7573722f7362696e2f6e6f6c
6f67696e0a7379733a783a333a333a7379733a2f6465763a2f7573722f7362696e2f6e6f6c6f67696e0a73796e633a783a343a3635353334
3a73796e633a2f62696e3a2f62696e2f73796e630a67616d65733a783a353a36303a67616d65733a2f7573722f67616d65733a2f7573722f
7362696e2f6e6f6c6f67696e0a6d616e3a783a363a31323a6d616e3a2f7661722f636163686652f6d616e3a2f7573722f7362696e2f6e6f6c
6f67696e0a6c703a783a373a373a6c703a2f7661722f73706f6f6c2f6c70643a2f7573722f7362696e2f6e6f6c6f67696e0a6d61696c3a78
3a383a383a6d61696c3a2f7661722f6d61696c3a2f7573722f7362696e2f6e6f6c6f67696e0a6e6577733a783a393a393a6e6577733a2f76
61722f73706f6f6c2f6e6577733a2f7573722f7362696e2f6e6f6c6f67696e0a757563703a783a31303a31303a757563703a2f7661722f73
706f6f6c2f757563703a2f7573722f7362696e2f6e6f6c6f67696e0a70726f78793a783a31333a31333a70726f78793a2f62696e3a2f7573
722f7362696e2f6e6f6c6f67696e0a7777772d646174613a783a33333a33333a7777772d646174613a2f7661722f7777773a2f7573722f73
62696e2f6e6f6c6f67696e0a6261636b75703a783a33343a33343a6261636b75703a2f7661722f6261636b7570733a2f7573722f7362696e
2f6e6f6c6f67696e0a6c6973743a783a33383a33383a4d61696c696e67204c697374204d616e616765723a2f7661722f6c6973743a2f7573
722f7362696e2f6e6f6c6f67696e0a6972633a783a33393a33393a697263643a2f7661722f72756e2f697263643a2f7573722f7362696e2f
6e6f6c6f67696e0a676e6174733a783a34313a34313a476e617473204275672d5265706f7274696e672053797374656d202861646d696e29
3a2f7661722f6c69622f676e6174733a2f7573722f7362696e2f6e6f6c6f67696e0a6e6f626f64793a783a36353533343a36353533343a6e
6f626f64793a2f6e6f6e6578697374656e743a2f7573722f7362696e2f6e6f6c6f67696e0a737973746d642d74696d6573796e633a783a
3130303a3130323a737973746d642054696d652053796e6368726f6e697a6174696f6e2c2c2c3a2f72756e2f737973746d643a2f6269
6e2f66616c73650a737973746d642d6e6574776f726b3a783a3130313a3130333a737973746d64204e6574776f726b204d616e616765
6d656e742c2c2c3a2f72756e2f737973746d642f6e657469663a2f62696e2f66616c73650a737973746d642d7265736f6c76653a783a
3130323a3130343a737973746d64205265736f6c7665722c2c2c3a2f72756e2f737973746d642f7265736f6c76653a2f62696e2f6661
6c73650a737973746d642d6275732d70726f78793a783a3130333a3130353a737973746d64204275732050726f78792c2c2c3a2f7275
6e2f737973746d643a2f62696e2f66616c73650a7379736c6f673a783a3130343a3130383a3a2f686f6d652f7379736c6f673a2f62696e
2f66616c73650a5f6170743a783a3130353a36353533343a3a2f6e6f6e6578697374656e743a2f62696e2f66616c73650a6d657373616765
6275733a783a3130363a3131303a3a2f7661722f72756e2f646275733a2f62696e2f66616c73650a75756964643a783a3130373a3131313a
3a2f72756e2f75756964643a2f62696e2f66616c73650a6c69676874646d3a783a3130383a3131343a4c6967687420446973706c6179204d
616e616765723a2f7661722f6c69622f6c69676874646d3a2f62696e2f66616c73650a77686f6f707369653a783a3130393a3131363a3a2f
6e6f6e6578697374656e743a2f62696e2f66616c73650a61766168692d6175746f6970643a783a3131303a3131393a417661686920617574
6f6970206461656d6f6e2c2c2c3a2f7661722f6c69622f61766168692d6175746f6970643a2f62696e2f66616c73650a6166168693a783a
3131313a3132303a417661686920 6d444e53206461656d6f6e2c2c2c3a2f7661722f72756e2f61766168692d6461656d6f6e3a2f62696e2f
66616c73650a636f6c6f72643a783a3131323a3132333a636f6c6f726420636f6c6f7572206d616e6167656d656e74206461656d6f6e2c2c
2c3a2f7661722f6c69622f636f6c6f72643a2f62696e2f66616c73650a646e736d6173713a783a3131333a36353533343a646e736d617371
2c2c2c3a2f7661722f6c69622f6d6973633a2f62696e2f66616c73650a68706c69703a783a3131343a373a48504c4950207379737465 6d20
757365722c2c2c3a2f7661722f72756e2f68706c69703a2f62696e2f66616c73650a6b65726e6f6f70733a783a3131353a36353533343a4b
65726e656c204f6f707320547261636b696e67204461656d6f6e2c2c2c3a2f3a2f62696e2f66616c73650a70756c73653a783a3131363a31
32343a50756c7365417564696f206461656d6f6e2c2c2c3a2f7661722f72756e2f70756c73653a2f62696e2f66616c73650a72746b69743a
783a3131373a3132363a5265616c74696d654b69742c2c2c3a2f70726f633a2f62696e2f66616c73650a464c41472d3a783a3131353a3635
3533343a4b65726e656c204f6f707320547261636b696e67204461656d6f6e2c2c2c3a2f3a2f62696e2f66616c73650a69636d703a783a31
30363a3131303a3a2f7661722f72756e2f646275733a2f62696e2f66616c73650a7061726963693a783a33333a33333a7777772d646174613
3a2f7661722f7777773a2f7573722f7362696e2f6e6f6c6f67696e0a696d63703a783a33333a33333a7777772d646174613a2f7661722f77
77773a2f7573722f7362696e2f6e6f6c6f67696e0a7061726c613a783a3131363a3132343a50756c7365417564696f206461656d6f6e2c2c
2c3a2f7661722f72756e2f70756c73653a2f62696e2f66616c73650a7573626d75783a783a3131393a34363a7573626d7578206461656d6f
6e2c2c2c3a2f7661722f6c69622f7573626d75783a2f62696e2f66616c73650a737065636368 2d6469737061746865723a783a3132303a
32393a537065656368204469737061746865722c2c2c3a2f7661722f72756e2f737065656368 2d6469737061746865723a2f62696e2f
66616c73650a6e697462783a783a313030303a313030303a6e697462782c2c2c3a2f686f6d652f6e697462783a2f62696e2f626173680a00
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
```

Redirigeons le output de commande dans xdd qui va convertir le tout en ASCII

```
tshark -r leak.pcap  -T fields -e data | xxd -p -r
```

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
messagebus:x:106:110::/var/run/dbus:/bin/false
uuidd:x:107:111::/run/uuidd:/bin/false
lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:109:116::/nonexistent:/bin/false
avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
colord:x:112:123:colord colour management daemon,,,:/var/lib/colord:/bin/false
dnsmasq:x:113:65534:dnsmasq,,,:/var/lib/misc:/bin/false
hplip:x:114:7:HPLIP system user,,,:/var/run/hplip:/bin/false
kernoops:x:115:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false
pulse:x:116:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:x:117:126:RealtimeKit,,,:/proc:/bin/false
FLAG-i:x:115:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false
icmp:x:106:110::/var/run/dbus:/bin/false
paric:x:33:33:www-data:/var/www:/usr/sbin/nologin
impp:x:33:33:www-data:/var/www:/usr/sbin/nologin
parla:x:116:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false
usbmux:x:119:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
speech-dispatcher:x:120:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
nitbx:x:1000:1000:nitbx,,,:/home/nitbx:/bin/bash
nitbx@ubuntu:~/Desktop$
```

Et voilà !

FLAG-icppariciimpparla