

Installing the BTSYNC.lua dissector

1. Download the BTSYNC.lua script from the link:

<http://www.markscanlon.co/tools/BTSYNC.lua>

[Download the WireShark Dissector »](#) (right click, save link/target as...)

[Download the Proof-of-Concept Application »](#)

© Mark Scanlon 2014

2. Check that your version of Wireshark supports lua (any version after 0.99)

in wireshark: HELP > ABOUT > Wireshark TAB (tab 1)



Network Protocol Analyzer

Version 1.10.3 (SVN Rev 53022 from /trunk-1.10)

Copyright 1998-2013 Gerald Combs <gerald@wireshark.org> and contributors.
This is free software; see the source for copying conditions. There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

Compiled (64-bit) with GTK+ 2.24.14, with Cairo 1.10.2, with Pango 1.30.1, with
GLib 2.34.1, with WinPcap (4_1_3), with libz 1.2.5, without POSIX capabilities,
without libnl, with SMI 0.4.8, with c-ares 1.9.1, with Lua 5.1, without Python,
with GnuTLS 2.12.18, with Gcrypt 1.4.6, without Kerberos, with GeoIP, with
PortAudio V19-devel (built Nov 1 2013), with AirPcap.

here you can see the version just under the logo and the fact that Lua is included.

3. Find the Wireshark installation folder

Windows: C:\Program Files\Wireshark by default

OSX: ~/.wireshark/plugins

Linux: ~/share/wireshark

(default locations, your system may vary)

4. Save the dissector BTSYNC.lua into the same folder as the file init.lua (this is usually the root wireshark install folder)

NB. make a copy of init.lua as a backup

4. Edit init.lua and uncomment the line at the bottom for dtd_gen:

change:

```
--dofile(DATA_DIR.."dtd_gen.lua")
```

to

```
dofile(DATA_DIR.."BTSYNC.lua")
```

```
-- deprecated function names
datafile_path = Dir.global_config_path
persconffile_path = Dir.personal_config_path
```

```
dofile(DATA_DIR.."console.lua")
--dofile(DATA_DIR.."dtd_gen.lua")
```

or add a new line: `dofile(DATA_DIR.."BTSYNC.lua")` but be aware that windows newline characters may break the file so use a linux compatible editor. (such as Notepad++)

You may need Admin or Root permissions to access or make permanent changes to init.lua (for windows 7, run your editor as administrator)

Save init.lua

5. Start Wireshark and your dissector will be loaded at startup.

Open a saved PCAP file or start a live capture. BTSYNC packets will be identified as BTSYNC as well as their classification

BTSYNC KEEPALIVE

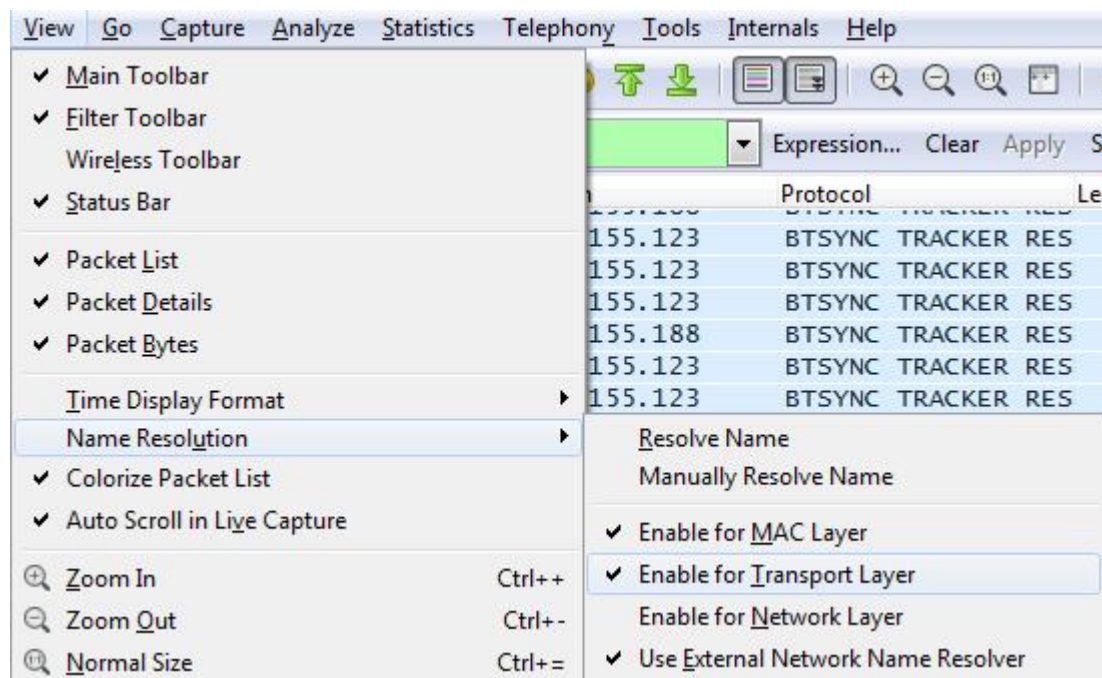
BTSYNC ACK

BTSYNC GET_PEERS

BTSYNC TRACKER RESPONSE

Optional Enhancement :

View --> name resolution --> untick "enable for transport layer"



this will stop wireshark from automatically resolving ports to protocols (hbci/remoteware for 3000 , sos for 3838, DIS as UDP 3000 etc) until the next time you start wireshark or re-enable the option in the menu.

To disable transport layer all the time edit the application preferences.