

SharkFest '16 Europe

HOWTO Contribute to #Wireshark

October 2016



#sf16eu

Alexis La Goutte
Network Engineer and Core-dev



- Alexis La Goutte (@alagoutte)

- Network Engineer @ Cheops
 - French integrator

- Contributor to Wireshark since 2008 (bug 2948)

- Core-dev since Avril 2011

- Author/contributor of HTTP2/QUIC/ieee80211/ISAKMP/Mongo...



CHEOPS TECHNOLOGY

The Cloud Customized For You !



How Contribute ?





Wireshark 2.2

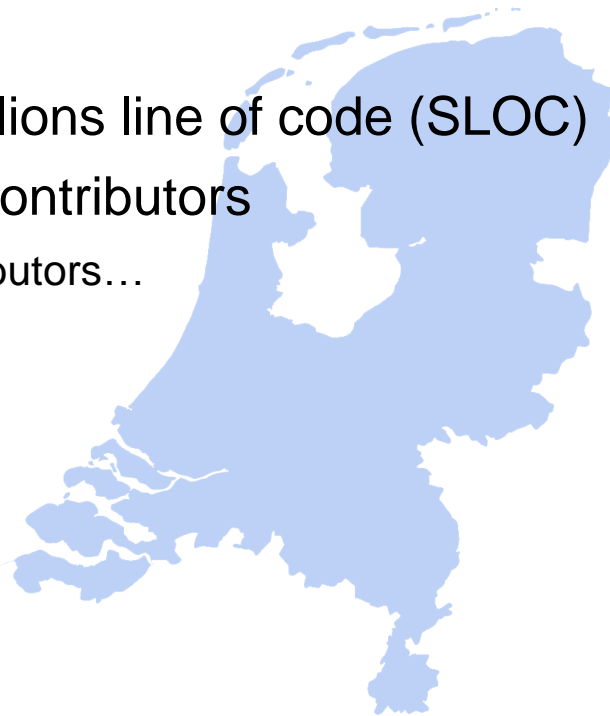
- for Wireshark 2.2.0 (since 2.0.0)
 - 4138 commits
 - from 221 contributors





Historic

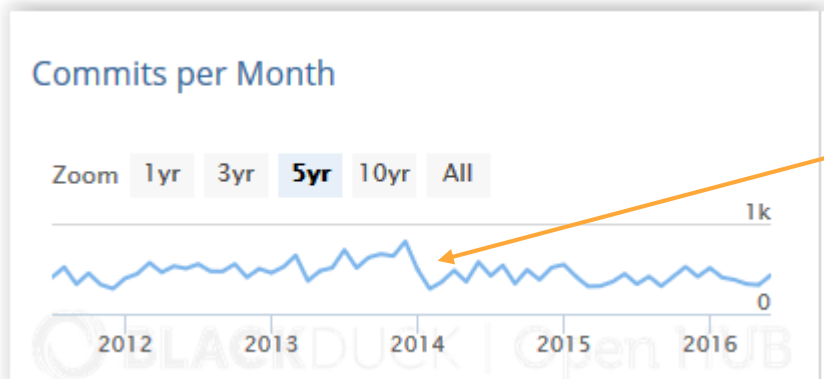
- **from start of project (1998)**
 - 65k commits
 - more than 2,5 millions line of code (SLOC)
 - more than 1200 contributors
 - but missing contributors...



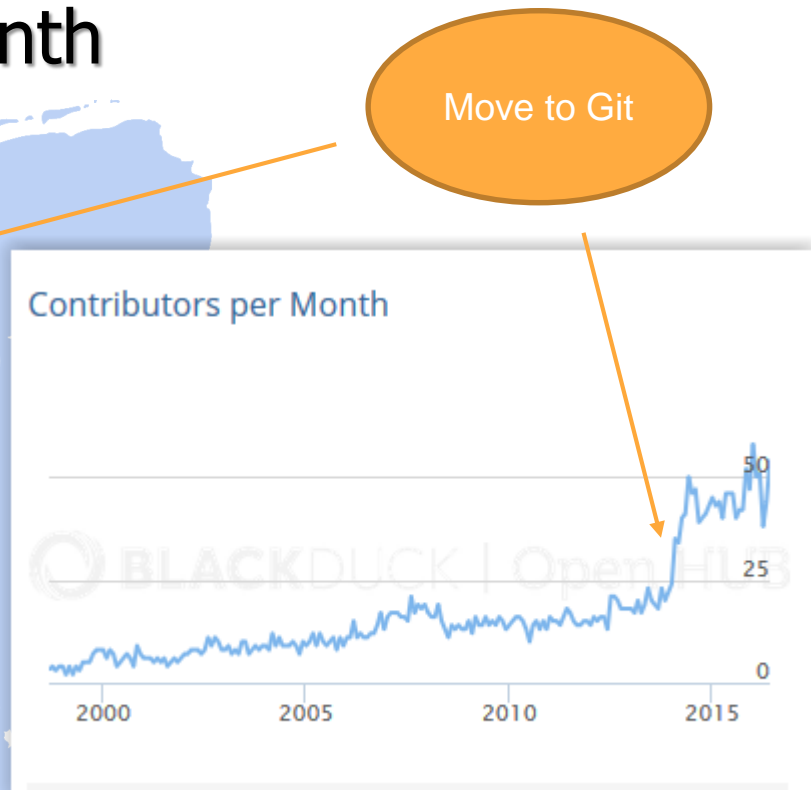


Actually

- More 300 commits by month



- New contributor every week
(look AUTHORS file !)



Move to Git



Contributors

- **Coming from everywhere**

- Network Vendor : Cisco, Juniper, Riverbed, HPE...
- Telecom Vendor: Qualcomm, Samsung, Ericsson, Nokia
- Big Internet company : Google, Facebook..
- University...

And individual people





Special Contributor (Core team)

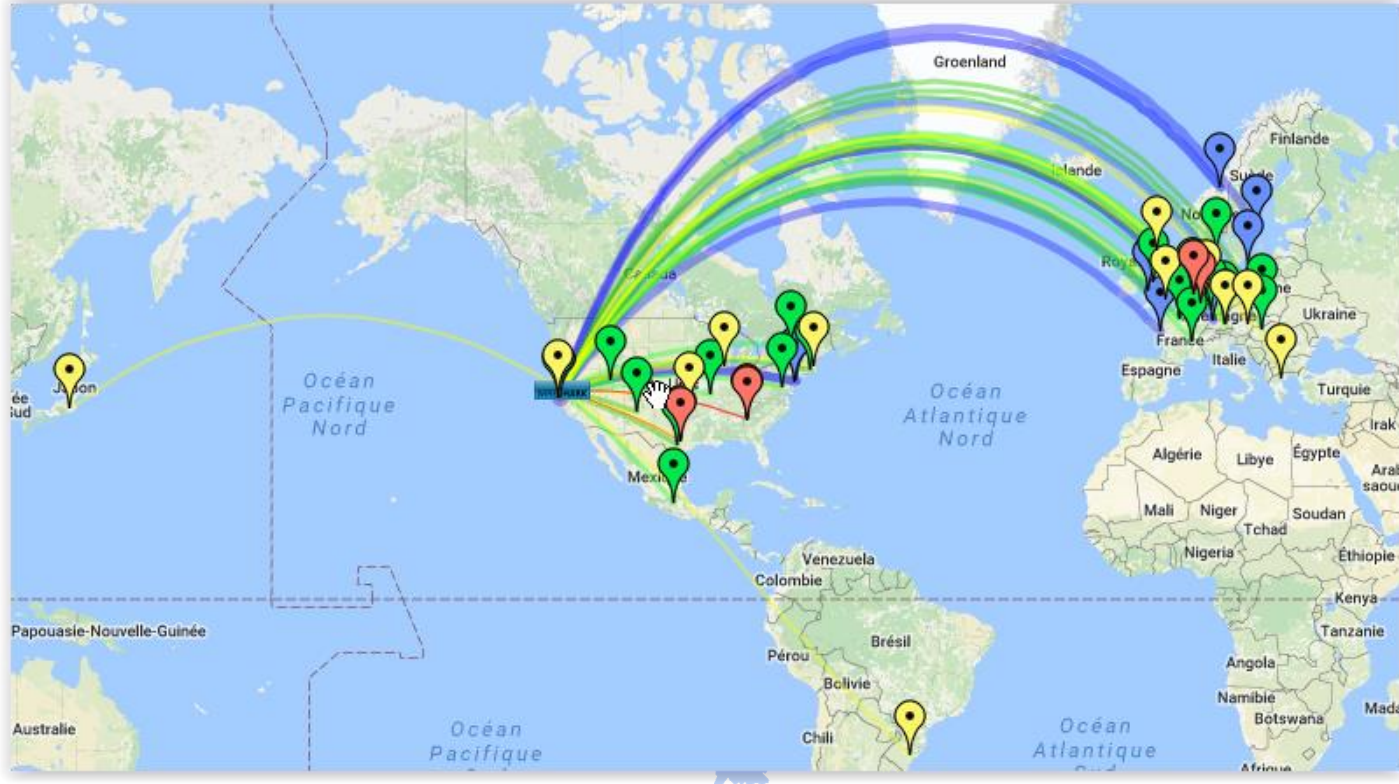
~ 50 peoples from
start of project

~ 20 « actives »





Special Contributor (Core team) : International Team !



SharkFest '16 Europe • Arnhem, Netherlands • October 17-19, 2016 • #sf16eu



Where Contribute ?



SharkFest '16 Europe • Arnhem, Netherlands • October 17-19, 2016 • #sf16eu



Wireshark on Social network

on Facebook

A screenshot of the Facebook group page for 'Wireshark'. The page features a blue header with the Facebook logo and a 'Sign Up' button. Below the header is a large blue banner with the word 'WIRESHARK' in white, stylized letters. To the left of the banner, it says 'Wireshark Public Group'. To the right, there is a 'Join Group' button. Below the banner, there are tabs for 'Discussion', 'Members', 'Events', 'Photos', and 'Files'. A search bar is located to the right of these tabs. At the bottom, there is a section for 'DESCRIPTION' which states: 'A Facebook group (created October 25 2010 by Nickelby Thane) for... See More'. There is also a '+ Join Group' button.

<https://facebook.com/groups/wireshark/>

SharkFest '16 Europe • Arnhem, Netherlands • October 17-19, 2016 • #sf16eu



Wireshark on Social network

- Facebook

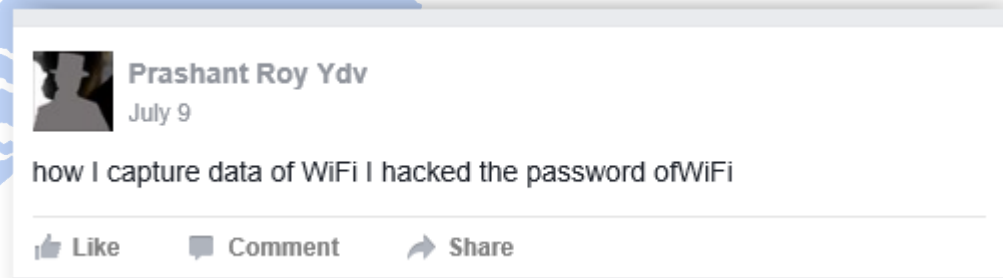


A screenshot of a Facebook post by Claudio Zenga. The post is dated October 9 at 2:19pm from Naples, Italy. The text of the post asks if anyone can explain why Wireshark doesn't find any TCP packets. Below the text are icons for Like, Comment, and Share.

Claudio Zenga
October 9 at 2:19pm · Naples, Italy

HLLO GUYS... ANYONE CAN SAY ME WHY MY WIRESHARK.. DON'T FIND ANY TCP PACKETS?

Like Comment Share



A screenshot of a Facebook post by Prashant Roy Ydv. The post is dated July 9. The text of the post claims to have hacked a WiFi password to capture data. Below the text are icons for Like, Comment, and Share.

Prashant Roy Ydv
July 9

how I capture data of WiFi I hacked the password ofWiFi

Like Comment Share



Wireshark on Social network

on Twitter

[@wiresharknews](https://twitter.com/wiresharknews)

WIRESHARK

TWEETS 460 FOLLOWING 21 FOLLOWERS 3,113 LIKES 6

[Follow](#)

Wireshark Foundation
@WiresharkNews

Official account of the Wireshark project, the world's foremost network protocol analyzer. Shared amongst several of the core team, but mostly @GeraldCombs.

Your Network
wireshark.org

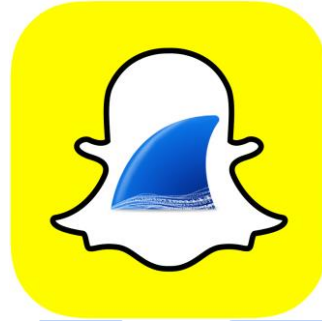
Wireshark Foundation @WiresharkNews · Jun 8
It is possible to add "SIP Custom Header" (Like HTTP) !
code.wireshark.org/review/15738 Thanks Pascal

<https://twitter.com/wiresharknews>



Not in...

No Wireshark snapchat



or Wireshark Instagram





ASK (Q&A)

- Questions and Answers about Wireshark

The screenshot shows the Wireshark Q&A website interface. At the top, there's a navigation bar with the Wireshark logo, a search bar, and buttons for 'Questions', 'Tags', 'Users', 'Badges', 'Unanswered', and 'Ask a Question'. Below the navigation bar, there's a list of questions. Each question entry includes the number of votes, answers, and views, the question title, tags, and the user who asked it along with the time ago. The questions listed are:

- Multi-threaded Tshark** (0 votes, 0 answers, 20 views) by hoangsonk49 71, 2 mins ago. Tag: multi-thread.
- How to find the ethernet dissector.** (0 votes, 1 answer, 29 views) by Anders • 4.3k, 38 mins ago. Tag: ethernet.
- Is Router Causing Latency** (0 votes, 0 answers, 38 views) by sindy 4.7k, 1 hour ago. Tags: latency, slowness.
- Reload capture when clicking on a custom Lua menu** (0 votes, 1 answer, 99 views) by TomLaBaude 51, 5 hours ago. Tag: lua.
- how to get/set pinfo.cols.xxx's value in lua, and how to add a column in pinfo?** (0 votes, 1 answer, 98 views) by Lekensteyn 1.5k, 12 hours ago. Tags: lua, columns, pinfo.

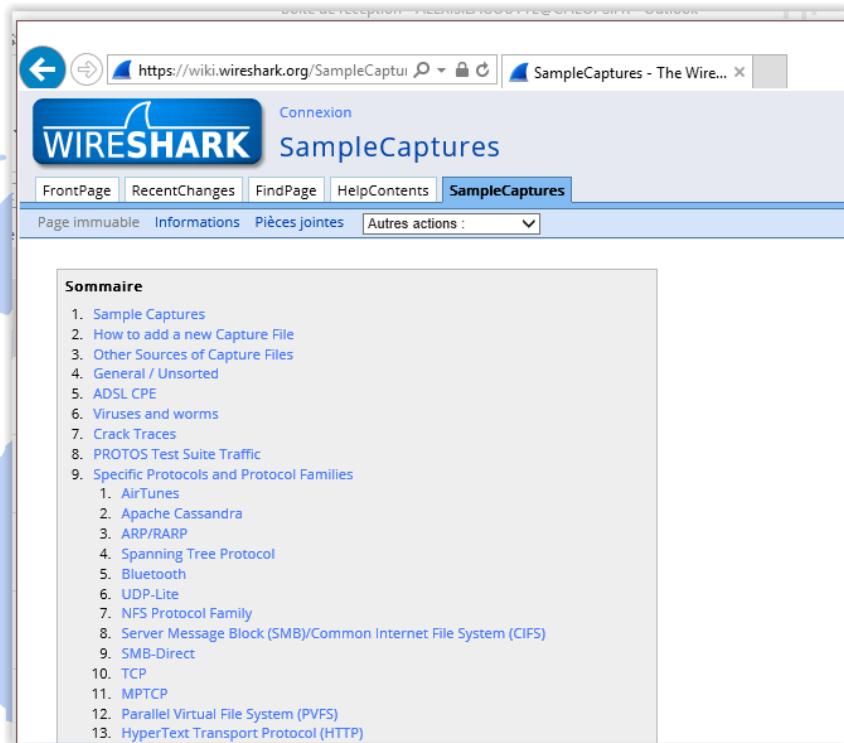
On the right side of the page, there's a 'Welcome to Wireshark Q&A' box with a brief description and links to 'about' and 'faq'. Below that, a statistics box shows '11876 Questions' and '12939 answers'.

<https://ask.wireshark.org>



- a (old) Wiki but there is always some good information

- Specialty the SampleCaptures page And Gerrit info

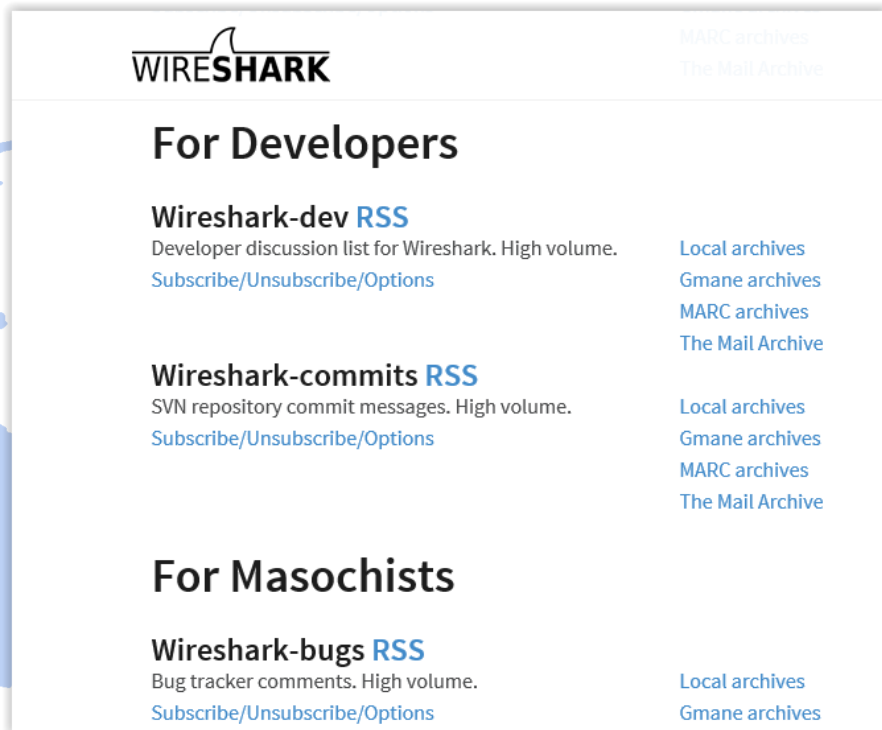


<https://wiki.wireshark.org>



Mailing List

- **Wireshark-users**
 - no very active (prefer Ask)
- **wireshark-dev**
 - About wireshark code
- **wireshark-commits**
 - Mail of each commit
- **wireshark-bugs**
 - Mail of each bugs..



The screenshot shows the Wireshark mailing list page. At the top left is the Wireshark logo. At the top right are links for "MARC archives" and "The Mail Archive". The page is divided into sections for "For Developers" and "For Masochists".

WIRESHARK

MARC archives
The Mail Archive

For Developers

Wireshark-dev [RSS](#)
Developer discussion list for Wireshark. High volume.
[Subscribe/Unsubscribe/Options](#)

[Local archives](#)
[Gmane archives](#)
[MARC archives](#)
[The Mail Archive](#)

Wireshark-commits [RSS](#)
SVN repository commit messages. High volume.
[Subscribe/Unsubscribe/Options](#)

[Local archives](#)
[Gmane archives](#)
[MARC archives](#)
[The Mail Archive](#)

For Masochists

Wireshark-bugs [RSS](#)
Bug tracker comments. High volume.
[Subscribe/Unsubscribe/Options](#)

[Local archives](#)
[Gmane archives](#)



For manage translations

The screenshot shows the Transifex web interface for the Wireshark project. The browser address bar displays the URL <https://www.transifex.com/wireshark/wireshark/dash>. The navigation menu includes 'transifex', 'Tableau de bord', 'Équipes', 'Rapports', 'Vos commandes', and 'Quoi de nouveau dans Transifex?'. On the right, there are links for 'Explorer', 'Aide', and 'Wireshark'. The main content area shows a summary: '28 langues de projet', '5 sans traducteurs', and '19 demandé'. Below this, a list of languages is displayed with their respective progress bars and status:

- Chinese (China) (zh_CN) 100% *prête à être utilisée*
- German (de) 100% *prête à être utilisée*
- Italian (it) 100% *prête à être utilisée*
- Polish (pl) 100% *prête à être utilisée*
- Japanese (Japan) (ja_JP) 96% 256 chaînes à traduire
- French (fr) 93% 562 chaînes à traduire
- Ukrainian (uk) 14% 7,131 chaînes à traduire
- Spanish (es) 7% 7,734 chaînes à traduire

A 'Create new project' button is visible in the dark sidebar on the left. At the bottom right of the dashboard, there is a link to 'Afficher toutes les langues'.

<https://www.transifex.com/wireshark>



HOW TO Contribute ?





Bugs (and feature)

- Use bugzilla

WIRESHARK Wireshark Bug Database – Main Page

Wireshark Home | New | Browse | Search | Search [?] | Reports | New Account | Log In | Forgot Password

File a Bug **Search** **Open a New Account** **All Open Bugs**

More Actions

- [Bugs requiring attention](#)
- [Most frequently reported bugs](#)
- [Summary reports and charts](#)

<https://bugs.wireshark.org>



Bug TODO list

- **for regression/bug**
 - How to reproduce the issue
 - a link to specification (it will be help often...)
 - Please attach a pcap (and **NOT** a screenshot)
- **for feature request (like new dissector)**
 - a link to specification (we are not magician)
 - a (or multiple) pcap(s) (and **NOT** a screenshot)



Make build environnement

- **Linux (more easy) :**

- can use debian-setup script (for debian family distro)
- can use rpm_for_devel (for rpm family distro)

- **macOS**

- can use macosx-setup script
- can use macos-setup-brew script (use HomeBrew)

- **Windows**

- Read documentation :

https://www.wireshark.org/docs/wsdg_html_chunked/ChSetupWin32.html



Official git mirror

But don't Accept Pull Request (PR)

Personal Open source Business Explore Pricing Blog Support This repository Search Sign in Sign up

wireshark / wireshark Watch 87 Star 565 Fork 291

Code Pull requests 0 Projects 0 Pulse Graphs

Read-only mirror of Wireshark's Git repository. GitHub won't let us disable pull requests. **THEY WILL BE IGNORED HERE** Please upload them at <https://code.wireshark.org/review/>.

64,863 commits 17 branches 458 releases 298 contributors GPL-2.0

Branch: master New pull request Find file Clone or download

Pascal Quantin CQL: free buffer earlier in case of Snappy decompression failure Latest commit 418b7d1 3 hours ago

.tx	Transifex: Add type of translation file	a year ago
capchild	cmake: make WERROR_COMMON_FLAGS a normal string	18 days ago
caputils	cmake: make WERROR_COMMON_FLAGS a normal string	18 days ago
cmake	CQL: add LZ4/Snappy decompression support on Windows	8 hours ago
codecs	CMake: Allow setting per target compiler warnings	2 months ago
debian	debian: Update lintian-overrides to cover updated manpages	8 hours ago

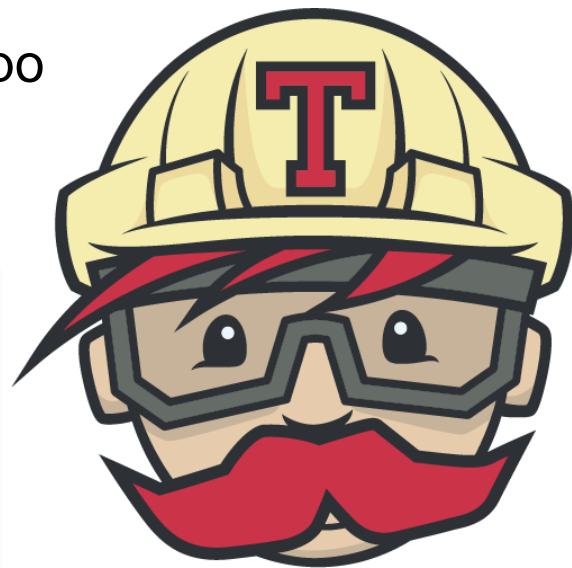
<https://github.com/wireshark/wireshark>



Travis

- **Build system from Github**

- Include a `.travis.yml` config file in Wireshark repo
- with already 5 jobs
 - clang/gcc/autotools/cmake and osx



Build Jobs		
🔔 # 183.1	🐙 </> Compiler: clang C++	📦 BUILD_CMAKE=no
🔔 # 183.2	🐙 </> Compiler: clang C++	📦 BUILD_CMAKE=yes
🔔 # 183.3	🐙 </> Compiler: gcc C++	📦 BUILD_CMAKE=no
🔔 # 183.4	🐙 </> Compiler: gcc C++	📦 BUILD_CMAKE=yes
🔔 # 183.5	🍏 </> Compiler: clang C++	📦 BUILD_CMAKE=yes



Gerrit

- the Official Git repo : use for code review

The screenshot shows the Gerrit web interface for the wireshark project. The search query is 'status:open'. The interface displays a table of reviews with columns for Subject, Status, Owner, Project, Branch, Updated, Size, CR, PD, and V.

Subject	Status	Owner	Project	Branch	Updated	Size	CR	PD	V
▶ Disable GTK+ by default.		Gerald Combs	wireshark	master (disable-gtk-default)	2:14 PM		✘		
fc00: Fix Dead Store (Dead assignment/Dead increment) Warning found by Clang		Alexis La Goutte	wireshark	master (clang)	2:12 PM				
Update MNC list for MCC 432 (Iran)		Babak Farrokhi	wireshark	master	2:08 PM		+1	✓	✓
Qt: Main welcome show/hide interface updates.		Gerald Combs	wireshark	master (enable-interfaces)	1:49 PM		■ +1	✓	
BGP: fix bgp.ls.tlv.link_protection_type_value is not of an FT_{U}INTn type]		Alexis La Goutte	wireshark	master (BGP)	1:45 PM				
mrcpv2: use ws_strtou function.		Dario Lombardo	wireshark	master (atoi)	1:43 PM			✓	✓
packet-dcerpc: improve the dissection of DCERPC Fault puds		Stefan Metzmacher	wireshark	master (dcerpc-fault)	1:35 PM		■		
ZigBee Green Power: fix commissioning cmd dissection		Vladlen Popov	wireshark	master (zbee_nwk_gp_commissioning_cmd)	1:31 PM		■	✓	

<https://code.wireshark.org/review/>



Push your change !

- Need some git skill
- git clone <https://code.wireshark.org/review/wireshark>
- make your change
- git commit
- git review -R (or git push origin HEAD:refs/for/master/)





Help for Gerrit

- There is page on Wiki can help you

<https://wiki.wireshark.org/Development/Workflow>

<https://wiki.wireshark.org/Development/SubmittingPatches>

<https://wiki.wireshark.org/Development/SubmittingPatches/GitForWindows>

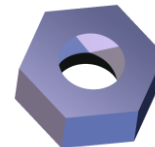




Buildbot

- (Continuous) Automatic build system

- Windows
- Linux (gcc/clang/clang-analyzer/fuzzing...)
- macOS
- For master, master-2.2 and master-2.0 branch



Home - [Waterfall](#) [Grid](#) [T-Grid](#) [Console](#) [Builders](#) [Recent Builds](#) [Buildslaves](#) [Changesources](#) - [JSON API](#) - [About](#)

Waterfall [waterfall help](#)

last build	Clang Code Analysis failed check-abi	OSX 10.6 x64 build successful	Ubuntu 16.04 x64 build successful	Visual Studio Code Analysis build successful	Windows 8.1 x86 build successful	Windows Server 2012 R2 x64 build successful	
current activity	building 12 pending	idle	building ETA in ~ 29 mins at 19:15	idle	building < 1 min	idle	
UTC	changes	Clang Code Analysis	OSX 10.6 x64	Ubuntu 16.04 x64	Visual Studio Code Analysis	Windows 8.1 x86	Windows Server 2012 R2 x64
19:15:34			distcheck		run tests		





Nightly build

- you can get « automated build »
- for Windows and macos



<https://www.wireshark.org/download/automated/>

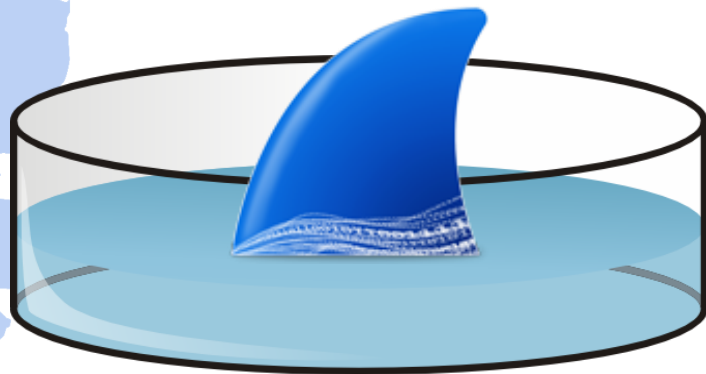


Petri Dish

- Automatic builds and tests before pushing to master

- For example :

- Build with GCC/clang (for Windows dev)
- Build with extra flag
- Build with MSVC (for Linux dev)
- Sanity checks: checkapi, pre-commit, license
-



Petri Dish Buildbot

Patch Set 1: Verified+1

Builder Ubuntu x86-64 Petri Dish succeeded (build successful) - <http://buildbot.wireshark.org/petri-dish/builders/Ubuntu%20x86-64%20Petri%20Dish/builds/8740>

Builder Windows x86 Petri Dish succeeded (build successful) - <http://buildbot.wireshark.org/petri-dish/builders/Windows%20x86%20Petri%20Dish/builds/2387>



ROADMAP

SharkFest '16 Europe • Arnhem, Netherlands • October 17-19, 2016 • #sf16eu



ROADMAP !

It is you make the ROADMAP !

Only need to contribute ! (patch, bug, feature...)

**But already 17 new dissectors (and a lot of bug fix
! Already more 1100 commits from 2.2)**



Questions ?



Thanks !