

Contributing to Zeek

Tim Wojtulewicz, Corelight

That's Woah-2-la-wits

If you were confused by all of the consonants jammed
together

Talking today about how to open pull requests for Zeek issues

Picking an issue (optional)

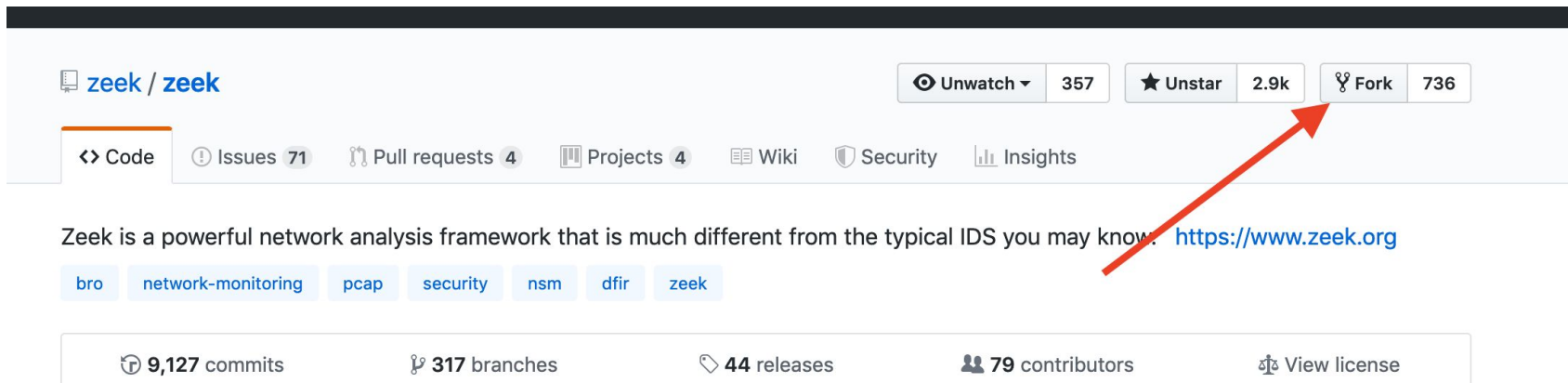
The screenshot shows the GitHub interface for the `zeek / zeek` repository. At the top, there are buttons for `Unwatch` (357), `Unstar` (2.9k), and `Fork` (736). Below these are navigation tabs for `Code`, `Issues 71`, `Pull requests 4`, `Projects 4`, `Wiki`, `Security`, and `Insights`. A search bar contains the text `is:issue is:open`. To the right of the search bar are buttons for `Labels 25` and `Milestones 2`, and a green `New issue` button.

The main content area displays a list of issues. The first issue is `Buffer overflow when reading` (#627) by `philrz`, opened 2 days ago. The second is `Revert cde28074a169212a` (#626) by `Oxxon`, opened 3 days ago. The third is `Container attributes are dis` (#625) by `jsbarbe`, opened 6 days ago. The fourth is `Whitespace at end of line i` (#624) by `sethhal`, opened 6 days ago. The fifth is `Sampling connection-orient` (#623) by `ckreibic`, opened 6 days ago. The sixth is `Allow print() to be redirect` by `ckreibic`. The issue `Sampling connection-orient` has labels `Area: Protocol Analysis` and `Type: Enhancement`. The issue `Allow print() to be redirect` has the label `Type: Enhancement`.

A modal titled `Filter by label` is open, showing a search bar `Filter labels` and a list of labels. A red arrow points to the `good first issue` label. The labels listed are:

- `Complexity: Substantial` (Red square): For the stout of heart.
- `good first issue` (Pink square): A good place to get started working with...
- `Priority: High` (Red square)
- `Priority: Low` (Green square)
- `Type: Bug` (Orange square): Unexpected behavior or output.
- `Type: Duplicate` (Gray square)

Fork the repo



The screenshot shows the GitHub repository page for 'zeek / zeek'. At the top, there are buttons for 'Unwatch' (357), 'Unstar' (2.9k), and 'Fork' (736). A red arrow points to the 'Fork' button. Below these buttons is a navigation bar with links for 'Code', 'Issues' (71), 'Pull requests' (4), 'Projects' (4), 'Wiki', 'Security', and 'Insights'. The main content area contains the text: 'Zeek is a powerful network analysis framework that is much different from the typical IDS you may know.' followed by a link to 'https://www.zeek.org'. Below this text are several topic tags: 'bro', 'network-monitoring', 'pcap', 'security', 'nsm', 'dfir', and 'zeek'. At the bottom, there is a summary bar with statistics: '9,127 commits', '317 branches', '44 releases', '79 contributors', and a link to 'View license'.

zeek / zeek

Unwatch 357 Unstar 2.9k Fork 736

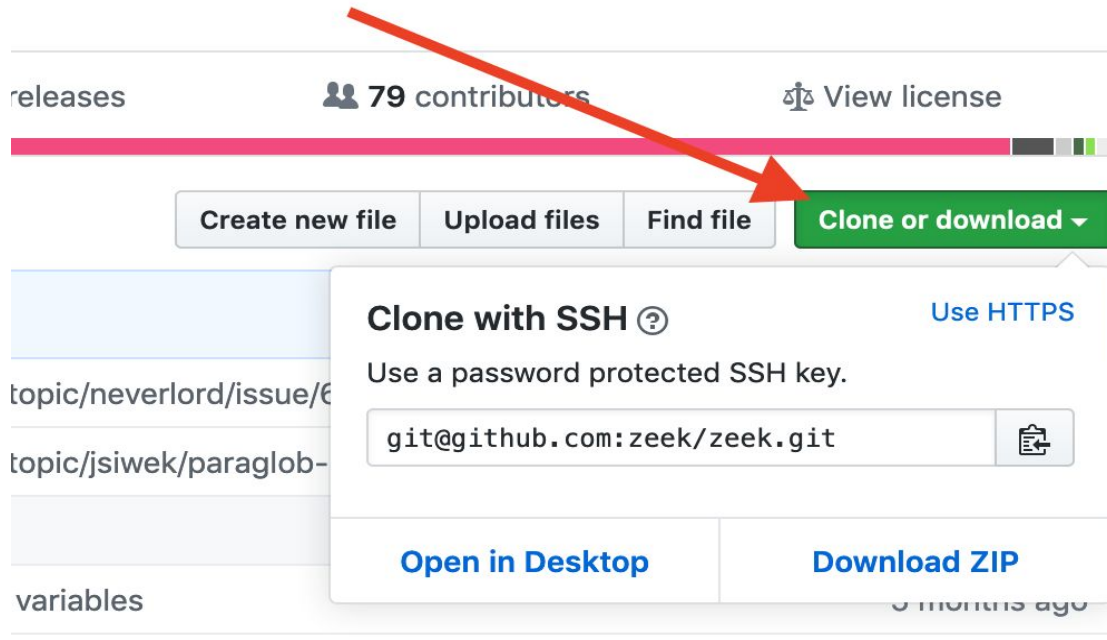
<> Code Issues 71 Pull requests 4 Projects 4 Wiki Security Insights

Zeek is a powerful network analysis framework that is much different from the typical IDS you may know. <https://www.zeek.org>

bro network-monitoring pcap security nsm dfir zeek

9,127 commits 317 branches 44 releases 79 contributors View license

Clone the repo



```
git clone git@github.com:zeek/zeek.git
```

Configure and build

```
cd zeek  
./configure --prefix=/some/path  
cd build  
make
```

**This is the part where you open
emacs and fix the issue**

You are using emacs, right?

Run the tests

```
cd testing/btest  
btest -j 6
```

If it succeeds:

```
981 tests successful, 67 skipped
```

Don't worry about those skipped tests, that's intentional.

Commit your change to your fork

```
git checkout -b <branchname>
```

```
git commit -a -m "GH-###: Some descriptive commit  
message"
```

```
git push -u origin -b <branchname>
```

The GH-### part will cause Github to automatically close the issue when the PR is merged.

Create the pull request, part 1

[Manage topics](#)

🔖 9,127 commits

🌿 317 branches

📦 44 releases

👤 79 contributors

📄 View license

Your recently pushed branches:

🌿 **fixing-something** (less than a minute ago)

🔗 Compare & pull request

Branch: master ▾

New pull request

Create new file

Upload files

Find file

Clone or download ▾

This branch is even with zeek:master.


🔗 Pull request

🔗 Compare

Create the pull request, part 2

Open a pull request

Create a new pull request by comparing changes across two branches. If you need to, you can also [compare across forks](#).

 base repository: **zeek/zeek** ▼


base: **master** ▼

←

head repository: **timwoj/zeek** ▼

compare: **fixing-something** ▼

✓ **Able to merge.** These branches can be automatically merged.



Adding a comment

Write

Preview

AA

B

i

“

<>

↺

≡

≡


≡

@

★

↶

Leave a comment

Attach files by dragging & dropping, selecting or pasting them. 

☒ Allow edits from maintainers. [Learn more](#)

Create pull request ▼

Reviewers

No reviews

Assignees

No one—assign yourself

Labels

None yet

Projects

None yet

Milestone

No milestone

Create the pull request, part 3

Open a pull request

Create a new pull request by comparing changes across two branches. If you need to, you can also [compare across forks](#).

base repository: **zeek/zeek** ▼

base: **master** ▼

head repository: **timwoj/zeek** ▼

compare: **fixing-something** ▼

✓ **Able to merge.** These branches can be automatically merged.


Adding a comment

Write

Preview

AA B i “ <> ↺ ⋮ ⋮ ✓ @ ★ ↶

Leave a comment

Attach files by dragging & dropping, selecting or pasting them. 

☒ Allow edits from maintainers. [Learn more](#)

Create pull request ▼

Reviewers

No reviews

Assignees

No one—assign yourself

Labels

None yet

Projects

None yet

Milestone

No milestone

Wait for someone to review

**Review feedback -> fixes -> new
commits -> more reviews**



Maintainer will merge to master

Dog tax?



PROPRIETARY AND CONFIDENTIAL