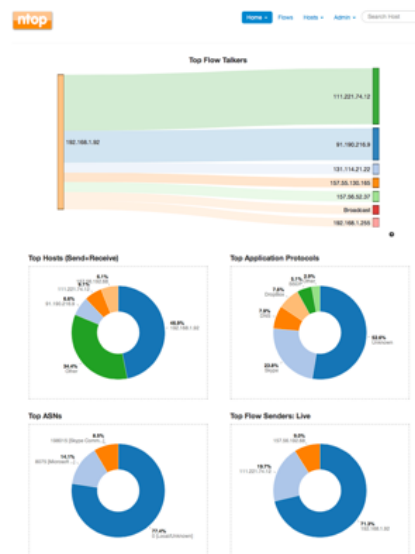


ntop  
*Visibility, Security Awareness*



# About ntop

- Private company devoted to development of open source network traffic monitoring applications.
- In September 1997 the development of the original ntop application started.
- 6 core development team members



# ntop and Wireshark [1/2]

- Met Gerald at IM 2001 in Seattle and started to use Ethereal.
- Contributions NetFlow dissector (2005) and extended with new information elements (2017).
- Wireshark education and training @ Unipi.
- Support local community of network administrators.
- Sponsor of Sharkfest since 2014: even if we're small we want to reward the Wireshark community.
- ntop meetup at Sharkfest EU 2016 and US 2017.



# ntop and Wireshark [2/2]

This repository

Search

Pull requests Issues Marketplace Explore

ntop / wireshark-ntop

Unwatch 6 Star 33 Fork 0

Code Issues 0 Pull requests 0 Projects 0 Wiki Insights Settings

Extensions for Wireshark

Edit

Add topics

5 commits 1 branch 0 releases 2 contributors

Branch: master New pull request Create new file Upload files Find file Clone or download

Author	Commit Message	Latest Commit
lucaderi	Update flow offload dissector	714eba7 19 seconds ago

README.md Update flow offload dissector 18 seconds ago

## wireshark-ntop

This repository contains open source extensions for Wireshark.

Here you can find:



- The [ntopdump extcap module](#): it can be used to open a PF\_RING interface (also those that are not listed in ifconfig) or to extract traffic from a n2disk dumpset.
- The [remotentopdump extcap module](#): it can be used to capture traffic from a PF\_RING interface on a remote machine, or extract traffic from a remote n2disk dumpset in Wireshark.
- The [ndpi plugin](#): it shows L7 protocol information provided by nDPI to complement internal protocol decoding. In order to do this, the ndpiReader application is used to provide Wireshark nDPI protocol dissection, and the ndpi plugin interprets nDPI information.
- The [Hardware Flow Offload Dissector](#) dissector: it can dissect messages produced by the hardware flow offload engine when flows are computed in hardware.

Enjoy!

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



# Upcoming Talk @ Sharkfest EU 2017

Day 01 6.11.2017	Day 02 7.11.2017	Day 03 8.11.2017	Day 04 9.11.2017	Day 05 10.11.2017
Atlantico Classroom		ParkSuite Classroom		Tropical Room
7:30am - 8:30am	Breakfast (Europa Room)			
8:30am - 9:30am	SharkBytes (Atlantico Room)			
9:45am - 11:00am	 16: My TCP ain't your TCP: Stack behavior back then, now and in the future Instructor: <a href="#">Simon Lindermann</a>			
11:15am - 12:30pm	 19: Turning Wireshark into a Traffic Monitoring Tool: Moving from packet details to the big picture Instructor: <a href="#">Luca Deri</a>			



# Our Tools

- Open Source
  - ntopng: Web-based monitoring application
  - PF\_RING: Accelerated RX/TX on Linux
  - nDPI: Deep Packet Inspection Toolkit
- Proprietary
  - PF\_RING ZC: 1/10/40/100 Gbit Line rate.
  - nProbe: 10G NetFlow/IPFIX Probe
  - nProbe Cento: flows+packets+security
  - n2disk/disk2n Network-to-disk and disk-to-network.
  - nScrub: Software DDoS Mitigation



# Ntop Meetup at Sharkfest EU 2017

Welcome

Hardware Flow-Offload, pfflow, Wireshark flow dissector

Integrating Grafana with ntopng

µProbes for Monitoring and Troubleshooting

PF\_RING Extcap, Remote Wireshark, DPI.

nEdge: IoT Monitoring and (Cyber)Security

Products Roadmap and Discussion

