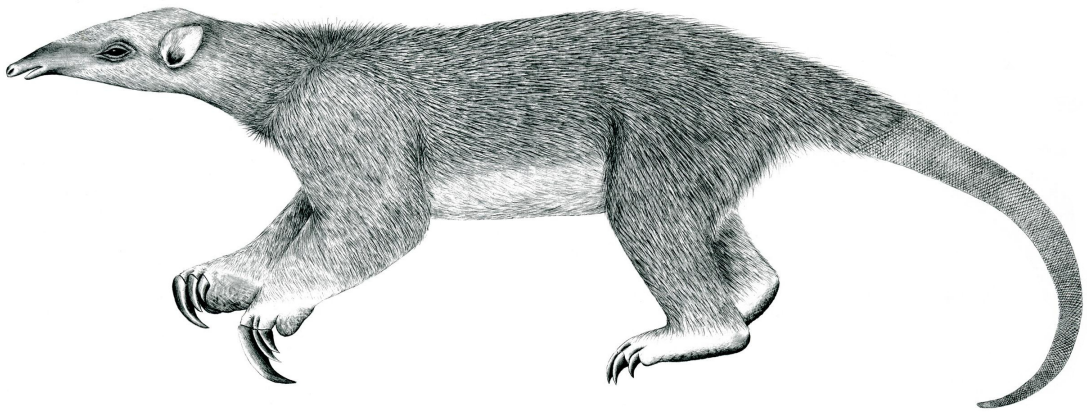
# Tranalyzer2

## nDPI

Classification Based on Content Analysis



Tranalyzer Development Team

# Contents

# 1 nDPI

## 1.1 Description

This plugin is a simple wrapper around the nDPI library: https://github.com/ntop/nDPI. It classifies flows according to their protocol/application by analyzing the payload content instead of using the destination port. This plugin produces output to the flow file and to a protocol statistics file. Configuration is achieved by user defined compiler switches in `src/nDPI.h`.

## 1.2 Dependencies

### 1.2.1 External Libraries

This plugin depends on the **libgcrypt** library.

| | | |
|---|---|---|
| **Ubuntu:** | `sudo apt-get install` | `libgcrypt20-dev` |
| **Arch:** | `sudo pacman -S` | `libgcrypt` |
| **Gentoo:** | `sudo emerge` | `libgcrypt` |
| **openSUSE:** | `sudo zypper install` | `libgcrypt-devel` |
| **Red Hat/Fedora**[1]**:** | `sudo dnf install` | `libgcrypt-devel` |
| **macOS**[2]**:** | `brew install` | `libgcrypt` |

## 1.3 Configuration Flags

The following flags can be used to control the output of the plugin:

| Variable | Default | Description |
|---|---|---|
| `NDPI_OUTPUT_NUM` | 0 | Output a numerical classification |
| `NDPI_OUTPUT_STR` | 1 | Output a textual classification |
| `NDPI_OUTPUT_STATS` | 1 | Output nDPI protocol distribution in a separate file |
| `NDPI_GUESS_UNKNOWN` | 1 | Try guessing unknown protocols |

## 1.4 Flow File Output

The nDPI plugin outputs the following columns:

| Column | Type | Description | Flags |
|---|---|---|---|
| `nDPIMstrProto` | U16 | nDPI numerical master protocol | `NDPI_OUTPUT_NUM=1` |
| `nDPISubProto` | U16 | nDPI numerical sub protocol | `NDPI_OUTPUT_NUM=1` |
| `nDPIclass` | S | nDPI based protocol classification | `NDPI_OUTPUT_STR=1` |

[1] If the `dnf` command could not be found, try with `yum` instead
[2] Brew is a packet manager for macOS that can be found here: https://brew.sh

## 1.5 Packet File Output

In packet mode (`-s` option), the nDPI plugin outputs the following columns:

| Column | Type | Description | Flags |
|---|---|---|---|
| nDPIMstrProto | U16 | nDPI numerical master protocol | NDPI_OUTPUT_NUM=1 |
| nDPISubProto | U16 | nDPI numerical sub protocol | NDPI_OUTPUT_NUM=1 |
| nDPIclass | S | nDPI based protocol classification | NDPI_OUTPUT_STR=1 |

## 1.6 nDPIMstrProto

The `nDPIMstrProto` column is to be interpreted as follows:

**0** Unknown
**1** FTP_CONTROL
**2** POP3
**3** SMTP
**4** IMAP
**5** DNS
**6** IPP
**7** HTTP
**8** MDNS
**9** NTP
**10** NetBIOS
**11** NFS
**12** SSDP
**13** BGP
**14** SNMP
**15** XDMCP
**16** SMBv1
**17** Syslog
**18** DHCP
**19** PostgreSQL
**20** MySQL
**21** Outlook
**22** VK
**23** POPS
**24** Tailscale
**25** Yandex
**26** ntop
**27** COAP
**28** VMware
**29** SMTPS
**30** DTLS
**31** UBNTAC2
**32** BFCP
**33** YandexMail
**34** YandexMusic
**35** Gnutella
**36** eDonkey
**37** BitTorrent
**38** Skype_TeamsCall
**39** Signal
**40** Memcached
**41** SMBv23
**42** Mining
**43** NestLogSink
**44** Modbus
**45** WhatsAppCall
**46** DataSaver
**47** Xbox
**48** QQ
**49** TikTok
**50** RTSP
**51** IMAPS
**52** IceCast
**53** CPHA
**54** iQIYI
**55** Zattoo
**56** YandexMarket
**57** YandexDisk
**58** Discord
**59** AdobeConnect
**60** MongoDB
**61** Pluralsight
**62** YandexCloud
**63** OCSP
**64** VXLAN

**65** IRC
**66** MerakiCloud
**67** Jabber
**68** Nats
**69** AmongUs
**70** Yahoo
**71** DisneyPlus
**72** HART-IP
**73** VRRP
**74** Steam
**75** HalfLife2
**76** WorldOfWarcraft
**77** Telnet
**78** STUN
**79** IPSec
**80** GRE
**81** ICMP
**82** IGMP
**83** EGP
**84** SCTP
**85** OSPF
**86** IP_in_IP
**87** RTP
**88** RDP
**89** VNC
**90** Tumblr
**91** TLS
**92** SSH
**93** Usenet
**94** MGCP
**95** IAX
**96** TFTP
**97** AFP
**98** YandexMetrika
**99** YandexDirect
**100** SIP
**101** TruPhone
**102** ICMPV6
**103** DHCPV6
**104** Armagetron
**105** Crossfire
**106** Dofus
**107** ADS_Analytic_Track
**108** AdultContent
**109** Guildwars
**110** AmazonAlexa
**111** Kerberos
**112** LDAP
**113** MapleStory
**114** MsSQL-TDS
**115** PPTP
**116** Warcraft3
**117** WorldOfKungFu
**118** Slack
**119** Facebook
**120** Twitter
**121** Dropbox
**122** GMail
**123** GoogleMaps
**124** YouTube
**125** Skype_Teams
**126** Google
**127** MS-RPCH
**128** NetFlow
**129** sFlow
**130** HTTP_Connect
**131** HTTP_Proxy
**132** Citrix
**133** NetFlix
**134** LastFM
**135** Waze
**136** YouTubeUpload
**137** Hulu
**138** CHECKMK
**139** AJP
**140** Apple
**141** Webex
**142** WhatsApp
**143** AppleiCloud
**144** Viber
**145** AppleiTunes
**146** Radius
**147** WindowsUpdate
**148** TeamViewer
**149** EthernetGlobalData
**150** LotusNotes
**151** SAP
**152** GTP
**153** WSD
**154** LLMNR

**155** TocaBoca
**156** Spotify
**157** FacebookMessenger
**158** H323
**159** OpenVPN
**160** NOE
**161** CiscoVPN
**162** TeamSpeak
**163** Tor
**164** CiscoSkinny
**165** RTCP
**166** RSYNC
**167** Oracle
**168** Corba
**169** UbuntuONE
**170** Whois-DAS
**171** SD-RTN
**172** SOCKS
**173** Nintendo
**174** RTMP
**175** FTP_DATA
**176** Wikipedia
**177** ZeroMQ
**178** Amazon
**179** eBay
**180** CNN
**181** Megaco
**182** RESP
**183** Pinterest
**184** VHUA
**185** Telegram
**186** CoD_Mobile
**187** Pandora
**188** QUIC
**189** Zoom
**190** EAQ
**191** Ookla
**192** AMQP
**193** KakaoTalk
**194** KakaoTalk_Voice
**195** Twitch
**196** DoH_DoT
**197** WeChat
**198** MPEG_TS
**199** Snapchat
**200** Sina
**201** GoogleMeet
**202** IFLIX
**203** Github
**204** BJNP
**205** Reddit
**206** WireGuard
**207** SMPP
**208** DNScrypt
**209** TINC
**210** Deezer
**211** Instagram
**212** Microsoft
**213** Starcraft
**214** Teredo
**215** HotspotShield
**216** IMO
**217** GoogleDrive
**218** OCS
**219** Microsoft365
**220** Cloudflare
**221** MS_OneDrive
**222** MQTT
**223** RX
**224** AppleStore
**225** OpenDNS
**226** Git
**227** DRDA
**228** PlayStore
**229** SOMEIP
**230** FIX
**231** Playstation
**232** Pastebin
**233** LinkedIn
**234** SoundCloud
**235** SteamDatagramRelay
**236** LISP
**237** Diameter
**238** ApplePush
**239** GoogleServices
**240** AmazonVideo
**241** GoogleDocs
**242** WhatsAppFiles
**243** TargusDataspeed
**244** DNP3

**245** IEC60870
**246** Bloomberg
**247** CAPWAP
**248** Zabbix
**249** S7Comm
**250** Teams
**251** WebSocket
**252** AnyDesk
**253** SOAP
**254** AppleSiri
**255** SnapchatCall
**256** HP_VIRTGRP
**257** GenshinImpact
**258** Activision
**259** FortiClient
**260** Z3950
**261** Likee
**262** GitLab
**263** AVASTSecureDNS
**264** Cassandra
**265** AmazonAWS
**266** Salesforce
**267** Vimeo
**268** FacebookVoip
**269** SignalVoip
**270** Fuze
**271** GTP_U
**272** GTP_C
**273** GTP_PRIME
**274** Alibaba
**275** Crashlytics
**276** Azure
**277** iCloudPrivateRelay
**278** EthernetIP
**279** Badoo
**280** AccuWeather
**281** GoogleClassroom
**282** HSRP
**283** Cybersec
**284** GoogleCloud
**285** Tencent
**286** RakNet
**287** Xiaomi
**288** Edgecast
**289** Cachefly
**290** Softether
**291** MpegDash
**292** Dazn
**293** GoTo
**294** RSH
**295** 1kxun
**296** PGM
**297** IP_PIM
**298** collectd
**299** TunnelBear
**300** CloudflareWarp
**301** i3D
**302** RiotGames
**303** Psiphon
**304** UltraSurf
**305** Threema
**306** AliCloud
**307** AVAST
**308** TiVoConnect
**309** Kismet
**310** FastCGI
**311** FTPS
**312** NAT-PMP
**313** Syncthing
**314** CryNetwork
**315** Line
**316** LineCall
**317** AppleTVPlus
**318** DirecTV
**319** HBO
**320** Vudu
**321** Showtime
**322** Dailymotion
**323** Livestream
**324** Tencentvideo
**325** IHeartRadio
**326** Tidal
**327** TuneIn
**328** SiriusXMRadio
**329** Munin
**330** Elasticsearch
**331** TuyaLP
**332** TPLINK_SHP
**333** Source_Engine
**334** BACnet

**335** OICQ
**336** Heroes_of_the_Storm
**337** FbookReelStory
**338** SRTP
**339** OperaVPN
**340** EpicGames
**341** GeForceNow
**342** Nvidia
**343** BITCOIN
**344** ProtonVPN
**345** Thrift
**346** Roblox
**347** Service_Location_Protocol
**348** Mullvad
**349** HTTP2
**350** HAProxy
**351** RMCP
**352** Controller_Area_Network
**353** Protobuf
**354** ETHEREUM
**355** TelegramVoip
**356** SinaWeibo
**357** TeslaServices
**358** PTPv2
**359** RTPS
**360** OPC-UA
**361** S7CommPlus
**362** FINS
**363** EtherSIO
**364** UMAS
**365** BeckhoffADS
**366** ISO9506-1-MMS
**367** IEEE-C37118
**368** Ether-S-Bus
**369** Monero
**370** DCERPC
**371** PROFINET_IO
**372** HiSLIP
**373** UFTP
**374** OpenFlow
**375** JSON-RPC
**376** WebDAV
**377** Kafka
**378** NoMachine
**379** IEC62056
**380** HL7
**381** Ceph
**382** GoogleChat
**383** Roughtime
**384** PrivateInternetAccess
**385** KCP
**386** Dota2
**387** Mumble
**388** Yojimbo
**389** ElectronicArts
**390** STOMP
**391** Radmin
**392** Raft
**393** CIP
**394** Gearman
**395** TencentGames
**396** GaijinEntertainment
**397** ANSI_C1222
**398** Huawei
**399** HuaweiCloud
**400** DLEP
**401** BFD
**402** NetEaseGames
**403** PathofExile
**404** GoogleCall
**405** PFCP
**406** FLUTE
**407** LoLWildRift
**408** TES_Online
**409** LDP
**410** KNXnet_IP
**411** Bluesky
**412** Mastodon
**413** Threads
**414** ViberVoip
**415** ZUG
**416** JRMI
**417** RipeAtlas
**418** HLS
**419** ClickHouse
**420** Nano
**421** OpenWire

## 1.7 Plugin Report Output

The following information is reported:

- Number of flows classified

## 1.8 Additional Output

If `NDPI_OUTPUT_STATS=1` then nDPI protocol distribution statistics are output in `PREFIX_nDPI.txt`.

## 1.9 Post-Processing

The `protStat` script can be used to sort the `PREFIX_nDPI.txt` file for the most or least occurring protocols (in terms of number of packets or bytes). It can output the top or bottom *N* protocols or only those with at least a given percentage:

- list all the options: `protStat --help`
- for better readability, use `protStat` with `tcol`: `protStat ... | tcol`
- sorted list of protocols (by packets): `protStat PREFIX_nDPI.txt`
- sorted list of protocols (by bytes): `protStat PREFIX_nDPI.txt -b`
- top 10 protocols (by packets): `protStat PREFIX_nDPI.txt -n 10`
- bottom 5 protocols (by bytes): `protStat PREFIX_nDPI.txt -n -5 -b`
- protocols with packets percentage greater than 20%: `protStat PREFIX_nDPI.txt -p 20`
- protocols with bytes percentage smaller than 5%: `protStat PREFIX_nDPI.txt -b -p -5`

## 1.10 How to Update nDPI to New Version

- download latest stable version (or git clone and checkout stable branch)
- delete `src/nDPI` and replace it with this new version
- run the `./new_ndpi_prepatch.sh` script
- build the nDPI plugin: `t2build -r nDPI`
- Replace the `proto.tex` file using the `prototex` utility and regenerate doc:

```
make -C prototex && ./prototex/prototex > doc/proto.tex
```

- Add the new files to SVN and delete removed files before commit.