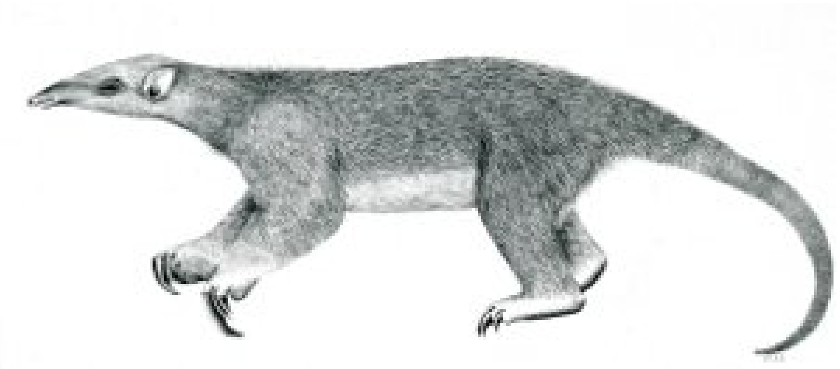
Tranalyzer2

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 Configuration Flags

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

Variable	**Default**	**Description**
`NDPI_OUTPUT_NUM`	0	Whether (1) or not (0) to output a numerical classification.
`NDPI_OUTPUT_STR`	1	Whether (1) or not (0) to output a textual classification.
`NDPI_OUTPUT_STATS`	1	Whether (1) or not (0) to output nDPI protocol distribution in a separate file.
`NDPI_GUESS_UNKNOWN`	1	Whether (1) or not (0) to try guessing unknown protocols.

1.3 Flow File Output

The nDPI plugin outputs the following columns:

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

1.4 nDPI Numerical Protocol Classification

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	Hotmail
22	Direct_Download_Link
23	POPS
24	AppleJuice
25	DirectConnect
26	ntop
27	COAP
28	VMware
29	SMTPS
30	FacebookZero

31	UBNTAC2
32	Kontiki
33	OpenFT
34	FastTrack
35	Gnutella
36	eDonkey
37	BitTorrent
38	SkypeCall
39	Signal
40	Memcached
41	SMBv23
42	Mining
43	NestLogSink
44	Modbus
45	Free
46	Free
47	Xbox
48	QQ
49	Free_49
50	RTSP
51	IMAPS
52	IceCast
53	PPLive
54	PPStream
55	Zattoo
56	ShoutCast
57	Sopcast
58	Tvants
59	TVUplayer
60	HTTP_Download
61	QQLive
62	Thunder
63	Soulseek
64	SSL_No_Cert
65	IRC
66	Ayiya
67	Unencrypted_Jabber
68	MSN
69	Oscar
70	Yahoo
71	BattleField
72	GooglePlus
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	PcAnywhere
91	SSL
92	SSH
93	Usenet
94	MGCP
95	IAX
96	TFTP
97	AFP
98	Stealthnet
99	Aimini
100	SIP
101	TruPhone
102	ICMPV6
103	DHCPV6
104	Armagetron
105	Crossfire
106	Dofus
107	Fiesta
108	Florensia
109	Guildwars
110	HTTP_ActiveSync
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
126	Google
127	DCE_RPC
128	NetFlow
129	sFlow
130	HTTP_Connect
131	HTTP_Proxy
132	Citrix
133	NetFlix
134	LastFM
135	Waze
136	YouTubeUpload
137	GenericProtocol
138	CHECKMK
139	AJP
140	Apple
141	Webex
142	WhatsApp
143	AppleiCloud
144	Viber
145	AppleiTunes
146	Radius
147	WindowsUpdate
148	TeamViewer
149	Tuenti
150	LotusNotes
151	SAP
152	GTP
153	UPnP
154	LLMNR
155	RemoteScan
156	Spotify
157	Messenger
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	Collectd
172	SOCKS
173	Nintendo
174	RTMP
175	FTP_DATA
176	Wikipedia
177	ZeroMQ
178	Amazon
179	eBay
180	CNN
181	Megaco
182	Redis
183	Pando_Media_Booster
184	VHUA
185	Telegram
186	Vevo
187	Pandora
188	QUIC
189	WhatsAppVoice
190	EAQ
191	Ookla
192	AMQP
193	KakaoTalk
194	KakaoTalk_Voice
195	Twitch
196	Free
197	WeChat
198	MPEG_TS
199	Snapchat
200	Sina(Weibo)
201	GoogleHangout
202	IFLIX
203	Github
204	BJNP
205	Free
206	PPStream
207	SMPP
208	DNScrypt
209	TINC
210	Deezer

211	Instagram
212	Microsoft
213	Starcraft
214	Teredo
215	HotspotShield
216	HEP
217	GoogleDrive
218	OCS
219	Office365
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	CSGO
236	LISP
237	Diameter
238	ApplePush
239	GoogleServices
240	AmazonVideo
241	GoogleDocs
242	WhatsAppFiles

1.5 Plugin Report Output

The following information is reported:

- Number of flows classified

1.6 Additional Output

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

1.7 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`
- 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`

1.8 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
- `cd src/nDPI/`
- edit `configure.ac`

```
--- configure.ac.origin
+++ configure.ac
@@ -119,9 +119,9 @@

 dnl> https://github.com/json-c/json-c
 AC_ARG_ENABLE([json-c],
-    AS_HELP_STRING([--disable-json-c], [Disable json-c support]))
+    AS_HELP_STRING([--enable-json-c], [Enable json-c support]))

-AS_IF([test "x$enable_json_c" != "xno"], [
+AS_IF([test "x$enable_json_c" = "xyes"], [
        PKG_CONFIG_PATH=/usr/local/share/pkgconfig:$PKG_CONFIG_PATH
        pkg-config --exists json-c
        AS_IF([test "$?" == "0"],
@@ -147,7 +147,7 @@

 AC_CHECK_LIB(pthread, pthread_setaffinity_np, AC_DEFINE_UNQUOTED(HAVE_PTHREAD_SETAFFINITY_NP
     , 1, [libc has pthread_setaffinity_np]))

-AC_CONFIG_FILES([Makefile example/Makefile example/Makefile.dpdk tests/Makefile libndpi.pc
    src/include/ndpi_define.h src/lib/Makefile])
+AC_CONFIG_FILES([Makefile libndpi.pc src/include/ndpi_define.h src/lib/Makefile])
 AC_CONFIG_HEADERS(src/include/ndpi_config.h)
 AC_SUBST(GIT_RELEASE)
 AC_SUBST(NDPI_MAJOR)
```

- edit `Makefile.am`

```
--- Makefile.am.origin
+++ Makefile.am
@@ -1,5 +1,5 @@
 ACLOCAL_AMFLAGS = -I m4
-SUBDIRS = src/lib example tests
+SUBDIRS = src/lib

 pkgconfigdir = $(prefix)/libdata/pkgconfig
 pkgconfig_DATA = libndpi.pc
```

- Replace the `proto.tex` file using the `prototex` utiliy and regenerate doc.
- Add the new files to SVN and delete removed files before commit.