darkstat – Ein Network–Traffic–Analyzer

by Mario M. Knopf (homepage)

About the author:

Mario beschäftigt sich leidenschaftlich gerne mit Linux, Netzwerken und sicherheitsrelevanten Themen.

Abstract:

Der Artikel stellt den Network–Traffic–Analyzer "*darkstat*" vor und liefert einen Überblick bezüglich Installation, Start und Benutzung des Programms.

Einleitung

Bei "*darkstat*" [1] handelt es sich um ein Network–Monitoring–Tool, das den anfallenden Traffic eines Netzwerks analysiert und anhand dieser Daten diverse Statistiken im HTML–Format generiert, welche dann komfortabel in einem Browser betrachtet werden können. Da der Programmautor Emil Mikulic über lange Zeit "*ntop*" [2] für diesen Zweck im Einsatz hatte, aber mit dessen Speicherumgang und Stabilität unzufrieden war, entwickelte er schließlich "*darkstat*". Die angesprochenen Statistiken beziehen sich auf die an der Kommunikation beteiligten Hosts, dem verursachten Traffic und den benutzten Portnummern bzw. den Übertragungsprotokollen. Weiterhin können Diagramme in Bezug auf die erfassten Zeitperioden und eine kurze Zusammenfassung der analysierten Datenpakete seit Programmstart betrachtet werden.

Installation

Die Quellen des Programms "*darkstat*" lassen sich direkt unter [3] beziehen. Alternativ kann auch einer der beiden Mirrors unter [4] und [5] besucht werden. Wer hingegen Debian–Pakete sucht, wird bei [6] fündig.

Wie bei vielen anderen Network–Monitoring–Tools besteht auch bei "*darkstat*" die Abhängigkeit zur Datei "*libpcap*" [7]. Dies ist eine Bibliothek für sogenannte Packet–Sniffer und bietet diesen eine Schnittstelle, um den Inhalt passierender Datenpakete mitzuschneiden und zu analysieren. Zwingende Voraussetzung zur Installation von "*darkstat*" ist also die Präsenz dieser Bibliothek.

Kompiliert wird dann mit dem allseits bekannten Dreisatz "*./configure && make && make install*" – wobei zu beachten ist, daß der letzte Befehl mit root–Rechten ausgeführt werden muß.

Start

"*darkstat*" stellt einige Parameter zur Verfügung, die direkt beim Programmaufruf übergeben werden können. Für einen ersten Test reicht jedoch ein Start ohne jegliche Optionen. Um seine Arbeit verrichten zu können, muß das Programm allerdings als root oder per "*sudo*" [8] gestartet werden:

```
neo5k@proteus> sudo /usr/local/sbin/darkstat

We trust you have received the usual lecture from the local System Administrator.
It usually boils down to these two things:

#1) Respect the privacy of others.
#2) Think before you type.

Password:
```

Nachdem der autorisierte Benutzer sein Passwort eingegeben hat, startet "*darkstat*" und liefert dabei diverse Statusmeldungen:

```
darkstat v2.6 using libpcap v2.4 (i686-pc-linux-gnu)
Firing up threads...
Sniffing on device eth0, local IP is 192.168.1.1
DNS: Thread is awake.
WWW: Thread is awake and awaiting connections.
WWW: You are using the English language version.
GRAPH: Starting at 8 secs, 51 mins, 22hrs, 30 days.
Can't load db from darkstat.db, starting from scratch.
ACCT: Capturing traffic...
Point your browser at http://localhost:666/ to see the stats.
```

Da der Test erfolgreich verlaufen ist und die Ausgaben selbsterklärend sind, können nun die möglichen Startparameter betrachtet werden.

Startoptionen

Wie bereits erwähnt, stellt "*darkstat*" diverse Optionen bzw. Parameter bereit, die beim Programmstart einfach angehängt werden können. Jene Parameter lauten folgendermaßen:

Durch Option "*−i*" läßt sich die Netzwerkschnittstelle spezifizieren, an welcher "*darkstat*" nach passierenden Paketen snifft:

darkstat −i eth1

Sofern "*darkstat*" ohne spezielle Parameter gestartet wird, öffnet er standardmäßig den privilegierten Port 666. Mit Hilfe der Option "*−p*" kann dies geändert werden:

darkstat −p 8080

Anhand der folgenden Option läßt sich ein bestimmter Port an die angegebene Schnittstelle binden. Im Beispiel an die lokale Loopback−Adresse:

darkstat −b 127.0.0.1

Für Leute, die über keine Standleitung oder Flatrate verfügen, könnte die Option "*−n*" interessant sein, da sie ständige DNS−Abfragen unterbindet.

darkstat −n

Um zu vermeiden, daß "*darkstat*" die jeweilige Schnittstelle in den "*promiscuous mode*" schaltet, bedient man sich der Option "*−P*". Dies ist allerdings nicht empfehlenswert, da "*darkstat*" dann nur noch die an die MAC der überwachten Netzwerkkarte adressierten Datenpakete analysiert und alle anderen verwirft.

darkstat −P

Der Schalter "*−l*" aktiviert korrektes "*SNAT*"−Verhalten im lokalen Netzwerk. "*SNAT*" steht für "*Source Network Address Translation*" und sagt aus, daß der Router die lokale IP−Adresse des Clients in seine öffentliche übersetzt und somit stellvertretend für den Client die Anfrage ins Internet schickt.

darkstat −l 192.168.1.0/255.255.255.0

Mit Parameter "*−e*" lassen sich spezielle Ausdrücke erzeugen, welche die Filterung bestimmter Ports betreffen.

darkstat −e "port not 22"

Ab Version 2.5 läßt sich "*darkstat*" mit dem Schalter "*−−detach*" von dem Terminal, in welchem es gestartet wurde, loslösen und arbeitet dadurch als Daemon.

darkstat −−detach

Durch die Option "*−d*" kann angegeben werden, in welchem Verzeichnis "*darkstat*" seine Datenbank speichert bzw. anlegt.

darkstat −d /directory

Parameter "*−v*" ist bereits von anderen Programmen bekannt und schaltet den sogenannten "*verbose mode*", also den ausführlichen Ausgabemodus, ein:

darkstat −v

Die Option "*−h*" zeigt neben der eingesetzten Versionsnummer auch alle verfügbaren Parameter und die von "*darkstat*" verlangte Syntax an.

darkstat −h

Betrieb

Nachdem "*darkstat*" das erste Mal gestartet wurde, kann dessen Startseite unter "*http://localhost:666/*" (Standard−Einstellung) betrachtet werden. Dort kann man bereits eine kurze und nicht allzu detaillierte Zusammenfassung der generierten Statistiken samt entsprechendem Diagramm seit Programmstart sehen:

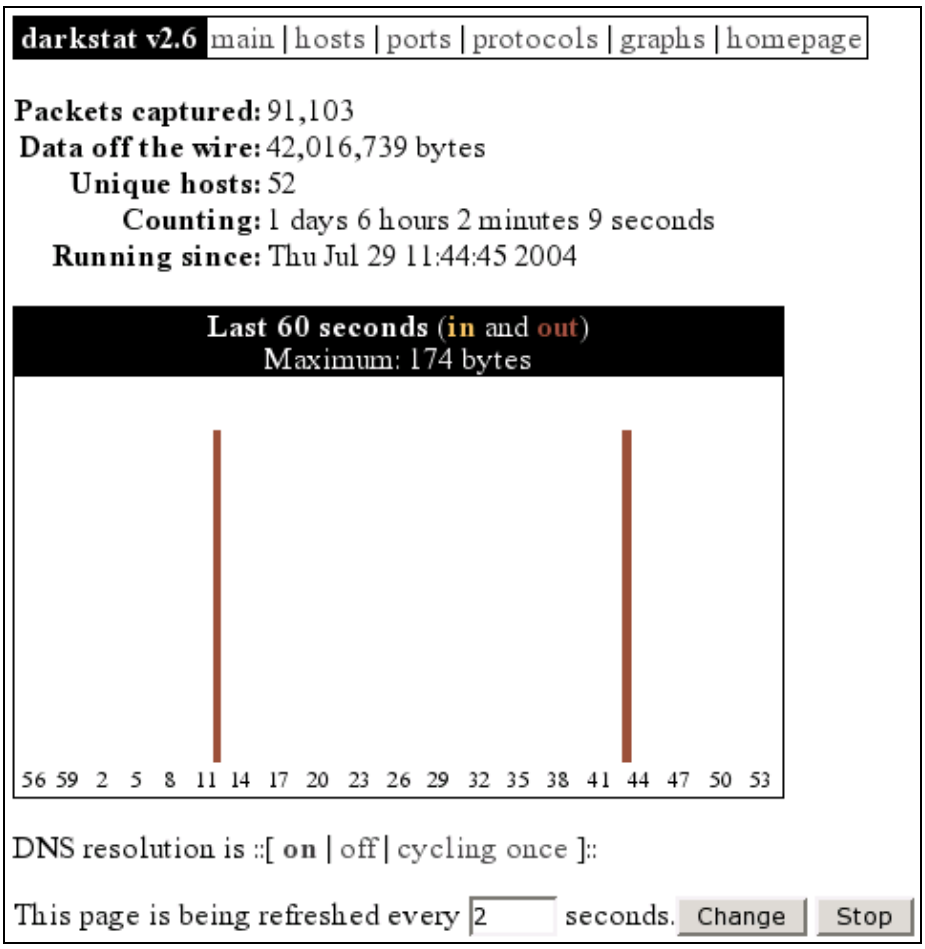
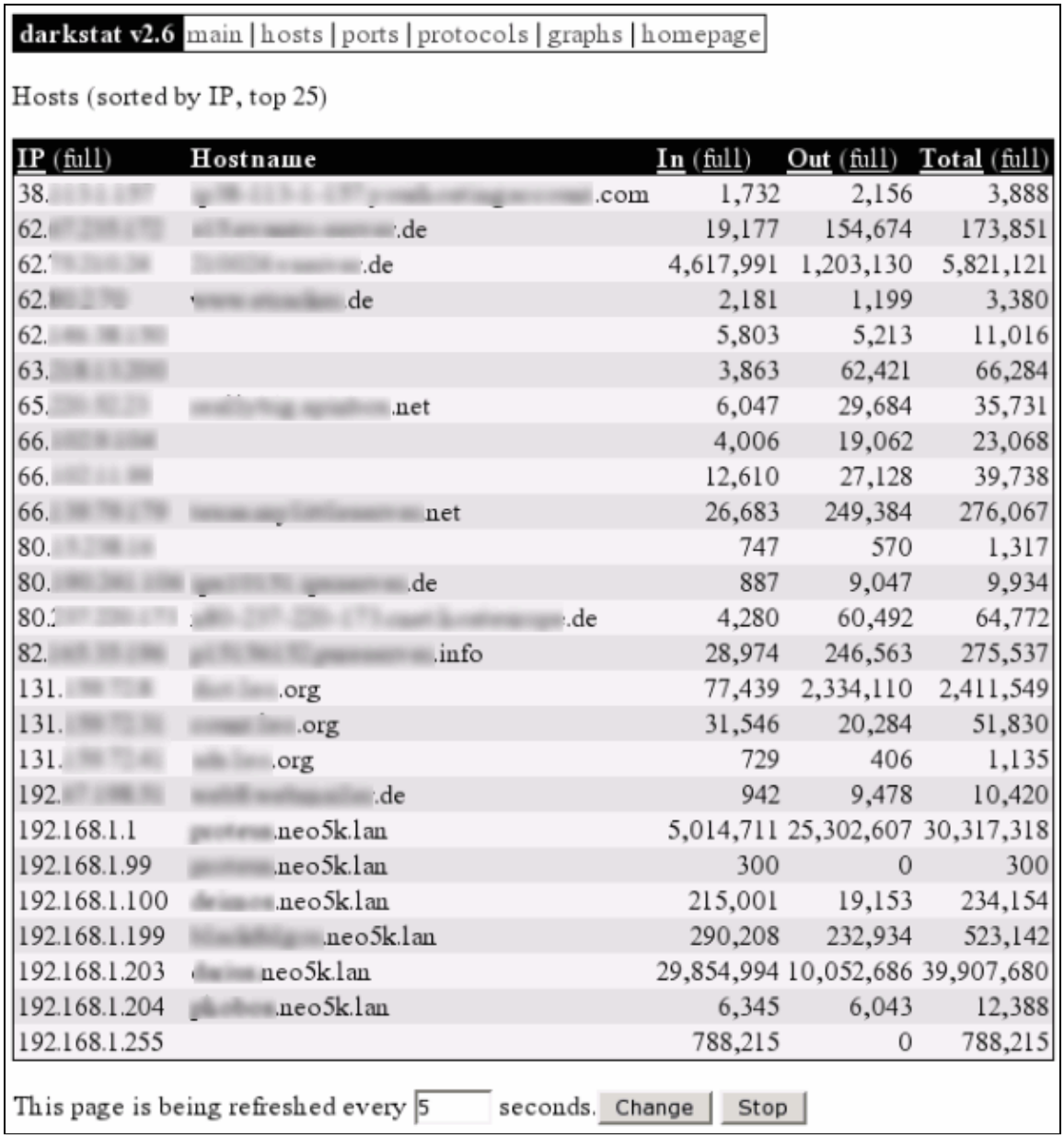


Abbildung 1: darkstat main

Unter "*hosts*" kann man alle an der Kommunikation beteiligten Maschinen erkennen. Diese lassen sich problemlos nach ihrer jeweiligen IP−Adresse oder dem verursachten Traffic anordnen. Durch diese Möglichkeit lassen sich die Rechner, die den höchsten Traffic im Netzwerk verursachen, sehr schnell ausfindig machen. Der zuständige System− bzw. Netzwerkadministrator kann der Ursache dann auf den Grund gehen. In nachfolgendem Screenshot wäre dies beispielsweise der Client mit der lokalen IP−Adresse "*192.168.1.203*".



darkstat v2.6 main | hosts | ports | protocols | graphs | homepage

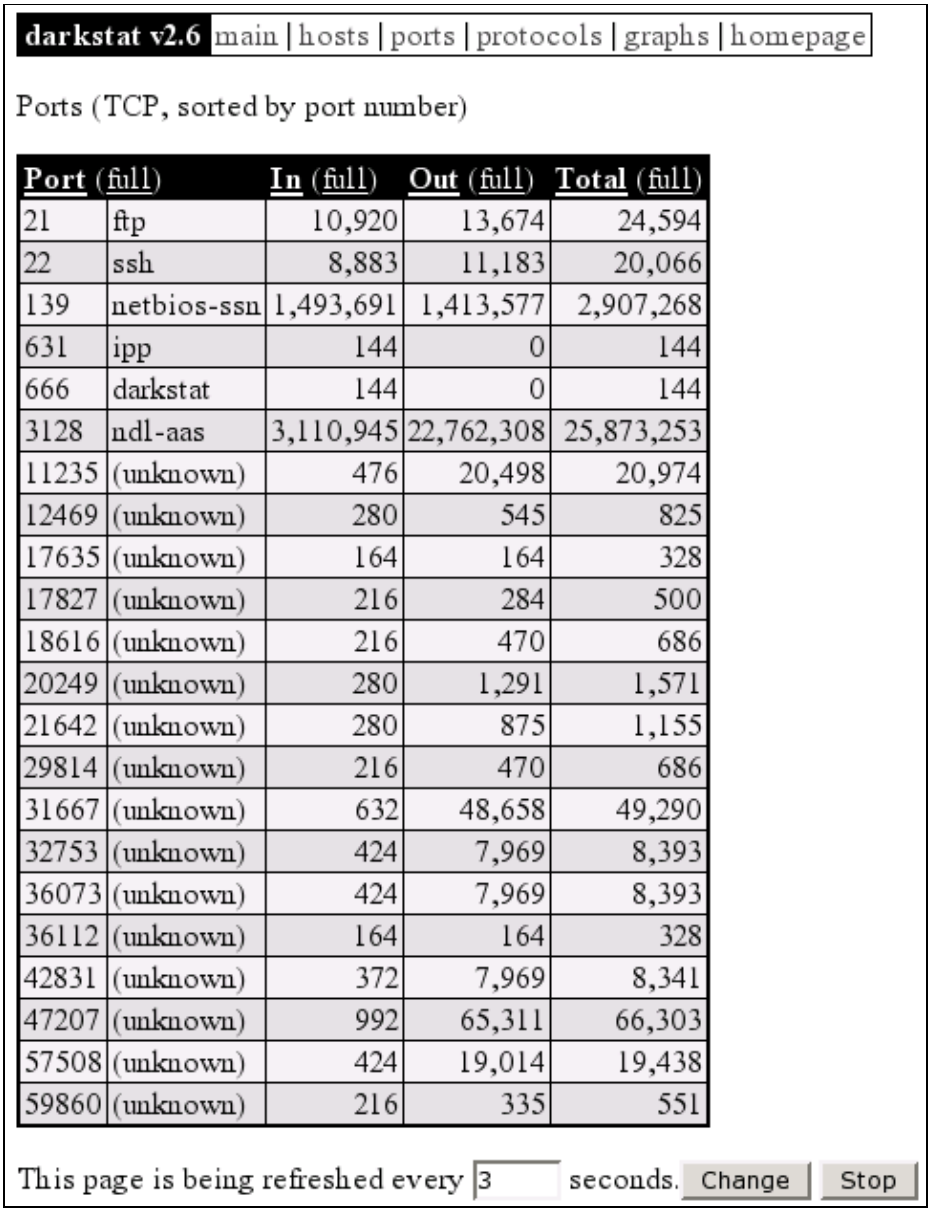
Hosts (sorted by IP, top 25)

IP (full)	Hostname	In (full)	Out (full)	Total (full)
38.	.com	1,732	2,156	3,888
62.	.de	19,177	154,674	173,851
62.	.de	4,617,991	1,203,130	5,821,121
62.	.de	2,181	1,199	3,380
62.		5,803	5,213	11,016
63.		3,863	62,421	66,284
65.	.net	6,047	29,684	35,731
66.		4,006	19,062	23,068
66.		12,610	27,128	39,738
66.	.net	26,683	249,384	276,067
80.		747	570	1,317
80.	.de	887	9,047	9,934
80.	.de	4,280	60,492	64,772
82.	.info	28,974	246,563	275,537
131.	.org	77,439	2,334,110	2,411,549
131.	.org	31,546	20,284	51,830
131.	.org	729	406	1,135
192.	.de	942	9,478	10,420
192.168.1.1	.neo5k.lan	5,014,711	25,302,607	30,317,318
192.168.1.99	.neo5k.lan	300	0	300
192.168.1.100	.neo5k.lan	215,001	19,153	234,154
192.168.1.199	.neo5k.lan	290,208	232,934	523,142
192.168.1.203	neo5k.lan	29,854,994	10,052,686	39,907,680
192.168.1.204	.neo5k.lan	6,345	6,043	12,388
192.168.1.255		788,215	0	788,215

This page is being refreshed every 5 seconds. Change Stop

Abbildung 2: darkstat hosts

In Abbildung 3 sieht man die von Serverdiensten bzw. Client−Applikationen benutzten Portnummern. Hier lassen sich sofort die von den entsprechenden Daemons genutzten Ports erkennen: *21 (FTP)*, *22 (SSH)*, *139 (Samba)*, *631 (CUPS)*, *666 (darkstat)*, *3128 (Squid)*. Nicht zu sehen sind hingegen die Portnummern der Dienste "*dhcpd*" und "*dnsmasq*", da diese per "*UDP*" kommunizieren. Alle anderen Ports größer 1024 sind unprivilegierte Ports und werden von den Clients zur Kommunikation benutzt. Eine Ausnahme stellt hierbei der Proxyserver "*Squid*" dar, da dieser standardmäßig den Port 3128 nutzt, aber trotzdem zu den Serverdiensten zählt. Eine gepflegte Übersicht aller Portnummern läßt sich bei der dafür zuständigen IANA [9] einsehen. Alternativ kann auch die auf jedem System vorhandene Datei unter "*/etc/services*" betrachtet werden.



darkstat v2.6 main | hosts | ports | protocols | graphs | homepage

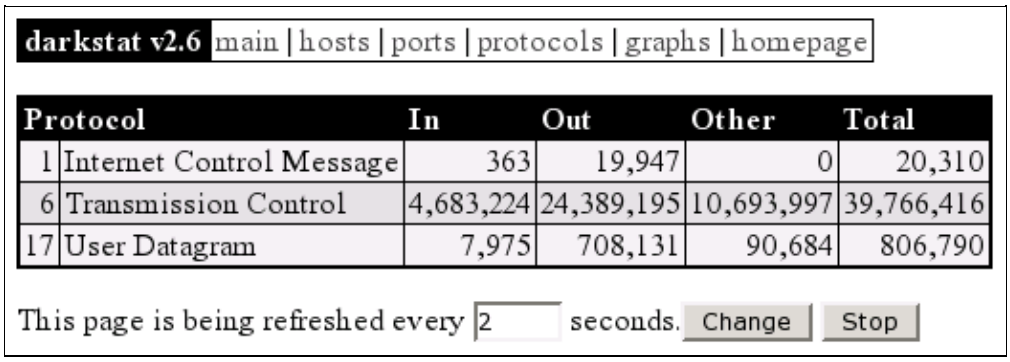
Ports (TCP, sorted by port number)

Port (full)		In (full)	Out (full)	Total (full)
21	ftp	10,920	13,674	24,594
22	ssh	8,883	11,183	20,066
139	netbios-ssn	1,493,691	1,413,577	2,907,268
631	ipp	144	0	144
666	darkstat	144	0	144
3128	ndl-aas	3,110,945	22,762,308	25,873,253
11235	(unknown)	476	20,498	20,974
12469	(unknown)	280	545	825
17635	(unknown)	164	164	328
17827	(unknown)	216	284	500
18616	(unknown)	216	470	686
20249	(unknown)	280	1,291	1,571
21642	(unknown)	280	875	1,155
29814	(unknown)	216	470	686
31667	(unknown)	632	48,658	49,290
32753	(unknown)	424	7,969	8,393
36073	(unknown)	424	7,969	8,393
36112	(unknown)	164	164	328
42831	(unknown)	372	7,969	8,341
47207	(unknown)	992	65,311	66,303
57508	(unknown)	424	19,014	19,438
59860	(unknown)	216	335	551

This page is being refreshed every 3 seconds. Change Stop

Abbildung 3: darkstat ports

Wie der Name "*protocols*" bereits vermuten läßt, zeigt die nächste Abbildung die Statistiken zu den für die Datenübertragung benötigten Protokolle "*ICMP*", "*TCP*" und "*UDP*" an. Wer sich näher für die genannten Protokolle interessiert, findet in den jeweiligen RFCs unter [10], [11] und [12] gute Einstiegspunkte.



darkstat v2.6 main | hosts | ports | protocols | graphs | homepage

Protocol		In	Out	Other	Total
1	Internet Control Message	363	19,947	0	20,310
6	Transmission Control	4,683,224	24,389,195	10,693,997	39,766,416
17	User Datagram	7,975	708,131	90,684	806,790

This page is being refreshed every 2 seconds. Change Stop

Abbildung 4: darkstat protocols

Der letzte Screenshot zeigt eine Zusammenfassung der erfassten Zeitperioden in Diagramm–Form:

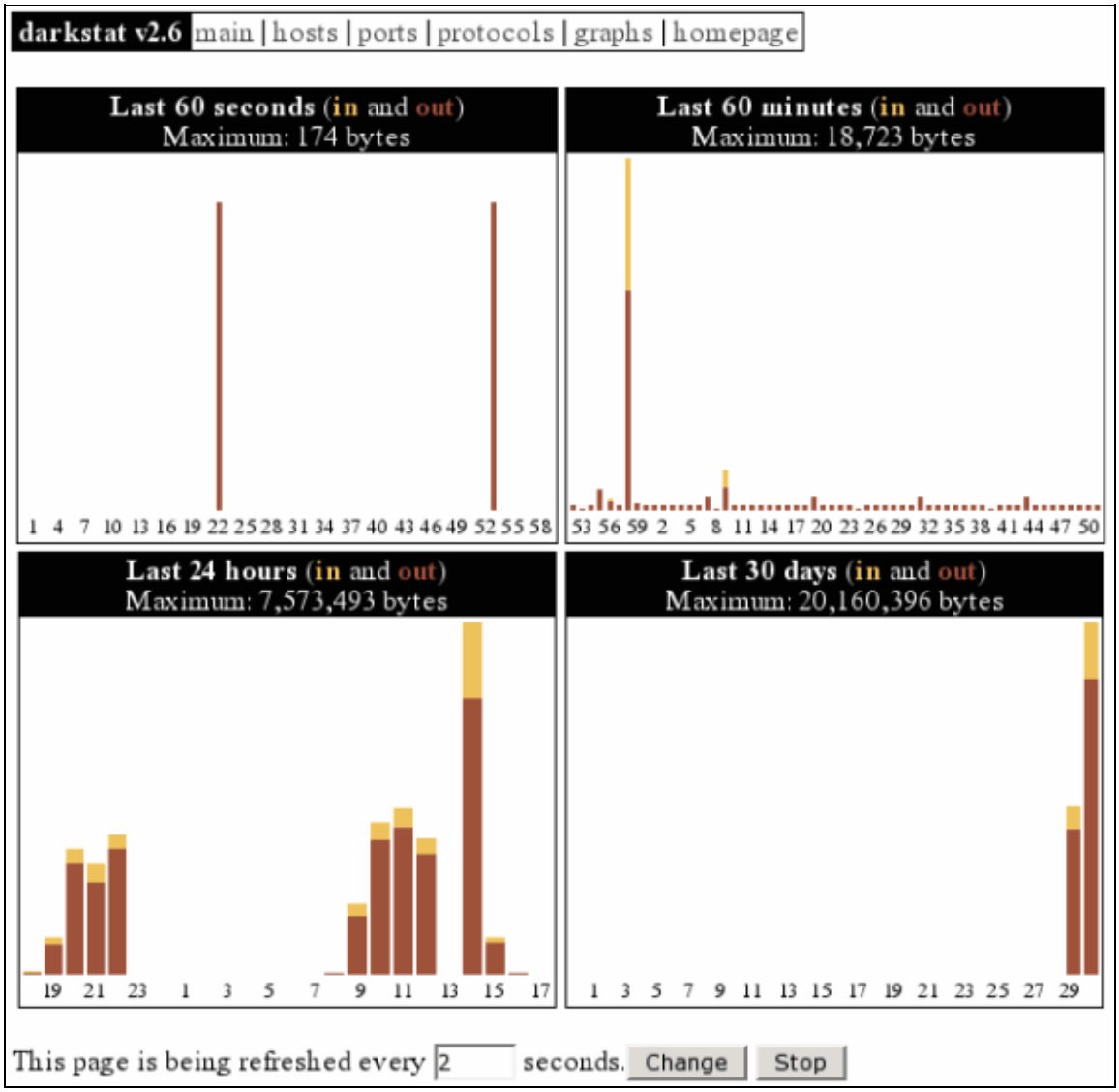


Abbildung 5: darkstat graphs

Ausblick

Die hier besprochene Version 2.6 von "*darkstat*" ist zwingend auf "*pthreads*" angewiesen, was aber auf anderen Plattformen wie beispielsweise NetBSD Probleme bereitet. Aus diesem Grund hat sich der Programmautor Emil Mikulic dazu entschlossen, die aktuelle Reihe 2 nicht mehr weiterzuentwickeln und arbeitet stattdessen bereits an Version 3.

In der neuen Version sollen Dinge wie die gleichzeitige Paketanalyse mehrerer Schnittstellen, ein Parser zur Modifikation der Konfigurationsdatei, eine optisch verbesserte Diagrammausgabe (vergleichbar mit dem RRDtool [13]), eine an die eigenen Bedürfnisse anpassbare CSS–Datei, die Möglichkeit zum Login und zur Änderung der Datenbank via Browser etc. implementiert werden.

Fazit

"*darkstat*" ist ein stabiles und performantes Network−Monitoring−Tool, das ausschließlich seinem Einsatzzweck − der Traffic−Analyse − dient und problemlos seine Arbeit verrichtet. Des Weiteren befindet es sich in ständiger Entwicklung und wird in der zukünftigen Version 3 sicherlich viele weitere interessante und brauchbare Funktionsmerkmale beinhalten. Bis dahin wünsche ich allerdings noch viel Erfolg auf der Suche nach den "Traffic−Sündern"!

Links

[1] http://purl.org/net/darkstat [Home of darkstat]
[2] http://www.ntop.org/ [Home of ntop]
[3] http://dmr.ath.cx/net/darkstat/darkstat−2.6.tar.gz [Download]
[4] http://yallara.cs.rmit.edu.au/~emikulic/_/darkstat−2.6.tar.gz [Download Mirror #1]
[5] http://neo5k.de/downloads/files/darkstat−2.6.tar.gz [Download Mirror #2]
[6] http://ftp.debian.org/debian/pool/main/d/darkstat/ [Debian Packages]
[7] http://www.tcpdump.org/ [Home of libpcap]
[8] http://www.courtesan.com/sudo/ [Home of sudo]
[9] http://www.iana.org/assignments/port−numbers [IANA Port−Numbers]
[10] ftp://ftp.rfc−editor.org/in−notes/rfc792.txt [RFC 792 − ICMP]
[11] ftp://ftp.rfc−editor.org/in−notes/rfc793.txt [RFC 793 − TCP]
[12] ftp://ftp.rfc−editor.org/in−notes/rfc768.txt [RFC 768 − UDP]
[13] http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/ [Home of RRDtool]

Translation information:
de −−> −− : Mario M. Knopf (homepage)

2005−01−11, generated by lfparser_pdf version 2.51