by Mario M. Knopf (homepage)

About the author:

Mario sangat menikmati untuk tetap sibuk bersama Linux, jaringan dan topik−topik lainnya yang berkaitan dengan masalah keamanan komputer.

darkstat – Penganalisa Trafik Jaringan

Abstract:

Artikel ini mempersembahkan penganalisa trafik jaringan "*darkstat*" dan memberikan gambaran mengenai instalasi , memulai dan menggunakan program ini.

Translated to English by:
Mario M. Knopf (homepage)

Perkenalan

"*darkstat*" [1] adalah tool untuk memonitor jaringan, yang menganalisa trafik keluaran dari jaringan dan menghasilkan keluaran Statistik HTML berbasis pada data keluaran. Statistik tersebut bisa dilihat dengan nyaman pada browser. Untuk semua kegunaan tersebut, Emil Mikulic, punya "*ntop*" [2] yang dia gunakan untuk waktu yang lama. Tetapi Dia terganggu karena ketidakstabilan dan perilaku jelek memory−nya. Untuk alasan inilah dia mengembangkan "*darkstat*". Statistik trafik yang dialamatkan mengarah ke komunikasi antar host, penyebab trafik dan alternatif nomer port yang terpakai melibatkan protocol transmisi.
Diagram−diagram tambahan untuk periode waktu (time periods) terkoleksi dan ringkasan pendek dari paket yang dianalisa sejak program berjalan bisa diandalka.

Instalasi

Kode sumber dari program "darkstat" didapatkan langsung pada [3]. Alternatif−nya juga salah satu dari dua mirror yang bisa Anda kunjungi di [4] dan [5]. Jika seseorang mencari paket Debian, bisa didapatkan pada [6].

"*darkstat*" juga tergantung paket lain, seperti alat monitor jaringan lainnya, pada file "*libpcap*" [7]. File ini adalah library, yang digunakan oleh packet sniffers dan menyediakan mereka sebuah antarmuka untuk menangkap dan menganalis paket dari perangkat jaringan. Untuk menginstall "*darkstat*" Anda membutuhkan library ini lebih dahulu.

Lalu Anda harus melakukan compile dengan menggunakan tiga set perintah yang telah dikenal "*./configure && make && make install*". Ini sangatlah penting, bahwa instruksi terakhir harus dilakukan dengan hak sebagai root.

Memulai

"*darkstat*" menawarkan beberapa parameter, yang bisa di atur saat program mulai berjalan. Bagaimanapun, untuk pertama kalinya mencoba memulai program ini tanpa opsi apa–apa sudah cukup. Dan untuk bisa melakukan pekerjaannya, bagaimanpun program harus dimulai sebagai root atau dengan "*sudo*"–privileges [8]:

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

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

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

Password:
```

Setelah user terdaftar memasukkan password, "*darkstat*" mulai dan mencetak berbagai pesan status:

```
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.
```

Karena test telah sukses dan output telah self–describing, kita bisa melihat pada beberapa parameter permulaan yang memungkinkan dipakai.

Opsi Permulaan

Seperti yang disebutkan sebelumnya, "*darkstat*" menyediakan beberapa opsi , yang mana bisa dengan sederhana disediakan saat startup. Paramater itu adalah:

Dengan opsi "*–i*" Anda bisa spesifikasikan interface mana yang akan di monitor.

darkstat –i eth1

Dimulai tanpa parameter spesial , "*darkstat*" membuka hak–hak pakai pada 666. Anda bisa menghindari kebiasaan ini , jika Anda memulainya dengan parameter "*–p*":

darkstat –p 8080

Dan untuk melakukan proses bind terhadapa beberapa port pada interface tertentu, Anda bisa menggunakan opsi "*−b*". Dalam contoh berikut terhadap alamat loopback lokal:

darkstat −b 127.0.0.1

Persistent DNS−Resolution bisa dihindari dengan menggunakan parameter "*−n*". Ini akan bagus untuk orang−orang yang tidak mempunyai koneksi *flatrate* atau *dedicated line*.

darkstat −n

Gunakan opsi "*−P*" untuk menghindarkan "*darkstat*" menempatkan interface kedalam mode "*promiscuous* ". Bagaimanapun, ini tidak dikeromendasikan, karenae "*darkstat*" hanya menangkap dan menganalisa paket−paket, yang dialamatkan ke alamat MAC dari interface jaringan yang termonitor. Seluruh paket−paket yang lain ditolak.

darkstat −P

Parameter "*−l*" mengaktifkan dengan benar "*SNAT*"−pada jaringan lokal. "*SNAT*" singkatan dari "*Source Network Address Translation*" dan berarti router Anda melakukan *masking* terhadap Alamat client IP lokal Anda dengan kepemilikan publiknya. Lalu mengirimkan ketersediaan *inquiry* untuk *inquire client* yang asli.

darkstat −l 192.168.1.0/255.255.255.0

Dengan parameter "*−e*" Anda bisa melakukan filter paket expresi.

darkstat −e "port not 22"

Dari versi 2.5 keatas Anda bisa melakukan "*detach darkstat*" dari terminal yang memulai program. Maka dia bekerja seperti daemon.

darkstat −−detach

Melalui parameter "*−d*" Anda bisa melakukan spesifikasi terhadap direktori mana "*darkstat*" akan menciptakan database−nya.

darkstat −d /directory

Opsi "*−v*" mengaktifkan "*verbose mode*":

darkstat −v

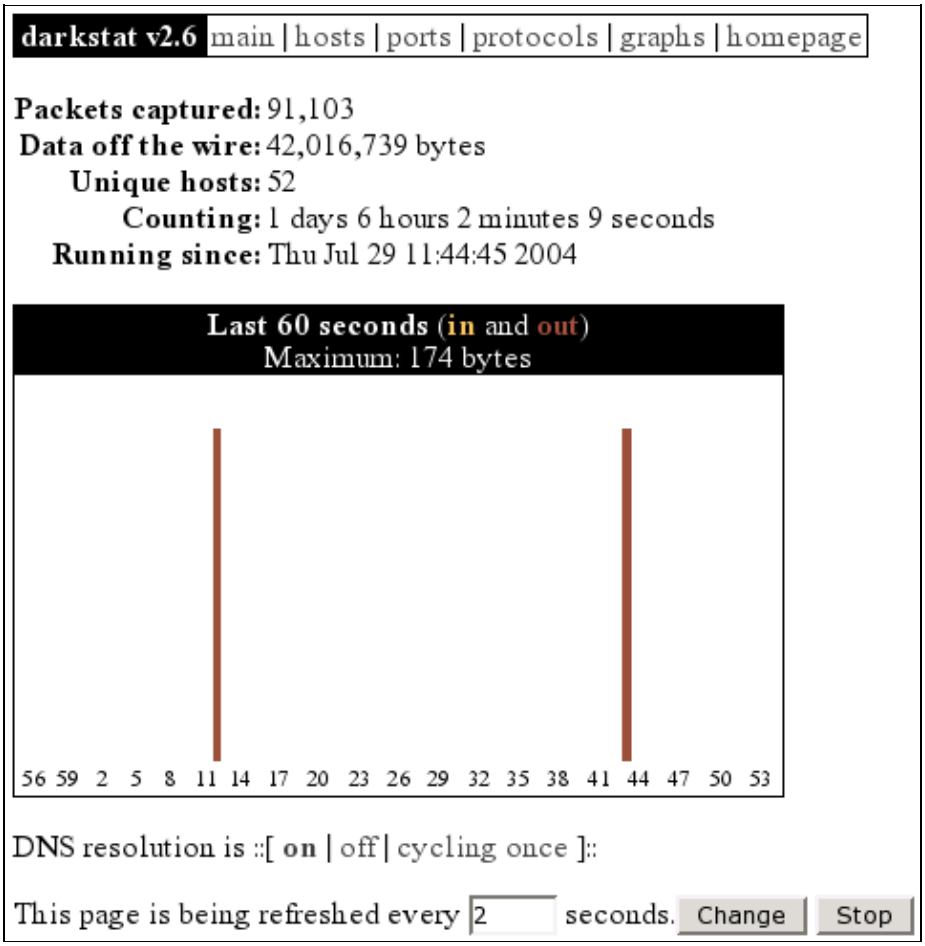
Jika Anda tertarik pada nomer versi dari "*darkstat*" atau pemakaian penuh dan syntax−nya, cobalah parameter "*−h*".

darkstat −h

Penanganan

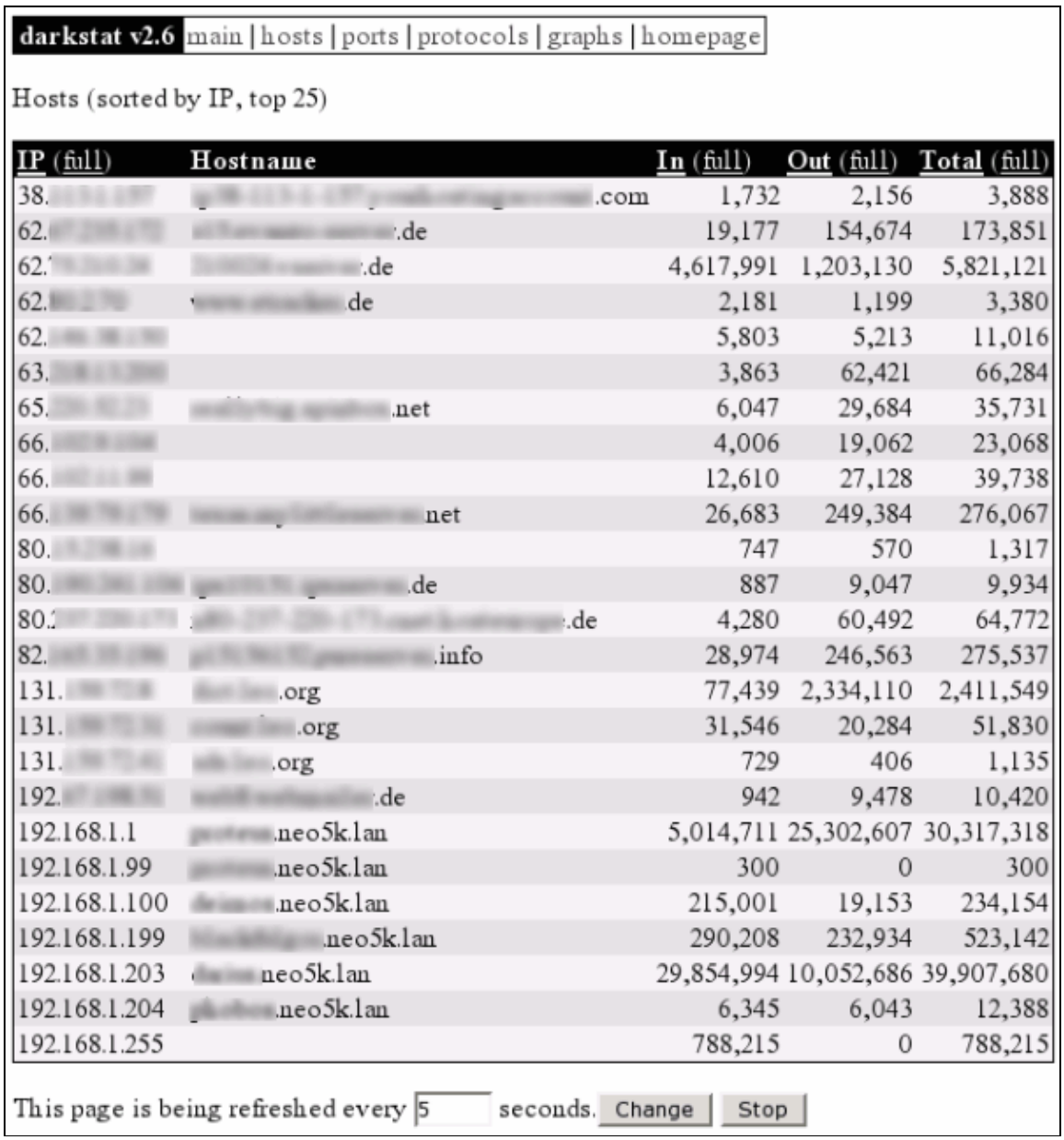
Setelah permulaan bekerja dari "*darkstat*" Anda bisa mengarahkan browser Anda ke "*http://localhost:666/*", yang menjadi defaultnya. Sekarang Anda bisa melihat pada summary singkat dari statistik keluaran dan

beberapa gambar yang dihasilkan oleh program sejak dijalankan:



Gambar 1: Tampilan Utama darkstat

Pada situs "*hosts*" Anda bisa melihat semua mesin yang terlibat pda proses komunikasi jaringan. Ini bisa diatur menggunakan *caused traffic* atau alamat IP partikular mereka. dengan kemungkinan ini Anda bisa mendeteksi mesin–mesin, yang menghasilkan trafik tertinggi pda jaringan lokal, dengan sangat cepat. Lalu system administrator yang bertanggung jawab mempunyai kesempatan untuk menyentuh dasar permasalahan jaringannya. Sebagai contoh, pada cuplikan gambar berikut adalah mesin client dengan Alamat IP lokal "*192.168.1.203*".



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

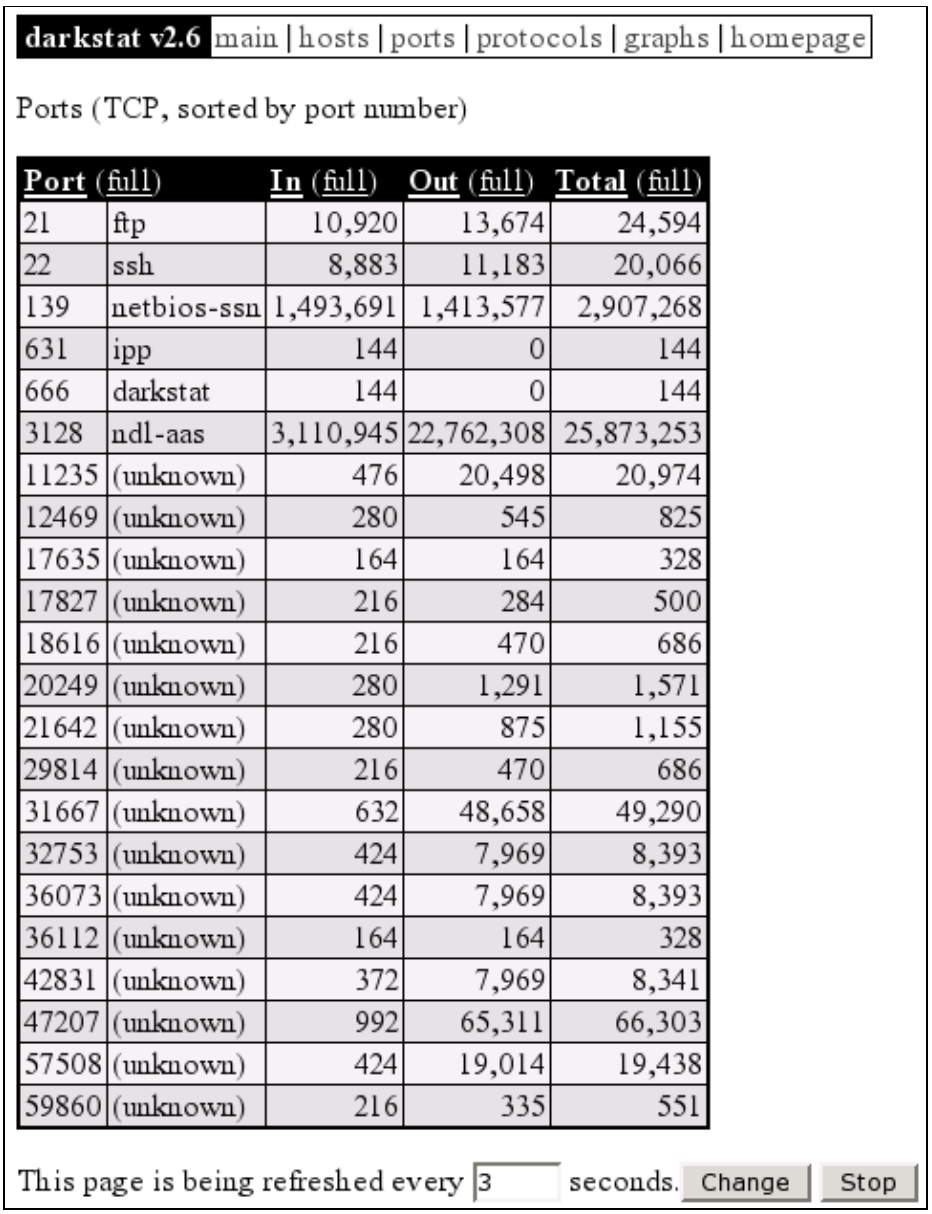
Hosts (sorted by IP, top 25)

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

Gambar 2: Hosts darkstat

Pada gambar 3 Anda dapat melihat nomer−nomer port yang digunakan oleh server dan aplikasi−aplikasi client. Lalu Anda secara langsung dapat mengenali nomer−nomer port berapa yang digunakan oleh daemon−daemon berikut ini: *21 (FTP)*, *22 (SSH)*, *139 (Samba)*, *631 (CUPS)*, *666 (darkstat)*, *3128 (Squid)*. Bagaimanapunr, dua servis "*dhcpd*" dan "*dnsmasq*" tidaklah terlihat, dikarenakan dua servis ini berkomunikasi melalui "*UDP*". Semua port yang lebih besar dari 1024 tidak di buka privilege−nya dan digunakan oleh aplikasi client untuk komunikasi. Server proxy "*squid*" mewakili pengecualian , karena dia menggunakan port 3128 sebagai setting default−nya. Anda bisa melihat daftar yang terurus dari seluruh nomor port pada IANA [9], yang bertanggungjawab terhadap hal ini. Sebagai alternative Anda bisa melihat pada file "*/etc/services*".



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

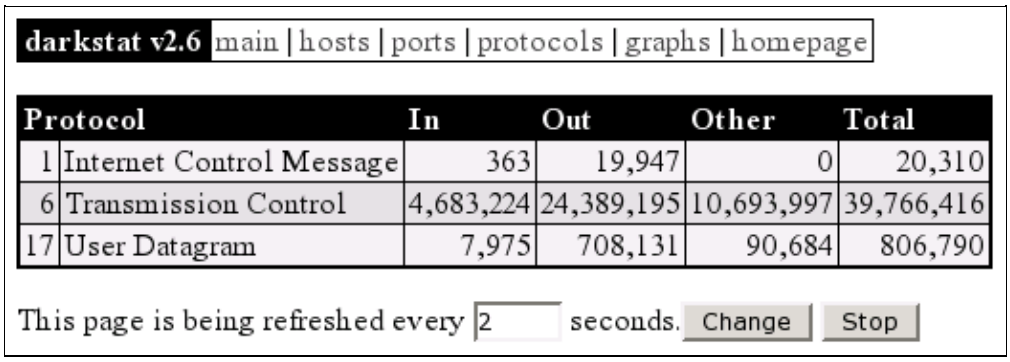
Ports (TCP, sorted by port number)

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

Gambar 3: Port−port darkstat

Pada gambar berikut Anda dapat melihat protokol−protokol "*ICMP*", "*TCP*" and "*UDP*" sebagai sarana transmisi file, yang juga terlibat pada even komunikasi jaringan. Jika seseorang tertarik pada protokol−protokol ini, dia akan menemukan pengenalan yang bagus pada RFC berikut di [10], [11] and [12].



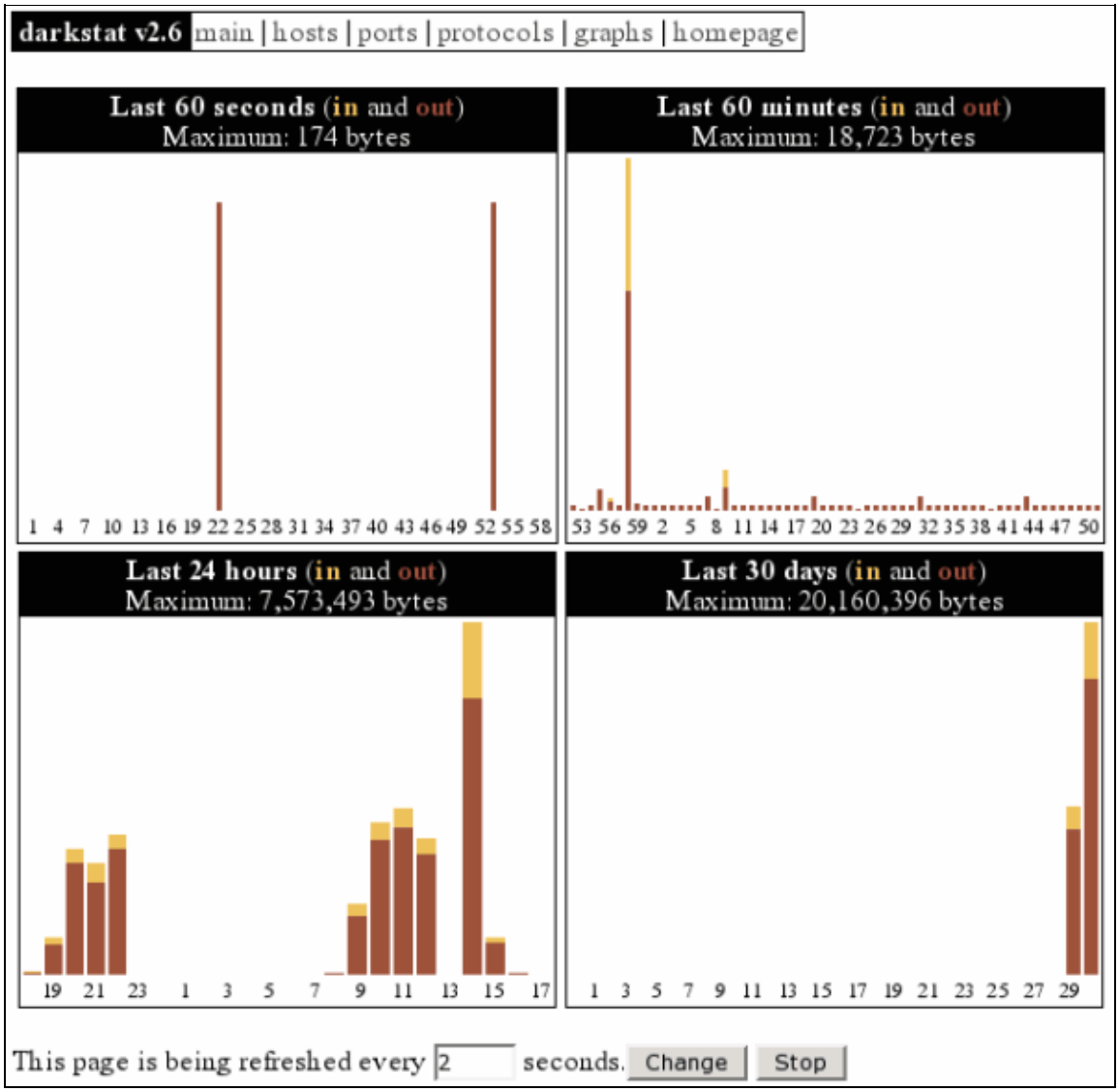
darkstat v2.6 main | hosts | ports | protocols | graphs | homepage

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

Gambar 4: Protokol−protokol darkstat

Cuplikan gambar yang terakhir menunjukkan sebuah hasil dari *collected time periods* dalam grafik:



Gambar 5: Grafik darkstat

Prospek Masa Depan

Versi 2.6 dari "*darkstat*" tentang apa yang kita diskusikan disini , sayangnya tergantung pada "*pthreads*". Ini menyebabkan beberapa masalah pada platform lain (contohnya : NetBSD). Untuk alasan ini pembuat program Emil Mikulic memutuskan untuk tidak mengembangkan versi 2.x lagi dan bekerja langsung pada versi 3.x.

Pada versi baru beberapa hal diimplementasikan seperti menangkap paket−paket dari beberapa interface secara simultan, konfigurasi file parser, output secara optikal yang meningkatkan output untuk diagram (bisa ditandingkan dengan RRDtool [13]), CSS−file yang bisa dikustomisasi, login admin dan pengeditan database melalui interface web dan lain−lain.

Kesimpulan

"*darkstat*" adalah alat pemantau jaringan yang cepat dan sangat stabil, yang secara ekslusif menyediakan kegunaan – untuk menganalisa trafik. Lebih jauh lagi alat ini bekerja tanpa masalah, dikembangkan secara konstan dan akan memiliki banyak fitur yang baru dan menarik pada versi yang akan datang . Lalu saya berharap untuk lebih sukses lagi dengan pencarian terhadap "traffic sinners" pada jaringan–jaringan lokal Anda.

Link–Link

[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)
de –> en: Mario M. Knopf (homepage)
en –> id: Razmal Djamal (homepage)

2005–01–10, generated by lfparser_pdf version 2.51