



par Mario M. Knopf ([homepage](#))

*L'auteur:*

Marios adore s'occuper avec Linux, les réseaux et les autres domaines touchants à des problèmes de sécurité.

## darkstat – un analyseur de trafic



*Résumé:*

Cet article présente l'analyseur de trafic "darkstat" et donne un aperçu concernant son installation, son démarrage et son utilisation.

---

*Traduit en Français par:*  
Guillaume Lehmann  
([homepage](#))

## Introduction

"darkstat" [1] est un outil d'analyse réseau qui analyse le trafic réseau et génère, depuis les données récoltées, tout un tas de statistiques au format html. Ces statistiques peuvent être simplement visualisées dans un navigateur web. En ce qui concerne l'auteur du programme, Emil Mikulic, il a utilisé "ntop" [2] pendant un long moment. Mais il s'en est désintéressé à cause de ces problèmes de stabilité et sa mauvaise gestion de la mémoire. Pour ces raisons, il développa "darkstat". Les statistiques se basent sur la communication entre les hôtes, le trafic engendré, et le numéro des ports utilisés (en alternative des protocoles de transmission). De plus, on peut visualiser des diagrammes sur la période de collecte et un court résumé sur les paquets analysés depuis que le programme est démarré.

## Installation

Le code source du programme "darkstat" est directement accessible ici [3]. En alternative, quelques miroirs peuvent être visités à [4] et [5]. Si quelqu'un cherche des paquets Debian, il les trouvera ici [6].

"darkstat" dépend aussi, comme de nombreux outils de monitoring réseau, de la bibliothèque "libpcap" [7]. C'est une bibliothèque utilisée par les sniffers de paquets et qui leur fournit une interface de capture et d'analyse des paquets venant de l'interface réseau. Pour installer "darkstat", vous avez donc besoin de cette bibliothèque.

Ensuite vous devez compiler les sources suivant la syntaxe bien connue `./configure && make && make install`. Il est important que la dernière instruction soit exécutée avec les droits du root.

## Démarrage

"*darkstat*" offre quelques paramètres qui peuvent être définis au démarrage du programme. Cependant, pour faire un premier test, un démarrage sans option est suffisant. Pour pouvoir effectuer son travail, il faut cependant démarrer le programme en tant que root ou avec les privilèges adéquats par l'intermédiaire de "*sudo*" [8] :

```
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:
```

Après que les utilisateurs autorisés aient entré leurs mots de passe, "*darkstat*" démarre et affiche divers messages d'état :

```
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.
```

Vu que le test s'est bien déroulé et que les messages en sortie le confirment, nous pouvons maintenant jeter un oeil aux paramètres de démarrage disponibles.

## Options de démarrage

Commen mentionné précédemment, "*darkstat*" fournit plusieurs options qui peuvent être indiquées au démarrage. Ces paramètres sont :

Avec l'option "*-i*" vous pouvez spécifier quelle interface est monitorée.

```
darkstat -i eth1
```

Démarré sans privilège spécifique, "*darkstat*" ouvre le port privilégié 666. Vous pouvez prévenir cette habitude en renseignant l'option "*-p*" au démarrage :

```
darkstat -p 8080
```

Afin de lier certains ports à une interface spécifique, vous pouvez utiliser l'option "-b". Dans l'exemple suivant, nous la liions à l'adresse de loopback :

```
darkstat -b 127.0.0.1
```

La résolution DNS persistante peut être prévue en utilisant le paramètre "-n". Cela peut être intéressant pour les personnes n'ayant pas de ligne spécialisée ou dédiée.

```
darkstat -n
```

Utilisez l'option "-P" pour que "darkstat" ne mette pas l'interface réseau en "mode promiscuité". Cependant, cela n'est pas recommandé, car "darkstat" ne pourra capturer et analyser que les paquets qui sont adressés à l'adresse MAC de l'interface réseau. Tous les autres paquets sont rejetés.

```
darkstat -P
```

Le paramètre "-l" active correctement le comportement "SNAT" sur le réseau local. "SNAT" signifie "Source Network Address Translation" (Translation d'adresse source), ce qui veut dire que votre routeur masque l'adresse IP locale du client en la remplaçant par sa propre adresse publique. Ainsi, il envoie une enquête représentative du client surveillé.

```
darkstat -l 192.168.1.0/255.255.255.0
```

Avec le paramètre "-e", vous pouvez définir une expression pour filtrer les paquets.

```
darkstat -e "port not 22"
```

Depuis la version 2.5, vous pouvez détacher "darkstat" du terminal dans lequel il a été démarré. Ainsi il fonctionne comme un démon.

```
darkstat --detach
```

Grâce au paramètre "-d" vous pouvez spécifier le répertoire où "darkstat" créera sa base de données.

```
darkstat -d /directory
```

L'option "-v" active le "mode verbeux":

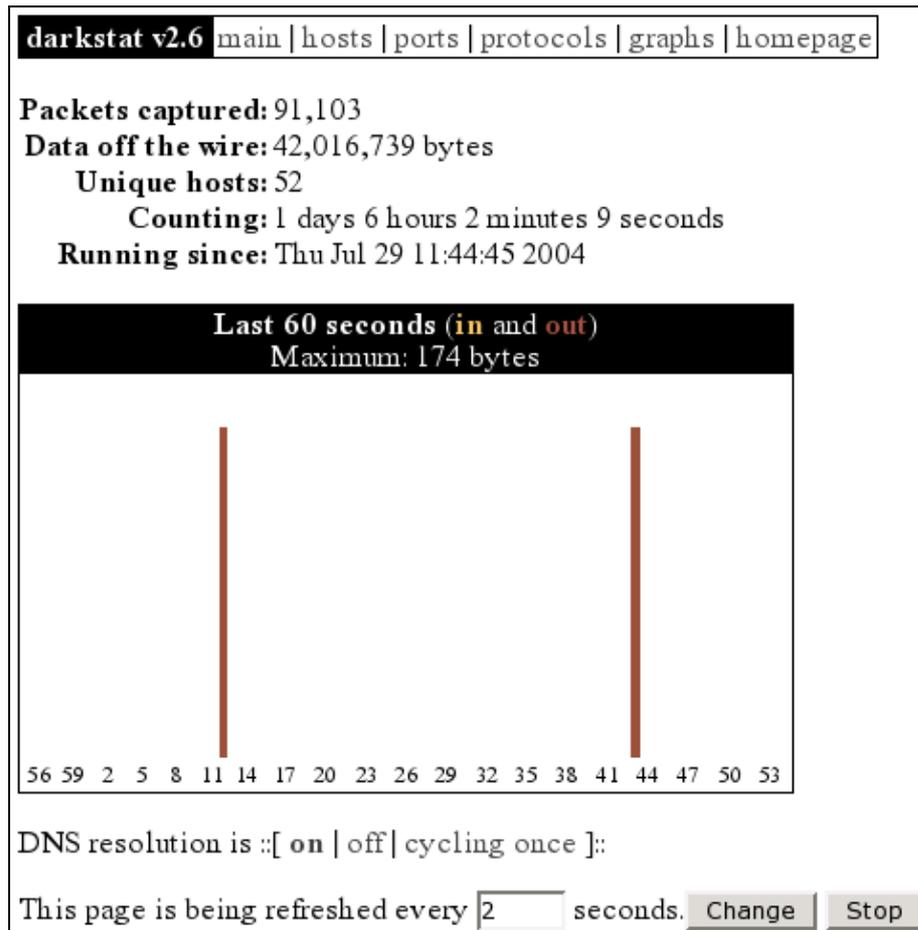
```
darkstat -v
```

Si vous êtes intéressé par le numéro de version de "darkstat" ou par toutes ses utilisations et syntaxes, essayez le paramètre "-h".

```
darkstat -h
```

## Manipulation

Après le démarrage de "darkstat" vous pouvez taper dans votre navigateur web "http://localhost:666/". C'est l'adresse par défaut. Maintenant, vous accédez à des statistiques donnant un court résumé et quelques graphiques générés sur des données collectées depuis que le programme est lancé :



*Illustration 1: page principale de darkstat*

Sur le site "hosts" vous pouvez voir toutes les machines qui prennent part à la communication. Cela peut être ordonné par trafic généré ou par adresse IP. Ainsi, vous pouvez détecter très rapidement la machine qui génère le plus de trafic sur le réseau local. De ce fait, l'administrateur système a une chance d'avoir la source d'un problème. Par exemple, dans la capture d'écran suivante, la source du problème pourrait bien être le client dont l'adresse IP est "192.168.1.203".



darkstat v2.6 <a href="#">main</a>   <a href="#">hosts</a>   <a href="#">ports</a>   <a href="#">protocols</a>   <a href="#">graphs</a>   <a href="#">homepage</a>				
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  seconds. [Change](#) [Stop](#)

Illustration 3: menu ports dans darkstat

Dans l'image suivante vous pouvez voir les protocoles "ICMP", "TCP" et "UDP" qui ont été impliqués dans les communications. Si quelqu'un est intéressé par ces protocoles, il trouvera des introductions intéressantes dans les RFC suivantes [10], [11] et [12].

darkstat v2.6 <a href="#">main</a>   <a href="#">hosts</a>   <a href="#">ports</a>   <a href="#">protocols</a>   <a href="#">graphs</a>   <a href="#">homepage</a>					
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  seconds. [Change](#) [Stop](#)

Illustration 4: menu protocols dans darkstat

La dernière capture d'écran montre un graphique-résumé sur la période de collecte :

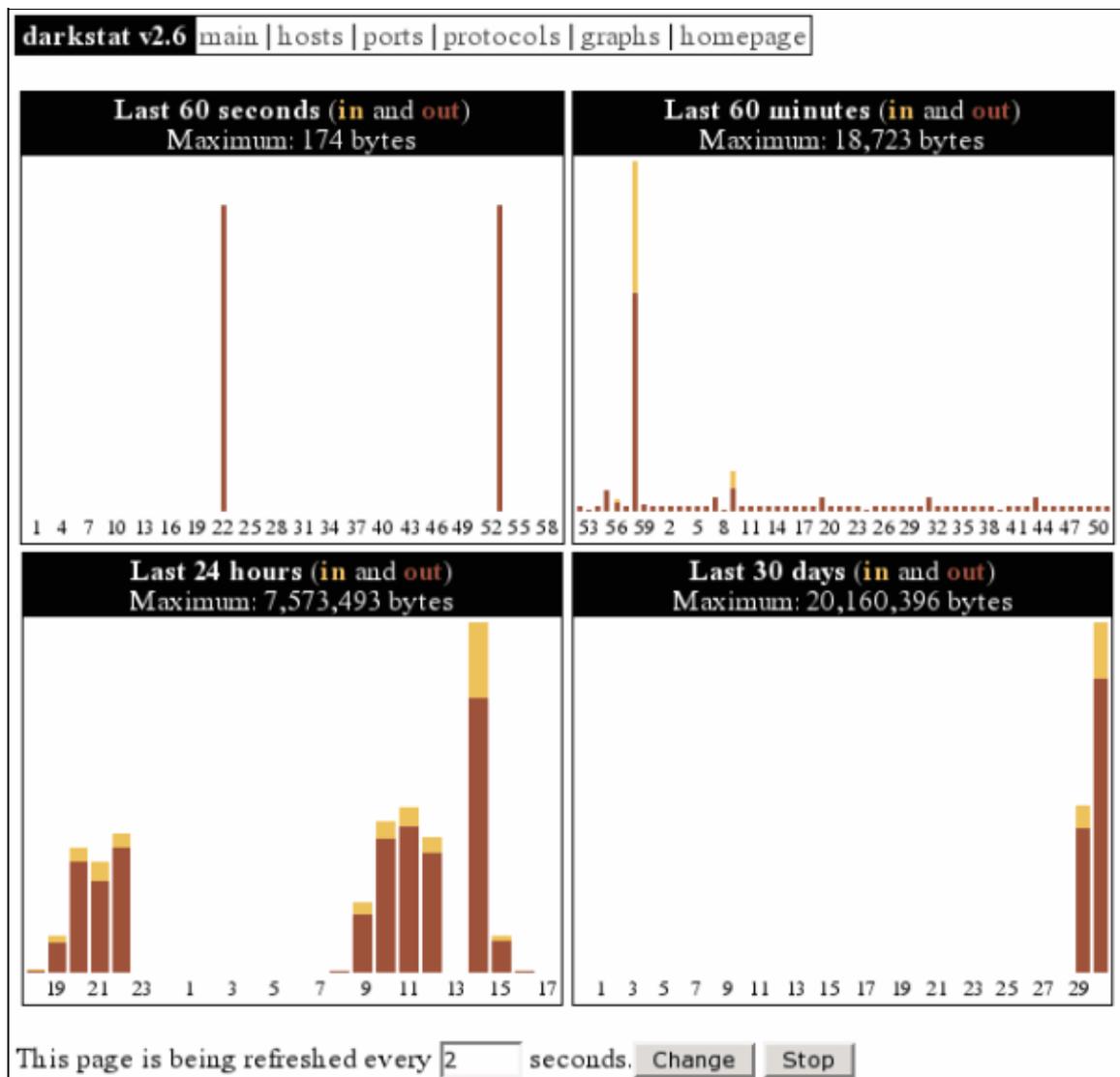


Illustration 5: menu graphs dans darkstat

## Futur du projet

La version 2.6 de "darkstat" que nous venons de voir, est malheureusement dépendante de "pthreads". Cela pose des problèmes sur certaines plateformes (comme NetBSD). Pour cette raison, l'auteur du programme, Emil Mikulic, a décidé de ne pas continuer de développer la branche 2.x et préfère travailler directement sur la 3.x.

Dans la nouvelle version, certaines nouveautés ont été implémentées comme la capture simultanée de paquets depuis plusieurs interfaces, un parseur de configuration (config parser), une amélioration de la présentation visuelle des diagrammes (comparable à RRDtool [13]), un fichier CSS personnalisable, la présence d'un login administrateur, la possibilité d'éditer la base de données à travers l'interface web, etc .

# Conclusion

"darkstat" est un outil de surveillance très stable et rapide. Il ne fait exclusivement que ce pourquoi il est écrit : analyser le trafic. En outre, il fonctionne sans problème, évolue constamment et contiendra de nombreuses nouvelles et intéressantes fonctionnalités dans les prochaines versions. Je vous souhaite du succès dans votre recherche de "trafics indésirables" dans votre réseau local.

## Liens

- [1] <http://purl.org/net/darkstat> [Site web de darkstat]
- [2] <http://www.ntop.org/> [Site web de ntop]
- [3] <http://dmr.ath.cx/net/darkstat/darkstat-2.6.tar.gz> [Téléchargement]
- [4] <http://yallara.cs.rmit.edu.au/~emikulic/ /darkstat-2.6.tar.gz> [Miroir pour le téléchargement #1]
- [5] <http://neo5k.de/downloads/files/darkstat-2.6.tar.gz> [Miroir pour le téléchargement #2]
- [6] <http://ftp.debian.org/debian/pool/main/d/darkstat/> [Paquets Debian]
- [7] <http://www.tcpdump.org/> [Site web de libpcap]
- [8] <http://www.courtesan.com/sudo/> [Site web de sudo]
- [9] <http://www.iana.org/assignments/port-numbers> [Numéros de ports référencés par l'IANA]
- [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/> [Site web de RRDtool]

<p>Site Web maintenu par l'équipe d'édition LinuxFocus © Mario M. Knopf "some rights reserved" see <a href="http://linuxfocus.org/license/">linuxfocus.org/license/</a> <a href="http://www.LinuxFocus.org">http://www.LinuxFocus.org</a></p>	<p>Translation information: de --&gt; -- : Mario M. Knopf (<a href="#">homepage</a>) de --&gt; en: Mario M. Knopf (<a href="#">homepage</a>) en --&gt; fr: Guillaume Lehmann (<a href="#">homepage</a>)</p>
---	---