

IP Tr@pper
ISS Dubai 2007



jean-philippe.lelievre@fr.thalesgroup.com



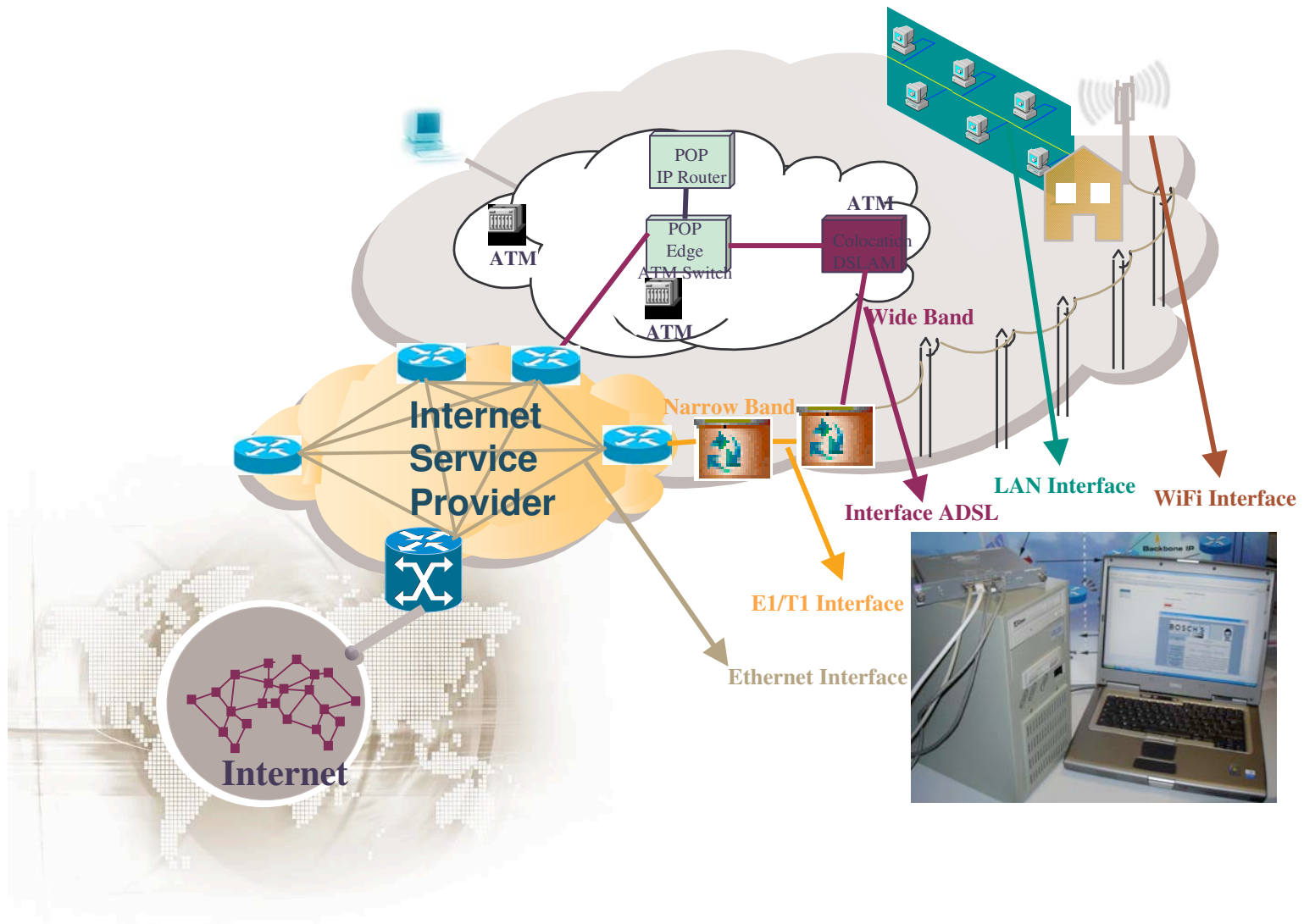
■ Autonomous facility for IP Monitoring :

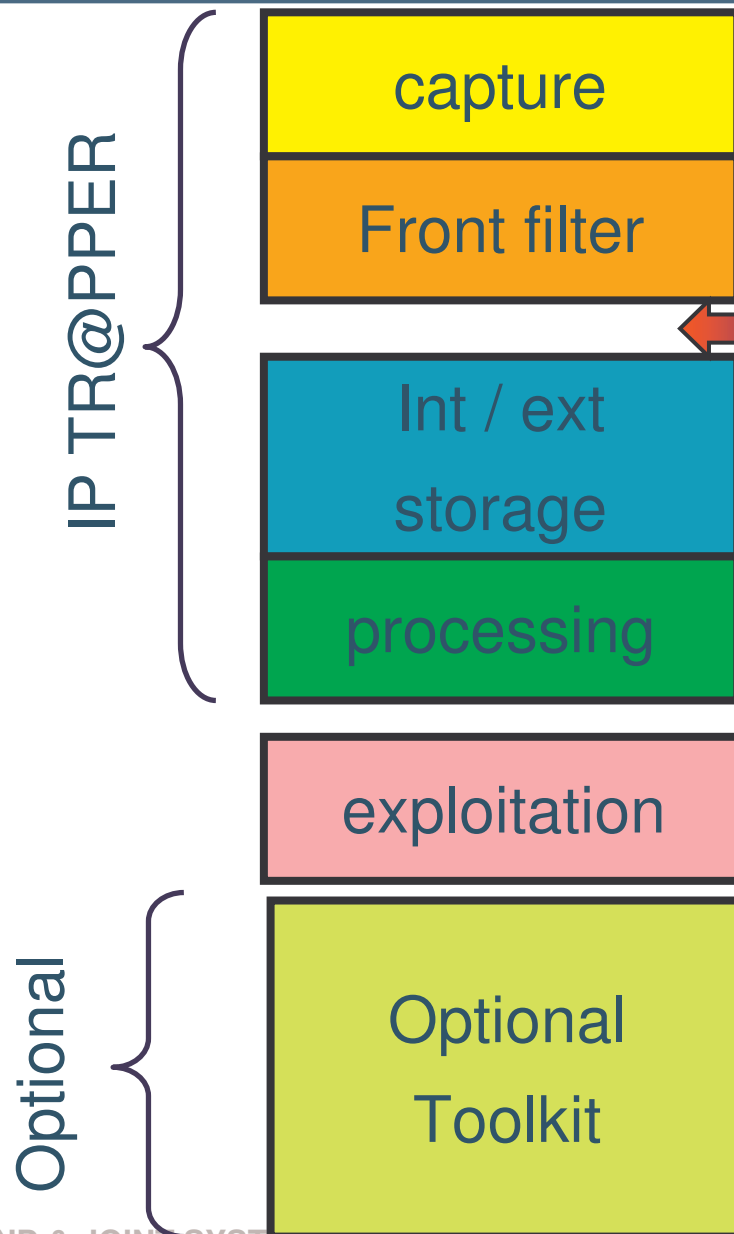
- Traffic Analysis
 - (Intranet)
 - for Internet (Internet access point)
 - among mail servers
 - for dedicated line as “Internet Cafés”
 - for Wireless connection as WIFI

■ Proposed Interfaces

- LAN : Ethernet 10/100/1G
- ADSL
- WIFI
- ATM
- (WiMax)

IP Monitoring Access point





- Passive monitoring through Tap equipment

- Real Time Filtering on port Nb, protocols, IP @ range

- Possibility to import IP traffic

- Secured Stockage of all monitored Data

- Automatic detection and decoding : web, mail, VoIP, data

- Local or remote operation

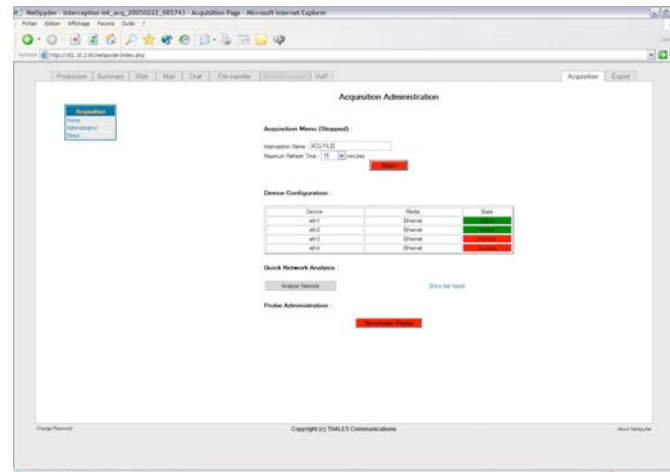
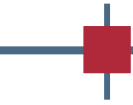
- Operation filtering

- Text mining

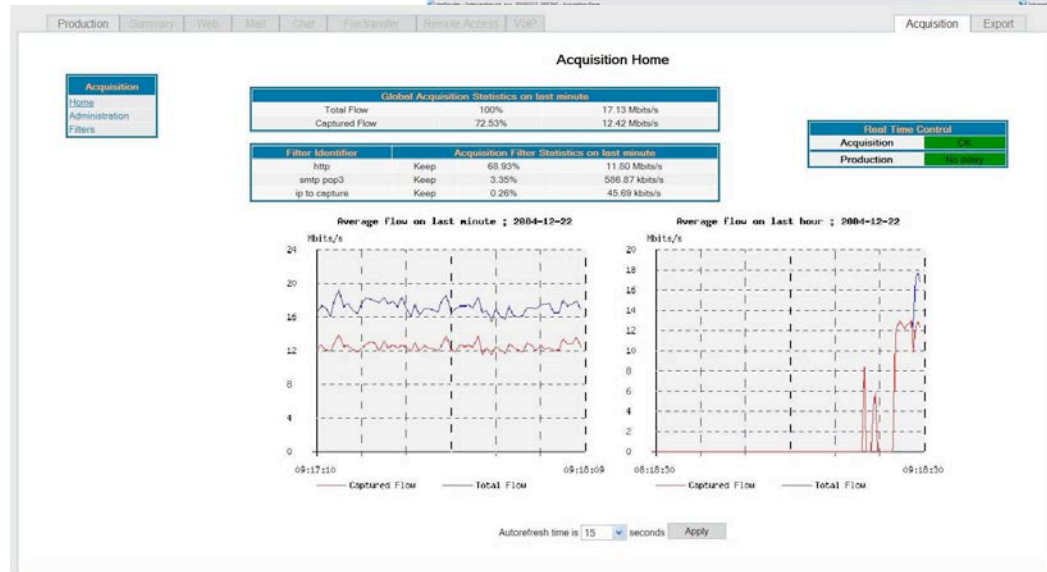
- Link analysis

- Encryption detection & information

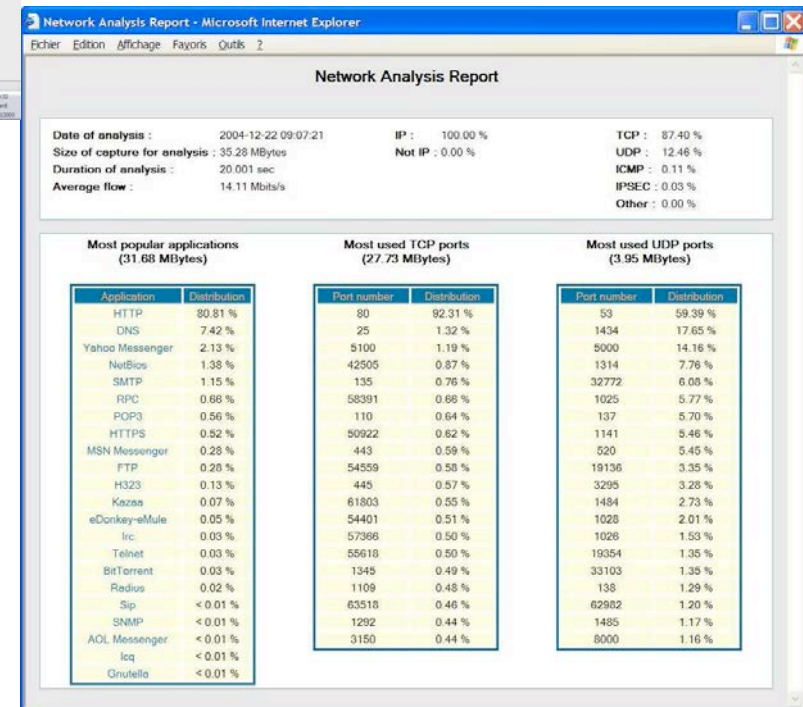
Traffic Analysis and Acquisition Control



Control Panel



Data Stream Display

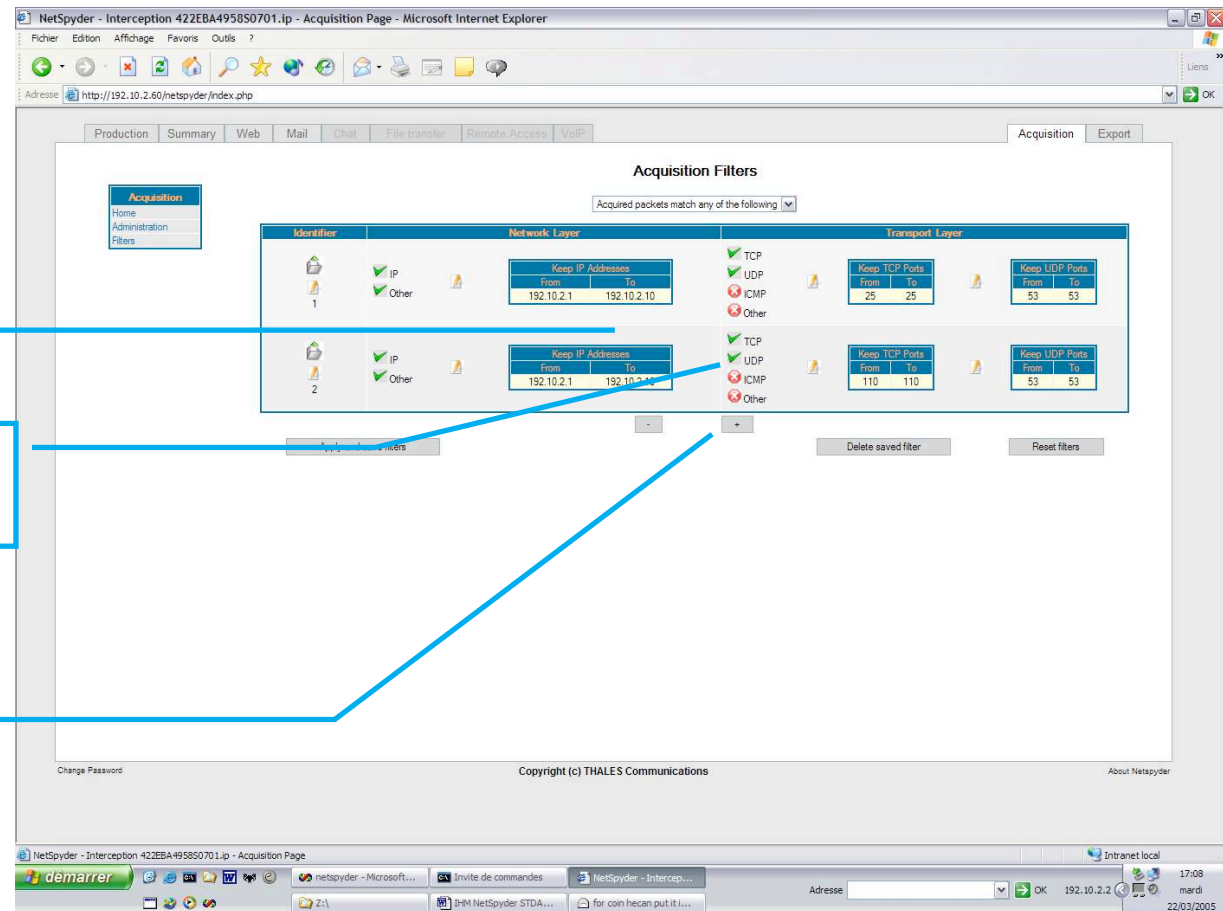


Protocol used

Set of Filters

Selection/Rejection

Addition/Deletion



IP Acquisition list : IP Application Summary

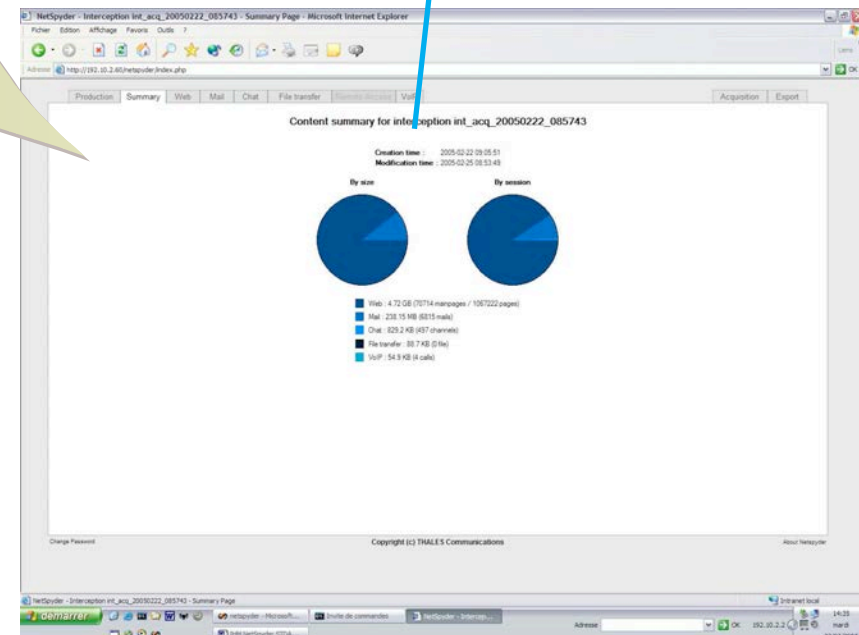


Name	Creation date	Modification date	Size
[111]	2005-02-21 13:43:33	2005-02-21 13:43:33	426 9 KB
HL_Acq_20050222_085743	2005-02-21 16:36:36	2005-02-22 09:51:41	8 470 KB
HL_Acq_20050222_085743	2005-02-22 09:51:41	2005-02-26 16:53:49	8 470 KB
420C107702a	2005-03-10 13:50:34	2005-03-10 13:50:36	134 6 KB
420C107702a	2005-03-10 13:51:02	2005-03-10 13:51:07	2 779 KB
420C107702a	2005-03-10 13:51:18	2005-03-10 13:51:16	4 114 KB
420C107702a	2005-03-10 13:51:26	2005-03-10 13:51:26	16 5 KB
420C107702a	2005-03-10 13:51:37	2005-03-10 13:51:39	307 5 KB
420C107702a	2005-03-10 13:51:46	2005-03-10 13:51:46	475 KB
420C107702a	2005-03-10 13:51:57	2005-03-10 13:51:57	1 72 KB
420C107702a	2005-03-10 13:52:08	2005-03-10 13:52:08	76 6 KB
420C107702a	2005-03-10 13:52:17	2005-03-10 13:52:18	271 KB
420C107702a	2005-03-10 13:52:26	2005-03-10 13:52:26	1 129 KB
420C107702a	2005-03-10 13:52:36	2005-03-10 13:52:36	8 KB
420C107702a	2005-03-10 13:52:41	2005-03-10 13:52:41	1 178 KB
420C107702a	2005-03-10 13:52:52	2005-03-10 13:52:53	26 2 KB
420C107702a	2005-03-10 13:53:01	2005-03-10 13:53:01	34 6 KB
420C107702a	2005-03-10 13:53:13	2005-03-10 13:53:13	3 KB
420C107702a	2005-03-10 13:53:23	2005-03-10 13:53:23	105 9 KB
420C107702a	2005-03-10 13:53:32	2005-03-10 13:53:32	116 KB
420C107702a	2005-03-10 13:53:41	2005-03-10 13:53:42	52 KB
HL_Acq_20050222_085743	2005-03-22 12:34:16	2005-03-22 12:34:16	8 KB

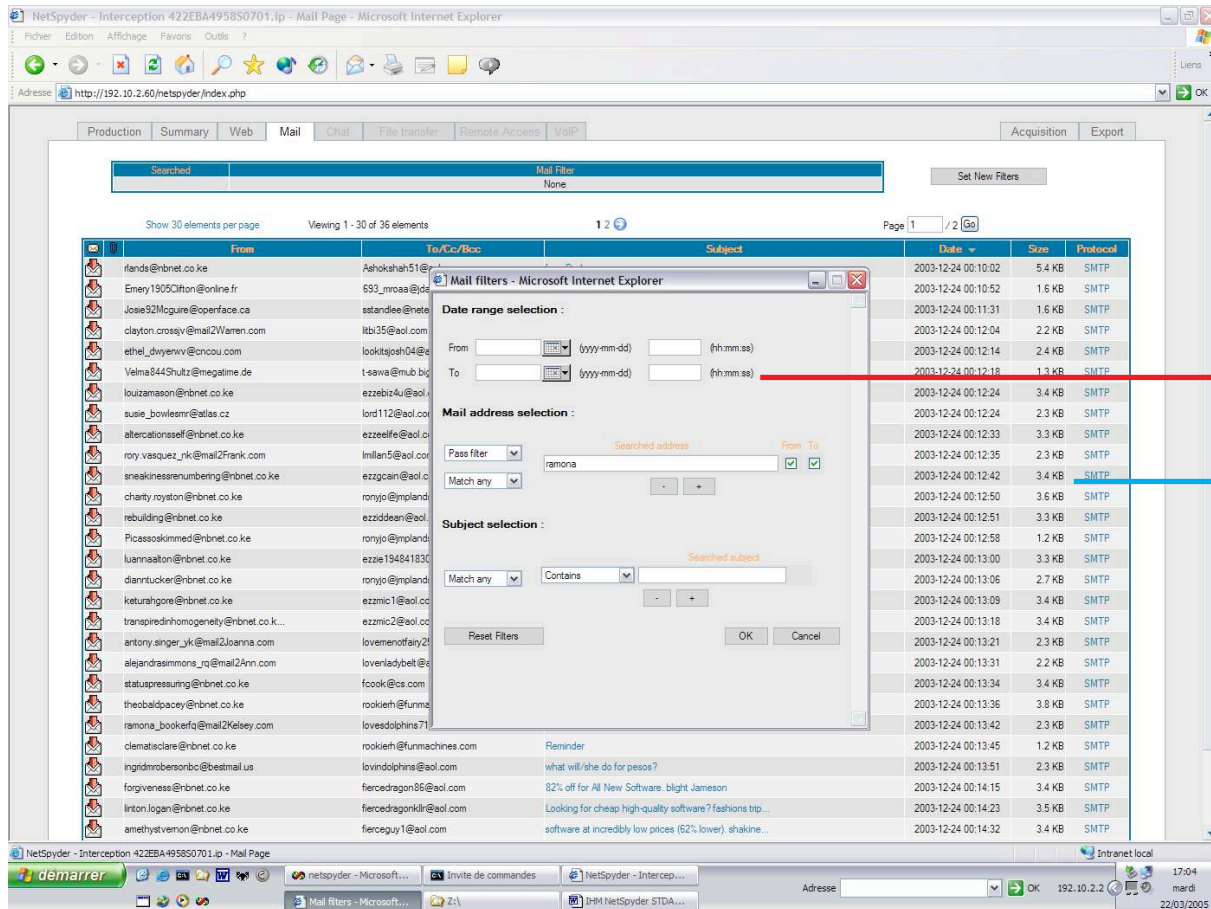
File Selection

Automatic
Application
Display

- Automatic Processing
- Automatic display of Identified Data as : web, mail, VoIP, chat, ftp
- Front filtering
- Back filtering
- Remote control
- Data importation or exportation available (pcap format...)



Operation : e-mail



The screenshot shows the NetSpyder Mail Page interface. At the top, there are tabs for Production, Summary, Web, Mail, Chat, File transfer, Remote Access, and VoIP. The Mail tab is selected. Below the tabs, there is a search bar and a 'Set New Filters' button. The main area displays a list of emails with columns for From, To/Cc/Bcc, Subject, Date, Size, and Protocol. A dialog box titled 'Mail filters - Microsoft Internet Explorer' is open, showing options for Date range selection, Mail address selection, and Subject selection. The dialog box has fields for 'From', 'To', 'Pass filter', 'Searched address', 'Match any', 'Searched subject', and 'Contains'. The 'Mail address selection' section is highlighted with a red box, and the 'Subject selection' section is highlighted with a blue box. The email list shows various emails from different domains, including rlands@nbnet.co.ke, Emery1905@online.fr, Josie92@openface.ca, clayton.crosby@mail2Warren.com, ethel_dwyer@conco.com, Velma844@shultz.megatime.de, louizamason@nbnet.co.ke, susie_bowles@atlas.cz, altercations@nbnet.co.ke, roly.vasquez_rk@mail2Frank.com, sneakiness@nbnet.co.ke, charity.royton@nbnet.co.ke, rebuilding@nbnet.co.ke, Picasoskinned@nbnet.co.ke, luanna@nbnet.co.ke, dianntucker@nbnet.co.ke, keturah@nbnet.co.ke, transpiedrinhomogeneity@nbnet.co.ke, antony.singer_yk@mail2Joanna.com, alejandra@nbnet.co.ke, status@nbnet.co.ke, theobald@nbnet.co.ke, ramona_booker@mail2Kelsey.com, clematis@nbnet.co.ke, ingrid@nbnet.co.ke, forgiveness@nbnet.co.ke, linton.logan@nbnet.co.ke, amethyst@nbnet.co.ke, and others. The list is sorted by Date, and the first page shows 30 elements per page.

From	To/Cc/Bcc	Subject	Date	Size	Protocol
rlands@nbnet.co.ke	Ashokah51@		2003-12-24 00:10:02	5.4 KB	SMTP
Emery1905@online.fr	693_pnoaa@		2003-12-24 00:10:52	1.6 KB	SMTP
Josie92@openface.ca	standee@		2003-12-24 00:11:31	1.6 KB	SMTP
clayton.crosby@mail2Warren.com	ltbi35@aol.com		2003-12-24 00:12:04	2.2 KB	SMTP
ethel_dwyer@conco.com	lookitajoh04@		2003-12-24 00:12:14	2.4 KB	SMTP
Velma844@shultz.megatime.de	t-sawa@mb.bq		2003-12-24 00:12:18	1.3 KB	SMTP
louizamason@nbnet.co.ke	ezzebi4u@aol.		2003-12-24 00:12:24	3.4 KB	SMTP
susie_bowles@atlas.cz	lord112@aol.co		2003-12-24 00:12:24	2.3 KB	SMTP
altercations@nbnet.co.ke	ezzeelfe@aol.c		2003-12-24 00:12:33	3.3 KB	SMTP
roly.vasquez_rk@mail2Frank.com	lmilan5@aol.co		2003-12-24 00:12:35	2.3 KB	SMTP
sneakiness@nbnet.co.ke	ezzagain@aol.c		2003-12-24 00:12:42	3.4 KB	SMTP
charity.royton@nbnet.co.ke	ronyo@ympland		2003-12-24 00:12:50	3.6 KB	SMTP
rebuilding@nbnet.co.ke	ezdiddean@aol		2003-12-24 00:12:51	3.3 KB	SMTP
Picasoskinned@nbnet.co.ke	ronyo@ympland		2003-12-24 00:12:58	1.2 KB	SMTP
luanna@nbnet.co.ke	ezzie19484183		2003-12-24 00:13:00	3.3 KB	SMTP
dianntucker@nbnet.co.ke	ronyo@ympland		2003-12-24 00:13:06	2.7 KB	SMTP
keturah@nbnet.co.ke	ezzm1@aol.co		2003-12-24 00:13:09	3.4 KB	SMTP
transpiedrinhomogeneity@nbnet.co.ke	ezzm2@aol.co		2003-12-24 00:13:18	3.4 KB	SMTP
antony.singer_yk@mail2Joanna.com	lovenottofain2		2003-12-24 00:13:21	2.3 KB	SMTP
alejandra@nbnet.co.ke	lovenlady@bkt		2003-12-24 00:13:31	2.2 KB	SMTP
status@nbnet.co.ke	fcok@cs.com		2003-12-24 00:13:34	3.4 KB	SMTP
theobald@nbnet.co.ke	rookieh@furnm		2003-12-24 00:13:36	3.8 KB	SMTP
ramona_booker@mail2Kelsey.com	lovedolphins71		2003-12-24 00:13:42	2.3 KB	SMTP
clematis@nbnet.co.ke	rookieh@furnmachines.com	Reminder	2003-12-24 00:13:45	1.2 KB	SMTP
ingrid@nbnet.co.ke	lovedolphins@aol.com	what will/she do for pesos?	2003-12-24 00:13:51	2.3 KB	SMTP
forgiveness@nbnet.co.ke	fiercedragon56@aol.com	82% off for All New Software blight Jameson	2003-12-24 00:14:15	3.4 KB	SMTP
linton.logan@nbnet.co.ke	fiercedragonktr@aol.com	Looking for cheap high-quality software? fashions trip...	2003-12-24 00:14:23	3.5 KB	SMTP
amethyst@nbnet.co.ke	fierceguy1@aol.com	software at incredibly low prices (62% lower), shake...	2003-12-24 00:14:32	3.4 KB	SMTP

Set of Filter

E-mail List

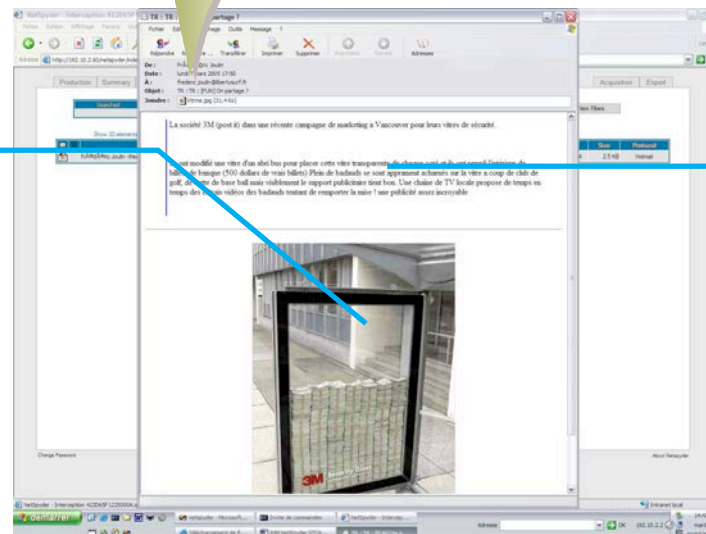
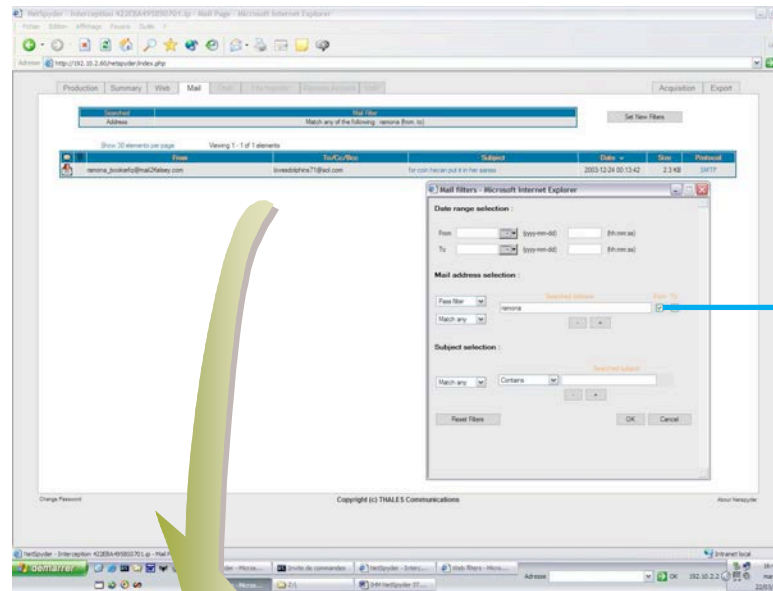
Mail Filtering Result

Operation
Filter

Attached File

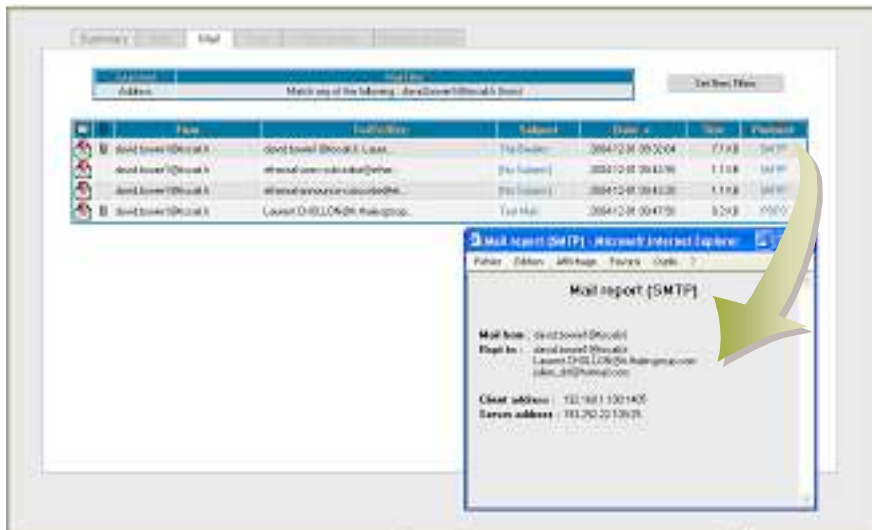
Mail Content

Mail Display



IP Operating Tools : Mail Reports

SMTP Report



Mail report (SMTP)

From	To	Subject	Date	Size	Protocol
dev@broadcom.com	dev@broadcom.com	Test Mail	2004-12-01 00:00:00	1.1 KB	SMTP
dev@broadcom.com	dev@broadcom.com	Test Mail	2004-12-01 00:00:00	1.1 KB	SMTP
dev@broadcom.com	dev@broadcom.com	Test Mail	2004-12-01 00:00:00	1.1 KB	SMTP
dev@broadcom.com	dev@broadcom.com	Test Mail	2004-12-01 00:00:00	1.1 KB	SMTP

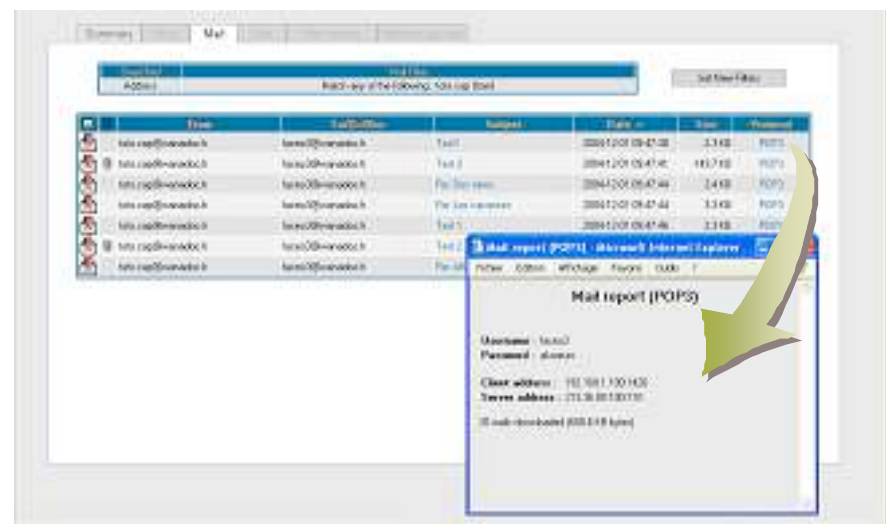
Mail report (SMTP) - Microsoft Internet Explorer

Folder: Mail | Action: Refresh | Search: 0

Mail report (SMTP)

Mail from: dev@broadcom.com
Mail to: dev@broadcom.com
Client address: 192.168.1.100:1435
Server address: 192.168.1.100:1435

POP 3 Report



Mail report (POP3)

From	To	Subject	Date	Size	Protocol
dev@broadcom.com	dev@broadcom.com	Test Mail	2004-12-01 00:00:00	1.1 KB	POP3
dev@broadcom.com	dev@broadcom.com	Test Mail	2004-12-01 00:00:00	1.1 KB	POP3
dev@broadcom.com	dev@broadcom.com	Test Mail	2004-12-01 00:00:00	1.1 KB	POP3
dev@broadcom.com	dev@broadcom.com	Test Mail	2004-12-01 00:00:00	1.1 KB	POP3

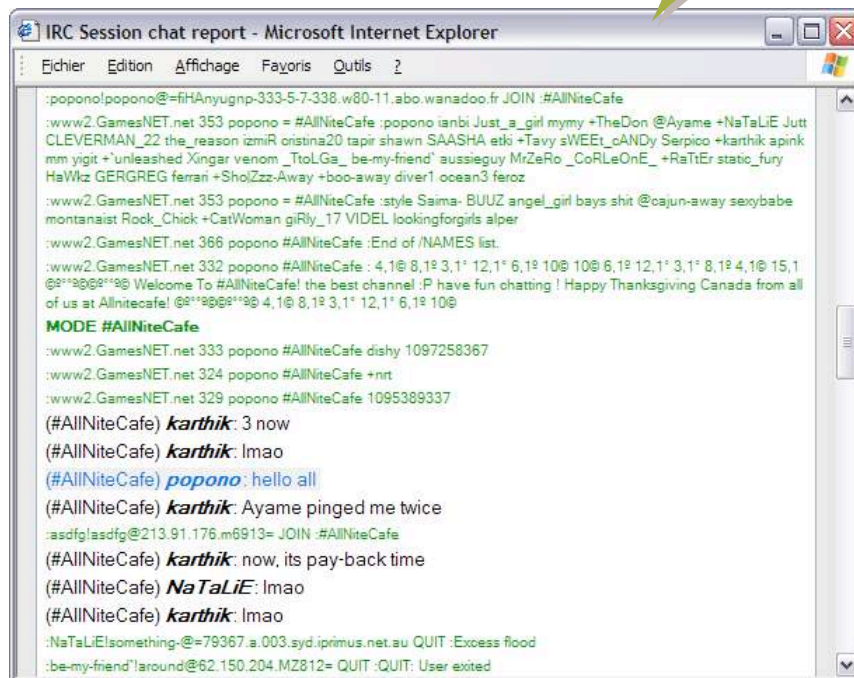
Mail report (POP3) - Microsoft Internet Explorer

Folder: Mail | Action: Refresh | Search: 0

Mail report (POP3)

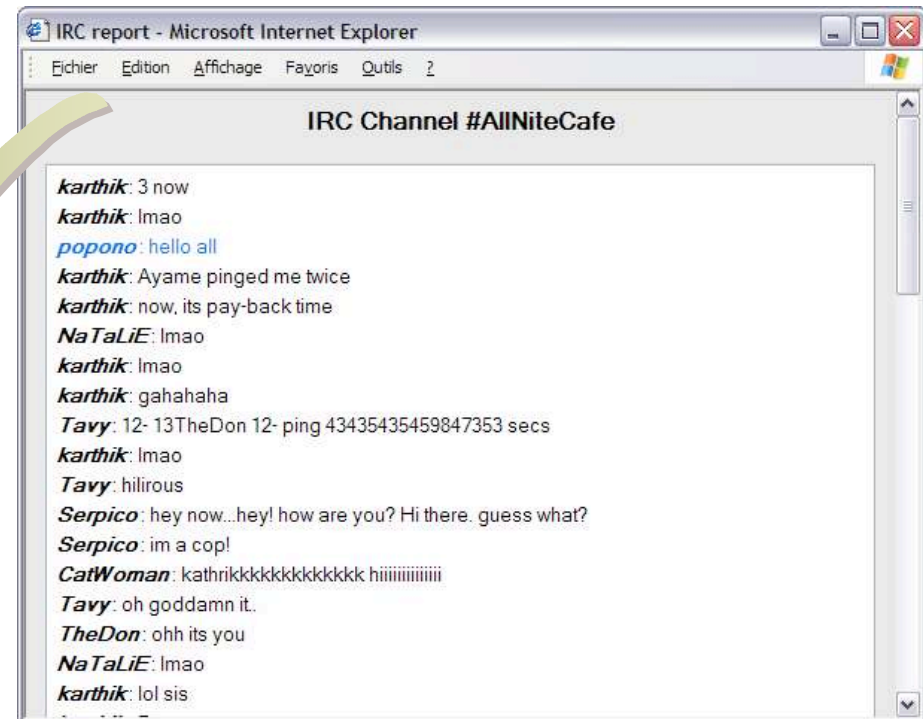
Mail from: dev@broadcom.com
Mail to: dev@broadcom.com
Client address: 192.168.1.100:1435
Server address: 192.168.1.100:1435
Mail size: 1.1 KB

IRC Report



```
IRC Session chat report - Microsoft Internet Explorer
Fichier Edition Affichage Favoris Outils ?

:popono!popono@=fiHAnyugnp-333-5-7-338.w80-11.abo.wanadoo.fr JOIN :#AllNiteCafe
:www2.GamesNET.net 353 popono = #AllNiteCafe :popono lanbi Just_a_girl mymy +TheDon @Ayame +NaTaLiE Jutt
CLEVERMAN_22 the_reason izmiR onistina20 tapir shawn SAASHA etki +Tavy sWEEt_cANDy Serpico +karthik apink
mm yigit +unleashed Xingar venom _TolGa_ be-my-friend aussieguy MrZeRo _CoRLeOnE_ +RaTiEr static_fury
HaWkz GERGREG ferrari +ShoZzz-Away +boo-away diver1.ocean3 feroz
:www2.GamesNET.net 353 popono = #AllNiteCafe :style Saima- BUUZ angel_girl bays shit @cajun-away sexybabe
montanaist Rock_Chick +CatWoman giRly_17 VIDEL lookingforgirls alper
:www2.GamesNET.net 366 popono #AllNiteCafe :End of /NAMES list.
:www2.GamesNET.net 332 popono #AllNiteCafe : 4,1@ 8,1@ 3,1* 12,1* 6,1@ 10@ 10@ 6,1@ 12,1* 3,1* 8,1@ 4,1@ 15,1
@8**@8**@ Welcome To #AllNiteCafe! the best channel :P have fun chatting ! Happy Thanksgiving Canada from all
of us at Allnitecafe! @8**@8**@ 4,1@ 8,1@ 3,1* 12,1* 6,1@ 10@
MODE #AllNiteCafe
:www2.GamesNET.net 333 popono #AllNiteCafe dishy 1097258367
:www2.GamesNET.net 324 popono #AllNiteCafe +nrt
:www2.GamesNET.net 329 popono #AllNiteCafe 1095389337
(#AllNiteCafe) karthik: 3 now
(#AllNiteCafe) karthik: lmao
(#AllNiteCafe) popono: hello all
(#AllNiteCafe) karthik: Ayame pinged me twice
:asdfglasdfg@213.91.176.m6913= JOIN :#AllNiteCafe
(#AllNiteCafe) karthik: now, its pay-back time
(#AllNiteCafe) NaTaLiE: lmao
(#AllNiteCafe) karthik: lmao
:NaTaLiE!something-@=79367.a.003.syd.iprimus.net.au QUIT :Excess flood
:be-my-friend!around@62.150.204.MZ812= QUIT :QUIT: User exited
```



```
IRC report - Microsoft Internet Explorer
Fichier Edition Affichage Favoris Outils ?

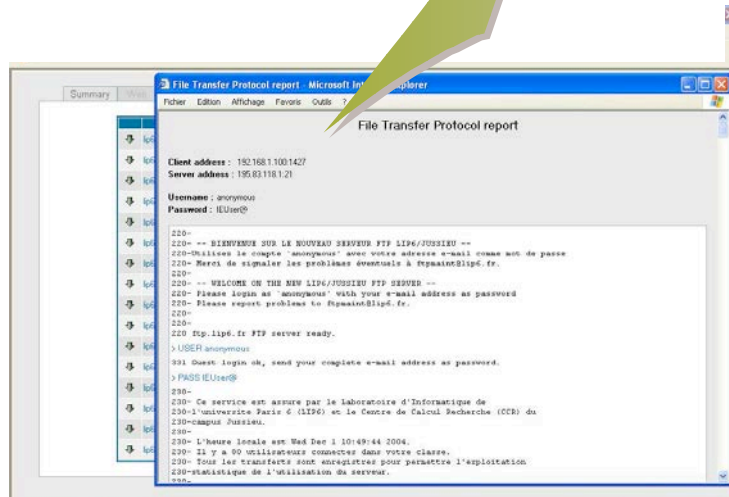
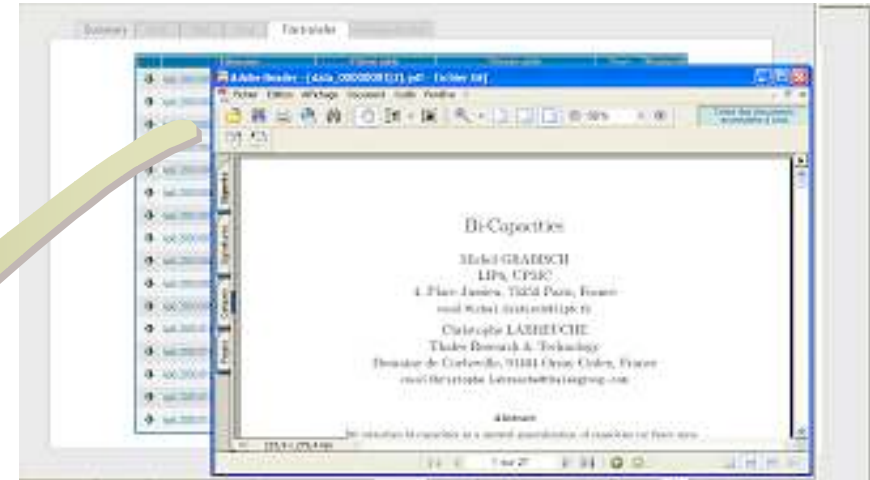
IRC Channel #AllNiteCafe

karthik: 3 now
karthik: lmao
popono: hello all
karthik: Ayame pinged me twice
karthik: now, its pay-back time
NaTaLiE: lmao
karthik: lmao
karthik: gahahaha
Tavy: 12- 13TheDon 12- ping 43435435459847353 secs
karthik: lmao
Tavy: hilirous
Serpico: hey now...hey! how are you? Hi there. guess what?
Serpico: im a cop!
CatWoman: kathrikkkkkkkkkkkkkk hiiiiiiiiiiii
Tavy: oh goddamn it.
TheDon: ohh its you
NaTaLiE: lmao
karthik: lol sis
```

IP Operating Tools : File Transfer



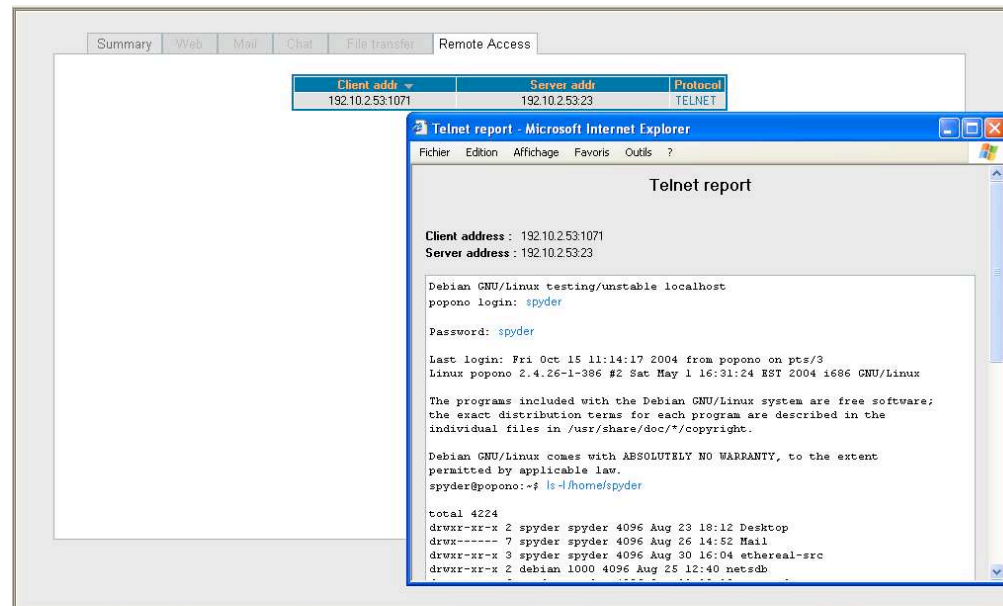
FTP Report



IP Operating Tools : Remote Access



Telnet Report



File Exportation



The screenshot shows the 'Export Http : File Parameters' dialog box. It has a tabbed interface with 'Production', 'Summary', 'Web', 'Mail', 'Chat', 'File transfer', 'Remote Access', 'VoIP', 'Acquisition', and 'Export'. The 'Export' tab is active. On the left, there is a sidebar titled 'Export Captures' with links: 'Home', 'Download http', 'Download ftp', and 'Permanent ftp'. The main area displays 'Estimated size of export : 589 MB'. Below this, there are two input fields: 'Download filename' with the value 'cap_20041221_085622to20041222_085430' and 'Max size of each downloaded file (MB)' with the value '250'. At the bottom, there are 'Continue' and 'Cancel' buttons.

File Importation



The screenshot shows the 'Export with http : File creation and Download' dialog box. It has the same tabbed interface as the previous dialog, with 'Export' selected. The sidebar 'Export Captures' is visible. The main area shows 'Export of selected capture from 2004-12-21 09:56:22 to 2004-12-22 09:54:30'. Below this, it says 'File (1) from 2004-12-21 09:56:22 to 2004-12-21 09:56:45'. There is a 'Download file' button. Below that, it says 'Go to next file (only when download is finished)'. At the bottom, there is a 'Cancel Download' button.



■ Questions?