cafe24

SUCCESS
PARTNER.

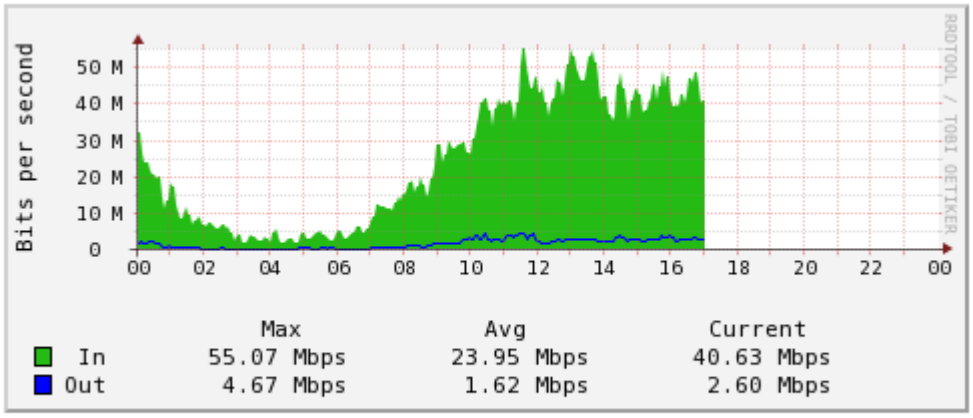
초과트래픽 확인매뉴얼

저희 카페 24 서버호스팅 상품을 이용하실경우 나의서비스관리 – 사용량 모니터링 메뉴를 통해 서버에서 발생하는 트래픽을 확인하실수 있습니다.

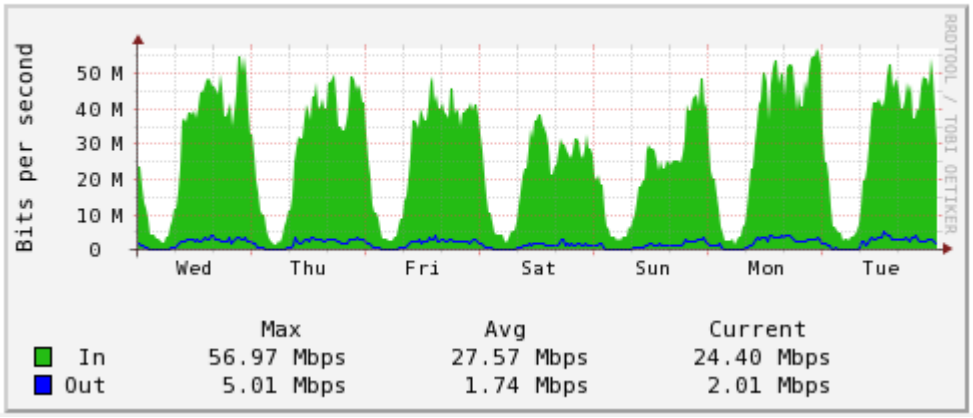
나의서비스관리 – 사용량 모니터링 바로가기 :

https://hosting.cafe24.com/?controller=myservice_hosting_monitor&method=serverHosting

나의서비스 관리 – 사용량 모니터링 – 모니터링



Weekly



나의서비스 관리 – 사용량 모니터링 – 일별 전송량 보기

조회기간

조회방법	◉ 월별보기 ○ 기간선택
기간선택	2014-10-11 ~ 2014-11-10 ▼

집계내역

5분단위 최대값 (A)	93.1 Mbps	
5분단위 평균 트래픽의 3배 (B)	104.7 Mbps	
과금 대상 트래픽	**93.1 Mbps**	A, B중 최소값
추정 전송량 합계	7,104 GB	
약정 트래픽	50 Mbps	
초과 트래픽	**43.1 Mbps**	

일별 트래픽 내역

날짜	5분단위 최대값	평균 트래픽	추정 전송량
2014년 10월 29일	56.5 Mbps	29.3 Mbps	317 GB
2014년 10월 28일	61.4 Mbps	35.4 Mbps	383 GB
2014년 10월 27일	65.8 Mbps	37.9 Mbps	410 GB
2014년 10월 26일	56.7 Mbps	25.5 Mbps	275 GB
2014년 10월 25일	46.4 Mbps	24.6 Mbps	267 GB
2014년 10월 24일	57.6 Mbps	32.6 Mbps	353 GB
2014년 10월 23일	59.9 Mbps	33.6 Mbps	364 GB
2014년 10월 22일	67.4 Mbps	35.0 Mbps	379 GB

나의서비스 관리 – 트래픽 알림 설정

서버호스팅상품 이용시 기본 네트워크 대역폭은 10Mbps 를 제공해드리고 있으며, 10Mbps 이상 트래픽이 발생하시는 경우 고객님께서 별도로 네트워크 대역폭을 설정하여 과다트래픽 발생시 고객님의 SMS 로 트래픽 알림 문자를 수신할수 있는 서비스 입니다.

• 트래픽 알림 설정

수신여부	수신함 설정하기
관리자 휴대폰번호	010-2922-8115
수신받을 이메일	ohrifs@gmail.com

초과트래픽이 주기적으로 발생하는 경우 여러가지방법을 통하여 초과트래픽이 발생하는 부분을 점검하여 악의적으로 발생하는 트래픽을 차단하여 네트워크 트래픽을 보다효율적으로 사용하실수 있습니다.

초과트래픽이 발생하는 원인은 여러가지 사유가 있으며, 몇가지 사례를 소개해드립니다.

1) 해외트래픽 발생으로 인한 트래픽 증가시 점검사항

각 해외 검색엔진에 의하여 트래픽이 증가하는 경우 점검사항

a) 웹서버 , DB 서버로그 확인, 웹서버 로그 분석
b) 해외트래픽 사용량 확인

해외트래픽 사용량 확인은 저희 카페 24 홈페이지 – 고객센터 – 문의게시판 – 서버호스팅 분류로 문의해주시면 별도로 해외트래픽 사용부분을 안내해드리고 있습니다

고객센터 – 문의게시판 바로가기 : http://help.cafe24.com/cs/cs_myqna_list.php

2) 해외트래픽 발생으로 인한 트래픽 증가시 조치사항

해외에서 접속이 없으시다면 해외망 전체차단 및 국가별 IP 대역을 차단하여 발생하는 트래픽을 절감하여 사용하실수 있습니다.

서버 OS 별 해외망 / 국가코드(IP 대역) 차단 설정 매뉴얼

리눅스 서버(Centos) : 해외 IP 차단 매뉴얼

윈도우 OS 버전별 해외망(중국, 미국) 차단하기

Window 2008 OS 계열

Windows 2003 중국 차단 설정하기

3) 서버 공격 발생에 의한 트래픽 증가시 서버 점검사항

리눅스 서버 :

a) Tmpfs 보안검사

: /tmp, /var/tmp, /dev/shm 경로에 해킹 파일에 존재하는지 검사 및 확인

b) 파일업로드 취약점을 이용한 서버 공격 유형:

홈페이지 파일업로드 디렉토리 확인하여 웹쉘 파일이 있는지 검사하여 웹쉘파일이 있을경우 삭제하거나 해당 파일 격리조치

c) 웹쉘검사:

한국 인터넷 진흥원 Whistl 툴을 통한 웹쉘 검검

KISA 한국인터넷 진흥원 Whistl 사용방법바로가기 : http://toolbox.krcert.or.kr/MMVF/MMVFView_V.aspx?MENU_CODE=14&PAGE_NUMBER=15

d) 그외 오픈소스를 통한 보안점검 : rkhunter, chkrootkit 외
e) 서버 로그점검 : /var/log 폴더에 쌓여있는 로그점검

/var/log/secure , /var/log/maillog, /var/log/messages, /var/log/dmesg, /var/log/vsftpd.log 외

f) 보안 점검

윈도우 서버:

a) 주기적인 바이러스 점검

V3 Net 평가판 또는 Microsoft microsoft security 를 통한 바이러스 점검

b) 웹쉘 검사

한국 인터넷 진흥원 Whistl 툴을 통한 웹쉘 검검

KISA 한국인터넷 진흥원 Whistl 사용방법바로가기 : http://toolbox.krcert.or.kr/MMVF/MMVFView_V.aspx?MENU_CODE=14&PAGE_NUMBER=15

c) 윈도우 서버 로그 점검

이벤트로그 확인

시작 – 실행 – cmd 창에서 eventvwr 명령어를 실행하시면 이벤트로그를 확인하실수 있습니다.

d) 웹서버(IIS 로그점검

C:₩WINDOWS₩system32₩LogFiles 폴더에 쌓여있는 로그를 점검합니다.

e) MSSQL 서버 로그점검

f) 그외 서버내부에서 사용되고 있는 어플리케이션 로그 점검

g) 보안 점검

2. 공개 프리웨어(오픈소스) 프로그램을 이용한 사이트 이미지 용량 확인하기

웹사이트 운영시 이미지 용량이 무거운 경우 사이트 로딩속도가 저하되게 되며, 트래픽이증가되게 됩니다. 이럴경우 이미지용량을 확인하여 사이즈를 줄이면 로딩속도를 줄일수있으며, 트래픽을 절감하여 사용하실수 있습니다.

1). 내 PC 에 설치되어있는 구글 크롬을 실행합니다

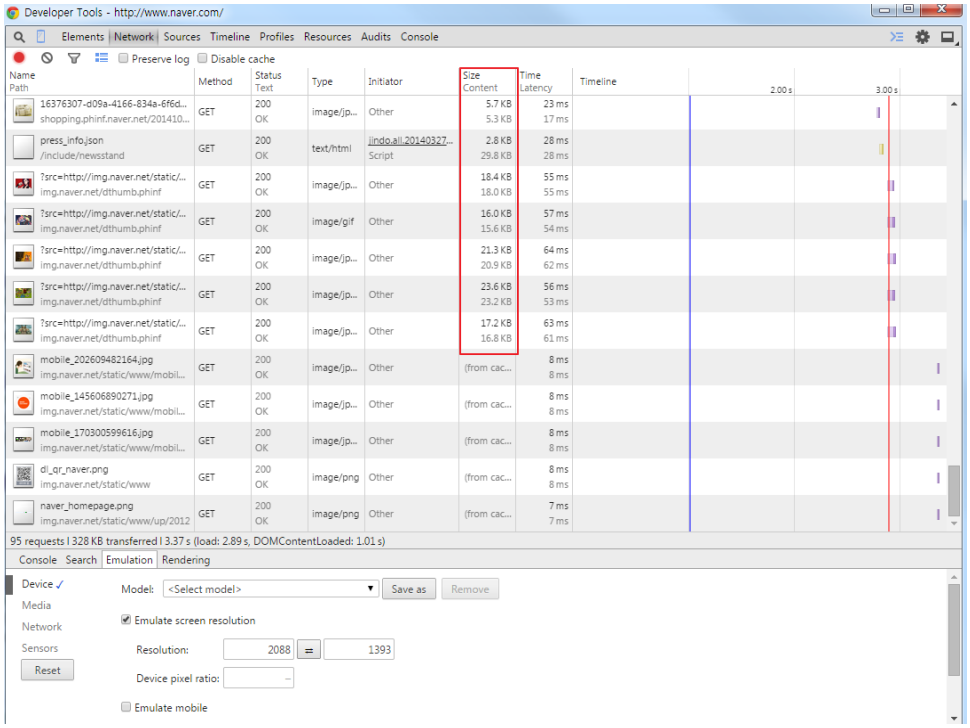
Google Chrome 이 설치되어 있지 않은경우 아래의 url 에서 다운로드하여 설치합니다.

다운로드 http://www.google.com/intl/ko/chrome/

크롬 브라우저 창에서 홈페이지 주소를 입력합니다

Tip) 크롬의 개발자 도구(Developer Tools) 간단히 실행하기

1) 크롬의 메뉴 -> 도구 -> 개발자 도구로 직접 실행
2) 단축키 Ctrl + Shift + i 로 실행
3) 기능키 F12 로 실행
4) 웹 페이지의 특정 요소 위에서 마우스 우크릭후 '요소 검사(N)' 선택
5) Network 텝 – Size 부분을 확인하시면 로딩되는 이미지 용량을 확인하실수 있습니다.



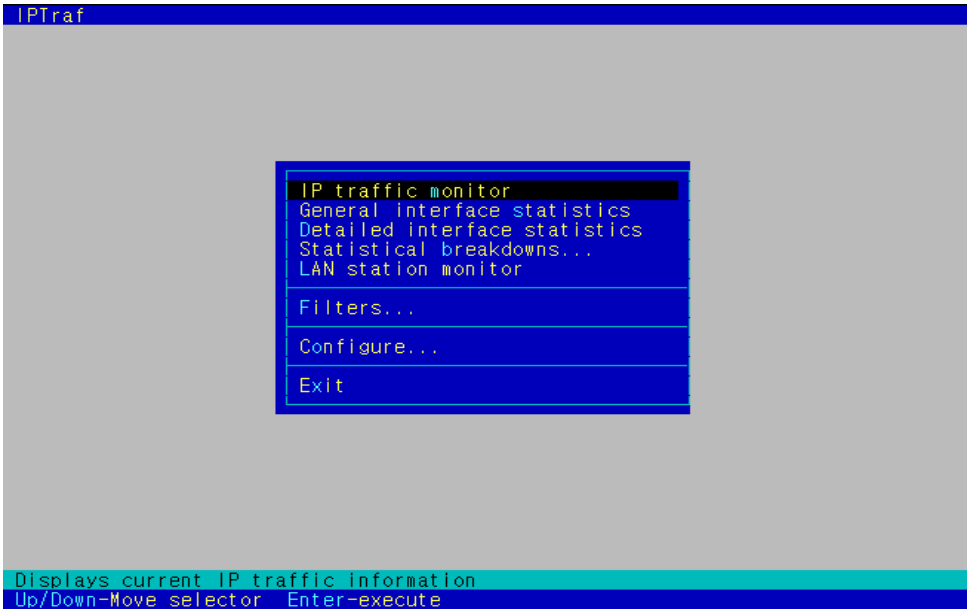
3. 오픈소스 툴(프로그램)을 통한 네트워크 트래픽 확인

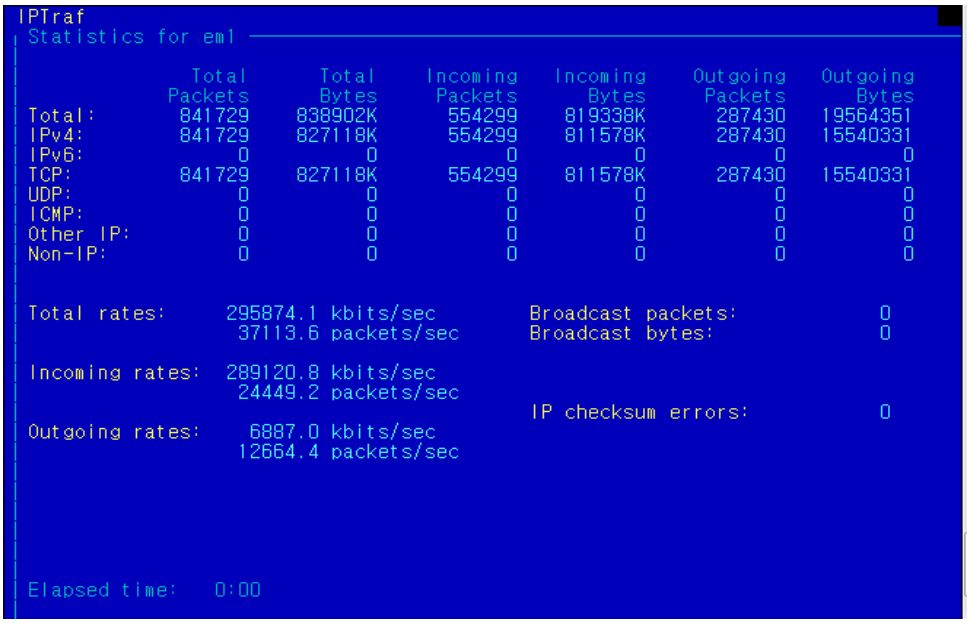
1) 리눅스 서버 O 의 경우 (Centos / Redhat 계열)

iptraf 프로그램을 이용하여 네트워크 트래픽 확인할수 있습니다

a) iptraf 설치 및 실행

설치 : yum –y install iptraf 명령어를 입력하여 설치후 iptraf 명령어를 실행합니다.





IP traffic monitor :

네트워크 인터페이스를 통해 송수신되는 트래픽을 IP 별로 보여줍니다.

General interface statistics - 트래픽의 통계를 네트워크 인터페이스 별로 보여줍니다..

Detailed interface statistics :

각 네트워크 인터페이스에서 송수신되는 트래픽을 상세히 보여줍니다.

Statistical breakdowns.. :

패킷 사이즈별, TCP/UTP 각 포트별 트래픽 통계를 보여줍니다.[By packet size]

LAN station monitor :

네트워크 내의 트래픽 송수신 목적지와 양을 보여줍니다.

Filters... :

패킷 모니터링에서 표시되는 정보 필터링을 설정합니다.

Configure... - IPTraf 의 환경설정입니다.

2) 윈도우(Windows) 서버 OS 의 경우 네트워크 트래픽 확인

2-1) Wfilter 프로그램을 이용한 네트워크 트래픽 확인

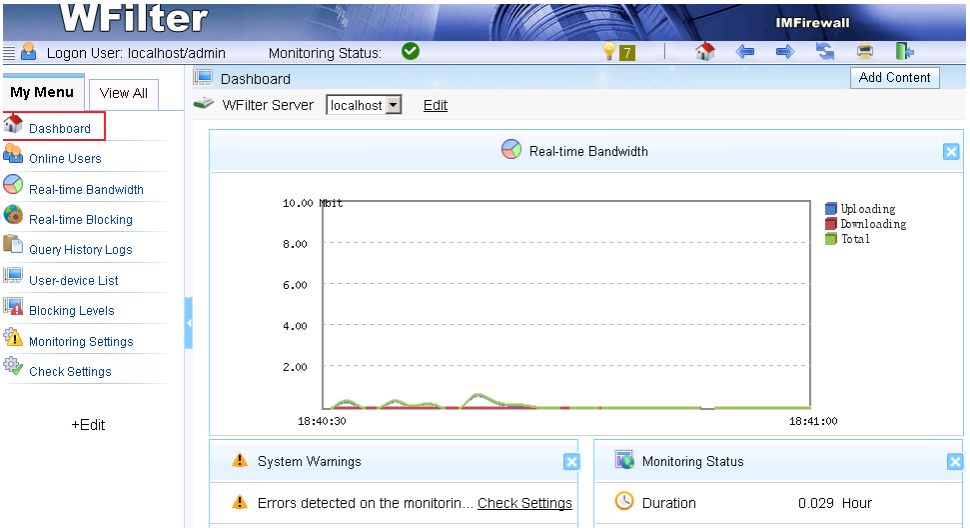
Wfilter 다운로드 : http://www.imfirewall.us/

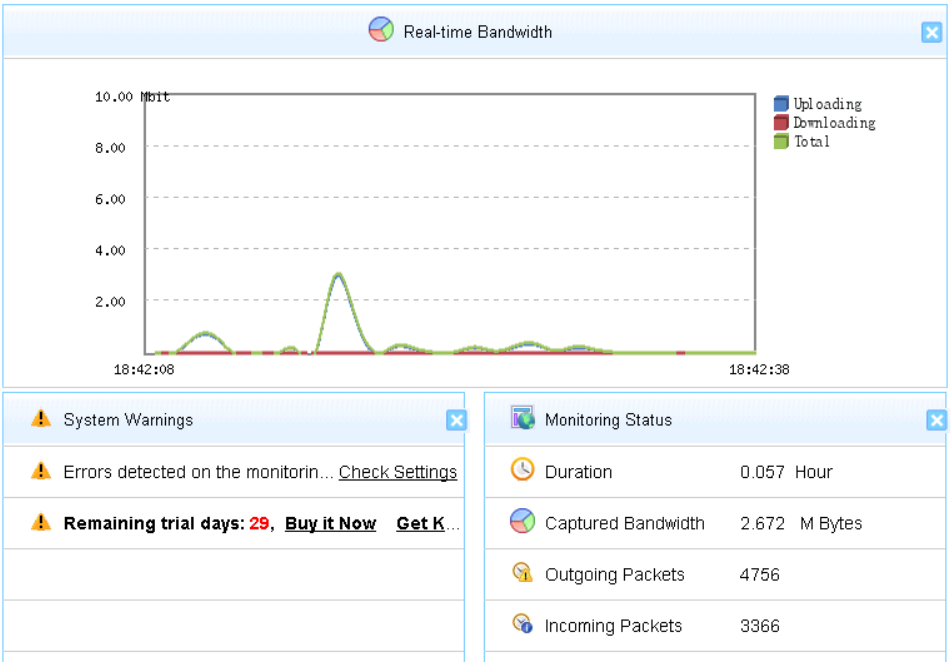
A) wfilter 접속

프로그램 설치후 서버 인터넷 브라우저를 실행하여 http://127.0.0.1:10090 으로 접속하여 프로그램을 사용하실수 있습니다

접속 ID: admin 이며 패스워드는 프로그램 설치시 입력한 패스워드로 로그인을 합니다.

로그인후 DashBoard 메뉴를 클릭하면 서버에서 발생되는 트래픽을 확인하실수 있습니다.





2-2) Microsoft Network monitor 프로그램을 이용한 네트워크 패킷 확인

Network Monitor (Netmon)는 네트워크 프로토콜 트래픽 분석 유틸리티입니다. Network Monitor 3.1 을 사용해서 네트워크 프로토콜을 수집하는 몇 가지 방법을 정리하였습니다

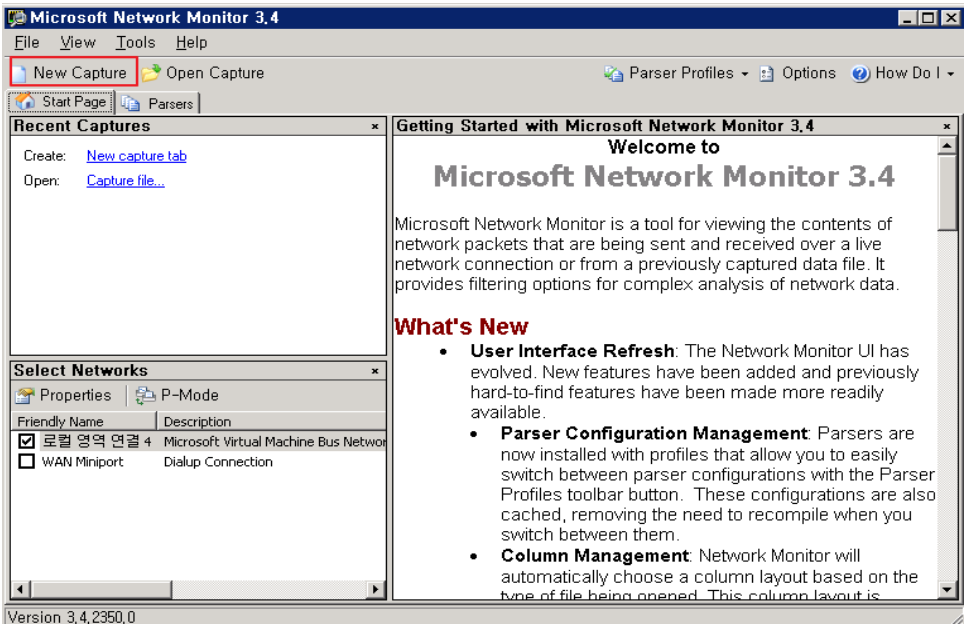
다운로드 : http://www.microsoft.com/en-us/download/details.aspx?id=4865

해당파일을 다운로드하여 서버에 설치합니다

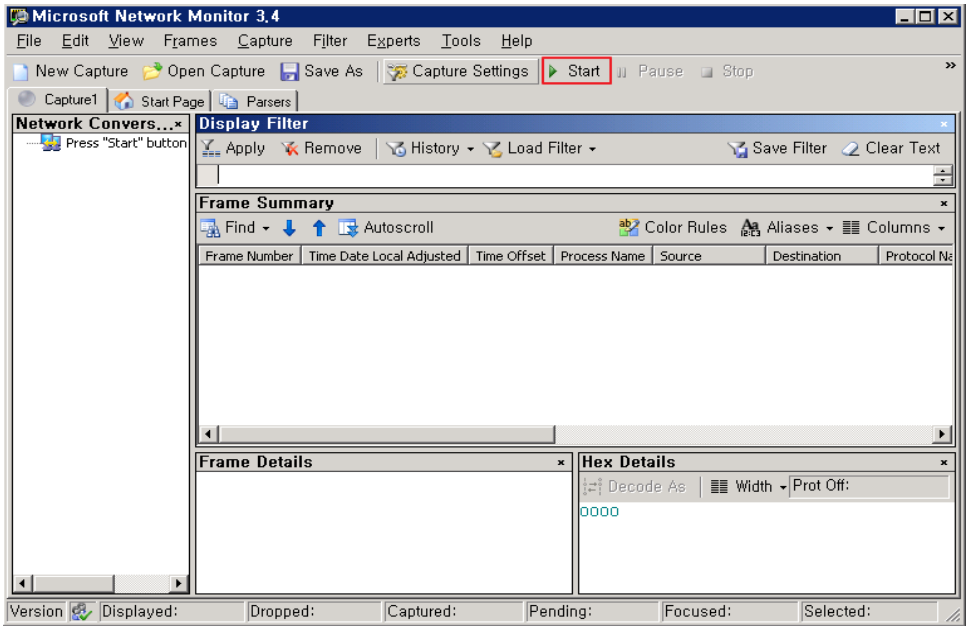
B) Microsoft Network Monitor 3.4 실행

시작 - 프로그램 - Microsoft Network Monitor 3.4 - Microsoft Network Monitor 3.4 파일을 실행합니다

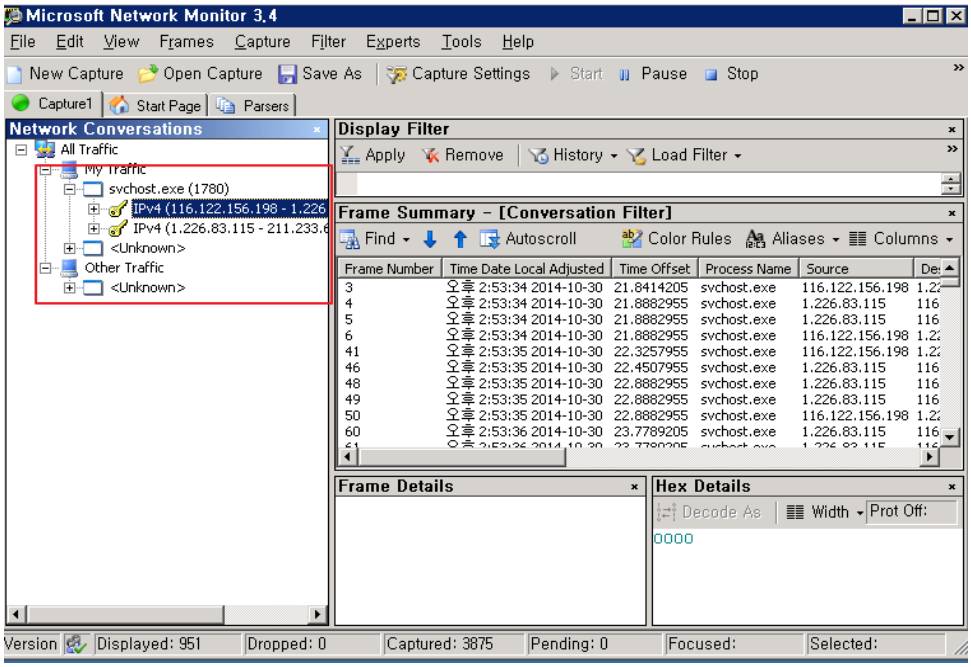
상단 메뉴중 New Capture 버튼을 누른후 Start 버튼을 누릅니다.



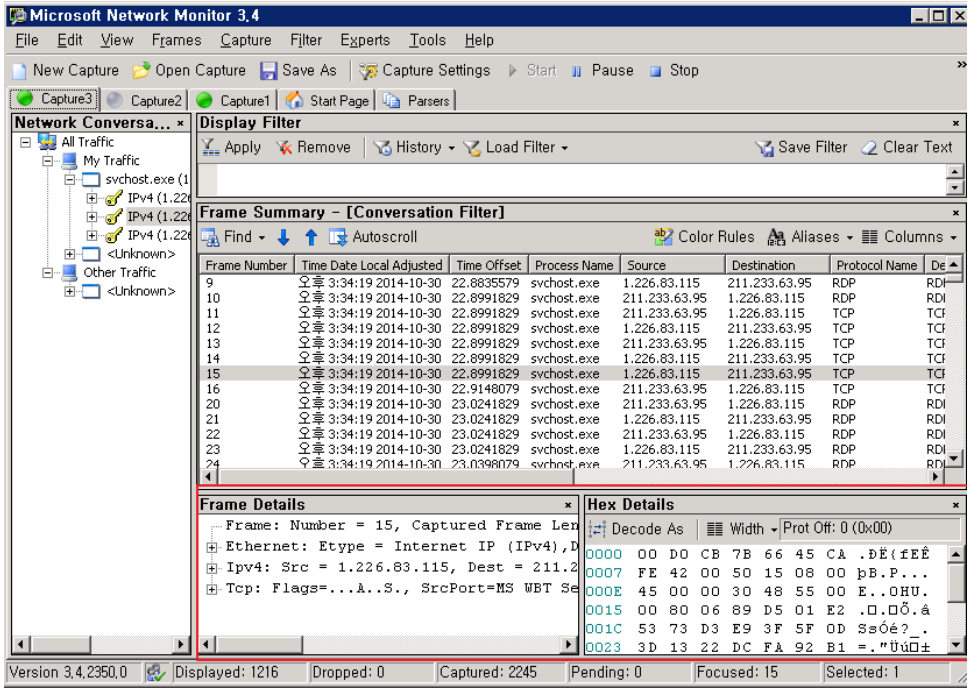
start 버튼을 누르면 실시간으로 네트워크 패킷을 확인할수 있습니다.



(윈도우 프로세스별 통신 상태 확인)

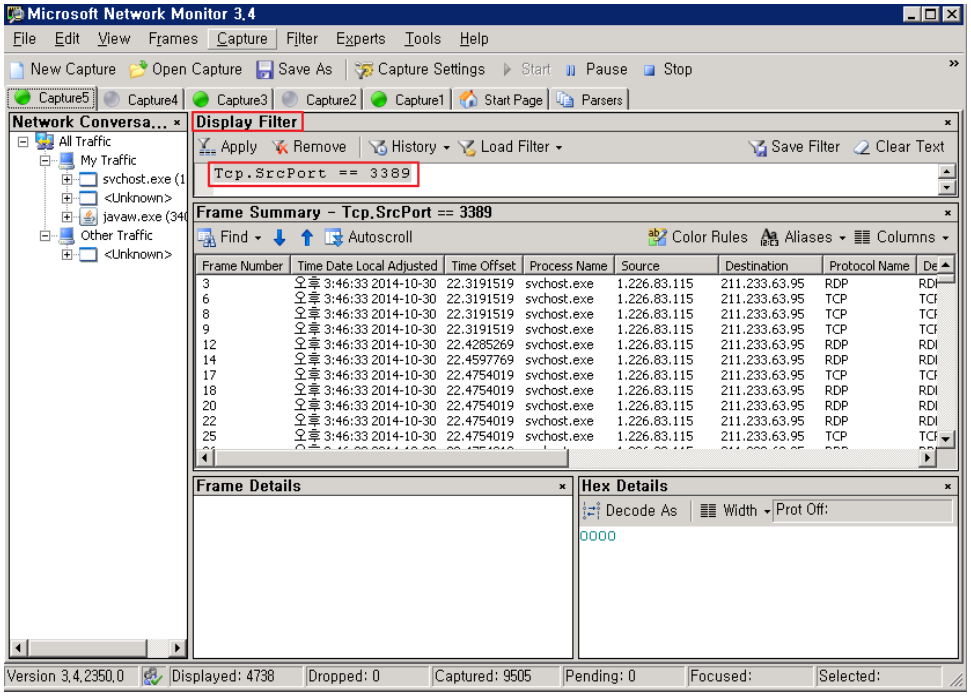


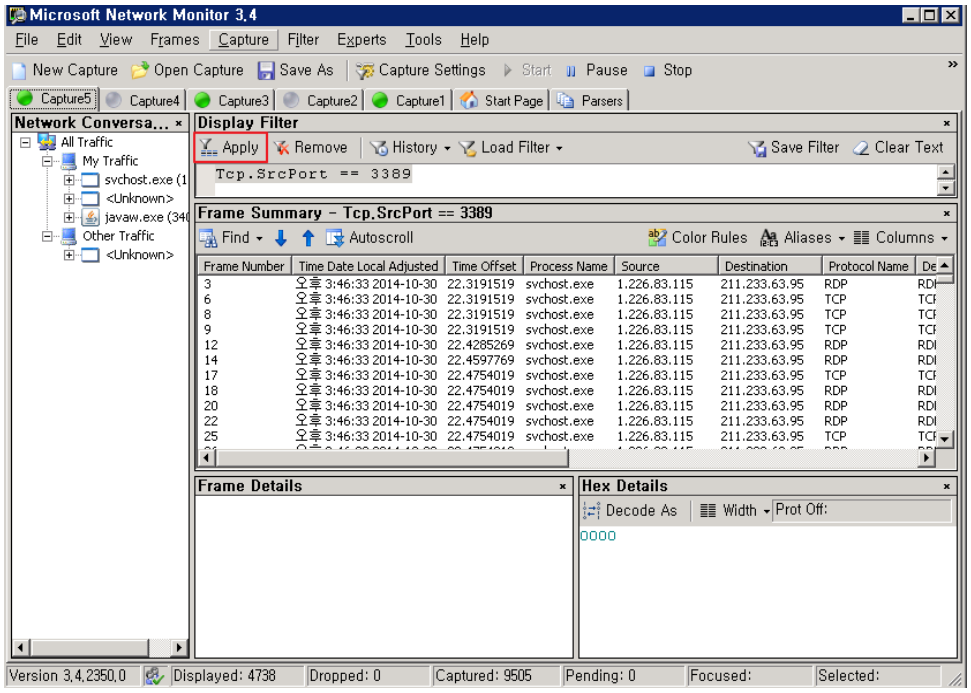
하단에 패킷 정보를 상세하는 분석하는 화면이며, Wireshark 와 비슷하게 프레임별/Hex 값으로 분석이 가능합니다.



C) 특정포트 : 3389 로 들어오는 패킷 확인방법

MicroSoft Network Monitor 실행화면에서 Display Filter 부분에 Tcp.SrcPort == 3389 입력후 Apply 메뉴를 실행합니다.





4. OS 별 로그분석툴 설치하기

1) CentOS / Redhat 계열

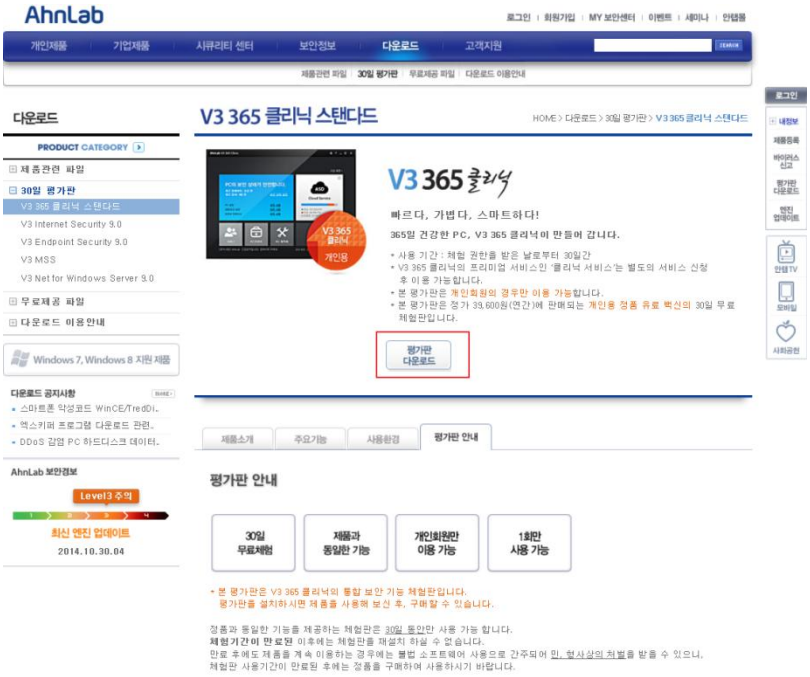
아파치 로그분석도구 Awstat 설치 및 사용

2) Windows 서버(Windows Server 2008) 계열

로그분석툴 awstats 설치(Windows Server 2008)

5. 윈도우 바이러스 점검

안랩홈페이지 http://ahnlab.com/ - 다운로드 – 30 일평가판 – V3 Net For Windows Server 9.0 을 선택후 30 일평가판을 서버쪽에 설치후 바이러스 점검작업을 진행합니다.



THANK YOU