

## S U C C E S S P A R T N E R .

# 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





## 나의서비스 관리 - 사용량 모니터링 - 일별 전송량 보기

#### 조회기간

조회방법	<ul> <li>● 월별보기</li> <li>○ 기간선택</li> </ul>
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
<u>2014년 10월 29일</u>	56.5 Mbps	29.3 Mbps	317 GB
<u>2014년 10월 28일</u>	61.4 Mbps	35.4 Mbps	383 GB
<u>2014년 10월 27일</u>	65.8 Mbps	37.9 Mbps	410 GB
<u>2014년 10월 26일</u>	56.7 Mbps	25.5 Mbps	275 GB
<u>2014년 10월 25일</u>	46.4 Mbps	24.6 Mbps	267 GB
<u>2014년 10월 24일</u>	57.6 Mbps	32.6 Mbps	353 GB
<u>2014년 10월 23일</u>	59.9 Mbps	33.6 Mbps	364 GB
<u>2014년 10월 22일</u>	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

수신며부	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 : <u>http://toolbox.krcert.or.kr/MMVF/MMVFView\_V.aspx?MENU\_CODE=14&PAGE\_NUMB</u> <u>ER=15</u>

- 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\_NU MBER=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 <u>http://www.google.com/intl/ko/chrome/</u>

크롬 브라우저 창에서 홈페이지 주소를 입력합니다

N NAVER ×		
← → C ♠ 🗋 www.naver.com		☆ 🔒 🧠 🗵 =
▶ 네이버 앱 다운로드 🛛 T 시스템글꼴 ▼ ?	A 🖂 Me	해피빈 <mark>주니어네이에 (</mark> GHənəəme
<b>NAVER</b>	Q 교황방한 사진전 가장 불신하는 집단 1위 토종 돌고래	Z44       방류
메일 카페 블로그 지식iN 쇼핑   사전 뉴스 증권 부동(	· 지도 영화 뮤직 책 웹툰 📘 그라폴리오 더보기 -	2 성민 ★207
	김민과 해는 영화보다, 이리엄한 관람포인트 영상 교조·	회원가입 아이디/비밀번호 찾가 아이디 로그인 비밀번호 로그인 일회용로그인
연합뉴스▶ '검열' 논란 카톡 탈퇴 급증…'사이버 망명' 기	속 네이버뉴스   연예   스포츠   경제   오늘의신문	<b>투데이</b> 10.14.(화)   TV편성 →
<b>뉴스스탠드 &gt; 전체인론사   M뉴스</b>	표 🗐 주요언론사 🔹	신문1면→ 디자인 스펙트럼, 그 무한의 영역 학습→ 영어로 듣는 뉴스   오늘의 글로벌 회화 스포츠→ 인치홍·김선빈, 시즌 끝나고 입대
NEWSIS() DECEMBENT D		스포츠 > 여자배구 "공공의 적 IBK기업은행" 생활위젯 " 1/3 < >
● REUTERS ● REUTER	ChimyAcus         Chose           Image: Acuse         Image: Acuse           Image: Acuse         Image: Acuse	학생부터 학부모, 선생님까지 재미있게 배우는 NAVER 소프트웨어야 놀자 중
주 구독설정   [알림] 언론사별 주요뉴스를 메인에서 바로 볼 수 있 다.	비요) 1/5 < >	MA AR

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.

💿 De	eveloper Tools - http://www.nave	r.com/									×	
Q	2 🖸 Elements   Network   Sources Timeline Profiles Resources Audits Console						)E (	<b>☆</b> ⊑	1			
٠	🛇 🗑 📒 🗆 Preserve log	Disable	cache									
Name Path		Method	Status Text	Туре	Initiator	Size Content	Time Latency	Timeline	2.00 s	3.00 s		
res E	16376307-d09a-4166-834a-6f6d shopping.phinf.naver.net/201410	GET	200 OK	image/jp	Other	5.7 KB 5.3 KB	23 ms 17 ms			1		^
	press_info,json /include/newsstand	GET	200 OK	text/html	jindo.all.20140327 Script	2.8 KB 29.8 KB	28 ms 28 ms					
53	?src=http://img.naver.net/static/ img.naver.net/dthumb.phinf	GET	200 OK	image/jp	Other	18.4 KB 18.0 KB	55 ms 55 ms					
	?src=http://img.naver.net/static/ img.naver.net/dthumb.phinf	GET	200 ОК	image/gif	Other	16.0 KB 15.6 KB	57 ms 54 ms					
	?src=http://img.naver.net/static/ img.naver.net/dthumb.phinf	GET	200 OK	image/jp	Other	21.3 KB 20.9 KB	64 ms 62 ms					
	?src=http://img.naver.net/static/ img.naver.net/dthumb.phinf	GET	200 OK	image/jp	Other	23.6 KB 23.2 KB	56 ms 53 ms					
256	?src=http://img.naver.net/static/ img.naver.net/dthumb.phinf	GET	200 OK	image/jp	Other	17.2 KB 16.8 KB	63 ms 61 ms					
	mobile_202609482164.jpg img.naver.net/static/www/mobil	GET	200 OK	image/jp	Other	(from cac	8 ms 8 ms				1	
٢	mobile_145606890271.jpg img.naver.net/static/www/mobil	GET	200 OK	image/jp	Other	(from cac	8 ms 8 ms				1	
	mobile_170300599616.jpg img.naver.net/static/www/mobil	GET	200 OK	image/jp	Other	(from cac	8 ms 8 ms				Т	
	dl_qr_naver.png img.naver.net/static/www	GET	200 OK	image/png	Other	(from cac	8 ms 8 ms				I.	
	naver_homepage.png img.naver.net/static/www/up/2012	GET	200 OK	image/png	Other	(from cac	7 ms 7 ms				1	Ŧ
95 re	quests I 328 KB transferred I 3.37 s	(load: 2.89 s	, DOMConte	ntLoaded: 1	.01 s)							
Cor	nsole Search Emulation Render	ring										
De	vice 🗸 Model: <sele< td=""><td>ct model&gt;</td><td></td><td></td><td>Save as</td><td>emove</td><td></td><td></td><td></td><td></td><td></td><td>î</td></sele<>	ct model>			Save as	emove						î
Me	edia 🕑 Emulate scre	en resolutio	'n									
Ne	twork Provide Line		2099		1202							
30	Reset Resolution:		2088	-	1292							
	Device pixel	ratio:										
	Emulate mot	pile										Ţ

#### 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.



<ul> <li>Statistics for a</li> </ul>	∍m1 ———					
Total: Pack Pack IPv4: 841 IPv6: 841 ICP: 841 UDP: ICMP: Other IP: Non-IP:	otal (ets   1729 83 1729 82 0 1729 82 0 0 0 0 0 0 0 0	Total I Bytes B902K 7118K 7118K 0 0 0 0 0	ncoming Packets 554299 554299 0 554299 0 0 0 0 0	Incoming Bytes 819338K 811578K 0 811578K 0 0 0 0	Outgoing Packets 287430 287430 287430 287430 0 0 0 0 0 0 0	Outgoing Bytes 19564351 15540331 0 15540331 0 0 0 0 0 0
Total rates:	295874.1 37113.6	kbits/sec packets/s	: ec	Broadcast pack Broadcast byte	kets: es:	0
Incoming rates:	289120.8 24449.2	kbits/sec packets/s	ec	IP checksum e	rrors:	0
outgoing fates.	12664.4	packets/sec	ec			
	0.00					
i Elapsed time:	0:00					

**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 <u>http://127.0.0.1:10090</u> 으로 접속하여 프로그램을 사용하실수 있습니다

🖉 WFilter Enterprise 4,1 - Windows Internet Explorer 📃
🕞 🕒 🔻 🔣 http://127,0,0,1:10090/ 💽 💀 🍫 🗙 📴 Live Search 🖉
파일(E) 편집(E) 보기(V) 즐겨찾기(A) 도구(T) 도움말(H)
😭 즐겨찾기 🛛 🏡 🏈 추천 사이트 👻 🔊 무료 Hotmail 🔊 연결 사용자 정의 🔊 웹 조각 갤러리 🗸
88 💌 🏈 WFilter editions comp 👿 WFilter Enterprise 4,1 🗙 👘 🏠 🔹 🗟 🕤 🖃 🖶 🛪 페이지(P) - 안전(S) - 도구(Q) - @
IMFirewall
Monitor and Filter Internet Activities
Password: Password
LOGIN
Notice: Please check <u>WFilter Installation Notes</u> for login issues.
Copyright@2014_IMFirewall Software. All rights reserved. Homepage   Support   Contact

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.

💯 Microsoft Network I	Monitor 3,4					
<u>File E</u> dit <u>V</u> iew F <u>r</u> an	mes <u>C</u> apture F <u>i</u> lter B	<u>x</u> perts <u>T</u> ools	<u>H</u> elp			
📄 New Capture  👌 Ope	en Capture 🛛 🔚 Save As	🏹 🐺 Capture Se	ttings 🕨 Start 💷 F	<sup>o</sup> ause 💷 Stop		»
🕘 Capture1 🚮 Start Pa	ge 🐚 Parsers					
Network Convers×	Display Filter					×
	🏠 Apply 🛛 🙀 Remove	🛛 🏹 History 👻	💪 Load Filter 👻	V 🖓 S	Save Filter 🏼 🥥 י	Clear Text
						÷
	Frame Summary					×
	强 Find 🗸 🖡 🕇 🗔 A	utoscroll	abg	Color Rules  🏘	, Aliases → 💷	Columns 🗸
	Frame Number Time Date	Local Adjusted   Tir	ne Offset   Process Name	Source	Destination	Protocol Na
	•					F
	Frame Details		× Hex Det	tails		×
			¦≓¦ Deco	de As 🛛 📰 Wid	dth → Prot Off:	
			0000			
Version 🛃 Displayed:	Dropped:	Captured:	Pending:	Focused:	Selected	1.

(윈도우 프로세스별 통신 상태 확인)

💭 Microsoft Network Monitor 3,4				-	. 🗆 🗙		
<u>File Edit View Frames Capture Fil</u>	er E <u>x</u> perts <u>T</u> ools	<u>H</u> elp					
📄 New Capture 👏 Open Capture  뒩 Sav	e As   🦐 Capture Sett	ings 🕨 Start 👖 Pause	e 🧧 Stop		*		
🥥 Capture1 🚮 Start Page 🐚 Parsers							
Network Conversations ×	Display Filter				×		
🖃 🛂 All Traffic	🋴 Apply 🛛 🙀 Remove	🗉 📉 History 👻 🏹 Load	l Filter 👻		»		
					-		
	E → svcbst.exe (1780)						
	Frame Summary -	[Conversation Filter]			×		
	强 Find 🗸 👃 🕇 🗔	Autoscroll 🛛 🔡 Color	Rules 🗛 Alia	ases 🕶 🃰 Colur	nns 🗸		
🖻 📲 Other Traffic	Frame Number   Time Dal	e Local Adjusted   Time Offse	t Process Name	Source	De: 🔺		
	3 오후2:5	3:34 2014-10-30 21.8414205	svchost.exe	116.122.156.198	1.22		
	4 오후2:5	3:34 2014-10-30 21.8882955	5 svchost.exe	1.226.83.115	116		
	5 エテ2:5 6 오言2:5	3:34 2014-10-30 21.8882955	svchostlexe	116.122.156.198	1.2		
	41 오후 2:5	3:35 2014-10-30 22.3257955	5 svchost.exe	116.122.156.198	1.22		
	46 오후 2:5	3:35 2014-10-30 22.4507955	5 svchost.exe	1.226.83.115	116		
	▲48 온후2:5	3:35 2014-10-30 22.8882955	5 svchost.exe	1.226.83.115	116		
	▲ 49 오후2:5	3:35 2014-10-30 22.8882955	i svchost.exe	1.226.83.115	116		
	50 오훈2:5	3:35 2014-10-30 22.8882955	svchost.exe	116.122.156.198	1.22		
	60 <u>오루 2:5</u>	3:36 2014-10-30 23.7789205	svchost.exe	1.226.83.115	116		
	•						
	Frame Details	× Hex	Details		×		
			Decode As 🛛 🖩	≣ Width → Prot C	)ff:		
		000	0				
Version 🕵 Displayed: 951 🛛 Dropped: 0	Captured: 3875	Pending: 0 Fo	cused:	Selected:			

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

💯 Microsoft Network M	onitor 3.4							
<u>F</u> ile <u>E</u> dit <u>V</u> iew F <u>r</u> ame	s <u>C</u> apture F <u>i</u> lter E <u>x</u> perts <u>T</u> ools <u>H</u> elp							
📄 New Capture  👏 Open	] New Capture 📂 Open Capture 🔚 Save As   🐺 Capture Settings 🕨 Start 💵 Pause 🍙 Stop 🔷 🤻							
Capture3 Capture2	🔵 Capture1 🚮 Start Page 🐚 Parsers							
Network Conversa ×	Display Filter	×						
🖃 😼 All Traffic	🖳 Apply 🙀 Remove 🛛 🖓 History 🗸 Load Filter 🗸 🛛 🏹 Save Filte	er 🥥 Clear Text						
🖃 🔜 My Traffic								
SVCNOSC.exe (1		•						
± √ IPv4 (1.226	Frame Summary - [Conversation Filter]	×						
	🖳 Find 🗸 🖡 😭 Autoscroll 🛛 🐉 Color Rules 🖓 Aliases	s 🕶 🏢 Columns 🗸						
🗄 🛄 <unknown></unknown>	Exame Number Time Date Local Adjusted Time Offset Process Name Source Destination	Protocol Name De						
Other Traffic	9 오후 3:34:19 2014-10-30 22.8835579 svchost.exe 1.226.83.115 211.233.63.95 R	RDP RD						
± <unknown></unknown>	10 오후 3:34:19 2014-10-30 22.8991829 svchost.exe 211.233.63.95 1.226.83.115 R	RDP RDI						
	11 오후 3:34:19 2014-10-30 22.8991829 svchost.exe 211.233.63.95 1.226.83.115 T	CP TCF						
	12 포우 3:34:19 2014-10-30 22:8991829 SVCNoSt.exe 1.225.83.115 211.233.63.95 1 13 오늘 3:34:19 2014-10-30 22:8091829 cychoct eve 211 233.63.05 1 226.83.115 T							
	14 9章 3:34:19 2014-10-30 22.8991829 svchost.exe 1.226.83.115 211.233.63.95 T	TCP TCF						
	15 오후 3:34:19 2014-10-30 22.8991829 svchost.exe 1.226.83.115 211.233.63.95 T	ICP TCF						
	16 오후3:34:19 2014-10-30 22.9148079 svchost.exe 211.233.63.95 1.226.83.115 T	CP TCF						
	20 오후 3:34:19 2014-10-30 23.0241829 svchost.exe 211.233.63.95 1.226.83.115 R	DP RDI						
	21 Y = 3:34:19 2014-10-30 23.0241829 svchost.exe 1.226.83.115 211.233.63.95 R	CDP RDI						
	22 포우 3:34:19 2014-10-30 23.0241829 SVCNOSt.exe 211.233.65.95 1.226.83.115 R 23 오늘 3:34:10 2014.10.30 23.0241829 cychoct eve 1.226.83.115 211.233.63.05 D	CUP RUI						
	23 11.223.03.119 2014-10-30 23.0241029 svchost.exe 1.220.03.119 2014-26.83.115 R							
		Þ						
	Frame Details * Hex Details	×						
	-Frame: Number = 15, Captured Frame Len int Decode As State Vidth - Prot Off:	0 (0×00)						
	Ethernet: Etype = Internet IP (IPv4), D coop oo po cp 7P cc 45 c							
	H-Ipv4: Src = 1.226.83.115, Dest = 211.20007 FF 42 00 50 15 06 45 C.	A .DE(IEE						
	Ten: Flags= 1 S SrcPort=MS NBT Second 45 on 20 20 40 55 00	о рв. р						
		2 D DÕ Å						
		2 .0.00.a						
	↓ 0023 3D 13 22 DC FA 92 B	1 =."ΠύΠ+ ▼						
Version 3, 4, 2350, 0 🐼 Dis	splayed: 1216 Dropped: 0 Captured: 2245 Pending: 0 Focused: 15 Se	elected: 1						

## C) 특정포트 : 3389 로 들어오는 패킷 확인방법

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

💭 Microsoft Network Ma	onitor 3,4					l X
<u>File E</u> dit <u>V</u> iew F <u>r</u> ame	s <u>C</u> apture F <u>i</u> lter E <u>x</u> perts <u>T</u> ools	<u>H</u> elp				
📄 New Capture 🛛 😁 Open	Capture 🔚 Save As 🛛 😿 Capture Se	ettings 🕨 Start 👖 P	ause 🥃 Stop			»
Capture5 Capture4	Capture3 Capture2 Capture1	🔥 Start Page 🗔 🕞 Pa	vsers			
Network Conversa ×	Disnlay Filter	10				×
🖃 🚂 All Traffic	🕮 Apply 🔏 Remove   🖓 History -	- 🔀 Load Filter -		🔏 Save F	ilter 🥏 Clear Te:	xt
🖻 📒 My Traffic	Tcp.SrcPort == 3389			100	-	
+ svchost.exe (1						•
i iavaw.exe (340	Frame Summary - Tcp.SrcPort ==	= 3389				×
🖻 🧾 Other Traffic	🔜 Find 🗸 👃 🕇 📑 Autoscroll		📸 Color	Rules 🖓 Alias	es 🗸 🏢 Columns	-
	Frame Number   Time Date Local Adjusted	Time Offset Process Nan	me Source	Destination	Protocol Name De	•
	3 오후 3:46:33 2014-10-30 2	22.3191519 svchost.exe	1.226.83.115	211.233.63.95	RDP RD	
	6 오후 3:46:33 2014-10-30 3 8 오후 3:46:33 2014-10-30 3	22.3191519 svchost.exe 22.3191519 svchost.exe	1.226.83.115	211.233.63.95	TCP TC	1
	9 오후 3:46:33 2014-10-30 2	22.3191519 svchost.exe	1.226.83.115	211.233.63.95	TCP TC	j
	12 오후 3:46:33 2014-10-30 2	22.4285269 svchost.exe	1.226.83.115	211.233.63.95	RDP RD	1
	14 오후 3:46:33 2014-10-30 2 17 오후 3:46:33 2014-10-30 2	22.4597769 svchost.exe 22.4754019 svchost.exe	1.226.83.115	211.233.63.95	RDP RD	4
	18 오후 3:46:33 2014-10-30 2	22.4754019 svchost.exe	1.226.83.115	211.233.63.95	RDP RD	, II
	20 오후 3:46:33 2014-10-30 2	22.4754019 svchost.exe	1.226.83.115	211.233.63.95	RDP RD	1
	22 오후 3:46:33 2014-10-30 3	22.4754019 svchost.exe	1.226.83.115	211.233.63.95	RDP RD	4
		22.4754019 svchost.exe	1.226.83.115	211.233.63.95		
	[1]				<u> </u>	
	Frame Details	× He	ex Details			×
		1≓	† Decode As 🛛 🗏	📱 Width 🖌 Prot O	ff:	
		00	000			
4 F						
Version 3.4.2350.0 🕺 Dis	splaved: 4738 Dropped: 0 Ca	aptured: 9505 Penc	ding: 0 Fo	cused:	Selected:	
		,				_ ///
Microsoft Network M	pnitor 3,4					×
<u>File E</u> dit <u>V</u> iew F <u>r</u> ame	s <u>C</u> apture F <u>i</u> lter E <u>x</u> perts <u>T</u> ools	<u>H</u> elp				
📄 New Capture 👏 Open	Capture 🛛 🔓 Save As 🛛 🐺 Capture Se	ettings 🕨 Start 👖 P	ause 🤉 Stop			»
Capture5 💿 Capture4	🔵 Capture3 🔍 Capture2 🔵 Capture1	🚺 🏠 Start Page 🗔 Pa	arsers			
Network Conversa ×	Disnlay Filter					×

	🖉 capitales 🔍 capitales 🖉 capitales 🚺 static rage 🖓 raiseis					
Network Conversa ×	Display Filter	×				
🖃 🛂 All Traffic	🏠 Apply 🛛 🛠 Remove 🛛 🖏 History 🗸 Load Filter 🗸 🛛 🥁 Save Filter 🖉 Clea	r Text				
My traffic	Tcp.SrcPort == 3389					
		-				
	Frame Summary - Tcp,SrcPort == 3389	×				
🖃 🧾 Other Traffic	🖫 Find 🗸 🧍 😨 Autoscroll 🛛 🐕 Color Rules 🖓 Aliases 🗸 🏢 Colu	.mns 🗸				
i <unknown></unknown>	Frame Number   Time Date Local Adjusted   Time Offset   Process Name   Source   Destination   Protocol Name	e D∈▲				
	3 오章 3:46:33 2014-10-30 22.3191519 svchost.exe 1.226.83.115 211.233.63.95 RDP	RD				
	6 오章 3:46:33 2014-10-30 22.3191519 svchost.exe 1.226.83.115 211.233.63.95 TCP	TCF				
	8 오후 3:46:33 2014-10-30 22.3191519 svchost.exe 1.226.83.115 211.233.63.95 TCP	TCF				
	9 오훈3:46:33 2014-10-30 22.3191519 svchost.exe 1.226.83.115 211.233.63.95 TCP	TCF				
	12 오후 3:46:33 2014-10-30 22.4285269 svchost.exe 1.226.83.115 211.233.63.95 RDP	RDI				
	14 오후 3:46:33 2014-10-30 22:4597769 svchost.exe 1.226.83.115 211.233.63.95 RDP	RDI				
	17 오후 3:46:33 2014-10-30 22:4754019 svchost.exe 1.226.83.115 211.233.63.95 TCP	TO				
	18 2 = 3:46:33 2014-10-30 22:4754019 svchost.exe 1.226.83.115 211.233.63.95 RDP	RDI				
	20 T = 3:46:33 2014-10-30 22:4754019 sydnost.exe 1.226.63.115 211.233.63.95 RDP	RDI DDI				
	22 E \$ 3:46:33 2014-10-30 22:4754019 StrubsLeve 1.226.03.115 211.233.63.95 RDP					
	Frame Details					
	;≓; Decode As   ≣≣ Width + Prot Off:					
	0000					
•						
Version 3.4.2350.0 🚳 Di	isplayed: 4738 Dropped: 0 Captured: 9505 Pending: 0 Encused: Selected:					

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

	제품관련 파일 / 30일	· 평가판 무료제공 파일 다운로드 이	용안내		
다운로드	V3 365 클리닉 스탠다드		HOME > 다문로드 > 30월	) 평가판 > V3 365 클리닉 스탠다드	
	BARE 20100 01.111				
3 제품관련 파일		1/2 365 = 2/4	4		
∃ 30일 평가판		V5 505 24	7		
V3 365 클리닉 스탠다드		빠르다, 가볍다, 스마!	트하다!		
V3 Internet Security 9.0	🐣 🔂 🛠 🛛 😽 365일 건강한 PC, V3 365 클리닉이 만들어 갑니다.				
V3 MSS	7/218	<ul> <li>사용 기간 : 체험 권한을 !</li> </ul>	받은 날로부터 30일간		
V3 Net for Windows Server 9.0		<ul> <li>* V3 365 클리닉의 프리미엄</li> <li>호 이용 가능합니다.</li> </ul>	넘 서비스인 '클리닉 서비스'	는 별도의 서비스 신청	
= 무료제공 파일		<ul> <li>본평가판은개인회원의</li> <li>보평가판은 개인회원의</li> </ul>	경우만 이용 가능합니다. 의(여가)에 파매되는 개인용	전품 응류 변식이 111의 무류	
∃ 다운로드 이용안내		체험판입니다.			
Windows 7, Windows 8 지원 제품		평가판 다운로드			
다운로드 공지사항					
<ul> <li>스마트폰 악성코드 WinCE/TredDi.</li> </ul>					
• 엑스키퍼 프로그램 다운로드 관련. • DDaS 같영 PC 하드디스크 데이터.	제품소개 주요가방 시	·용환경 평가판 안내			
AhnLab 보안경보	평가판 안내				
Level3 주의					
최신 전신 업데이트	30일 제품과 모르체험 도입하기는	개인회원만 이용 가는	1회만 사용 기능		
2014 10 20 04	1.00-110 0.000-10	-10,10	-10 - 10		

성용과 확실한 기능을 계용하는 적합년은 <u>30일 보았던</u> 사용 가능 합니다. **특별기간인 맨로인** 이유석는 체험들을 제설치 정복 수 있습니다. 만로 추려도 제품을 <sup>4</sup> 에 응하는 공부에는 특별 소프트웨어 사용으로 간주되어 <u>만, 학사상의 처벌</u>을 받을 수 있으니, 체험단 사용기간인 만로본 추측는 호흡을 구매하여 사용하시기 바랍니다.

Cafe24"



www.cafe24.com I www.simplexi.com