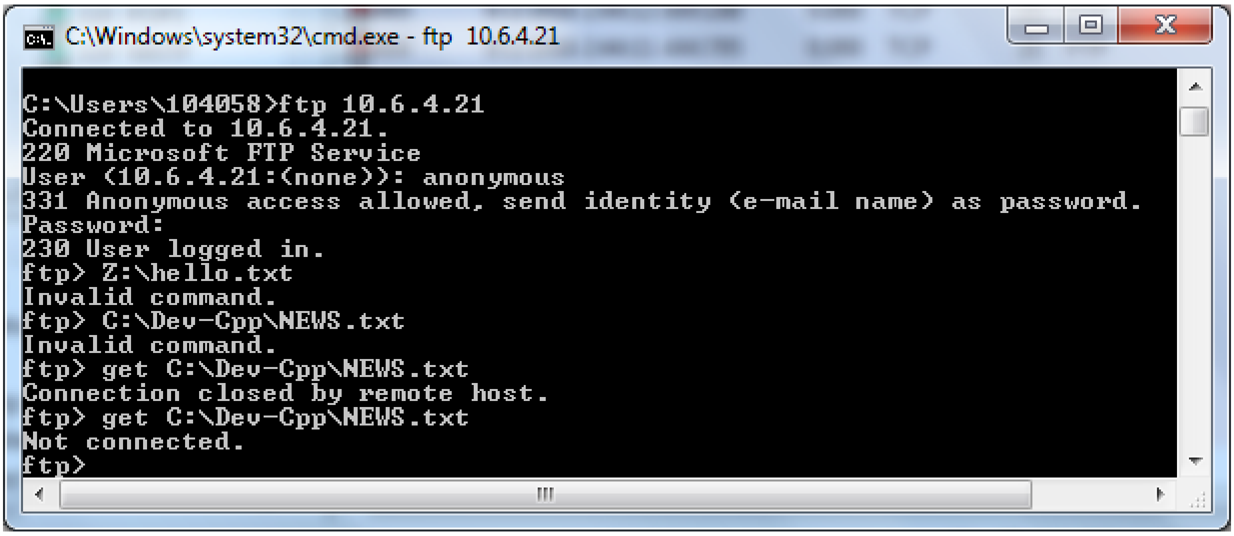
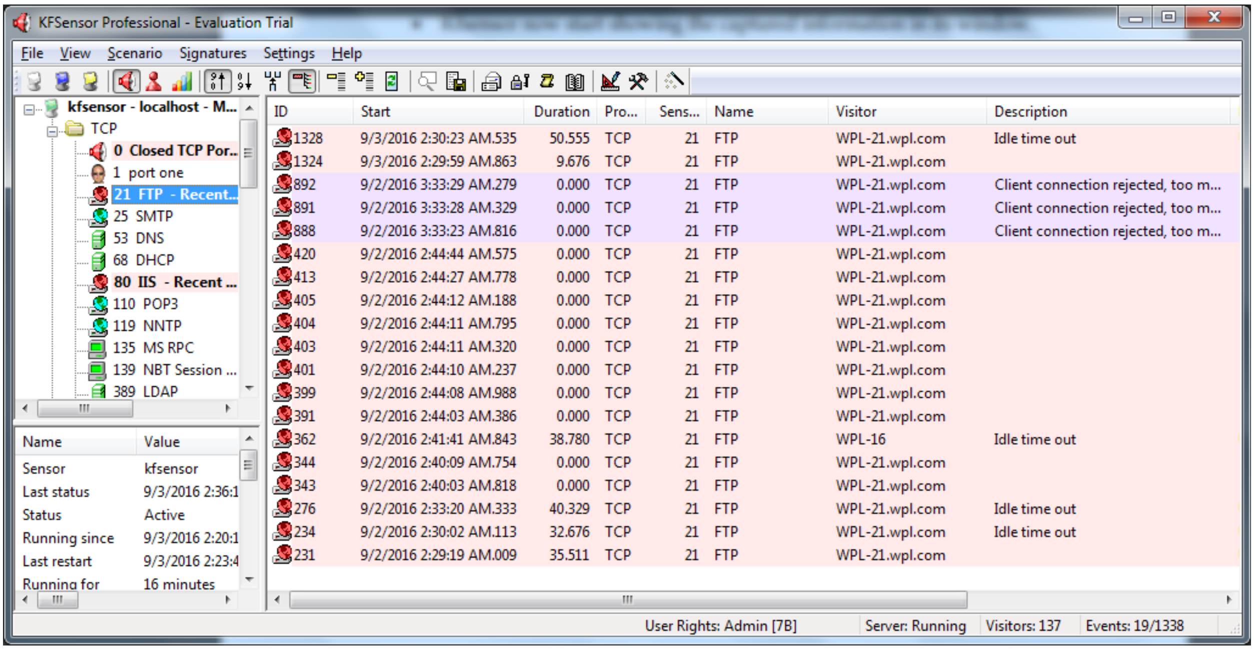
FTP



C:\Windows\system32\cmd.exe - ftp 10.6.4.21

```
C:\Users\104058>ftp 10.6.4.21
Connected to 10.6.4.21.
220 Microsoft FTP Service
User (10.6.4.21:(none)): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
ftp> Z:\hello.txt
Invalid command.
ftp> C:\Dev-Cpp\NEWS.txt
Invalid command.
ftp> get C:\Dev-Cpp\NEWS.txt
Connection closed by remote host.
ftp> get C:\Dev-Cpp\NEWS.txt
Not connected.
ftp>
```

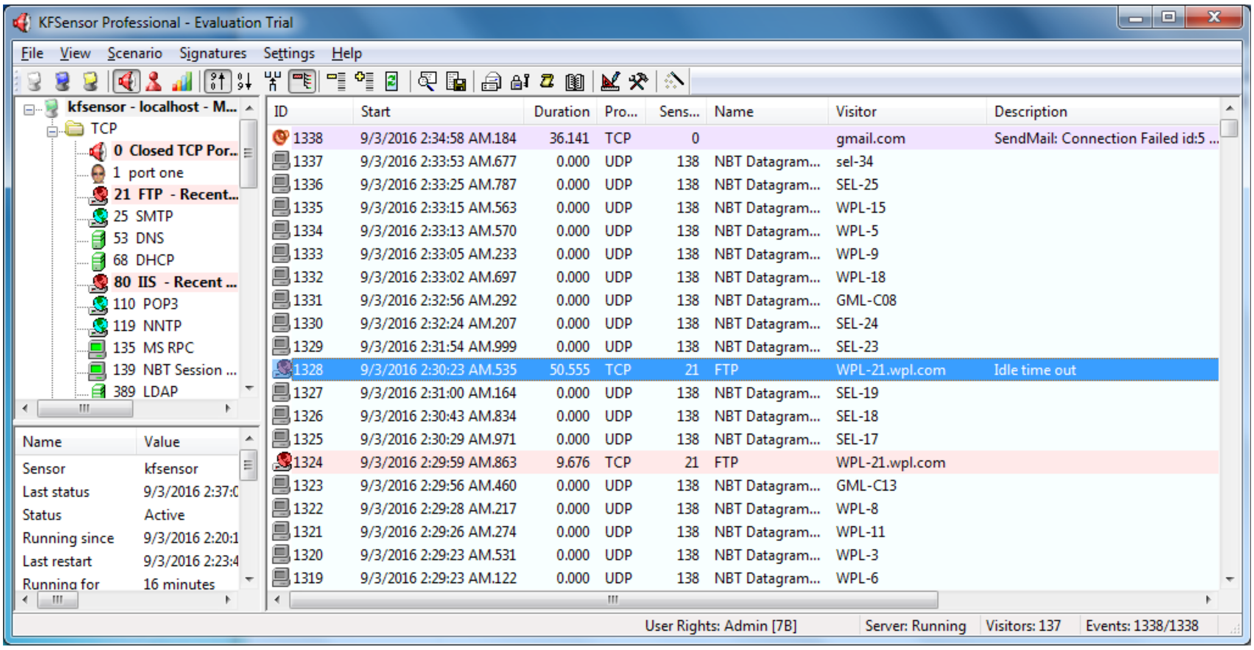


KFSensor Professional - Evaluation Trial

Name	Value
Sensor	kfsensor
Last status	9/3/2016 2:36:1
Status	Active
Running since	9/3/2016 2:20:1
Last restart	9/3/2016 2:23:4
Running for	16 minutes

ID	Start	Duration	Pro...	Sens...	Name	Visitor	Description
1328	9/3/2016 2:30:23 AM.535	50.555	TCP	21	FTP	WPL-21.wpl.com	Idle time out
1324	9/3/2016 2:29:59 AM.863	9.676	TCP	21	FTP	WPL-21.wpl.com	
892	9/2/2016 3:33:29 AM.279	0.000	TCP	21	FTP	WPL-21.wpl.com	Client connection rejected, too m...
891	9/2/2016 3:33:28 AM.329	0.000	TCP	21	FTP	WPL-21.wpl.com	Client connection rejected, too m...
888	9/2/2016 3:33:23 AM.816	0.000	TCP	21	FTP	WPL-21.wpl.com	Client connection rejected, too m...
420	9/2/2016 2:44:44 AM.575	0.000	TCP	21	FTP	WPL-21.wpl.com	
413	9/2/2016 2:44:27 AM.778	0.000	TCP	21	FTP	WPL-21.wpl.com	
405	9/2/2016 2:44:12 AM.188	0.000	TCP	21	FTP	WPL-21.wpl.com	
404	9/2/2016 2:44:11 AM.795	0.000	TCP	21	FTP	WPL-21.wpl.com	
403	9/2/2016 2:44:11 AM.320	0.000	TCP	21	FTP	WPL-21.wpl.com	
401	9/2/2016 2:44:10 AM.237	0.000	TCP	21	FTP	WPL-21.wpl.com	
399	9/2/2016 2:44:08 AM.988	0.000	TCP	21	FTP	WPL-21.wpl.com	
391	9/2/2016 2:44:03 AM.386	0.000	TCP	21	FTP	WPL-21.wpl.com	
362	9/2/2016 2:41:41 AM.843	38.780	TCP	21	FTP	WPL-16	Idle time out
344	9/2/2016 2:40:09 AM.754	0.000	TCP	21	FTP	WPL-21.wpl.com	
343	9/2/2016 2:40:03 AM.818	0.000	TCP	21	FTP	WPL-21.wpl.com	
276	9/2/2016 2:33:20 AM.333	40.329	TCP	21	FTP	WPL-21.wpl.com	Idle time out
234	9/2/2016 2:30:02 AM.113	32.676	TCP	21	FTP	WPL-21.wpl.com	Idle time out
231	9/2/2016 2:29:19 AM.009	35.511	TCP	21	FTP	WPL-21.wpl.com	

User Rights: Admin [7B]   Server: Running   Visitors: 137   Events: 19/1338



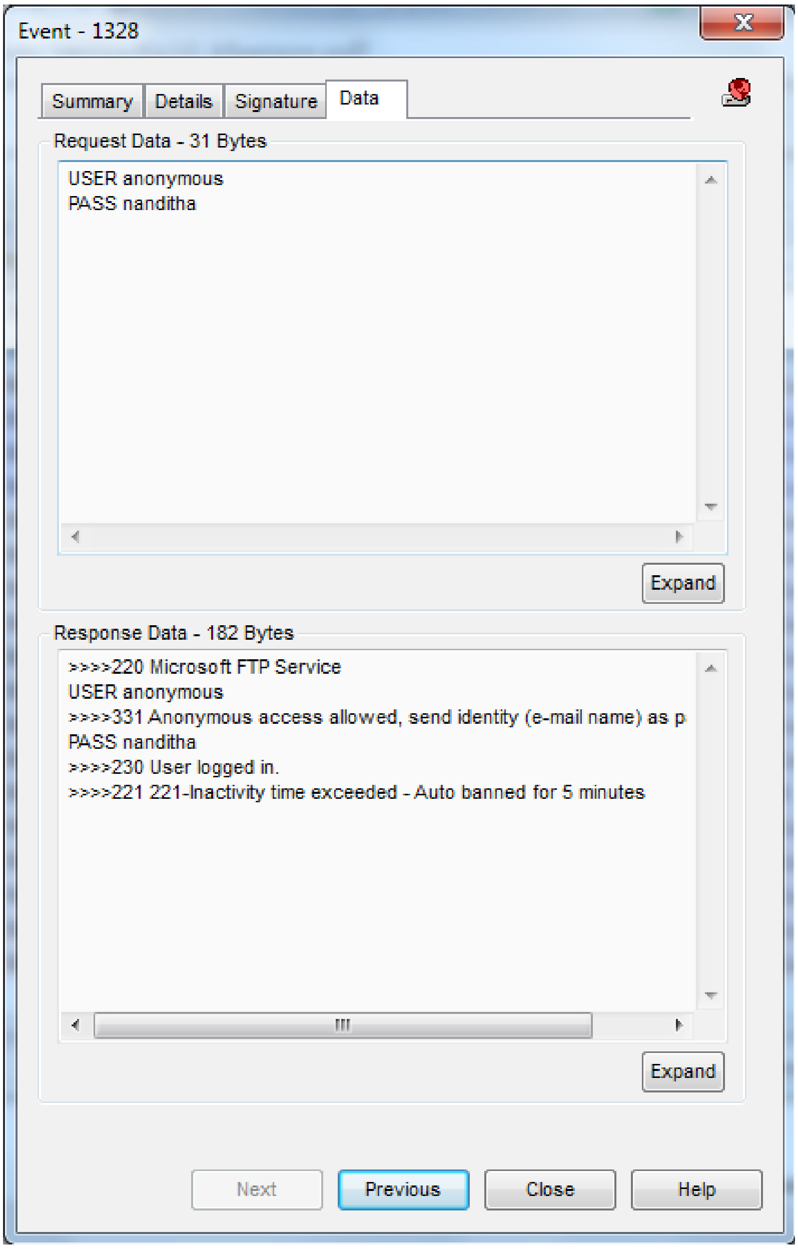
KFSensor Professional - Evaluation Trial
File View Scenario Signatures Settings Help

kfsensor - localhost - M...
TCP
0 Closed TCP Por...
1 port one
21 FTP - Recent...
25 SMTP
53 DNS
68 DHCP
80 IIS - Recent ...
110 POP3
119 NNTP
135 MS RPC
139 NBT Session ...
389 LDAP

Name	Value
Sensor	kfsensor
Last status	9/3/2016 2:37:(
Status	Active
Running since	9/3/2016 2:20:1
Last restart	9/3/2016 2:23:4
Running for	16 minutes

ID	Start	Duration	Pro...	Sens...	Name	Visitor	Description
1338	9/3/2016 2:34:58 AM.184	36.141	TCP	0		gmail.com	SendMail: Connection Failed id:5 ...
1337	9/3/2016 2:33:53 AM.677	0.000	UDP	138	NBT Datagram...	sel-34	
1336	9/3/2016 2:33:25 AM.787	0.000	UDP	138	NBT Datagram...	SEL-25	
1335	9/3/2016 2:33:15 AM.563	0.000	UDP	138	NBT Datagram...	WPL-15	
1334	9/3/2016 2:33:13 AM.570	0.000	UDP	138	NBT Datagram...	WPL-5	
1333	9/3/2016 2:33:05 AM.233	0.000	UDP	138	NBT Datagram...	WPL-9	
1332	9/3/2016 2:33:02 AM.697	0.000	UDP	138	NBT Datagram...	WPL-18	
1331	9/3/2016 2:32:56 AM.292	0.000	UDP	138	NBT Datagram...	GML-C08	
1330	9/3/2016 2:32:24 AM.207	0.000	UDP	138	NBT Datagram...	SEL-24	
1329	9/3/2016 2:31:54 AM.999	0.000	UDP	138	NBT Datagram...	SEL-23	
1328	9/3/2016 2:30:23 AM.535	50.555	TCP	21	FTP	WPL-21.wpl.com	Idle time out
1327	9/3/2016 2:31:00 AM.164	0.000	UDP	138	NBT Datagram...	SEL-19	
1326	9/3/2016 2:30:43 AM.834	0.000	UDP	138	NBT Datagram...	SEL-18	
1325	9/3/2016 2:30:29 AM.971	0.000	UDP	138	NBT Datagram...	SEL-17	
1324	9/3/2016 2:29:59 AM.863	9.676	TCP	21	FTP	WPL-21.wpl.com	
1323	9/3/2016 2:29:56 AM.460	0.000	UDP	138	NBT Datagram...	GML-C13	
1322	9/3/2016 2:29:28 AM.217	0.000	UDP	138	NBT Datagram...	WPL-8	
1321	9/3/2016 2:29:26 AM.274	0.000	UDP	138	NBT Datagram...	WPL-11	
1320	9/3/2016 2:29:23 AM.531	0.000	UDP	138	NBT Datagram...	WPL-3	
1319	9/3/2016 2:29:23 AM.122	0.000	UDP	138	NBT Datagram...	WPL-6	

User Rights: Admin [7B] Server: Running Visitors: 137 Events: 1338/1338

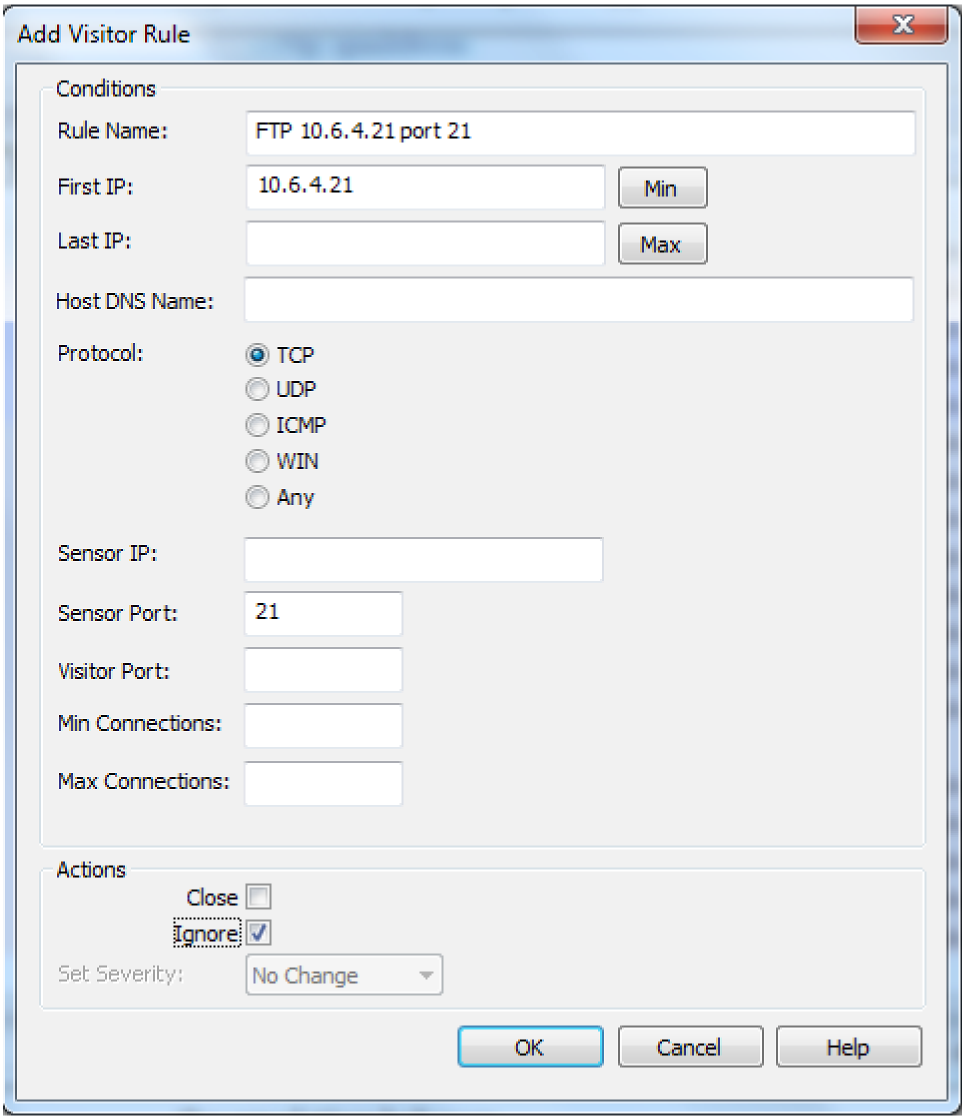


Request Data - 31 Bytes

```
USER anonymous
PASS nanditha
```

Response Data - 182 Bytes

```
>>>>220 Microsoft FTP Service
USER anonymous
>>>>331 Anonymous access allowed, send identity (e-mail name) as p
PASS nanditha
>>>>230 User logged in.
>>>>221 221-Inactivity time exceeded - Auto banned for 5 minutes
```



Conditions

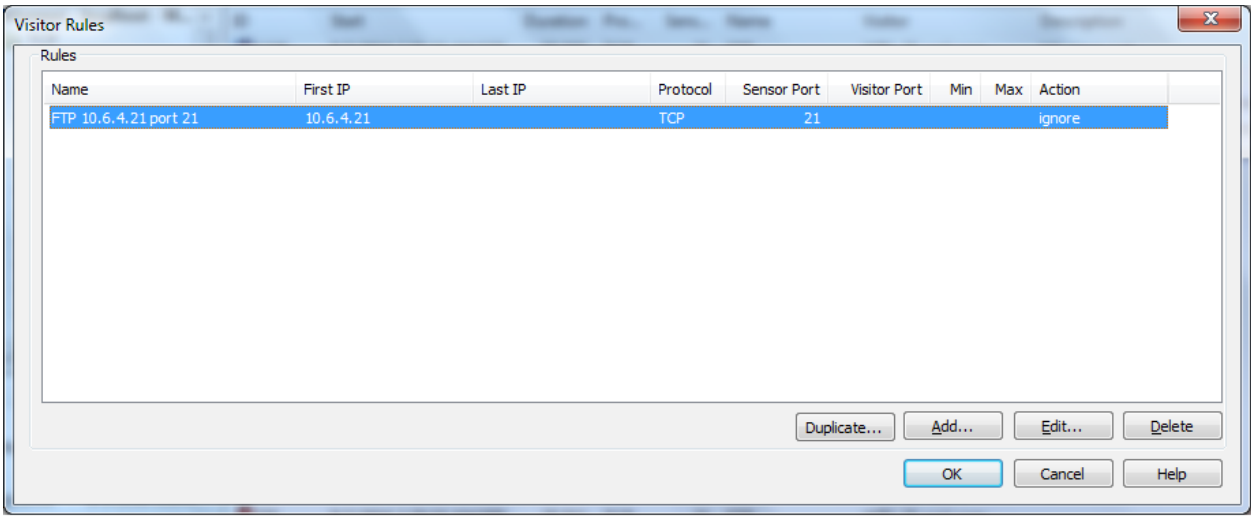
Rule Name:	FTP 10.6.4.21 port 21
First IP:	10.6.4.21
Last IP:	
Host DNS Name:	
Protocol:	● TCP ○ UDP ○ ICMP ○ WIN ○ Any
Sensor IP:	
Sensor Port:	21
Visitor Port:	
Min Connections:	
Max Connections:	

Actions

Close □

Ignore ☑

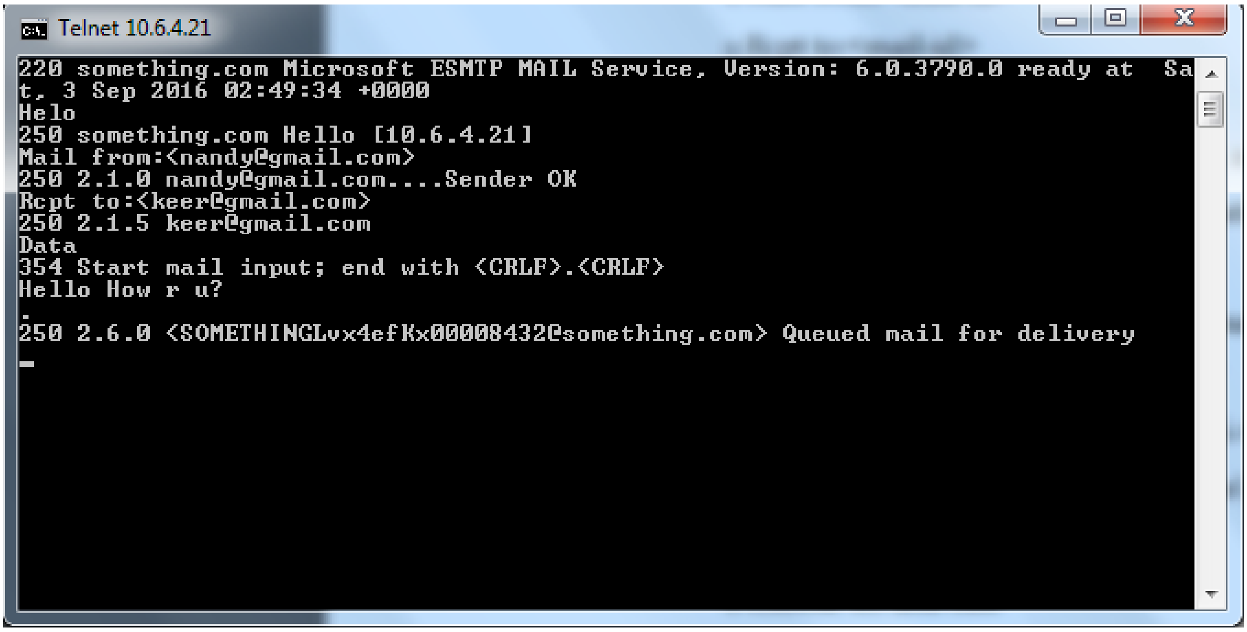
Set Severity: No Change



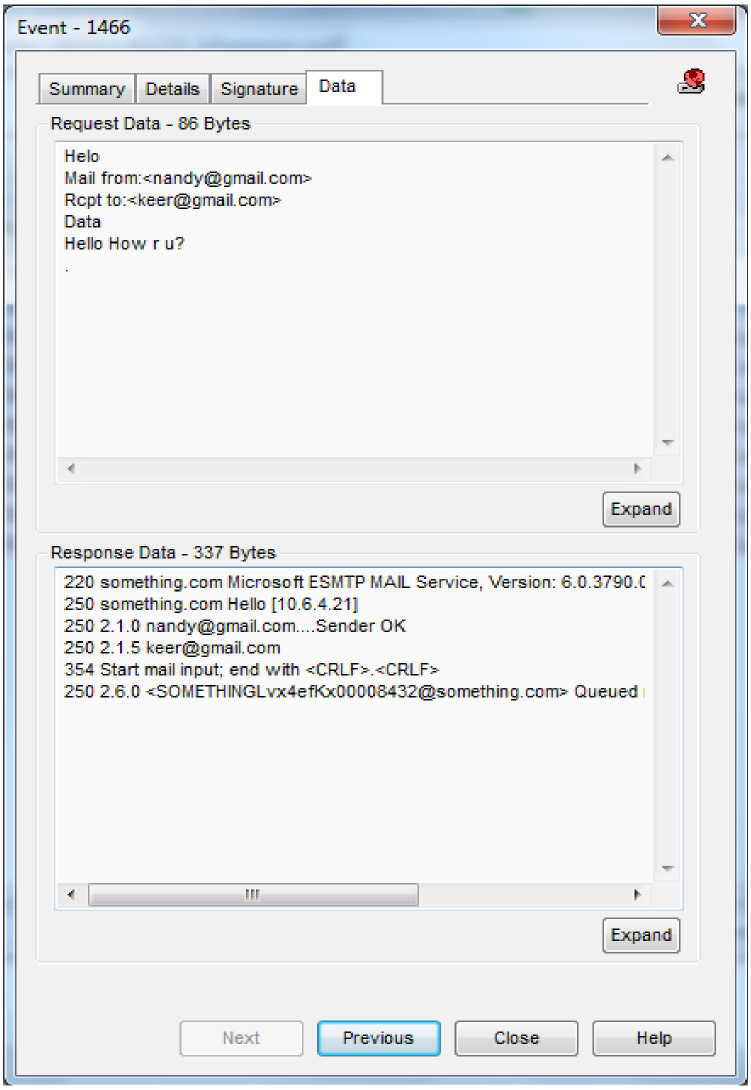
Rules

Name	First IP	Last IP	Protocol	Sensor Port	Visitor Port	Min	Max	Action
FTP 10.6.4.21 port 21	10.6.4.21		TCP	21				ignore

SMTP



```
220 something.com Microsoft ESMTP MAIL Service, Version: 6.0.3790.0 ready at  Sa
t, 3 Sep 2016 02:49:34 +0000
Helo
250 something.com Hello [10.6.4.21]
Mail from:<nandy@gmail.com>
250 2.1.0 nandy@gmail.com....Sender OK
Rcpt to:<keer@gmail.com>
250 2.1.5 keer@gmail.com
Data
354 Start mail input; end with <CRLF>.<CRLF>
Hello How r u?
.
250 2.6.0 <SOMETHINGLvx4efKx00008432@something.com> Queued mail for delivery
_
```



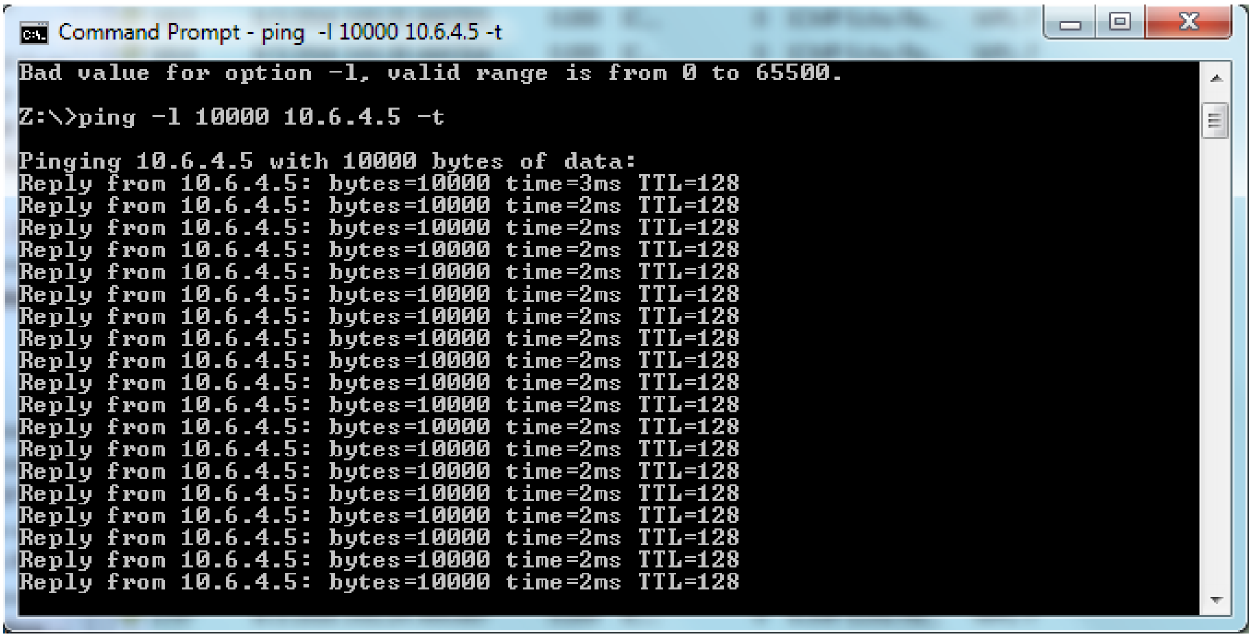
Request Data - 86 Bytes

```
Helo
Mail from:<nandy@gmail.com>
Rcpt to:<keer@gmail.com>
Data
Hello How r u?
.
```

Response Data - 337 Bytes

```
220 something.com Microsoft ESMTP MAIL Service, Version: 6.0.3790.(
250 something.com Hello [10.6.4.21]
250 2.1.0 nandy@gmail.com....Sender OK
250 2.1.5 keer@gmail.com
354 Start mail input; end with <CRLF>.<CRLF>
250 2.6.0 <SOMETHINGLvx4efKx00008432@something.com> Queued
```

<u>DOS</u>

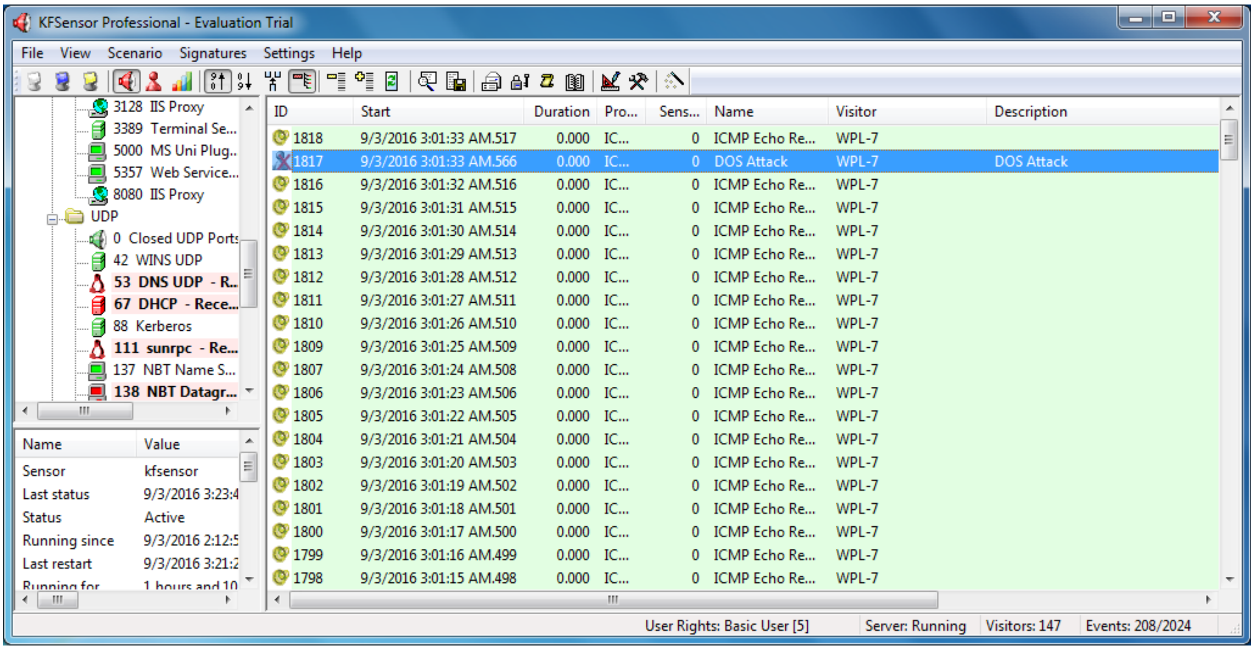


Command Prompt - ping -l 10000 10.6.4.5 -t

```
Bad value for option -l, valid range is from 0 to 65500.

Z:\>ping -l 10000 10.6.4.5 -t

Pinging 10.6.4.5 with 10000 bytes of data:
Reply from 10.6.4.5: bytes=10000 time=3ms TTL=128
Reply from 10.6.4.5: bytes=10000 time=2ms TTL=128
Reply from 10.6.4.5: bytes=10000 time=2ms TTL=128
Reply from 10.6.4.5: bytes=10000 time=2ms TTL=128
Reply from 10.6.4.5: bytes=10000 time=2ms TTL=128
Reply from 10.6.4.5: bytes=10000 time=2ms TTL=128
Reply from 10.6.4.5: bytes=10000 time=2ms TTL=128
Reply from 10.6.4.5: bytes=10000 time=2ms TTL=128
Reply from 10.6.4.5: bytes=10000 time=2ms TTL=128
Reply from 10.6.4.5: bytes=10000 time=2ms TTL=128
Reply from 10.6.4.5: bytes=10000 time=2ms TTL=128
Reply from 10.6.4.5: bytes=10000 time=2ms TTL=128
Reply from 10.6.4.5: bytes=10000 time=2ms TTL=128
Reply from 10.6.4.5: bytes=10000 time=2ms TTL=128
Reply from 10.6.4.5: bytes=10000 time=2ms TTL=128
Reply from 10.6.4.5: bytes=10000 time=2ms TTL=128
Reply from 10.6.4.5: bytes=10000 time=2ms TTL=128
Reply from 10.6.4.5: bytes=10000 time=2ms TTL=128
Reply from 10.6.4.5: bytes=10000 time=2ms TTL=128
```

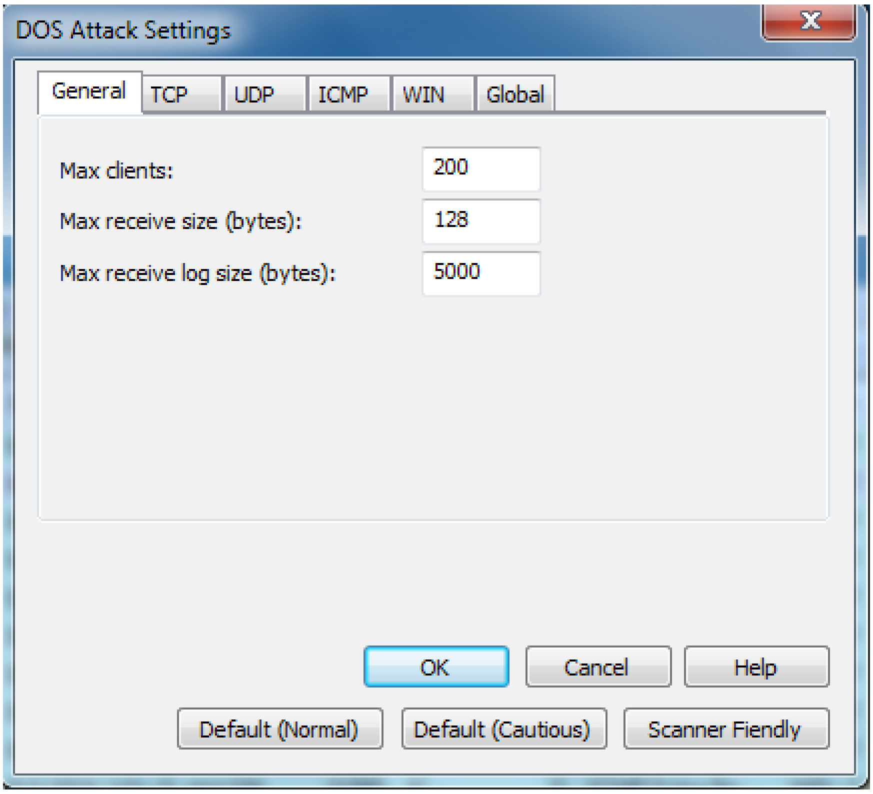


3128 IIS Proxy
3389 Terminal Se...
5000 MS Uni Plug..
5357 Web Service...
8080 IIS Proxy
UDP
0 Closed UDP Ports
42 WINS UDP
53 DNS UDP - R...
67 DHCP - Rece...
88 Kerberos
111 sunrpc - Re...
137 NBT Name S...
138 NBT Datagr...

Name	Value
Sensor	kfsensor
Last status	9/3/2016 3:23:4
Status	Active
Running since	9/3/2016 2:12:5
Last restart	9/3/2016 3:21:2
Running for	1 hours and 10

ID	Start	Duration	Pro...	Sens...	Name	Visitor	Description
1818	9/3/2016 3:01:33 AM.517	0.000	IC...	0	ICMP Echo Re...	WPL-7	
1817	9/3/2016 3:01:33 AM.566	0.000	IC...	0	DOS Attack	WPL-7	DOS Attack
1816	9/3/2016 3:01:32 AM.516	0.000	IC...	0	ICMP Echo Re...	WPL-7	
1815	9/3/2016 3:01:31 AM.515	0.000	IC...	0	ICMP Echo Re...	WPL-7	
1814	9/3/2016 3:01:30 AM.514	0.000	IC...	0	ICMP Echo Re...	WPL-7	
1813	9/3/2016 3:01:29 AM.513	0.000	IC...	0	ICMP Echo Re...	WPL-7	
1812	9/3/2016 3:01:28 AM.512	0.000	IC...	0	ICMP Echo Re...	WPL-7	
1811	9/3/2016 3:01:27 AM.511	0.000	IC...	0	ICMP Echo Re...	WPL-7	
1810	9/3/2016 3:01:26 AM.510	0.000	IC...	0	ICMP Echo Re...	WPL-7	
1809	9/3/2016 3:01:25 AM.509	0.000	IC...	0	ICMP Echo Re...	WPL-7	
1807	9/3/2016 3:01:24 AM.508	0.000	IC...	0	ICMP Echo Re...	WPL-7	
1806	9/3/2016 3:01:23 AM.506	0.000	IC...	0	ICMP Echo Re...	WPL-7	
1805	9/3/2016 3:01:22 AM.505	0.000	IC...	0	ICMP Echo Re...	WPL-7	
1804	9/3/2016 3:01:21 AM.504	0.000	IC...	0	ICMP Echo Re...	WPL-7	
1803	9/3/2016 3:01:20 AM.503	0.000	IC...	0	ICMP Echo Re...	WPL-7	
1802	9/3/2016 3:01:19 AM.502	0.000	IC...	0	ICMP Echo Re...	WPL-7	
1801	9/3/2016 3:01:18 AM.501	0.000	IC...	0	ICMP Echo Re...	WPL-7	
1800	9/3/2016 3:01:17 AM.500	0.000	IC...	0	ICMP Echo Re...	WPL-7	
1799	9/3/2016 3:01:16 AM.499	0.000	IC...	0	ICMP Echo Re...	WPL-7	
1798	9/3/2016 3:01:15 AM.498	0.000	IC...	0	ICMP Echo Re...	WPL-7	

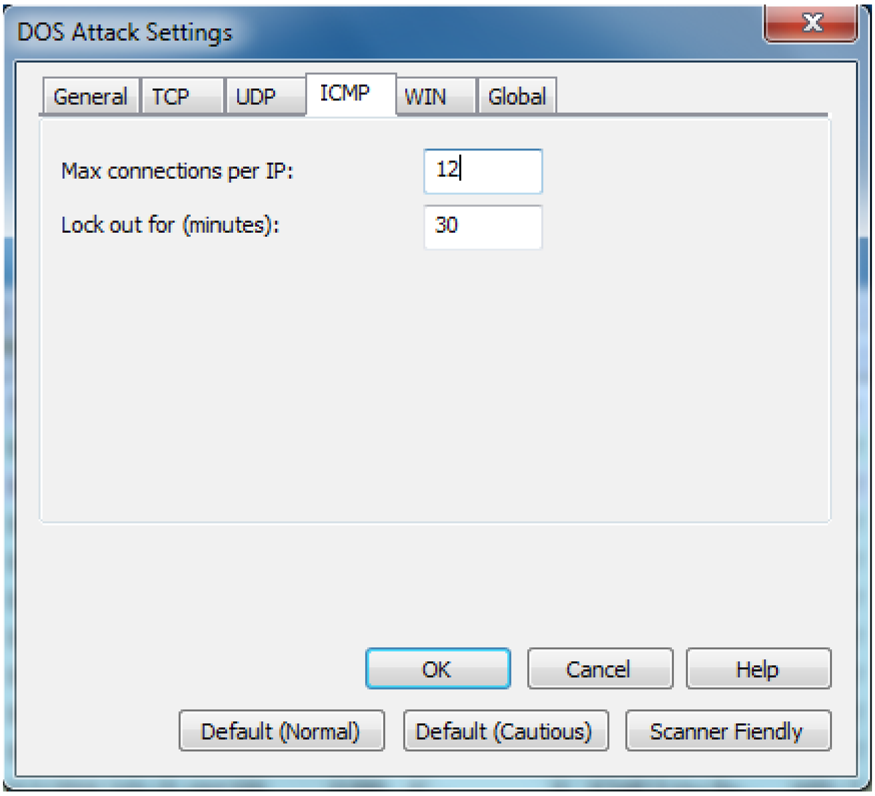
User Rights: Basic User [5]   Server: Running   Visitors: 147   Events: 208/2024



Max clients: 200

Max receive size (bytes): 128

Max receive log size (bytes): 5000



Max connections per IP: 12

Lock out for (minutes): 30