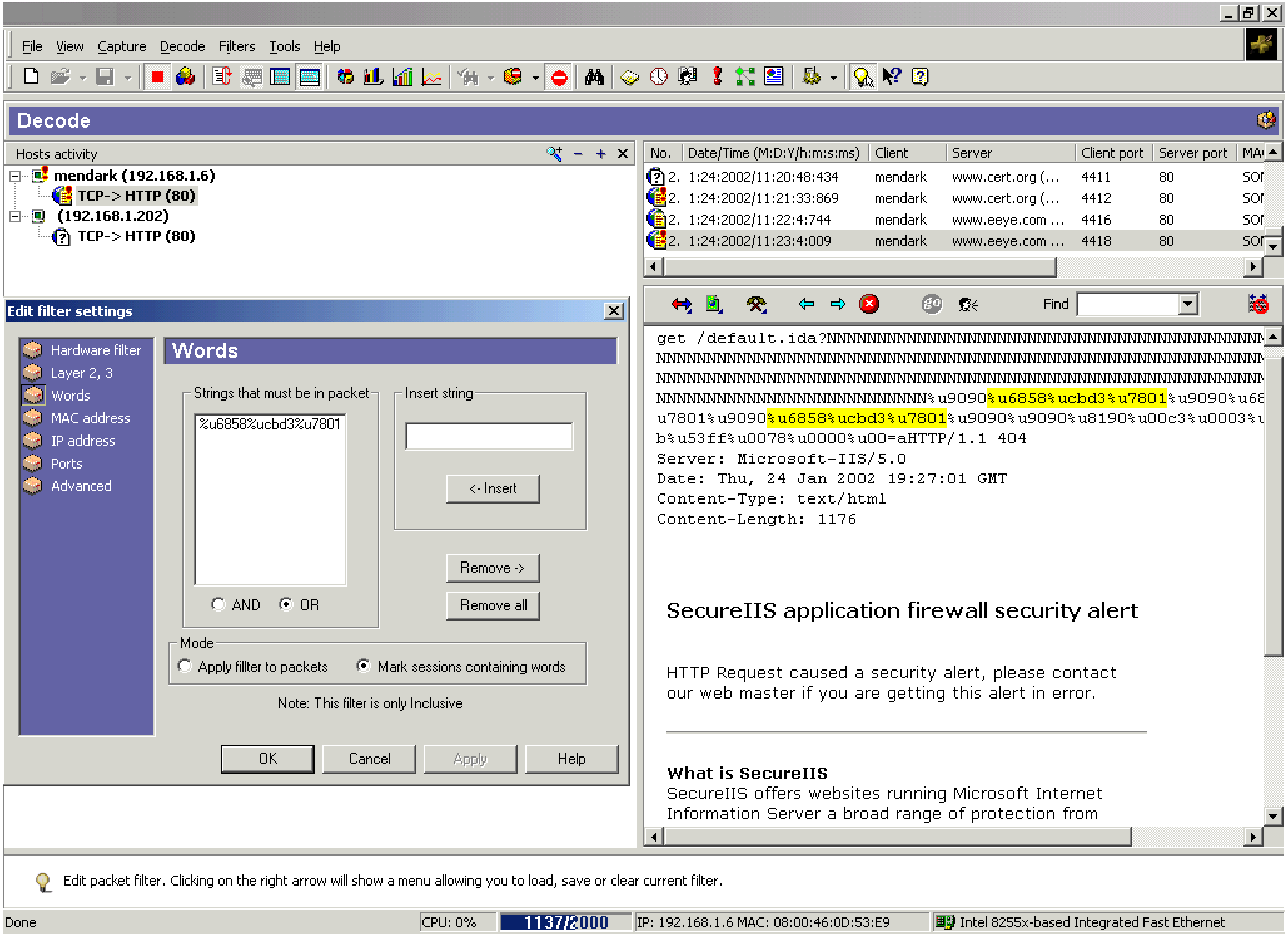
File View Capture Decode Filters Tools Help
Decode
Hosts activity
mendark (192.168.1.6)
TCP-> HTTP (80)
(192.168.1.202)
TCP-> HTTP (80)
No. Date/Time (M:D:Y/h:m:s:ms) Client Server Client port Server port
2. 1:24:2002/11:20:48:434 mendark www.cert.org (... 4411 80
2. 1:24:2002/11:21:33:869 mendark www.cert.org (... 4412 80
2. 1:24:2002/11:22:4:744 mendark www.eeye.com ... 4416 80
2. 1:24:2002/11:23:4:009 mendark www.eeye.com ... 4418 80
Find
Edit filter settings
Hardware filter
Layer 2, 3
Words
MAC address
IP address
Ports
Advanced
Words
Strings that must be in packet
%u6858%ucbd3%u7801
AND
OR
Insert string
<- Insert
Remove ->
Remove all
Mode
Apply filter to packets
Mark sessions containing words
Note: This filter is only Inclusive
OK
Cancel
Apply
Help
get /default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u6858%ucbd3%u7801%u9090%u68
u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u
b%u53ff%u0078%u0000%u00=aHTTP/1.1 404
Server: Microsoft-IIS/5.0
Date: Thu, 24 Jan 2002 19:27:01 GMT
Content-Type: text/html
Content-Length: 1176
SecureIIS application firewall security alert
HTTP Request caused a security alert, please contact our web master if you are getting this alert in error.
What is SecureIIS
SecureIIS offers websites running Microsoft Internet Information Server a broad range of protection from
Edit packet filter. Clicking on the right arrow will show a menu allowing you to load, save or clear current filter.
Done
CPU: 0%
1137/2000
IP: 192.168.1.6 MAC: 08:00:46:0D:53:E9
Intel 8255x-based Integrated Fast Ethernet