İçindekiler

[DOKÜMAN TARİHÇESİ 2](#_Toc329872435)

[RECORDER GELİŞTİRME İSTEK FORMU 3](#_Toc329872436)

[ÖRNEK PARSING 4](#_Toc329872437)

[TEMEL PARSING YAPISI 6](#_Toc329872438)

# DOKÜMAN TARİHÇESİ

|  |  |  |  |
| --- | --- | --- | --- |
| Tarih | Versiyon | Açıklama | Yazan |
| 2014-02-04 | 1.0.0 |  | Nihat Yüceyürek |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# RECORDER GELİŞTİRME İSTEK FORMU

|  |  |
| --- | --- |
| Belge numarası |  |
| Ürün Adı | FortigateSyslog Recorder |
| Versiyonu |  |
| Log Toplama Tipi |  |
| Dosya sıralama Tipi |  |
| Recorder Tipi |  |
| Tam recorder ismi |  |
| İstek yapan Adı Soyadı | Nihat Yüceyürek |
| Geliştirici Adı Soyadı |  |
| İstek tarihi | 27.01.2014 |
| İstek yapılan kurum adı | TCDD 2. BÖLGE (ANKARA) |
| Log makinesi işletim sistemi türü |  |
| Config Guide belge no |  |
| İlgili ham log yolu/dosya ismi |  |
| İlişkili form adı |  |
| Servis Yetkilisi Notları |  |
| Geliştirici Notları |  |

# ÖRNEK PARSING

|  |  |
| --- | --- |
| **date=****2014-01-27,time=14:50:19,devname=****TCDD2\_BOLGE,devid=****FGT1KC3911800232,logid=****0000000013,type=****traffic,subtype=****forward,level=****notice,vd=root,srcip=****10.6.4.23,srcport=****50810,srcintf="****port1",dstip=****50.19.234.35,dstport=****80,dstintf="wan1",sessionid=3390102,status=close,policyid=2,dstcountry="United States",srccountry="Reserved",trandisp=snat,transip=212.156.70.78,transport=50810,service=****HTTP,proto=6,appid=34038,app="HTTP.BROWSER\_IE",appcat="Web.Others",applist="B+Âlge-Genel",duration=****179,sentbyte=****869,rcvdbyte=****355,sentpkt=6,rcvdpkt=4,utmaction=passthrough,utmevent=webfilter,utmsubtype=ftgd-cat,urlcnt=1,hostname="****ping.chartbeat.net",catdesc="Information Technology"** | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | **2014-01-27 14:50:19** |
| SOURCENAME | **notice** |
| EVENTCATEGORY | **forward** |
| EVENTTYPE | **traffic** |
| USERSID |  |
| LOGNAME | **FortigateSyslog Recorder** |
| COMPUTERNAME | **TCDD2\_BOLGE** |
| CUSTOMSTR1 | **FGT1KC3911800232** |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 | **10.6.4.23** |
| CUSTOMSTR4 | **50.19.234.35** |
| CUSTOMSTR5 | **port1** |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 | **HTTP** |
| CUSTOMSTR8 | **ping.chartbeat.net** |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 | **50810** |
| CUSTOMINT2 | **80** |
| CUSTOMINT3 |  |
| CUSTOMINT4 | **179** |
| CUSTOMINT5 |  |
| CUSTOMINT6 | **355** |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 | **869** |
| CUSTOMINT10 |  |
| DESCRIPTION | **date=2014-01-27,time=14:50:19,devname=TCDD2\_BOLGE,devid=FGT1KC3911800232,logid=0000000013,type=traffic,subtype=forward,level=notice,vd=root,srcip=10.6.4.23,srcport=50810,srcintf="port1",dstip=50.19.234.35,dstport=80,dstintf="wan1",sessionid=3390102,status=close,policyid=2,dstcountry="United States",srccountry="Reserved",trandisp=snat,transip=212.156.70.78,transport=50810,service=HTTP,proto=6,appid=34038,app="HTTP.BROWSER\_IE",appcat="Web.Others",applist="B+Âlge-Genel",duration=179,sentbyte=869,rcvdbyte=355,sentpkt=6,rcvdpkt=4,utmaction=passthrough,utmevent=webfilter,utmsubtype=ftgd-cat,urlcnt=1,hostname="ping.chartbeat.net",catdesc="Information Technology"** |

# ÖRNEK PARSING

|  |  |
| --- | --- |
| **date=****2014-01-27,time=****14:50:19,devname=****TCDD2\_BOLGE,devid=****FGT1KC3911800232,logid=0954024577,type=****utm,subtype=****dlp,eventtype=dlp,level=****notice,vd="root",filteridx=1,dlpextra="1 kB",filtertype=file-size,filtercat=file,policyid=2,identidx=0,sessionid=3400502,epoch=1999404112,eventid=1,srcip=****10.6.4.242,srcport=****56598,srcintf="****port1",dstip=****195.175.69.139,dstport=****80,dstintf="wan1",service=****http,filetype="unknown",sentbyte=****549,rcvdbyte=****7143,hostname="****ts1.mm.bing.net",url****="/th?id=H.4720093001482256&w=190&h=140&c=7&rs=1&url=http%3a%2f%2fwww.haberefor.com%2fhaber%2fpolis-ve-gosterici-birbirlerini-teselli-etti-7307.html&pid=1.7",action="log-only",profile="Content\_Archive"** | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | **2014-01-27 14:50:19** |
| SOURCENAME | **notice** |
| EVENTCATEGORY | **dlp** |
| EVENTTYPE | **utm** |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME | **TCDD2\_BOLGE** |
| CUSTOMSTR1 | **FGT1KC3911800232** |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 | **10.6.4.242** |
| CUSTOMSTR4 | **195.175.69.139** |
| CUSTOMSTR5 | **port1** |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 | **http** |
| CUSTOMSTR8 | **ts1.mm.bing.net** |
| CUSTOMSTR9 | **="/th?id=H.4720093001482256&w=190&h=140&c=7&rs=1&url=http%3a%2f%2fwww.haberefor.com%2fhaber%2fpolis-ve-gosterici-birbirlerini-teselli-etti-7307.html&pid=1.7** |
| CUSTOMSTR10 |  |
| CUSTOMINT1 | **56598** |
| CUSTOMINT2 | **80** |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 | **7143** |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 | **549** |
| CUSTOMINT10 |  |
| DESCRIPTION |  |

|  |  |
| --- | --- |
| **date=****2014-01-27,time=****14:50:19,devname=****TCDD2\_BOLGE,devid=****FGT1KC3911800232,logid=0317013312,type=****utm,subtype=****webfilter,eventtype=ftgd\_allow,level=notice,vd="root",policyid=2,identidx=0,sessionid=3400534,srcip=****10.6.11.136,srcport=****55320,srcintf="****port1",dstip=****83.66.162.13,dstport=****80,dstintf="wan1",service="****http",hostname="****haberyorumlari.hurriyet.com.tr",profiletype="Webfilter\_Profile",profile="genel\_web",status="passthrough",reqtype="referral",url="/****writecomment.aspx?DocID=25666161&PageUrl=www.hurriyet.com.tr/gundem/25666161.asp",sentbyte=****863,rcvdbyte=****4039,msg="URL belongs to an allowed category in policy",method=domain,class=0,cat=36,catdesc="News and Media"** | |
| **NATEK KOLONU** | **DEĞER** |
| DATE\_TIME | **2014-01-27 14:50:19** |
| SOURCENAME |  |
| EVENTCATEGORY | **webfilter** |
| EVENTTYPE | **utm** |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME | **TCDD2\_BOLGE** |
| CUSTOMSTR1 | **FGT1KC3911800232** |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 | **10.6.11.136** |
| CUSTOMSTR4 | **83.66.162.13** |
| CUSTOMSTR5 | **port1** |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 | **http** |
| CUSTOMSTR8 | **haberyorumlari.hurriyet.com.tr** |
| CUSTOMSTR9 | **writecomment.aspx?DocID=25666161&PageUrl=www.hurriyet.com.tr/gundem/25666161.asp** |
| CUSTOMSTR10 |  |
| CUSTOMINT1 | **55320** |
| CUSTOMINT2 | **80** |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 | **4039** |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 | **863** |
| CUSTOMINT10 |  |
| DESCRIPTION |  |

# TEMEL PARSING YAPISI

|  |  |
| --- | --- |
| **NATEK COLUMNS** | **RECORDER COLUMNS** |
| DATE\_TIME |  |
| SOURCENAME |  |
| EVENTCATEGORY |  |
| EVENTTYPE |  |
| USERSID |  |
| LOGNAME |  |
| COMPUTERNAME |  |
| CUSTOMSTR1 |  |
| CUSTOMSTR2 |  |
| CUSTOMSTR3 |  |
| CUSTOMSTR4 |  |
| CUSTOMSTR5 |  |
| CUSTOMSTR6 |  |
| CUSTOMSTR7 |  |
| CUSTOMSTR8 |  |
| CUSTOMSTR9 |  |
| CUSTOMSTR10 |  |
| CUSTOMINT1 |  |
| CUSTOMINT2 |  |
| CUSTOMINT3 |  |
| CUSTOMINT4 |  |
| CUSTOMINT5 |  |
| CUSTOMINT6 |  |
| CUSTOMINT7 |  |
| CUSTOMINT8 |  |
| CUSTOMINT9 |  |
| CUSTOMINT10 |  |
| DESCRIPTION |  |