T.C
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SİSTEM GÜNLÜKLERİNİN ANALİZİ İÇİN YÜKSEK SEVİYELİ ALGORİTMA VE YAZILIM GELİŞTİRİLMESİ

YÜKSEK LİSANS TEZİ

Mohamed MOHAMUD

(122113110)

Tezin Enstitüye Verildiği Tarih : 12 Mayıs 2015

Tezin Savunulduğu Tarih : 05 Haziran 2015

Tez Danışmanı : Yrd. Doç.Dr. Ayhan AKBAL (F.Ü)

Diğer Jüri Üyeleri : Yrd. Doç.Dr. Turgay KAYA (F.Ü)

Yrd. Doç. Dr. Musa ÇIBUK (BEU)

Haziran -2015

ÖNSÖZ

Ağ üzerinde iletişim halinde bulunan cihazlar arasında farklı veri alışverişi vardır ayrıca mevcut ağ yoğunluğu ve haberleşen sistemlerin sayısı arttığında cihazlar arasındaki veri alışverişi karmaşık ve zor olmaktadır. Bu durumda sistem çalışırken ortaya çıkan sorunların ve hataların tanımlanarak analiz edilmesi oldukça zorlaşmaktadır. Bu sorunu çözmek için sistem üzerinde bulunan cihazlar kendilerine loglama (bir bilgi sistemi üzerinde gerçekleşen aktivitelere ilişkin kayıt) yapıp, Günlük dosyalarını kayıt etmektedir. Günlük dosyaları (Günlük olaylarının kaydedildiği dosya), bilgilendirme, uyarı, hata, hata ayıklama ve alarm mesajlarını verebilmektedir.

Bir uçağın kara kutusunun bütün uçak sistemini takip ettiği gibi günlük tutmak da bilişim sistemleri içerisindeki olayları kaydetmektedir. Ne kara kutusuz bir uçak kazası ne de sağlıklı loglama yapılmamış bir ortamdaki bilişim olayı istenildiği gibi aydınlatılamaz. Günlük dosyalar; web sunucuları, uygulama sunucuları, dağıtım sunucuları ve benzeri (çalışan uygulamaların) faaliyetlerin kaydını alır. Günlük dosyaları kayıt edilen uygulama hakkında; uygulamayı çalıştıran kullanıcıyı, uygulamanın hangi saatte hangi tarihte kullanıldığı vb. bilgileri kayıt eder. Kayıt edilen Günlük dosyaları sayesinde, sunucularda bulunan kötü niyetli faaliyetlerin tespiti kolaylaşmaktadır.

Bu yüksek lisans tezi, bilgi sistemi üzerinde kullanılan sunucular ve ağ cihazları trafından üretilen günlük kayıtları ve metin dosyalarında bulunan günlük iletilerini alıp veritabanına kaydedilebilen ve aynı zamanda analiz edebilen bir sistem geliştirilmeye odaklanmaktadır.

TEŞEKKÜR

Çalışmalarım boyunca değerli yardımları ve katkılarıyla beni yönlendiren danışmanım Yrd.Doç.Dr. Ayhan AKBAL'a, yine tecrübelerinden faydalandığım kıymetli hocalarım Doç.Dr.Arif GÜLTEN'e ve Yrd.Doç.Dr.Hasan GÜLER'e ayrıca Elektrik-Elektronik Mühendisliği Bölümü Başkanı Prof.Dr.Yakup DEMİR'e en kalbi teşekkürlerimi sunarım.

Çalışmam boyunca yardımcı olan ve manevi destekleriyle de beni hiçbir zaman yalnız bırakmayan arkadaşlarım Mehmet SÖNMEZ'e, Kürşat SALMAN'a, Musab COŞKUN'a ve bütün Fen Bilimleri Enstitüsü personeline teşekkür ederim.

Hayatım boyunca her anında bana koşulsuz maddi ve manevi destek olan, sevgisini, ilgisini ve her türlü yardımını esirgemeyen canım ailem; annem, babam, eşim, kardeşlerim ve bana yardımcı olan ve dua eden herkese çok teşekkür ederim.

Mohamed Mohamud MOHAMED

İÇİNDEKİLER

ÖZET

Bilgi sistem ağlarında kullanılan ağ cihazlarında olaylar hakkında günlük (log) tutulması oldukça önlemlidir. Bu günlükler sayesinde ağ üzerinde güvenlik olaylarının belirlenmesi ve saldırılara karşı önlem alınması sağlanmaktadır. Günlük analizi sayesinde sisteme girmeye çalışan kişilerin adres bilgilerine ulaşılmaktadır. Ayrıca sistem içinde bulunan kullanıcıların gerçekleştirdikleri (dosya kaydetme, yazıcıdan çıktı alama gibi) işlemlerin kontrol edilmesi mümkün olmaktadır.

Günlük dosyalarının boyutları sistem içerisinde arttığı için bu dosyalardan yararlı bilgileri elde edebilmek zorlaşmaktadır. Bu yüzden, günlük dosyalarından önemli bilgilerin kısa bir sürede analiz edilmesi oldukça önemlidir. Ayrıca, günlük dosyalarının belirli aralıklarda analiz edilmesi gerekmektedir. Bu dosyalarda bulunan veriler büyük boyutlu olduğu için manuel olarak bu dosyaları kontrol veya kategorize etmek de oldukça fazla zaman almaktadır ve neredeyse imkânsız olmaktadır. Bu amaçla hataları tespit etmek ve günlük dosya mesajlarını sınıflandırmak amacıyla otomatik analiz araçları kullanmak gerekmektedir.

SUMMARY

DEVELOPING HIGH-LEVEL ALGORITHM AND SOFTWARE FOR ANALYZING INFORMATION SYSTEMS' EVENT LOGS

The logs generated by the operating systems, and application programs, network devices, web browsers and all devices found in information systems during their normal course of operation are very important and allow system administrators to ensure that they have a reliable information system. With log events, you can track what is going on your system, such as what web sites your clients accessed, whom they are sending e-mails to and receiving e-mails from and what applications are used.

Log messages are accumulating each day in our systems. In that situation, it is very difficult to utilize the logs for checking our system health and get the meaningful information from them. Therefore, log files should been checked and analyzed frequently. However, the data in the log files is huge and typically contains billions to trillions of records. To analyze and categorize such large sets of data manually, for anomaly detection or reporting purposes, is tedious and nearly impossible. Therefore, to understand the health of our information system, automated analysis is important and practical task.

ŞEKİLLER LİSTESİ

Sayfa No

TABLOLAR LİSTESİ

Sayfa No

KISALTMALAR

KISALTMA	AÇIKLAMASI
ANSI	American National Standards Institute (*Amerikan Ulusal Standartlar Enstitüsü*)
BSD	Berkeley Software Distribution (*Berkeley Yazılım Dağıtımı*)
DNS	Domain Name System (*Alan Adı Sistemi*)
DTLS	Datagram Transport Layer Security (*Datagram Taşıma Katmanı Güvenliği*)
HTTP	Hypertext Text Transfer Protocol (*Köprü Metni Aktarım Protokolü*)
IDMEF	Intrusion Detection Message Exchange Format (*Saldırı Tespit Mesaj Değişim Formatı)*
IIS	Internet Information Service
IP	Internet Protocol
ISO	International Organization for Standardization (*Uluslararası Standartlar Organizasyonu*)
LAN	Local Area Network (*Yerel Alan Ağı*)
MAC	Media Access Control (*Medya erişim kontrolü*)
MSG	Message
OS	Operating System (*Işletim Sistemi*)
PRI	Priority
RFC	Request for Comments (*Açıklama İsteği*)
SCP	Secure Copy Protocol(*Güvenli kopya Protokolü*)
SDEE	Security Device Event Exchange (*Güvenlik Cihaz Olay Değişimi*)
SFTP	Secure File Transfer Protocol(*Güvenli Dosya Aktarım Protokolü*)
SNMP	Simple Network Management Protocol(*Basit Ağ Yönetimi Protokolü*)
SOAP	Simple Object Access Protocol (*Basit Nesne Erişim Protokolü*)
SQL	Structured Query Language (*Yapılandırılmış Sorgu Dili*)
TCP	Transmission Control Protocol(*İletim Kontrol Protokolü*)
UDP	User Datagram Protocol (*Kullanıcı Datagram Protokolü*)
VPN	Virtual Private Network (*Sanal Özel Ağ*)
W3C	World Wide Web Consortium
WAN	Wide Area Network (*Geniş Alan Ağı*)
XML	Extensible Markup Language (*Genişletilebilir İşaretleme Dili*)

1. GİRİŞ

1.1. Çalışma Alanı

Ağ cihazları ve yazılım uygulamaları genellikle log (günlük) dosyaları olarak bilinen bazı metin dosyaları ürettirmektedir. Bu tür dosyalar, yazılım geliştirme zamanı sorunlarını gidermek, sistem arızalarının hatalarını ayıklamak, ağ trafiğini izlemek ve sistemde oluşabilecek tehditleri algılamak için kullanılır. Log dosyaları kalıcı sistem izlemek için yaygın olarak kullanılmakta ve işletim sistemleri, bilgisayar ağları ve dağıtık sistemler için de oldukça önemlidir. Ayrıca log dosyaları; web sunucuları, uygulama sunucuları, dağıtım sunucuları ve benzeri (çalışan uygulamaların) faaliyetlerin kaydını alır.

Bir uçağın kara kutusunun bütün uçak sistemini takip ettiği gibi log dosyaları da bilişim sistemleri içerisindeki olayları kaydetmektedir. Ne kara kutusuz bir uçak kazası ne de sağlıklı loglama yapılmamış bir ortamdaki bilişim olayı istenildiği gibi aydınlatılamaz. Günlük dosyaları kayıt edilen uygulama hakkında uygulamayı çalıştıran kullanıcıyı, uygulamanın hangi saatte hangi tarihte kullanıldığı vb. bilgileri kayıt eder. Kayıt edilen günlük dosyalar sayesinde, sunucularda bulunan kötü niyetli faaliyetlerin tespiti kolaylaşmaktadır.

Günlük yönetimi ve analizi, yazılım ile donanım arızası ve güvenlik saldırılarına karşı önemli bir savunmadır. Daha önceleri bir hatayla karşılaşıldığında veya bir sistemin sorununu çözmek için günlük kayıtları incelenirken günümüzde sadece hata ya da sorunla karşılaşıldığında değil güvenlik ve standartların sağlanması için aşağıda sıralanan nedenlerden dolayı da günlük kayıtlarını takip etmek gerekmektedir [1, 2, 3].

- Hangi zaman aralıklarında kimler oturum açtı?
- USB bellek kullanımı oldu mu?
- Sistem yöneticileri takip ediliyor mu?
- Bilgisayar adı (hostname), IP adresi, MAC adresi değişikliği oldu mu?
- Kimler hangi IP adresi aldı?
- Bu IP adresleri ile nerelere erişildi?
- Sisteme uzaktan bağlantı gerçekleşti mi?
- Kimler hangi saatte VPN (Virtual Private Network?) bağlantısı kurdu?

- Donanım değişikliği yapıldı mı?
- Kim hangi dosyaya erişti?
- Erişilen dosyalardan silinen var mı?
- Başarılı parola (password) değişiklikleri?
- Bilgisayar hesabı ya da kullanıcı hesabı oluşturuldu mu?
- Kimler hangi dokümanların çıktısını (print) aldı?
- Domain admin hesabına kullanıcı eklendi mi?
- MSN ‘den dosya transferi yapıldı mı?

Yukarıda verilen nedenlerde dolayı günlük dosyası izleme, bir sistemin sağlığını anlamak ve aynı zamanda ağiçi ve ağlar arası müdahaleleri takip etmek için bize yardımcı olmaktadır.

1.2. Motivasyon

Log dosyaları bize güvenlikle ilgili olayların tespitinde kolaylık sağlar. Mesela başarılı ya da başarısız olan girişleri, tespit etmek için log dosyaları kullanılabilir ve sonuca göre başarılı ve başarısız olayların toplam sayısı kullanılarak karşılaştırma yapılabilir. Log dosyaları sayesinde oluşturulan dosya veya klasörler, erişilmiş, incelemiş, silinmiş, değiştirilmiş, yeniden adlandırılmış dosyalar ve tüm değişiklikler incelenebilir. Log dosyaları, girişimleri azaltmak, dosya sağlamlığını izlemek, günlük adli analizi yapmak, kullanıcıların imtiyazlı olarak izlemek, vb. için yardımcı olur.

Günlük dosyalar, genellikle çok büyük ve karmaşık bir yapıda olabilir. İşlem günlüğü dosyalarını oluşturmak oldukça basit ve anlaşılır olsa da, günlük dosya analizi yüksek donanımlı bilgisayarlar kullanmayı gerektirebilir ve oldukça uzun ve karmaşık işlem sürecini gerektiren özel fonksiyonlu bir yapı olabilir. Günlük dosyaları, sistem içerisinde gün geçtikçe biriktiği için bu dosyalardan yararlı bilgileri elde edebilmek zorlaşmaktadır. Bu yüzden, günlük dosyalarından önemli bilgilerin kısa bir sürede analiz edilmesi oldukça önemlidir. Ayrıca, günlük dosyalarının sürekli olarak belirli aralıklarda analiz edilmesi gerekmektedir. Bu dosyalarda bulunan veriler büyük boyutlu olduğu için manuel olarak bu dosyaları kontrol veya kategorize etmek de oldukça fazla zaman almaktadır ve neredeyse imkânsız olmaktadır. Bu amaçla hataları tespit etmek ve günlük dosya mesajlarını sınıflandırmak amacıyla otomatik analiz araçları kullanmak daha pratiktir.

Özet olarak, günlük dosya verilerinin analizini gerçekleştirmek ve ayrıca olağanüstü durumlarda uyarı yapmak ve rapor etmek için otomasyon sistemi gereklidir. Bununla birlikte, olay korelasyon programı ve merkezi bir loglama, analiz sürecini otomatikleştirmek için büyük bir katkı sağlamaktadır. Ancak işlemin etkinliği, verilerin kalitesine ve veri üzerinde kullanılan algoritmalara bağlıdır.

1.2.1. Katkı

Log Yönetimi ve analizi farklı aşamalardan ve süreçlerden geçer. İlk olarak, ağ cihazları, sistem donanım veya günlükleri üretebilen programlar günlükleri üretmek ve oluşturmak amacıyla özel bir mimaride yapılandırılır ve daha sonra yerel veya uzak depoya günlük iletileri kaydedilir. İkincisi, log kolektör programı önceden oluşturulan günlük iletilerini toplar ve normalleştirir. Son olarak da analiz, günlük iletileri üzerinde gerçekleştirilir ve daha sonra analizden yürütülen raporlara göre gerekli olan önlemler alınmaktadır.

Günlükler gerçek zamanlı olarak toplamak ve merkezi bir veritabanında depolamak için sunucuya günlükler doğrudan gönderilebilir ancak çoğu durumda log mesajlar oldukça büyük ağ trafiğine neden olduğu için çoğu kurumlar bu yöntemi kullanmamaktadır ve aynı zamanda, çok maliyetli ve çok özel bir sistem kullanımı gerektiği için de yaygın olarak kullanılan bir yöntem değildir. Dolayısıyla doğrudan veritabanına günlük iletilerini yazmak sadece günlük mesajının boyutunun yeterince düşük olması durumunda mantıklıdır, aksi takdirde günlük mesajları yalnızca metin dosyalarına yazılır. Metin dosyalarının içine günlük iletilerinin yazılmasının bazı avantajları vardır; en önemlisi de çok hızlı ve verimli olmasıdır. Ancak metin dosyalarında depolanan verilerin doğru yönetimi, analizi ve raporlanması için metin dosyalarına erişim kolay değildir. Bunu yapmak için, günlük mesajlarının bir veri tabanında olması gerekmektedir.

Bu yüksek lisans tezi, bilgi sistemi üzerinde kullanılan sunucular ve ağ cihazları tarafından üretilen günlük kayıtlarını ve metin dosyalarında bulunan günlük iletilerini alıp veritabanına kaydedilebilen ve aynı zamanda analiz edebilen bir sistem geliştirmeye odaklanmaktadır. Bu program, bilgi sisteminde şebeke trafiği tarafından üretilen logları analiz ederek bilgi sistemlerinin problemlerini azaltmakta olup aynı zamanda sistemi daha verimli hale getirmektedir.

2. İLGİLİ ve ÖNCEKI ÇALIŞMALAR

2.1. Giriş

Bu bölümde günlük iletilerin analizini yapmış önceki çalışmalara yer verilmiştir. Log mesajları, sistem bakımı, yazılım testi, doğrulama ve aykırılık durumları tespiti için çeşitli amaçlarla geçmişte analiz edilmiş birçok çalışma vardır. Sağlam ve güvenli günlük mesajlarının analizini yapabilen ve tutabilen birçok ticari uygulama bulunmaktadır. Bu çözümlerden bazılarını satın aldıktan sonra, bir şirkete ait olan gerekli değişiklikleri uygulayarak log yönetimi sorunları çözülebilmektedir. Mevcut olan çözümler iki kategoride incelenmektedir [4]:

a) *Gerçek zamanlı olay izleme çözümleri*: bu tür çözümler gerçek zamanlı olaylar üzerine uyarılar ve özet raporlar oluşturur ve genellikle günlük log değerlendirmeleri yapmak için gereken süreyi ve zamanı azaltma özelliğine sahiptir. Ama önceki bölümde değinildiği gibi, çoğu durumlarda log olayları oldukça fazladır ve yüksek bir ağ trafiği oluşturur. Yani, çok maliyetli ve oldukça özel bir sistem gerektirmektedir. Aynı zamanda günlük olaylarının her an izlenmesi zordur. Bu yüzden, kurumların çoğu bu tür çözümleri kullanmayı tercih etmemektedir.
b) *Günlük dosyası analizör çözümleri*: Bu çözümler, bir düz metin dosyasını doğrudan kaydeden günlük olaylarını analiz etmektedir. Bu çözümler sayesinde log olaylarını değerlendirmek ve yararlı bilgileri bulmak için metin log dosyalarında kolaylıkla arama yapılabilir. Fakat dosyadalardaki veriler metin olarak kaydedildiği için verileri sınıflandırmak ve ayıklamak çok zordur ve dolayısıyla kısa bir zamanda faydalı bilgiler bulmak kolay değildir.

Diğer bölümde bu iki tip çözüm gözden geçirilmiştir ama bu analizler mevcut olan çözüm kümesinin tamamını kapsamamaktadır.

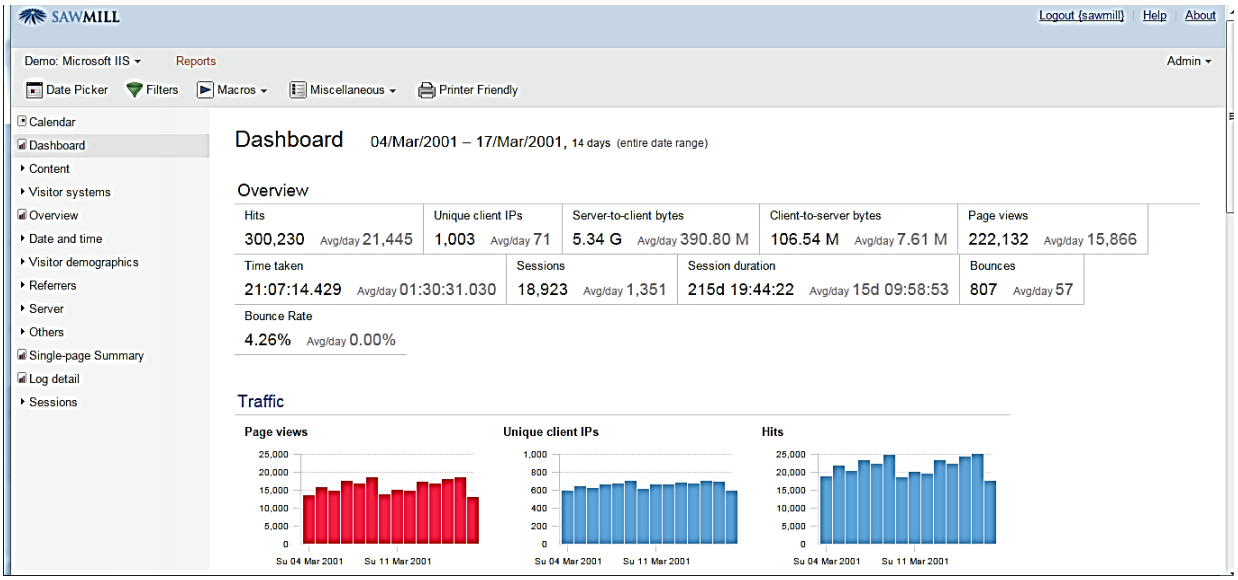
2.2. Gerçek zamanlı olay izleme çözümleri

2.2.1 Sawmill

Sawmill Log Analytics, Flowerfire Inc. tarafından geliştirilen bir kurumsal ve ticaret yazılım paketidir. İlk sürümü 1998 yılında kullanılmaya başlanmış ama ilk istikrarlı sürümü

(8.6.3) 9 Temmuz 2013 tarihinde üretilmiştir. Windows, UNIX ve UNIX gibi platformlar, değişik platformlarda çalışabilen bir yazılımdır. Sawmill, günlük dosyaları istatistiksel analiz ve gerçek zamanlı raporlama ve gerçek zamanlı uyarılar için tasarlanmış bir yazılım paketidir [5].

Sawmill Log Analytics, log olayları üreten herhangi bir aygıt veya yazılım (Proxy sunucuları, Web Sunucusu, Apache Sunucuları, Güvenlik duvarları, FTP sunucuları, posta sunucuları, ağ cihazları (anahtarlar ve yönlendiriciler vb), syslog sunucuları, veritabanları) gibi birçok cihazı analiz etmektedir. Sawmill, arka aşamada veritabanı olarak (MySQL, MSSQL, Oracle) gibi ilişkisel veritabanını kullanır. Bu veritabanında günlük mesajları depolanarak ve veritabanını sorgulayarak raporlar oluşturulmaktadır. Yalnız, veritabanı güncelleştirilirken Sawmill yavaş çalışmaktadır. Ayrıca veritabanı aynı anda birden fazla cihazı ve yazılımı güncellediği için ağ trafik sorunları meydana gelmektedir ve uzun süren süreçler ile karşı karşıya gelinmektedir [5]. Aşağıdaki şekil Sawmill ekranını gösterir



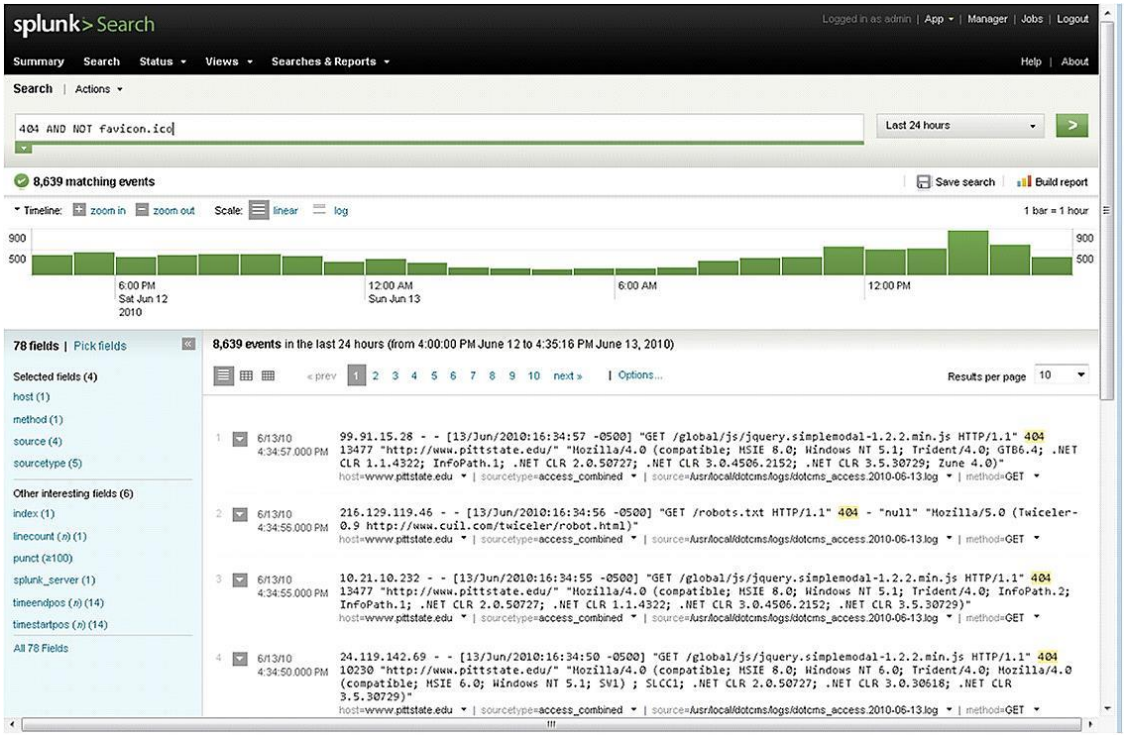
Şekil 2:1 Sawmill Log Analytics ekranını

2.2.2 Splunk

Splunk, Amerikan çok uluslu Splunk denilen bir şirket tarafından geliştirilen kurumsal ve ticari yazılımdır ve 2011 yılında uygulanmaya başlamıştır. Splunk, log olayları ve diğer makine verilerini toplamak ve analiz etmek için kullanılan bir araçtır. Makine verileri;

uygulamalar, sunucular, ağ cihazları, güvenlik cihazları ve işletmeyi diğer sistemler tarafından oluşturan tüm veriler demektir [6].

Üretici firma, ücretli lisansı ile karşılaştırıldığında bazı sınırlamaları (endeksli verilerin günde maksimum 500 MB gibi) olan ücretsiz lisans sunmaktadır. Halbuki, gerçek zamanlı izleme ve uyarı verme özellikleri sadece ücretli sürümünde bulunmaktadır. Ancak üretici firma, yazılımı değerlendirmek ve denemek için 60 gün boyunca ücretli sürümü kullanmaya izin verir.



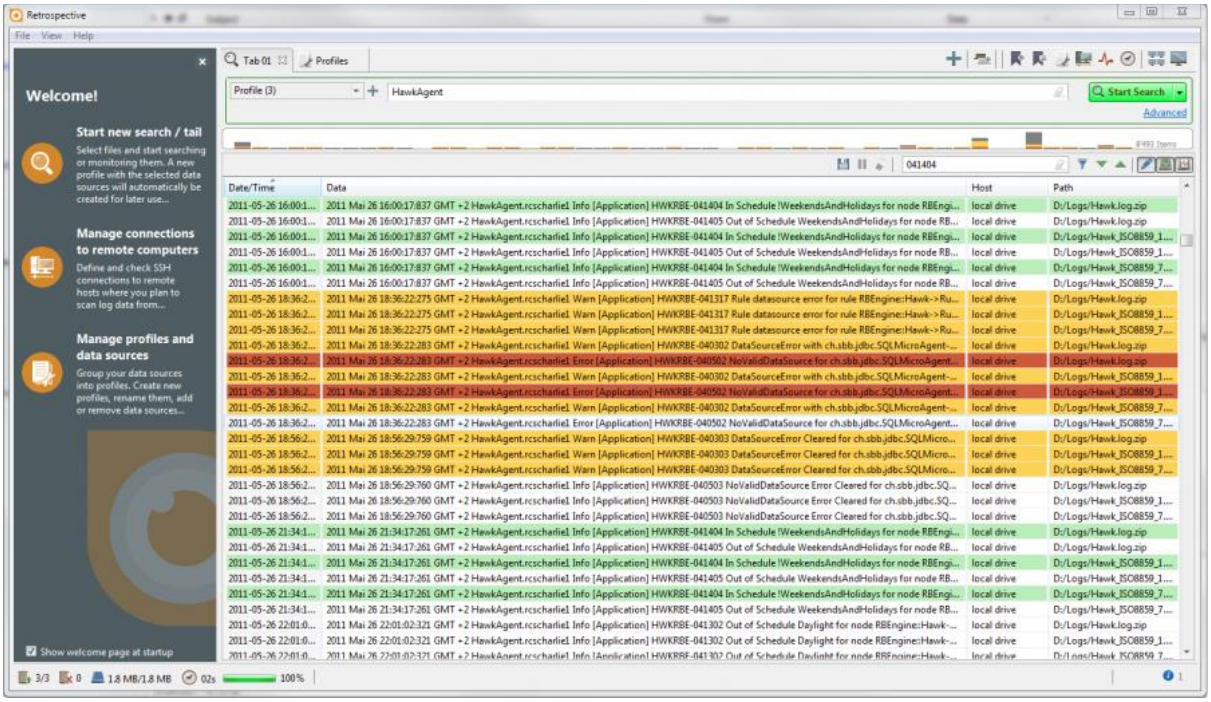
Şekil 2:2 Splunk ekranı

2.2.1. Retrospective Log Analizör

Retrospective Log Analyzer Centeractive şirketi tarafından geliştirilen bir yazılımdır. Retrospective, günlük mesajları analiz etmek ve sunucu izlemek amacıyla tasarlanmış ve geliştirilmiş bir olay günlüğü yönetimi programıdır. Retrospective, bilgi sistemleri uzmanlarına Microsoft Windows, Mac veya Linux üzerinde kendi kurumsal günlük verilerini yönetmenizi sağlar ve aşağıdaki özelliklere sahiptir [7].

- Yeni gelen günlük girişlerini analiz ederek günlük olayları gerçek zamanlı izleme.

- Bir filtre oluşturarak kritik, başarısızlık, hata gibi belirli ifadeler içeren günlük mesajlarını görüntüleme.
- Uygun bir kullanıcı arayüzü.



Şekil 2:3 Retrospective ekranı

2.3. Günlük dosyası analizör çözümleri

2.3.1. LogExpert

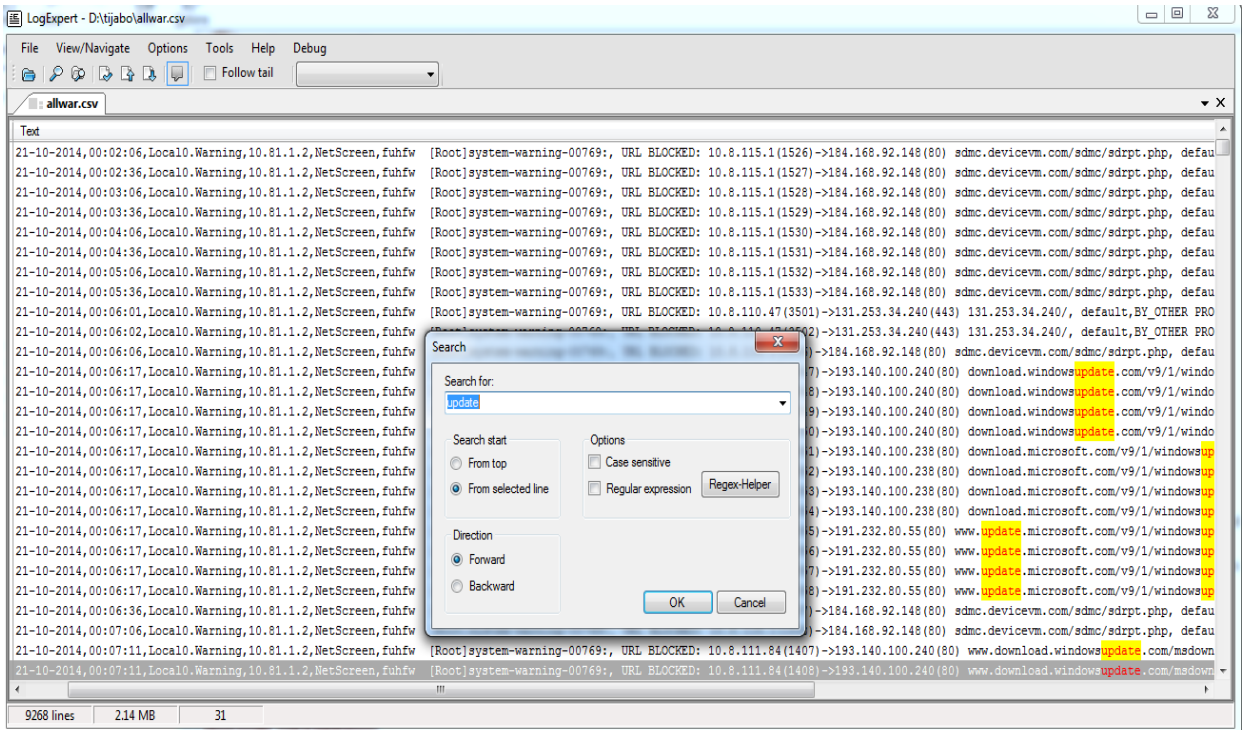
LogExpert, *Hagen Raab* tarafından geliştirilen bir Windows programdır. İlk sürümü 2011 yılında yayımlanmıştır ama şu andaki sürüm (V1.5) 4 Mart 2012 yılında kullanılmaya başlanmıştır. LogExpert özelliklerinin özeti aşağıda sıralandığı gibidir [8]:

- Birden fazla belge için arayüz,
- Arama fonksiyonu,
- İyi bir filtre fonksiyonu,
- Arama kriterleri aracılığıyla hataları vurgulama

LogExpert aracılığıyla bazı analizleri yapmak için ya da belirli bir öğeyi bulmak için arama fonksiyonu çalıştırılabilir ya da filtre kriterleri ile benzer olan tüm satırları

görüntülemek için programın filtre fonksiyonu kullanılabilir. LogExpert bazı dezavantajlara da sahiptir [8].

- **Dosya Boyutu**: Çok büyük dosyaları analiz edemez ve bazı satırları ortadan kaldırabilir.
- **Çizgi Genişliği**: Ayrıca 20.000'den fazla karakter olan çizgileri kısaltır.
- **Hesaplama**: Sayı içeren sütunları hesaplamak veya filtrelemek için matematiksel ifadeleri desteklemez.
- **Sütun başlığı**: Sütun başlıkları metin satırı içinde ise metin satırından sütunların başlıklarını ayırmaz.
- **Grafik görüntüleme**: Günlük mesajlarının grafiğini görüntülemek için bir özelliği yoktur.



Şekil 2:4 LogExpert ekranı

2.3.2. Microsoft Log Ayrıştırıcı

Pek çok kuruluş günlük olarak Windows'u kullanmak için ve Windowsun kendisine özel günlüklere ve gereksinimlere sahip olduğu için Microsoft kendine ait bir log analiz programı üretmiştir. Microsoft tarafından belirtildiği gibi Log Parser; günlük dosyaları, XML dosyaları ve CSV formatı dosyaları gibi bütün metin tabanlı verilerin yanı sıra Windows Olay Günlüğü, dosya sistemi ve Active Directory gibi Windows işletim sistemi üzerinde anahtar veri kaynaklarına evrensel sorgu erişim sağlayan güçlü ve çok yönlü bir araçtır [9,4].

Log Parser, veri kaynaklarından bilgileri ayıklamak için bir SQL kullanan komut satırı arayüzü aracıdır ve bu özelliği onun kullanımını zorlaştırmaktadır. Log Parser'in daha çok kullanışlı özelliklerinden biri, SQL benzeri komutları kullanarak Windows Olay günlüğü sorgulama kabiliyetidir [9,4].

Şekil 2:5 Log Parser

3. GÜNLÜK TANIMI ve GENEL KAVRAMLAR

3.1. Tanımlar

Loglama, log yönetimi ve analizi için kullanılan terimler anlaşılmaz, yanıltıcı veya birden fazla anlama sahip olabilirler. Bazı durumlarda, özel durumlar için kullanılırken bazı durumlarda da bu terimler birbirlerinin yerine kullanılabilirler. Bu terimlerin bazıları aşağıdaki gibi tanımlanabilir.

- **Olay** (event): Bir ortam içerisinde dikkat çekici bir durum değişimini içeren bir ortamdaki oluşumdur. Bir olay genellikle, olayın etkilerini ve nedenlerini anlamaya ve açıklamaya yardım edebilen bir ortamı açıklamaya çalışan detay konularını, oluşumu ve zamanı içermektedir [10].
- **Olay alanı** (event field): Olay alanı, bir olayın herhangi bir özelliğini tarif etmektedir. Herhangi bir olay alanın örnekleri; tarih, zaman, kaynak IP, kullanıcı ve ana bilgisayar kimliği belirlenmesini içermektedir [10].
- **Olay kaydı** (event record):Olayların bütününün toplanmasıdır. "Veri günlüğü", "etkinlik günlüğü", "denetim günlüğü", "denetim izi", "günlük dosyası", ve "olay günlüğü" gibi terimler genellikle günlük olarak aynı anlama gelmektedir [10].
- **Uyarı veya Alarm** (Alert or Alarm): Birilerinin veya herhangi bir şeyin dikkatini çekme işlemi olup bir olaya yanıt verme işlemidir. Bir olaya göre yanıt vermek amacıyla gerçekleştirilen bir işlemdirve genellikle birisinin dikkatini çekmek amaçlanmıştır [10].
- **Günlük** (log): Bir bilgi sistemi üzerinde gerçekleşen aktivitelere ilişkin kayıttır [11].
- **Loglama** (Logging): Log dosyası içerisine olay kayıtlarını gelecekte inceleyebilmek amacıyla toplama ve kaydetme işlemine loglama yada günlük tutma denir [10]. Bir günlük dosyası içine günlük girdilerini depolamak ve veri tabanlarında denetim kayıt verilerini kaydetmek günlük tutma örnekleri arasında gösterilebilir.
- **Günlük Dosyası** (log file): Bir iletişim sistemi, bir uygulama programı ya da bir işletme servisi tarafından gönderilen uyarıların kaydedildiği dizi dosyadır [10].

- **Günlük mesajı** (log message): Bir bilgisayar sistemi, donanım veya yazılım birimi gibi ünitelerden gelen uyarılara yanıt olarak oluşturulan iletiye günlük mesajı denir [10].
- **Günlük Veri** (log data) : Günlük verisinin asıl anlamı log mesajdır [10]. Başka bir ifadeyle, log mesajın neden üretildiğini bize aktaran günlük iletilerin toplamıdır.

3.2. Günlük Nasıl Toplanır ve İletilir?

Günlük veri iletimi ve alınması kavramsal olarak basittir. Günlük tutma sistemi uygulayan bilgisayar ya da cihaz, ihtiyaç duyduğu herhangi bir zamanda ileti üretebilir. Belirleme işlemi tamamen cihazın kendisi tarafından gerçekleştirilir. Örneğin, kullanıcı cihazın yapılandırma seçeneğini seçebilir veya cihaz önceden belirlenmiş mesaj listesini üretmek için sabit olarak kodlanabilir. Diğer yandan günlük mesajların gönderilmesi ve alınması için bir yerin bulunması gerekir. Bu yer genellikle loghost olarak ifade edilir. Bir loghost, günlük iletilerin toplandığı merkezi bir birim olan genellikle Windows sunucusu veya UNIX sistemi olabilen bir bilgisayar sistemidir. Merkezi bir günlük toplayıcı kullanmanın avantajları aşağıda görüldüğü gibi sıralanabilir [12, 13]:

- Birden fazla yerden gelen günlük iletileri kaydetmek için merkezi bir yerdir.
- Günlüklerin yedeklemesini gerçekleştirir.
- Günlük verilerin analizi gerçekleştirilen bir yerdir.

Ayrıca, merkezileştirilmiş bir günlük toplayıcı olmaksızın olan ortamında, çok farklı uygulama sunucularının tarafından oluşturan ve herhangi birinde işlenmiş olabilir tek bir işlem arama bir lojistik kâbusu olmaktadır. Basit bir durum olarak, günlük mesajları, bir tek günlük dosyasında kaydedilmektedir. En yaygın şekilde günlük iletileri Syslog protokolü üzerinden iletilir. Syslog, günlük ileti değişimi için standart bir protokoldür. Genellikle Unix sistemlere kurulur, ancak Windows ve diğer non-Unix tabanlı platformlarda da bulunmaktadır.

3.3. Günlük Mesajı

Daha önce anlatıldığı gibi, bir günlük iletisi sistemde oluşan herhangi bir olayı göstermek için bazı cihazlar veya sistemleri tarafından üretilen bir mesajdır. Ancak günlük iletisinin nasıl görüldüğü daha önceden açıklanmamıştır. Bir günlük iletisi için temel içerikler aşağıda sıralandığı gibidir [10, 14]:

- Zaman
- Kaynak
- Veri

Eğer mesaj Syslog'a yoluyla gönderiliyorsa, Microsoft Olay Günlüğü'ne yazılıyorsa veya bir veritabanında depolanıyorsa bu işlemler önemli değildir. Bu temel öğeler her zaman mesajın bir parçasıdır. Zaman damgası günlük mesajın oluşturulduğu zamanı göstermektedir. Kaynak, günlük iletisinin oluşturulduğu sistemdir ve bu genellikle bir IP adres veya bilgisayar adı biçiminde ifade edilir. Son olarak veri, herhangi bir günlük iletisini göstermektedir. Yalnız, bir günlük iletisinde verinin nasıl gösterildiğinin herhangi bir standardı maalesef yoktur. Bir günlük mesajında bulunabilecek en yaygın veri elemanlarından bazıları; kaynak ve hedef IP adresleri, kaynak ve hedef pörtleri, kullanıcı adları, program adları, kaynak nesne (dosya, dizin, vb.), olarak ifade edilebilir.

Günlük iletiler aşağıdaki gibi genel bir kategoride sınıflandırılabilirler [16, 13, 15]:

- ***Bilgilendirici***: Bu tür iletiler, iyi bir şey meydana geldiğinde kullanıcılara ve yöneticilere bildirmek için tasarlanmıştır.
- ***Hata Ayıklama***: Çalışan uygulama kodlu problemleri tanımlamak ve gidermek için yazılım geliştiricilere yardım eden yazılım sistemlerinden üretilen iletilerdir.
- ***Uyarı***: Uyarı mesajları, bir sistem için gerekli olan prosedürlerin eksik olduğu durumlar ile ilgilidir. Ancak bu prosedürlerin sağlanmaması sistemin çalışmasını etkilememektedir.
- ***Hata***: Bilgisayar sisteminde çeşitli seviyelerde oluşan hataları düzeltmek için kullanılır.
- ***Alarm***: Dikkat çekici herhangi bir olay olduğunun habercisidir. Uyarılar, genel olarak, etki alanı güvenlik cihazları ve sistemleri ile ilgili olmaktadır.

3.3.1. Günlük Mesajı Transferi

Kendi taşıma yöntemleri haricinde logging mekanizmaları (örneğin, yerel günlük dosyası) gibi mevcut Syslog'da, WS(Web Servisleri) yönetiminde ve çeşitli özellikli ürüne özel log iletim sistemlerinde birçok olay taşıma protokolü vardır.

Bazı iyi bilinen günlük taşıma mekanizmaları aşağıda verilmiştir [17,10].

- syslog UDP.
- syslog TCP.
- Şifreli syslog.
- HTTP üzerinden SOAP.
- SNMP.
- FTPS veya SCP gibi normal dosya aktarımı.

Örneğin, syslog UDP günümüzde milyonlarca Unix sistemi ve ağ aygıtları tarafından kullanılan en popüler günlük taşıma mekanizmasıdır.

3.3.2. Günlük Mesaj Biçimi

Günlük sözdizimi ve formatı, günlük bilgilerinin nasıl iletildiklerini, biçimlendirildiklerini, analiz edildiklerini ve kaydedildiklerini tanımlar. En önemsiz durumda her olay kaydı bir tekst dizisi gibi davranabilir ve günlük kullanıcısı tutarlılık için günlük üzerinde tam tekst araştırması yapabilir. Ama güvenilir otomatik olay analizi için, olay tüketicisinin ve üreticisinin olay kaydının sözdizimin anlaması gerekmektedir [18, 11, 14].

Bazı bilinen günlük biçimleri aşağıda verilmiştir:

- W3C genişletilmiş günlük dosya biçimi (ELF) [19].
- Apache erişim günlüğü [20].
- Cisco SDEE/CIDEE [21].
- Syslog (RFC3195 ve yeni RFC5424). [15,16].

Burada günlük dosyalarına çeşitli biçimde bir birkaç örnek verilmiştir:

W3C

Bir W3C günlüğü, kaynak Internet Protokolü (IP) adresi, HTTP sürümü, tarayıcı türü, yönlendirme sayfası ve zaman damgası içeren bir metin günlüğüdür. Onun biçimi, World Wide Web Konsorsiyumu (W3C), Web evrimi için standartları teşvik eden bir kuruluş, tarafından geliştirilmiştir.

Örnek

```
#Software: Microsoft Internet Information Services 7.5
#Version: 1.0
#Date: 2014-11-24 16:17:49
#Fields: date time s-ip cs-method cs-uri-stem
2014-11-24 16:17:49 ::1 GET / - 80 - ::1 Mozilla/5.0+OPR/26.0.1656.24 200 0 0 3918
```

Burada her satırın ne anlama geldiğini anlatalım

```
#Software: Microsoft Internet Information Services 7.5
```

Bu çalışan IIS sürümünü gösterir.

```
#Version: 1.0
```

Bu günlük dosyası biçimini gösterir.

```
#Date: 2014-11-24 16:17:49
```

günlük dosyasının oluşturulduğu zamanı gösterir.

```
#Fields: date time s-ip cs-method cs-uri-stem 2014-11-24 16:17:49 ::1 GET ..
```

Bu günlük dosyasında kaydedilen alanları ve hangi düzen ile kaydedildiğini gösterir.

Apache CLF

Apache HTTP Sunucusu çok kapsamlı ve esnek bir günlükleme yeteneğine sahiptir. Apache Ortak Günlük Biçeminde(Common Log Format) kullanılarak üretilen Apache günlük mesajlarını örnek olarak alalım.

```
"%h %l %u %t \"%r\" %>s %b"  - Ortak Günlük Biçemi
```

```
127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700] "GET /apache_pb.gif HTTP/1.0" 200 2326
```

[22]'ye göre bu Apache günlük mesajının parçalarının açıklaması şöyledir:

127.0.0.1(%h): bu, sunucuya istek yapan istemcinin (uzak konağın) IP adresidir.

- (%l): istenen bilgi parçasının mevcut olmadığı anlamına gelir.

frank (%u): belge isteğinde bulunan kişinin kimliğidir.

[10/Oct/2000:13:55:36 -0700] (%t): isteğin alındığı tarih ve saat.

"GET /apache_pb.gif HTTP/1.0" (\"%r\"): istemciden alınan istek çift tırnak içinde verilir.

200 (%>s): sunucunun istemciye geri gönderdiği durum kodudur.

2326 (%b): istemciye geri gönderilen nesnenin uzunluğudur.

Basit bir Syslog mesajın örneği

```
Nov 21 17:27:53 MM-PC LOGANALYZER[13163]: Program started by User 1000
Nov 21 17:27:53 MM-PC LOGANALYZER[13163]: Ouch an ERROR!
```

Bu günlük mesajının biçimi tarih ve saati, damgası, makine adını, program adını ve mesajı içermektedir.

Günümüzde, çoğu günlük ya önceden belirlenmiş bir formatı takip etmez ya da sadece zaman damgası gibi çok küçük bir bölümü takip edebilir ve bu serbest biçimli metin sayılmaktadır.

Metin formatı dışında var olan diğer günlük biçimleri bulunmaktadır. İlk olarak, günlük dosyası biçimi ikili veya ASCII formatında olabilir. İnsan ASCII ve Metin biçimleri kolayca okuyabilir ama ikili formatı insan-okunabilir değildir. Bir ikili günlük dosyasının en yaygın örneği, Windows Olay günlüğüdür. Olay Günlüğü okuma için Olay Görüntüleyicisi (Event Viewer) kullanılmasını gerektirmektedir. Bu Olay Görüntüleyicisi yardımcı programı, ikili günlüğü okunabilir bir olay haline dönüştürür. Bir başka günlük formatı ve çok süslü bir ikili biçimi olarak kabul edilebilir tipi ilişkisel veritabanıdır. İlişkisel veritabanı ikili günlükleri bir tablo içinde depolamaktadır.

Günlük tipleri arasındaki bir diğer fark formatın gizli veya açık olup olmamasıdır. Açık format, standart bir doküman (örneğin, ISO, ANSI veya bir Internet standardı) veya referans bir doküman (örneğin, bir RFC) olarak herhangi bir yerde bir gizli olmayacak bir biçimde sunmaktır. Gizli format ise dokümanter edilmiş veya edilmemiş olabilir ve ayrıca özel bir cihaz satıcısı tarafından kullanılabilir.

3.3.3. Günlük Mesajı Sözdizimi

Herhangi bir formattaki her bir günlük dosyasının bir söz dizimi vardır. Günlük söz dizimi Türkçe dili gibi kavramsal olarak benzerdir. İnsan dilindeki bir söz dizimi tipik olarak bir nesne, bir özne, bazen de bir yüklem içerir. Cümle sözdizimi, cümleyi oluşturan elemanlar ve onların anlamları arasındaki ilişkiyi kapsar. Unutmamak gerekir ki söz dizimi iletinin içeriğini değiştirmez. Başka bir deyişle, sözdizimi bizim ile ilgili söz dizimlerini nasıl kullanacağımızı ve ne söyleyeceğimizi istediğimiz gibi seçebiliriz [11, 12, 15, 17].

O zaman günlük iletileri içerisinde söz dizimi ne anlama gelmektedir? Her günlük iletinin bir yapısı vardır. Bazı günlük iletiler insan dilinin parçalarını içerir. Ne olursa olsun günlük iletiler çeşitli tipteki bilgilerin örneklerini içerir. Düzenlemelere bağlı olarak birisi günlük alanlarının ortak bir ayarlamasını tanımlayabilir. Örneğin, en yaygın alanları şunlardır [11, 14, 15,17]:

- Tarih/Saat
- Günlük girdisi türü
- Günlük üretilen sistem
- Üretilen uygulama veya bileşeni.
- Başarılılık, başarısızlık göstergesi
- Bir günlük iletisinin önemi, önceliği ve ağırlık derecesi (tipik olarak, tüm syslog iletilerinde mevcuttur).
- Bir kullanıcı kaydındaki gibi herhangi bir yolda kullanıcı aktiviteleri ile ilgili günlükler için.

Ağ cihaz üreticileri genellikle kendi günlüklerinin çoğunda yukarıdakileri takip ederler, ama eksik olan bazı günlük detayları önemli istisnalardır.

3.3.4. Günlük Mesajı Türleri

Log dosyaları, kaynak ve tipik içerik formatlarına göre farklı farklı kategorilere ayrılırlar. Bu tez çalışmasında tamamını listelemek mümkün olmadığından sadece önemli türler açıklanacaktır.

İçeriğe göre: Günlük içeriği bilgi, uyarı, alarma, ya da çok önemli bir hata olabilir. Apache ve IIS (Internet Information Services) erişim dosyaları, bilgi günlük dosyaları örnekleridir. Uyarılar, alarmlar ve çok önemli hatalar genellikle tek bir 'hata' dosyası içerisinde toplanır (Unix işletim sisteminde bu dosyayı 'syslog' olarak kullanılır.) Fakat Windows işletim sisteminde birçok hata veya kaynak belirli gruplara bölünerek kaydedilebilir [13].

Kaynağa göre: Günlük dosyaları her şeyden gelir. Mesela, uygulamalardan, sistemden, farklı sürücülerinden ve kütüphanelerinden gelebilir. Kaynak bir sınıflandırma yöntemi olarak kullanılmaktadır. Örnek olarak, güvenlik alt sistemi kendi özel günlük dosyasına sahip olabilir, ya da günlük dosyasının nerede ve nasıl güncelleştirildiğini tanımlayabilir. İşletim sistemleri tarafından sistem günlük dosyaları üretilir, uygulama loğları geçici dosyalara veya merkezi birim sistem günlük dosyalarına kaydedilebilir [13].

Biçimine göre: Günlük dosyalar tekst, ikili ya da ilişkisel veritaban formatta olabilir. Daha kolay çalışılması nedeniyle ve üreticiler ve okuyucuların bakış açısına göre tekst daha popülerdir. Bazı işleme formları olmadan ikili genellikle imkânsızdır ancak ikili günlükteki bir bilgi daha iyi formatlanabilir ve saat, sınıflama ve tarih gibi elemanlar için veri tipleri tanımlanabilir ve özel uygulamalar için kullanılabilir [22, 13]. Tarih ve saat ikili yakın veri örnekleridir, ancak tekstte kullanılabilir ve tanınabilir olmaları için tanımlanmalıdırlar. Kaynak biçimi, konumu ve içeriği, günlük dosyalarından yararlı bir bilgi almak için işlenmiş olmaları gerekir. Genellikle, günlük dosyasının biçimi önceden belirlenebilir. Syslog için standartlar, HTTP günlük dosyaları ve diğer dosyalar kullanılabilir. Bununla birlikte, belirli uygulamalarda günlük dosyalarının çıktı şekli değiştirebilirsiniz.

3.4. Günlük Kaynağı Sınıflandırmaları

Günlükler, kullanıcı aktiviteleri ile ilgili bilgiler içerebilir: kimin giriş yaptığı, onların ne yaptığını, alınan ve gönderilen mailleri gibi. Günlükler disk hataları gibi bozulan veya bozulan şeyler hakkındaki bilgileri bize bildirirler. Günlükler kaynak kullanımı ve performans bilgilerinin yanında iyi çalışan nesneleri de bildirirler.

Günlük analiz işleminin ilk adımı günlük kaynağının ve sınıfının ne demek olduğunu anlamaktır. Bazı uygulamalar ve sistemler varsayılan olarak günlük olaylar vardır, bazılarında

da yoktur. Bazı durumlarda, uygulama günlüğü veri gönderme işlemi olabilir, ama veriyi alabilmek için herhangi bir özel duruma gerek yoktur. [15,17, 12-19]:

3.4.1. Güvenliği ile ilgili ana bilgisayar(host) günlükleri

Bu kategori, sistem üzerinde çalışan diğer uygulamalar kadar çeşitli ağ günlükleri gibi sistem bileşenlerinin çalışmasıyla üretilen ana bilgisayar günlükleridir. Mesajlarının çoğu sadece veya öncelikle performans izleme, denetim ya da sorunlar gibi nedenlerle üretilmiş iken, bunların büyük bir çoğunluğu da aynı zamanda güvenlik için faydalı uygulamalardır [23].

3.4.2. İşletim sistem günlükleri

İşletim sistemleri, oldukça yoğun bir çeşitlilikte olan günlük mesajları tutmaktadır. İşletim sistemleri tarafından üretilen mesajların güvenlikle ilgili türlerinden bazıları aşağıda verilmektedir [23]:

- Kimlik Doğrulama (Authentication): kullanıcının oturum açması, giriş yapması ve benzerlileri gibi.
- Sistem başlatma, kapatma ve yeniden başlatma.
- Servis başlatma, kapatma ve durum değişikliği.

Genel olarak, işletim sistemi mesajları iki ana nedenden dolayı güvenlikle ilgili kabul edilir: Bu mesajlar, izinsiz girişlerin ve saldırıların (*intrusion detection)* tespiti için yararlıdır, bu yüzden, başarılı ve başarısız saldırılar genellikle günlüklerde daha önce görülmemiş izler bırakacaktır. Ana bilgisayar saldırı tespit sistemleri (Host intrusion detection systems (HIDS)) ve güvenlik bilgi ve olay yönetim sistemleri (security information and event management systems (SIEMs)) iletileri toplar ve geçmişteki ve gelecekteki girişimlere karşı bir yargılama yapar [12, 23]. Başarılı saldırılar çeşitli güvenlik güvencelerin varlığına rağmen gerçekleşecektir ancak bu sistemler aynı zamanda olaya müdahale(*incident response)* etmek için faydalıdırlar [23].

3.4.3. Ağ Daemon günlükleri

Ağ Daemon genellikle aşağıdaki kategorilerin güvenlikle ilgili mesajlar günlüğünü tutmaktadır [23]:

- Bağlantı sunucuyla başarılı olarak kurulmuştur.
- Bağlantı sunucuyla kurulamadı.
- Bağlantı kuruldu, ama erişime izin verilmedi.
- Çeşitli hata durum iletileri.

Ağ Daemon günlükleri genellikle genel işletim sistemi günlükleri kadar yararlıdır. Aslında, bunlar normalde aynı yere kaydedilir, Örneğin, Unix ve Windows üzerinde aynı günlük mekanizma yaygın olarak kullanılır.

3.4.4. Uygulama Günlükleri

Uygulamalar da günlükleri çok çeşitli şekilde günlükleri tutmaktadır. Uygulamaların günlük türleri aşağıdaki gibi listeleyebiliriz [23]:

- Uygulama kullanıcı etkinliği
- Ayrıcalıklı kullanıcı etkinliği
- Rutin ama kritik bir aktivite
- Yeniden yapılandırılması

3.4.5. Güvenlikle İlgili Ağ Günlükleri

Bu kategori ağ altyapısı tarafından oluşturulan ağ günlüklerini kapsar. Yönlendiricilerin (Routers) ve anahtarların (switches) çalışmasının yanı sıra bağlı bulundukları trafik ile ilgili günlük mesajları çok çeşitli günlük iletiler içeriklerinden oluşur [23].

3.4.6. Ağ Altyapısı Günlükleri

Ağ altyapısı, yönlendiricileri, anahtarları ve ağı içeren diğer sunucular ile bağlantı yapan diğer cihazları içerir ve bu tür cihazlardan gelen günlükler sistemin güvenliğinde kritik bir rol oynayabilir. En sık görülen mesajlar aşağıdaki kategorilere ayrılır [23]:

- Giriş ve çıkışlar.
- Servisile Bağlantı kurulması
- İçeri ve dışarı byte transferi
- Yeniden başlama
- Yapılandırma değişiklikleri

3.5. Günlük Toplama Araçları

Bir ağda bulunan sunucuların günlüklerini bir merkezde toplamak çok önemli ve mantıklı bir fikirdir. Bu şekilde, tüm cihazlar, sunuculara ait olan günlükleri belli bir düzenleme içerisinde tutabilir ve ilerisi için düzenli bir şekilde kaydedebilir. Aynı zamanda günlükleri herhangi bir araç ile tek yerden monitör edilebilir.

İşte bu tip avantajların olan bazı toplama araçlar bu bölümde, nedir, nasıl çalışır, gibi konular kısa bir şekilde anlatmaktadır. Genellikle, Günlük toplama araçları iki genel kategoriye ayrılabilir [12]:

- İtme-merkezli (Push-based)
- Çekim-merkezli (Pull-based)

İtme-merkezli günlük toplama, cihaz veya uygulama birimi yerel disk veya ağ üzerinde log mesajları yaymaktadır. Ağ üzerinden yayılması durumunda, mesajı toplaması için hazır bir günlük toplayıcının olması gerekmektedir. Syslog, SNMP ve Windows Olay Günlüğü üç ana İtme-merkezli günlük toplama araçlarıdır. Bu birimler günlük mesajların iletildiği protokolleridir. Teknik olarak Windows olay günlüğü protokolü, taşıma mekanizmasını, depolamayı ve almayı kapsamaktadır.

Çekim-merkezli ile: bir uygulama kaynaktan günlük mesajı alır. Bu yöntem hemen hemen her zaman bir işlemci-sunucu modeline bağlıdır. Bu şekilde çalışan çoğu sistem bazı özel formatta kendi günlük verilerini depolamaktadır. Örneğin, Checkpoint geliştiricilerin uygulamaları yazmak için kullandıkları OPSEC kütüphanesini sunar, sonrasında bu uygulamalar kullanılarak Checkpoint güvenlik duvarı günlüklerine ulaşılabilir. Diğer ürünleri kendi veri depolamak için (MSSQL, Oracle, MySQL, vs gibi) veritabanları kullanmaktadır.

Bir veritabanından günlükleri çekilmesi biraz kolay ve bir komut kodu veya bir program kullanılarak yapılabilmektedir.

En yaygın kullanılan günlük toplama protokolleri syslog protokol, SNP ve Windows olay günlüğü olup bunlar bir sonraki bölümde açıklanmaktadır.

3.5.1. Syslog protocol

3.5.1.1. Syslog Nedir ?

Unix sisteminde, çekirdek (kernel) ve birçok uygulama Syslog kullanarak günlük iletilerini kaydetmektedir. Syslog başlangıçta ayıklanmış hatalı bilgileri toplamak için kullanılmıştır. Syslog'unda, güvenli günlük analizi için uygun olmayan bazı sınırlamaları vardır. Her şeye rağmen, syslog, UNIX tabanlı sistemlerde uygulama olaylarının kaydedilmesi için en yaygın yöntem haline gelmiştir [15 - 17].

```
21-10-2014     00:00:06       Local0.Warning 10.81.1.2      fuhfw:
NetScreen device_id=fuhfw  [Root]system-warning-00769: UF-MGR: URL
BLOCKED: 10.8.115.1(1522)->184.168.92.148(80)
sdmc.devicevm.com/sdmc/sdrpt.php CATEGORY: default REASON:
```

Şekil 3:1 Syslog Loglari - Fırat Üniversitesinin Hastanesinin sistemi alınan bir Syslog logu

Syslog, Unix sistemlerdeki çeşitli kaynakları, uygulamaları ve üretilen günlükleri (olay mesajları) işlemek amacıyla kullanılan bir uygulamadır. Syslog günlük mesajları üreten yazılım, depolayan sistemlerinden, rapor veren ya da analiz yapan yazılımlardan ayrılmasını sağlar. Syslog, bilgisayar sistemi yönetiminin, güvenlik denetiminin, yanı sıra genel bilgisel, analiz ve hata ayıklama gibi amaçlar ile kullanılabilir [15-18].

Syslog, (syslogd)'dan oluşmaktadır. Normalde, Syslog sırasıyla cihazın kapanması halinde kapanır ve açılması halinde de başlamaktadır. Uygulamalar rsyslog (3) kütüphane çağrı yoluyla syslog ile iletişim kurmaktadır. Syslogd bir Unix alan soketi üzerinden uygulamaları ve çekirdekten günlük kayıtları almaktadır. Syslogd ayrıca isteğe bağlı olarak UDP iletileri aracılığıyla uzak birimlerden 514 portu üzerinden veri alabilir. Modern sürümleri ve rsyslog ve syslog-ng gibi syslog değiştirmeleri TCP ile çalışabilir [24,15,18].

RFC 3164, Syslog sunucuları olarak da bilinen Olay mesaj toplayıcısına IP ağlar üzerinden bir cihazın olay bildirim iletilerini göndermesine izin veren bir taşıyıcı görevini üstlenir. Protokol olay iletileri üreten cihazdan toplayıcıya ileti taşımak için tasarlanmıştır. Toplayıcı mesajların alındığı zamanı bildirim olarak geri göndermemektedir.

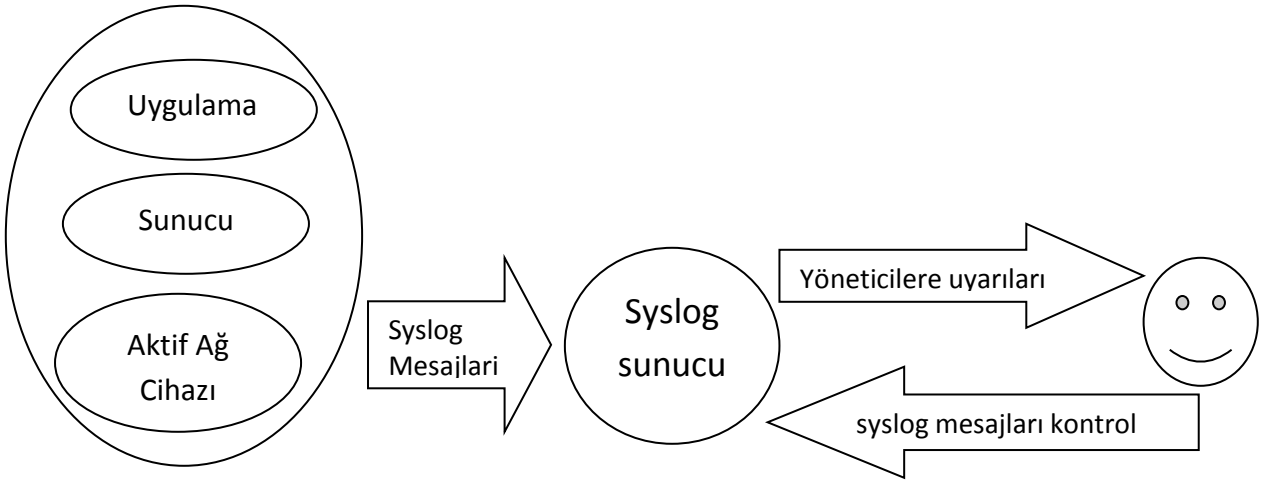
UNIX işletim sisteminde, çekirdek(kernel) ve diğer iç bileşenlerin mesajları ve uyarıları üretilir. Bu mesajlar genellikle bir dosya sisteminde depolanır veya syslog mesajlar biçiminde başka bir cihaza aktarılır. Syslogd adlandırılan bir içsel daemon, Syslog işlemini yönetir. Bu daemon çoğu UNIX / Linux dağıtımlarının ayrılmaz bir parçasıdır ve kurulum ve indirme gerektirmemektedir [12].

3.5.1.2. SYSLOG'un Kısa Tarihi

[18]'ye göre, Eric Allman onun programı, Sendmail, için başlangıçta bir günlük servisi olarak syslog'u 1980 yılında biçimlendi. Ancak, diğer geliştiricileri de syslog'u çok sevip ve kendi uygulamalarında kullanmaya basladilar. ve sonunda Unix ve Linux için fiili bir standart haline gelene kadar basarali ve popüler bir protokol olmuştur.

Syslog, Unix ve Unix benzeri sistemlerde günlük çözüm durumları için bir standart olarak gelmiştir. Yalnız tüm Unix programlarında Syslog ile günlük iletiler yazılamamaktadır. Modern Linux sistemi üzerinde, Apache, Exim ve Samba performans nedenleri için varsayılan kendi dosyalarını yazan üç örnektir [15-18].

Yıllar boyunca, Syslog protokolü için standart RFC3194 kullanmıştır. Şimdi, RFC5424 Syslog protokolü için yeni önerilen taslak standarttır. Başka bir deyişle, RFC5424 RFC3194'ü rafa kaldırmıştır. RFC5424, Eski protokola göre bir daha ihtiyaç olan düzeltmeler kapsamaktadır. Yeni Protokolünde en büyük değişikliklerden biri zaman damgasının belirtimisidir. Eski protokol zaman damgaları çok iyi bir şekilde belirtmedi. Genellikle zaman damgasında yıl yoktur ve saat dilimi bilgilerini mevcut değildi. Bu analiz açısından çok zorlaştırıyordu.



Şekil 3:2 Merkezli Log toplama

Syslog sistem günlüklerini toplamak ve işlemek için merkezi bir nokta görevindedir. Bu sistem günlükleri gelecekte sorun giderme ve denetim yapmak amacıyla fayda sağlamaktadır. Örneğin, bir hacker bir sistemi kırdığı zaman, hacker'in sistem üzerinde gerçekleştirdiği uygulamalar Syslog iletileri sayesinde kaydedilir. Bu mesajlar daha sonra, gerçekleştirilen saldırının nedenini anlamak, saldırı sonuçlarını değerlendirmek ve sistemi düzeltmek için kullanılabilir.

Çeşitli Cisco cihazları, yönlendiriciler ve anahtarlar sistem bilgisi ve uyarılar için Syslog iletileri oluştururlar. Örneğin, Cisco yönlendirici bir arayüz arıza verdiğinde veya yapılandırmada değişme olduğunda bir Syslog ileti üretebilir. Benzer bir şekilde, Cisco PIX Firewall, bir TCP bağlantısı engellendiğinde Syslog mesaj üretebilir [12].

Cisco cihazları merkezi bir Syslog sunucusu gibi davranan harici bir makineye Syslog mesajları gönderebilir. Ancak, Cisco cihazı ve Syslog sunucusu arasındaki bağlantı bir şekilde ortadan kaybolursa, hiçbir Syslog iletilesi sunucu tarafından yakalanamayacaktır. Bu gibi durumlarda, Cisco cihazları tarafından yerel olarak Syslog mesajları depolanır ve sorunun ana nedenini belirlemek için tek bilgi kaynağı bu mesajlardır.

Haberleşme için Syslog, Kullanıcı Datagram Protokolü (UDP) port 514'ü kullanır. Bağlantısız bir protokol olan UDP, onay sağlamaz. Ayrıca, uygulama katmanında Syslog sunucuları, alınan mesajlar için göndericiye onay göndermez. Sonuç olarak, ileti gönderen cihaz Syslog sunucusunun mesajları alıp almadığını bilmeden Syslog için iletileri oluşturmaya

devam eder. Aslında Syslog sunucusu olmasa bile verici cihaz mesaj göndermektedir [25 - 27,16].

3.5.1.3. Rsyslog

Rsyslog, syslogd'nin geliştirilmiş halidir. Çoğunu syslog ile rsyslog kullanarak, günlükleri MySQL, SQL, Oracle vs gibi databaselere yazdırılabilir. Alınan günlüklerin formatlarını istedikleri gibi oynatabilir. Günlükları şifreleme (encrypt) edebilir. Örnekleri çoğaltmak da mümkündür. Rsyslog'un yetenekleri ile ilgili tam bir liste [27]'de mevcuttur.

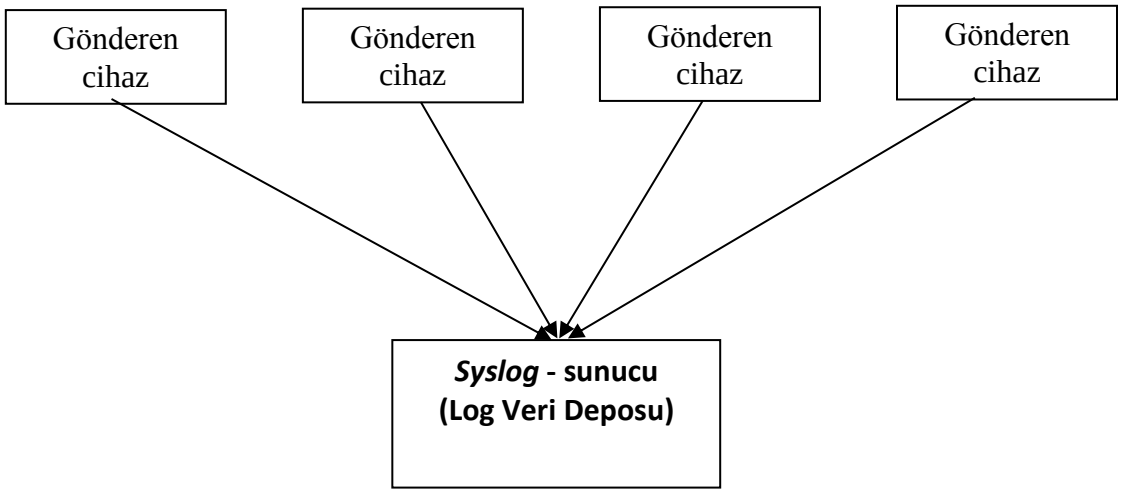
3.5.1.4. Syslog ne için kullanılmaktadır?

Syslog pek çok farklı uygulamayı yönetmek için kullanılır [12]:

- Ağ üzerinden olay bildirimlerini ve iletileri gönderme
- Yönlendiriciler, güvenlik duvarları, vb gibi ağ aygıtlarının sorunlarını giderme
- Yükleme sırasında günlük olayların kaydedilmesi
- Problem durumlarında hatanın kaynağını yalıtma
- Yasal olmayan faaliyetler veya girişimler için ağ veya sistem aktivitelerini izleme
- Denetleme ve yönetme işlemlerini takip etme
- Yönetici ve kullanıcı etkinliğini izleme

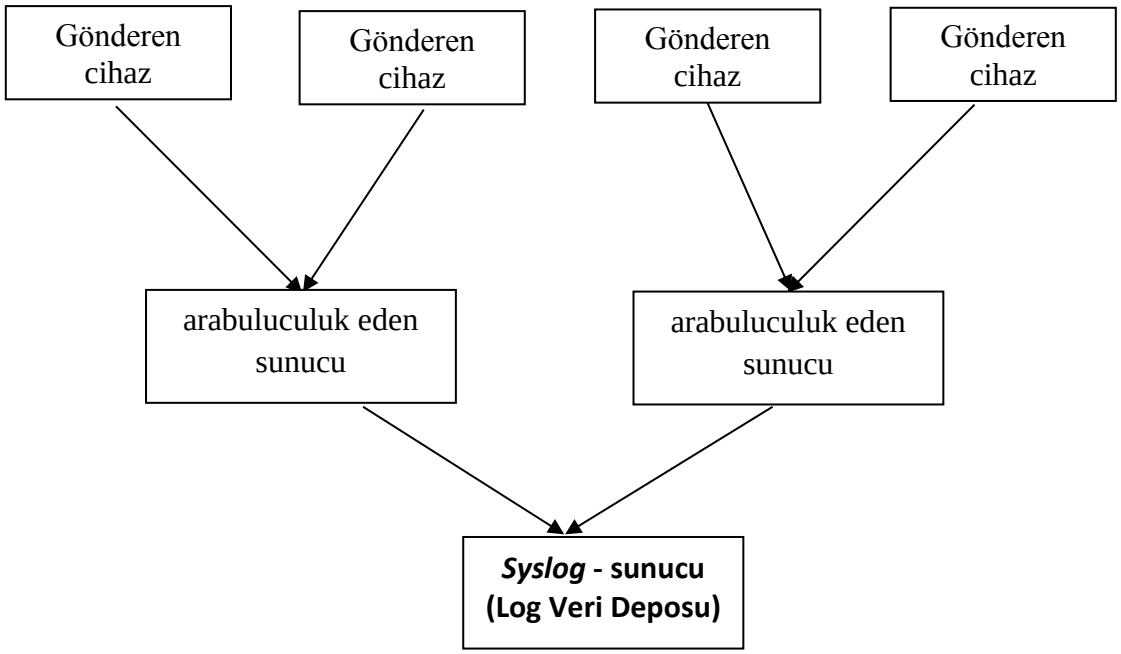
3.5.1.5. Normal Syslog kurulumu

Küçük LAN içinde bir veya birden fazla gönderi tek bir merkezi Syslog sunucuya veri gönderebilir. Syslog sunucusu daha sonra veriyi alıp depolamaktadır. Ayrıca alınan veriyi üzerinde oynayabilir ve veriyi analiz edebilir ve tipik olarak onların aynı LAN'da bulunması gerekmektedir [14,17].



Sekil 3:3 Syslog Sunucu _ küçük ağlarda

Genis ağlarda ve yoğun olan sistemlerde, günlük mesajları gönderenler, bir arabuluculuk eden Syslog sunucuya veri gönderir. Busunucu verileri alıp filtre ettikten sonra, son varış noktası olan depo edici Syslog sunucusuna verileri iletmektedir. Bu tip iletimler genellikle büyük kuruluşların ağlarında bulunmaktadır [14,17].



Sekil 3:4 Syslog Sunucu _ büyük ağlarda

3.5.1.6. Syslog Rolleri

Syslog farklı ve önemli roller oynar. Bunlardan bazıları şunlardır [12]:

- **Cihaz**: Syslog, mesaj, uyarı ve alârm üreten bir aygıt olarak bir rol oynayabilir
- **Toplayıcı**: Syslog iletileri alır ve isteğe bağlı olarak depolamaktadır.
- **Röle**: mesajları ve paketleri alıp ve ileten bir röle'ün rolünü rol almaktadır.
- **Gönderici**: syslog mesajları gönderebilir.
- **Alıcı**: syslog iletileri alabilir.

3.5.1.7. Syslog Mesajı Alanları

Syslog mesajın tam biçimi üç ana farklı bölümden oluşmaktadır. Format olarak: *"<pri> header msg"* şeklindedir. Her bölümün kendi içerisinde alanı bulunmaktadır [10-13, -17]. Bu bölümde genellikle bulunan alanlar anlatılmaktadır.

- Öncelik(PRI)-priority
    - Önem kodu (severity code)
    - Tesis Kodu (facility code)
- Başlık (header)
    - Zaman Damgası (timestamp)
    - Sunucu (host)
- Mesaj (msg)
    - Etiket (tag)
    - İçerik Alanı (content field)

Tek bir mesajda tüm alanların mevcudiyeti genellikle uygulama ve yapılandırmasına bağlıdır. Alanları filtreleme ve işleme veri günlükleri için kullanılabilir. Syslog mesajını ve alanlarını içeren paketin toplam uzunluğu 1.024 baytı geçemez ve minimum uzunluğu yoktur.

3.5.1.8. Öncelik(PRI) - priority

Öncelik kısmı, açılı parantezler içinde bulunan bir sayıdır. Bu sayı, mesajın önem kodunu ve tesis kodunu temsil eder ve sekiz bitlik bir sayıdır. İlk 3'u mesajın önem kodunu

temsil eder ve bu 3 bit ile 8 farklı önem kodu temsil edebilmektedir. Diğer kalan 5 bit'i mesajın tesis kodunu temsil eder. Syslog Daemon'ın içinde bulunan olayları belirli filtreler uygulamak için önem kodu ile tesis kodu kullanarak filtre edebilmektedir. Ama unutmayın ki! Syslog Daemon, bu önem ve tesis Kodları'nın değerlerini oluşturamamaktadır. Bunlar, olayları oluşturulan uygulamaları veya cihazları tarafından oluşturmaktadır.

Aşağıdaki önem ve tesis kodlarıdır.

3.5.1.9. Önem kodları

Önem seviyesi kodu, mesajın ne kadar önemli olduğunu gösterir. Örneğin, '0' olan bir önem seviyesi, acil bir durumdur ve '1' de acil fiili ihtiyacı bir uyarı olduğunu gösterir. Bu tablo önem kodlarını göstermektedir [15,16, 18]:

Tablo 3-1 Önem Seviyesi Kodları

Kod	Anahtar sözcük	Önem	Açıklama
0	emerg	Acil durum	Sistem kullanılmaz halinde
1	alert	Alarm	Bir fiil hemen alınmalıdır
2	crit	Kritik	Kritik durumları
3	err	Hata	Hata durumları
4	warn	Uyarı	Uyarı durumları
5	notice	Bildirimi	Bildirimi ama önemli bir durum değildir
6	info	Bilgilendirici	Bilgilendirici mesajları
7	debug	Hata Ayıklama	Hata ayıklama seviyesi mesajları

3.5.1.9.1.Tesis Kodları

Bir tesis kodu, günlük mesajı gönderen kaynağı herhangi bir tür olduğu belirtmek için kullanılır.Örneğin, '0' olan bir tesis kodu Çekirdek mesajı olduğunu ve '11'olan tesis kodu ise bir FTP mesajı olacağını gösterir. Bu yapılandırma dosyası, farklı tesislerden gelen mesajları

farklı bir biçimde elde edebileceğini, belirtmesini sağlar. Aşağıdakiler mevcut tesis kodlarının listesidir [15,16, 18]:

Tablo 3-2 Tesis Kodları

Tesis Kodu	Anahtar sözcük	Tesis Kodun Açıklaması
0	kern	Çekirdek(Kernel) mesajları
1	user	Kullanıcı seviyesi mesajları
2	mail	Posta sistemi
3	daemon	Sistemin daemon'u
4	auth	Güvenlik / yetkilendirme mesajları
5	syslog	Syslogd tarafından dâhil olarak üretilen mesajları
6	lpr	Satır yazıcı alt sistemi
7	news	Ağ haber alt sistemi
8	uucp	UUCP alt sistemi
9	clock daemon	Daemon'ın Saati
10	Authpriv	Güvenlik / yetkilendirme mesajları
11	ftp	FTP daemon
12	NTP subsystem	NTP alt sistemi
13	log audit	Günlük denetimi
14	log alert	Günlük uyarıları
15	cron	Daemon'ın Saati
16	local 0-local 7	Yerel kullanım 0-7

3.5.1.9.2. Öncelik(priority) değeri hesaplama

Öncelik değeri, ‘8’ ile tesis kodun sayısı çarpılıp ve Önem kodunun sayısal değeri eklenerek hesaplanmaktadır. Örneğin, Acil (Şiddeti = 0) bir Şiddeti ile bir çekirdek ileti (Tesis = 0), 0 bir Öncelik değerine sahip olacaktır. Örneğin, Eğer Çekirdek (kernel) mesajın tesis kodunun değeri 0 olursa ve Acil durumunun önem kodunun değeri 0 olursa, kesinlikle Öncelik değeri 0 olması lazımdır. "Yerel kullanım 4" mesajı 20'ye eşit bir tesisi kodu varsa ve Uyarı önemi, 5’e eşit olan bir değere sahip olursa, Öncelik değeri 165 olması gerekmektedir. Syslog mesajın önceliği bölümünde, bu değerler sırasıyla<0> ve<165> olarak açılı ayraçlar arasında yerleştirilmektedir.

3.5.1.9.3. Tesis ve önem değerlerini öncelik değerinden hesaplama

Belirli bir Öncelik değerine ima edilen Tesis numarasını almak için, 8 ile Öncelik numarası bölünmektedir. Sonra, çarpma sonucunda elde edilen sayının tamsayı kısmı tesis kodu olarak kabul edilmektedir. Önem kodunun değerini bulmak için ise bulanan tesis koduyla 8’içarpıp öncelik değerinden çıkarılarak bulunur.

Örneğin:

Öncelik = <165>

Tesis değeri elde etmek için:

165/8 = 20,625

ona göre, tesis kodu = 20.

Önem değeri elde etmek için:

165 - (20 * 8) = 5, Önem kodu = 5.

3.5.1.10. Başlık(header)

Başlık bölümü: Zaman damgası ve ana bilgisayar adı içerir:

3.5.1.10.1. Zaman Damgası

Zaman damgası, mesajın üretildiği zamanı, mesaj gönderen cihazın yerel saati, ay, gün, saat, dakika ve saniye olarak biçimde olması gerekir ve bu yüzden alıcı sistemin saatinden farklı olabilmektedir. RFC 3164 bir zaman dilimi (time zone) kullanımını belirtmese de, cihazlar Syslog paketin mesaj bölümüne zaman dilimi bilgilerini göndermek için, Cisco IOS bir yapılandırma vermektedir. Bu tür damgaları, Syslog sunucusundan mesajı yanlış anlamaya engel olmak için, genellikle özel bir karakter bir yıldız (*) veya kolon (:) gibi bir karakterle başlamaktadır. Zaman dilimi bilgilerini içeren, bir zaman damgası biçimi, MMM DD HH:MM:SS Zaman dilimi,bunun gibidir [15,16, 18].

3.5.1.10.2. Ana bilgisayar adı (Hostname)

Hostname, Syslog mesajı gönderen cihazın adı veya IP adresidir. Bir yapılandırmasına bağlı olarak, bazen mevcut, bazen eksik ve bazen de anlamsız ya da geçersiz olabilir. Birden fazla ağ takip edildiği zaman hostname genellikle kopya olabilir. Onun kullanılmasının amacı, günlük mesajı Syslog rölelerini geçerken, mesajı ilk gönderen cihazın adının sağlanmasıdır [15,16, 18].

3.5.1.11. Mesaj

MESAJ bölümü, Syslog paketinden kalan kısmı doldurur. Bu genellikle, mesajı üreten işlemin bazı ek bilgileri ve sonra da mesajın metnini içermektedir. Mesaj bölümünde iki alan:(Etiket alanı, İçerik alanı) vardır [15,16, 18].

3.5.1.11.1. Etiket alanı

Etiket alanındaki mesajı oluşturan programın adı veya sürecin adı olmaktadır. Bu sabit bir süreç adını ve yeniden her başlatıldıktan(reboot) sonra değişen dinamik bir sürecin kimliğini içerir. Ama onun gerçek biçimi uygulamaların arasında çok farklıdır.

3.5.1.11.2. İçerik alanı

İçerik alanı, mesajın detaylarını içerir.

3.5.1.12. Syslog sınırlamaları

Syslog aşağıdaki sınırlamalara sahiptir [15,16, 18]:

- Sadece 1.024(1 K) bayt boyutlu bir paket alabilir.
- Syslog protokolü UDP tabanlı olduğundan dolayı, güvenilir değildir. Mesajların teslimini garanti etmez. Onlar ya ağ sıkışıklığı(jam) ile düşer ya da kötü niyetli (istenmeyen) spam olarak yakalanabilirler.
- Yukarıda belirtildiği gibi, her süreç, uygulama ve işletim sistemi biraz bağımsız olarak yazıldığından dolayı Syslog mesajlarınını içeriğinde mevcut olan şeylerde çok az bir tekdüzelik vardır. Bu nedenle, mesajların biçimlendirmeleri veya içerikleri üzerinde hiç tahmin yapılmamaktadır. Protokol sadece olay mesajları toplamak ve mesaj transferi yapmak için tasarlanmıştır.
- Sistem Günlüğü (log) paketin alıcısı, bildirilen gönderici tarafından mesajın gönderilip gönderilmediğini, tespit etmesi mümkün değildir. Böylece bağlı olan bir sorunun doğruluğunu kanıtlaması (Authentication) olduğunu belirtmektedir. Yabancı bir cihaz başka bir yerel cihaz gibi kendisini temsil eden bir Syslog mesajı Syslog Daemon'a gönderebilir ve o yüzden yönetimsel personel kararsız bir hale gelebilir. Çünkü alıcı mesajları bekleyen göndericinin ne durumda olduğunu ve mesajların doğru olup olmadığını yansıtamamış olabilir. Doğruluğunu kanıtlama (Authentication) ile ilgili diğer bir sorun; bir saldırgan, bir makinede bir sorun var gibi gösteren sahte mesajlar gönderebilir. Ona göre, bu sistem yöneticilerin dikkatini alabilir ve iddia edilen sorunu araştırma yapmaktan dolayı onların zamanı geçirebilir. Bu süre içerisinde, saldırgan farklı bir makinde veya aynı makinede farklı bir işlem yapabilmektedir.

3.5.1.13. Syslog Güvenilirliği

Geleneksel olarak, Syslog küçük ağlar üzerinde iyi çalışır, fakat ağ çok büyük ve yoğun bir halde iken bazı paket kaybının olacağı beklenmektedir. Yoğun ağlarda, Syslog trafiğinde büyük bir patlama gerçekleştiğinden dolayı mesaj gönderen cihaz veya alıcı meşgul olur ve daha sonra ağ yavaşlar. Bu gibi durumlarda analizörü yapan program içinde bazı küçük paket kaybı planı olması gerekmektedir. Çoğu durumda, deneyim syslog kullanmayı yeterince güvenilir olduğunu gösterir özellikle yeni gelişmeler daha iyi güvenilirlik sözü vermektedir. Bu yüzden yeni standartlarının (RFC 3195!) kullanılması, uygulanması, Syslog

alıcı merkezi takip edilip ve yedeklenmesi her zaman emin olmasını tavsiye etmektedir [15,16, 18].

3.5.1.14. Syslog-ng

Yıllardır Unix sistemlerinde bulunan syslog protokolü, onu kullananların amaçlarına göre yeterince iyi olduğunu tespit etti. Ama zaman geçtikçe kullanıcıların, uygulamaları, sistemleri ve kuruluşların ihtiyaçları değişik olup ve yeni bir şeye ihtiyacı olduğunu ortaya çıktı. Bu durumda Syslog-ng, eski Syslog'un içinde bulunamadı ve daha fazla seçenek ve özellikleri ile kullanıcılara bilgi oluşturmak için bir çaba başlandı.

Daha önce de değinildiği gibi, klasik syslog'un birden fazla sorunu vardır. Örneğin, veri transferi tekniği UDP kullanılır ve UDP güvenilmez bir tekniktir. Syslog-ng bu problemleri çözmek için çalışmaktadır. UDP kullanacağı yerde TCP kullanmaktadır. Daha dikkat çekici syslog-ng özelliklerinden bazıları şunlardır [20]:

- TCP desteği: Bu Sylog mesajları daha güvenilir bir transfer verir.
- Veritabanı desteği: syslog-ng; MySQL, Oracle, MSSQL ve PostgreSQL gibi uzak bir veritabanına syslog mesajları göndermeyi destek etmektedir. Bu özelliği önemli bir avantaj, günlük mesajları ilişkisel bir veritabanında (relational database) kaydedilmesi, sağlamasıdır. Bu raporlama, arama ve diğer analiz tekniklerini çok kolay hale getirir.
- IPv4 ve IPv6 desteği: syslog-ng her iki tipinden gelen ve giden syslog mesajlarını işliyor.
- Yüksek performans: syslog-ng yüksek mesajı oranları işleyebilir ve güvenilir bir şekilde saniyede yüz binlerce mesajı ele alabilmektedir.

3.5.2. SNMP

SNMP (Simple Network Management Protocol), ağ yöneticilerinin artan ihtiyaçlarını karşılamak için tasarlanmıştır. 1990'larından itibaren, SNMP, aklınıza gelebilecek neredeyse mümkün olan her ağ sistemine entegre edilmiştir ve birçok ağ güvenlik sistemlerine dahil edilmiştir. SNMP sorgulama yapmak ve aygıtları yapılandırmak için kullanılan bir protokoldür. SNMP bildirimleri, özel bir olay meydana geldiğinde bir cihaz tarafından üretilen

SNMP mesajının bir türüdür. Birçok ağ cihazı syslog üzerinden olay bilgilerini gönderebiliyorken, bazı cihazlar özellikle eski cihazlar, bunu gerçekleştirememektedir, eğer olay bilgileri gönderilemeseydi SNMP bildirimlerini toplamak imkansız hale gelirdi. Bu yöntem cihazlardan olay bilgi almanın bir yöntemdir. Ayrıca bazı durumlarda, SNMP yoluyla gönderilen bilgi türü Syslog üzerinden gönderilenden daha farklıdır [12, 14].

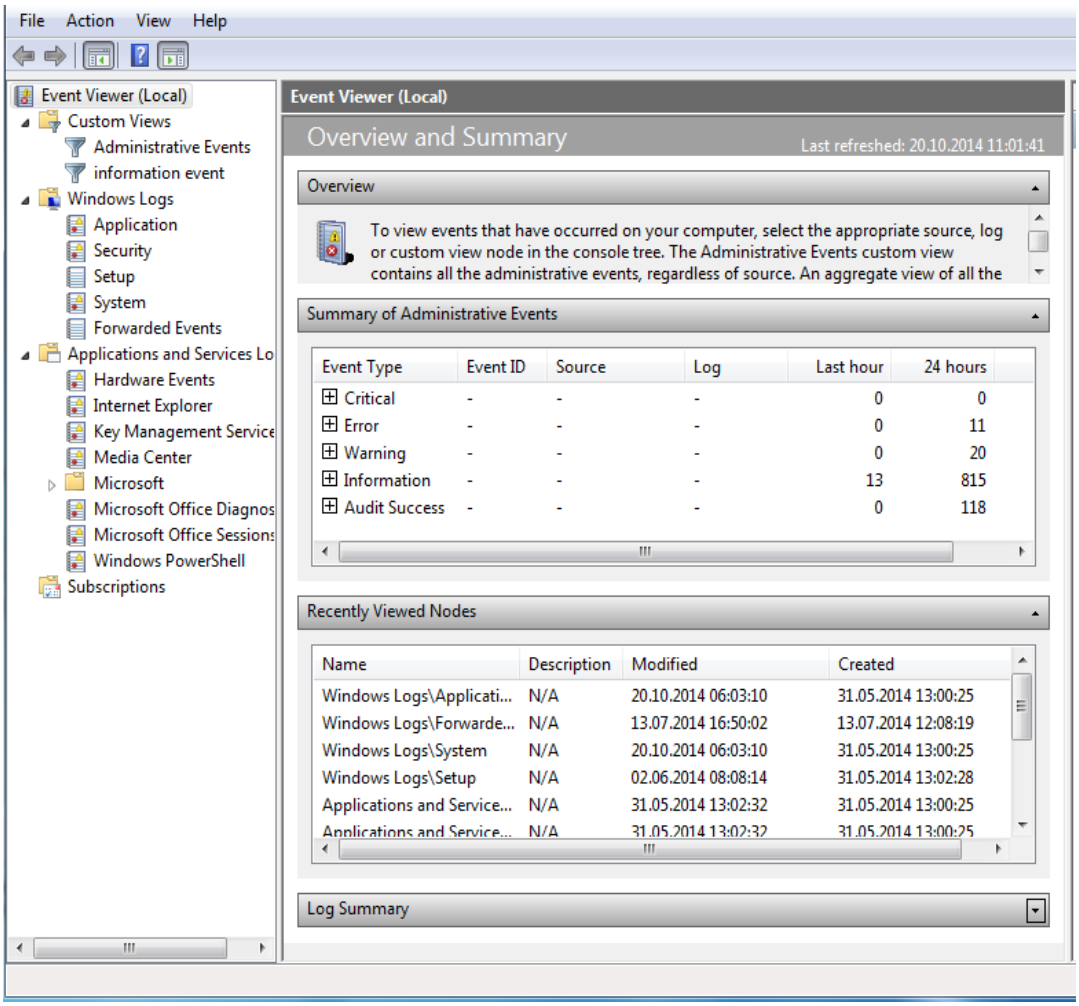
3.5.3. Windows olay günlüğü

Microsoft, kendi günlük kaynak ve toplama sistemini uygulamaya koyma kararını uzun zaman önce vermiştir. Bu sisteme Olay Günlüğü (Event Log) denir. Onu yıllar boyunca geliştirmiş olup ve neredeyse bu süre zarfında Windows gibi hemen hemen diğer işletim sistemlerinde bu uygulama gerçekleştirilmiştir. Bugünün Olay Günlüğü bazı gelişmiş özelliklere sahiptir. Olay Günlüğü günlükleri esas olarak iki günlük türünü toplamak ve açıklamak için kullanılmıştır [12, 14, 16]:

- Windows Günlükleri (Windows Logs)
- Uygulama Günlükleri (Application Logs)

Windows Günlükleri en az bir Uygulama, Güvenlik ve Sistemi kapsamaktadır. En önemlilerinden birisi Güvenlik günlüğüdür. Bu bir oturum açma, oturum kapama, kaynak erişimi (paylaşım, dosyaları, vb) gibi uygulamalardır. Uygulama Günlükleri kendisini oldukça iyi açıklamaktadır. Uygulamalar durumunu, hatalarını ve diğer önemli öğeleri kaydetmek için bu günlüğe yazabilmektedir.

Kısa bir şekilde Windows Olay Günlüğü'ne göz atalım. Olay Görüntüleyicisi'ni açmak için **Başlat** düğmesini --> **Denetim Masası'nı** --> **Yönetimsel Araçlar'ı** --> **Olay Görüntüleyicisi'ni** çift tıklayarak çalıştırılabilmektedir. Şekil 3.5 **Olay Görüntüleyicisi'ni** göstermektedir. Pencerenin sol bölümünde çeşitli günlük mesaj türleri bulunmaktadır. Ortada, sol bölmede seçilen günlük türünün gerçek günlük mesajını gostermektedır. Ortada günlük mesajın altında, günlük mesajının ayrıntıları bulunmaktadır.



Şekil 3:5 Windows Olay Günlüğünün Görüntüleyicisi

4. KENDİ ÇÖZÜMÜ PLANLAMA

Önceki bölümlerde ve özellikle 2. bölümde farklı log analiz çözümleri anlatılmıştır fakat tüm bu çözümler ve hatta değinilmeyen diğer çözümler her kurumun sistem ihtiyaçlarına uyumlu değildir. Bu bölümde, herhangi bir log çözümünün satın alınması planlanıyorsa veya yeni bir log analiz sisteminin geliştirilmesi düşünülüyorsa önce göz önüne alınması gereken bazı önemli noktaların üzerinde durulması gerekmektedir [2, 4].

4.1. İhtiyaçları Belirlemek

Bir log analiz sistemini geliştirmeye karar vermeden önce böyle bir sistemi ortaya çıkarmak ve sistemin gerekliliğinin nedeninin anlaşılması gerekmektedir. Dikkat edilmesi gereken bazı durumlar aşağıdaki gibi sıralanabilir:

- Kullanım durumu: Böyle bir sistemin nerede ve nasıl kullanılacağını tam olarak gösteren senaryolar tanımlanabilir mi? Örneğin, son 24 saat içinde sistemdeki Windows sunucularının oturum açma başarısızlıklarını gösterebilen bir raporun elde edilmesinin istenmesi.
- Sürücüler: Böyle bir proje geliştirmek için tasarımcıyı zorlayan veya yönlendiren nedir? Bu ihtiyaç sistemde mi gerekli yoksa hükümet düzenlemeleri ya da kurallar nedeniyle mi gerekli? Bu soruların cevapları açıkça zamanın, paranın ve kaynakların nasıl tahsis edebileceğinin anlaşılması için tasarımcıya yardımcı olabilir.
- Diğer sorunları çözme: Bu günlük analiz sisteminin çalıştırılması diğer sorunları çözmeye yardımcı olacak mı? Örneğin, günlük analiz sistemi tarafından toplanmış olacak bilgilerin tipine göre sistem sunucularını ve ağ cihazlarını izleme ve ağ sorunlarını giderme tasarımcıya yardımcı olabilir.
- Güvenlik: Bu sistem, ağın güvenliğini arttırır mı? Ayrıca bu sistem, düzenleyiciler, denetçiler ve benzerleriyle uyumlu bir şekilde çalışır mı?
- Servis iyileştirme: Bu sistemi kurduktan ve çalıştırdıktan sonra, eski sistemin servis durumu nasıl değiştirilebilir? Yeni sistem kaliteyi arttırır mı yoksa yavaş çalışması gibi olumsuz etkilere sahip olur mu?

Özet olarak, planlanmakta olan bir log analiz sistemi uygulanmaya ve geliştirilmeye başlamadan önce, yukarıdaki durumların gözden geçirilmesi gerekir.

4.2. Loglama aygıtları

İyi Loglama cihazlarına sahip olmayan bir log analiz sistemi iyi değildir. Planlama sürecinde önemli olan bir işlem, loglama yapan sistemleri ve cihazları değerlendirmek ve seçmek için güçlü bir kriter oluşturmaktadır. Günlük olayların kaynaklarını seçmek için örnek kriterler aşağıdaki gibi olabilir [28, 3]:

- Kritiklilik: Günlük olaylarının kaynaklarından hangisinin sistem ortamında önemli olduğunu ve bu kaynağın ne kadar kritik olduğunu anlamak gerekmektedir. Şirketin birincil Web sunucusu mu? Ya da şirketin gizliliği ile kritik bir araştırma ve geliştirme sunucusu mu? Eğer bir cihaz tehlike anında şirketin varlığını riske atabiliyorsa, o cihaz loglama listesinin başında olmalıdır. Örneğin, kredi işleme sunucu, alan adı sistemi (DNS) sunucusundan daha kritik duruma sahip olabilir.
- Onaylama: Bir günlük olay kaynağı belirlendikten sonra, kaynağın gerçekten kritik bir varlık olduğunu ve log analiz sistemine getirilmesinin gerekli olduğunu ilgilendiren kaynaklar ile birlikte doğrulanmaktadır.
- Olay Müdahale: Son olarak, belirli bir günlük olay kaynağı tehlikede olduğu zaman, olayın çözülmesini ve olay olduğunda aranması gereken kişinin kim olduğunun belirlenmesini, genellikle olaya müdahale etmek için nasıl bir yöntem geliştirmenin gerekliliğini ortaya koymaktadır.

4.3. Log Politikasının Tanımlanması

Rutin olarak her gün kullanılan bir dizi prosedürü oluşturmaya Log Politikası denir. Bu bölümde bir log analiz sisteminin kurulması planlanırken dikkate alınması gereken daha yaygın ve gerekli olan log politikalarına kısaca değinilmiştir. Ayrıca periyodik ve düzenli olarak kuruluşun, ihtiyaçlarının gereksinimleri ile uyum içinde olduğundan emin olmak için log politikalarını kontrol etmesi ve gözden geçirmesi önemlidir. İyi bir log politikası kurmak için dikkatle planlanması gereken konulardan bazıları aşağıdaki gibidir [29-32,4].

4.3.1. Loglama (Günlük) Politikası

İlk olarak endişe edinilen, olayın organizasyonu için bir loglama politikasının kurulması ve tanımlanmasıdır. Günlük politikalarının bir dizini şunlardır [2, 4, 29]:

- Kaydedilen log olayının türleri (oturum açma/kapatma, kaynak erişimi, güvenlik duvarı kabul edilen/reddedilen, IPS/IDS uyarıları, vb) ve yeterli loglamanın kurulması.
- Log toplama ve saklama (1 yıl, vb).
- Log korunması
- Logların devamlı olarak incelemesi

4.3.2. Log Dosyasının Rotasyonu

Log dosyasının rotasyonu, tanımlanması gereken başka bir log politikasıdır. Günlük dosyalar büyüdükçe, yerel sistemdeki disk dolmaktadır. Diskler dolduğu zaman, uygulamalar normal olarak çalışmayacaktır. Daha kötüsü, potansiyel kritik günlük iletileri kaybı oluşacaktır. Bu yüzden, işletme çapında aşağıdaki gibi bir günlük dosyası rotasyon politikasının geliştirilmesi gerekmektedir.

- Zaman tabanlı: Zaman sınırları belirli (yani dakika, saat, vb) olan log dosyalara dönüştürmek.
- Uzun süreli depolama: Döndürülmüş günlükler incelenmek istendiğinde yararlı olduğu için yeterince uzun süreli saklanmalıdır.

4.3.3. Log Mesajları Koleksiyon

Veri toplama, bir log analiz sisteminin en önemli parçasıdır. Veri toplama olmadan log analiz sistemi ile başarı sağlanamaz. Bu yüzden ortamda hangi cihazların günlük verilerinin oluşturulması isteniyorsa cihazın yapılandırılması gerekir. Örneğin, bir lazer baskı log verilerini oluşturabilmesi, onun logları toplaması gerektiği anlamına gelmez. Log veri toplama ortamının politikayla uygun olması gerekir. Meselâ bazı ortamlarda, sadece dış güvenlik duvarları ve IDS / IPS sistemlerinden günlük iletilerinin elde edilmes, gerekiyor olabilir. Ya da ağdaki her güvenlik duvarı, IPS, sunucu ve masaüstü 'den günlük kayıtlarını toplamak gerekebilir. Ne olursa olsun organizasyon ihtiyaçlarının veri toplama politikaları ile uyum

içinde olduğundan emin olmak için, bu politikanın her 3-6 ayda devamlı olarak bir incelemeye tabi tutulması gerekir [2, 28].

4.3.4. Tutma / Depolama

Log saklama genellikle birçok düzenlemenin gereğidir. Günlük saklama aslında üç aşamadan oluşmaktadır: Log depolama, erişilebilirlik ve loğların silinmesi. Bir günlük saklama sistemi olarak, syslog sunucusu asla kullanılmamalıdır. Ayrıca log tutmak için gerekli olan depolama boyutunun ne kadar olacağının dikkate alınması gerekmektedir. Bunu anlamak için basit bir işlem aşağıdaki gibi verilebilir [4]:

Saniyede log kaydı (bayt olarak) * 86400

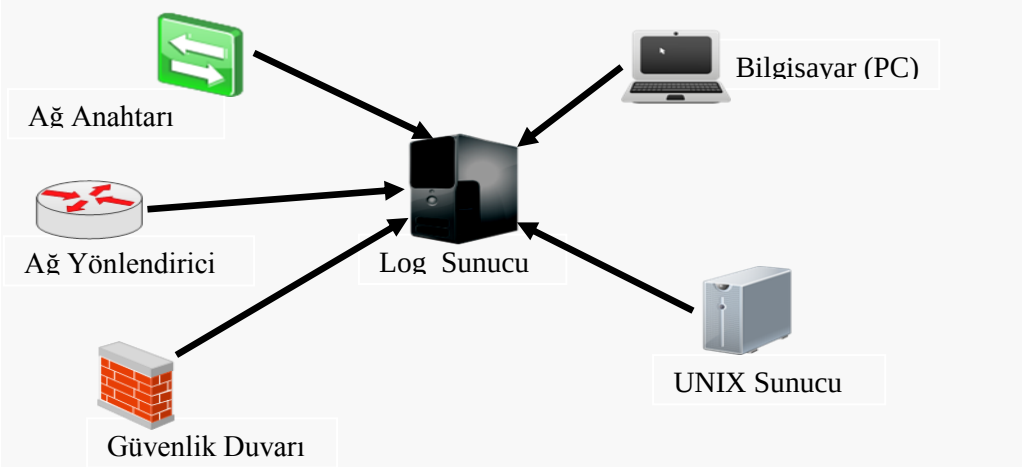
Genel bir kural olarak, log tutma kapasitesi ihtiyaçlarına % 25 eklemek beklenmedik olayların planlamasına yardımcı olmaktadır.

4.4. Altyapı

Log analiz sistemlerinin konuşlandırılması büyük ölçüde ağının büyüklüğüne ve aynı zamanda, ağdaki log mesajlarının nereden toplanacak olmasına bağlıdır. Aşağıda bazı temel altyapı modelleri verlimiştir [4]:

4.4.1. Basit

Bu temel altyapı modeli basitçe kullanılabilen en kolay modeldir. Bu basit yapıda, çeşitli cihazlar tek bir günlük sunucusuna günlük mesajları göndermektedir. Şekil 4.1 bu durumu göstermektedir.

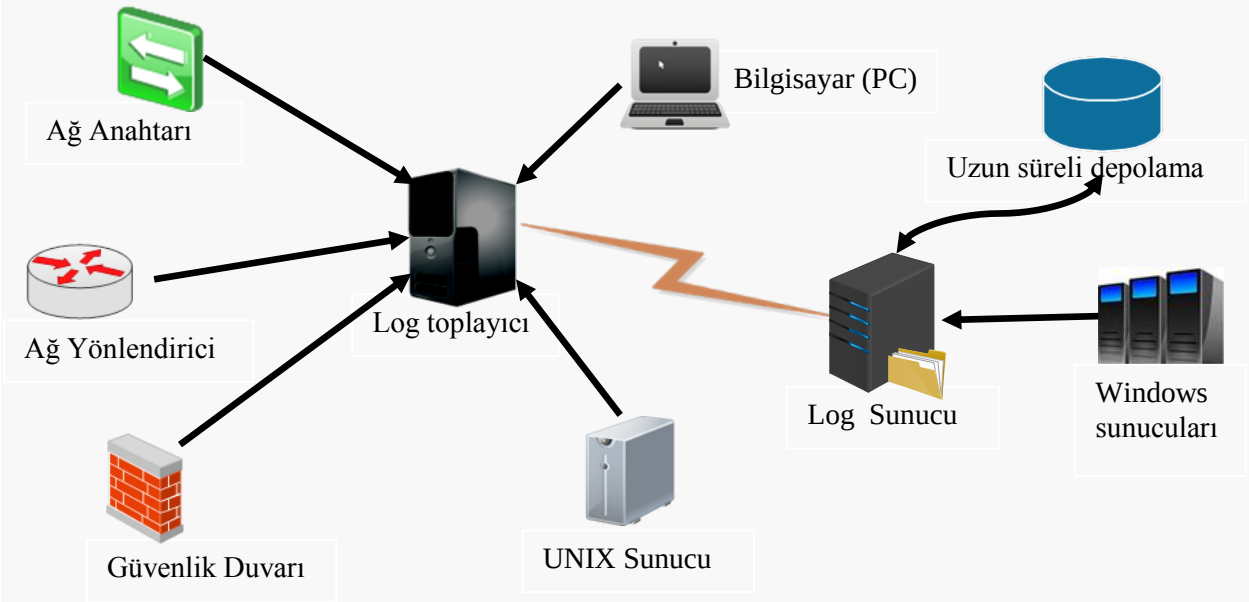


Şekil 4:1 Temel model altyapısı

Bu modelde, genellikle günlük mesajlarını incelemek için günlük sunucusuna giriş yapmak gerekmektedir. Bu durum en ideal durum değildir ama bazı durumlarda bunun yapılması en iyisidir.

4.4.2. Log sunucusu ve Log Kollektör

Diğer bir yaygın kullanılan altyapı modeli ağdaki stratejik noktalara günlük toplayıcıları koyarak kurulmaktadır. Bu günlük toplayıcılar ağda bulunan cihazlardan log mesajlarını toplayıp merkezi bir log sunucusuna yönlendirecektir. Şekil 4.2 bu yapıyı göstermektedir.

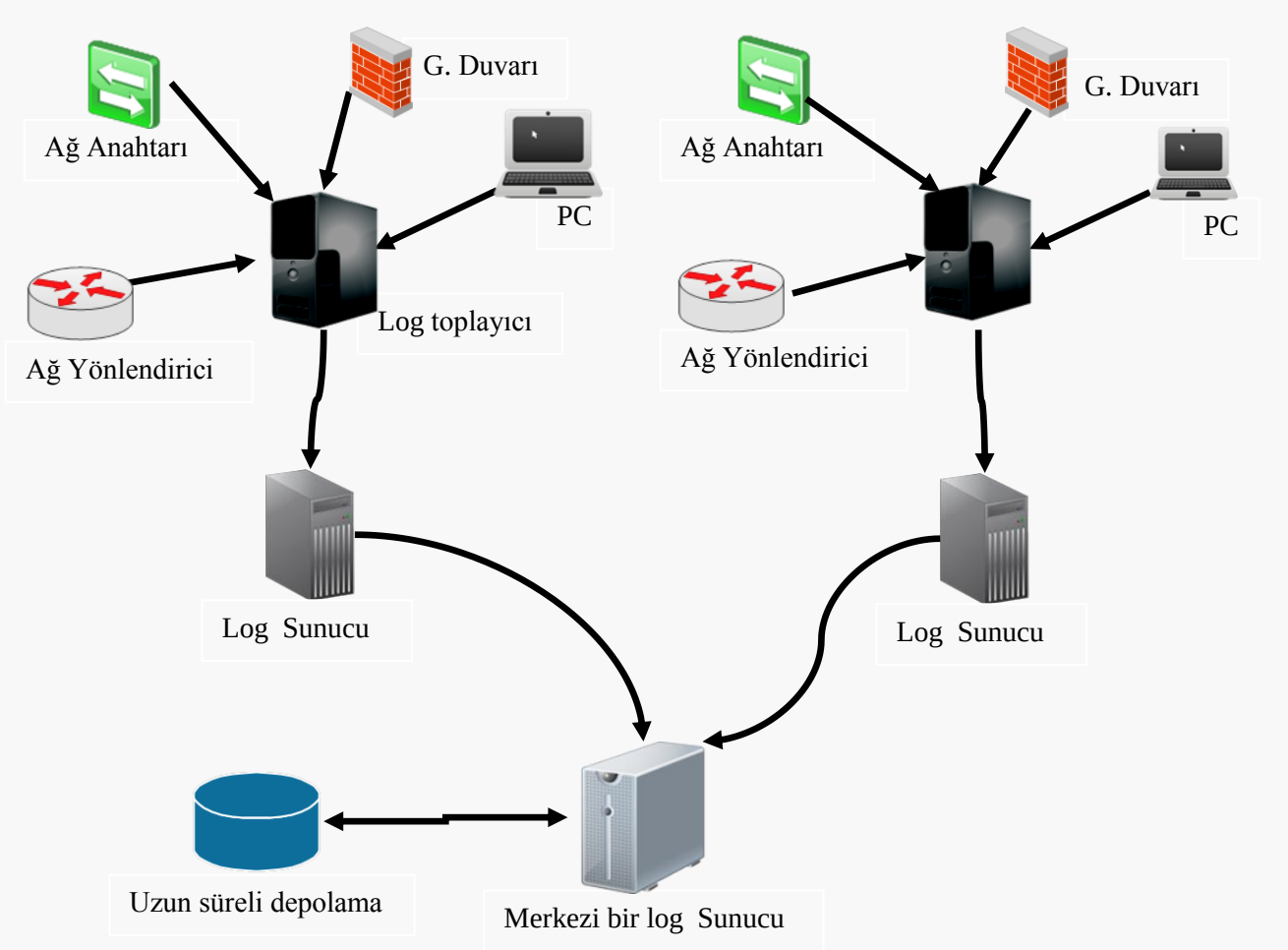


Şekil 4:2 Log sunucusu ve Log Kollektör model altyapısı

Bu sistemde günlük sunucusuna günlük mesajları gönderen bir günlük toplayıcısı vardır. Aynı zamanda günlük sunucusunun kendisi bir günlük kolektör (Windows sunucu tarafından) olarak davranabilir. Günlük sunucusu, günlükleri analiz etmek ve incelemek için merkezi bir yer olarak hareket etmektedir. Şirketin gerekliliğine göre uzun süreli depolamalar günlük sunucusuna eklenebilir.

4.4.3. Dağıtılmış

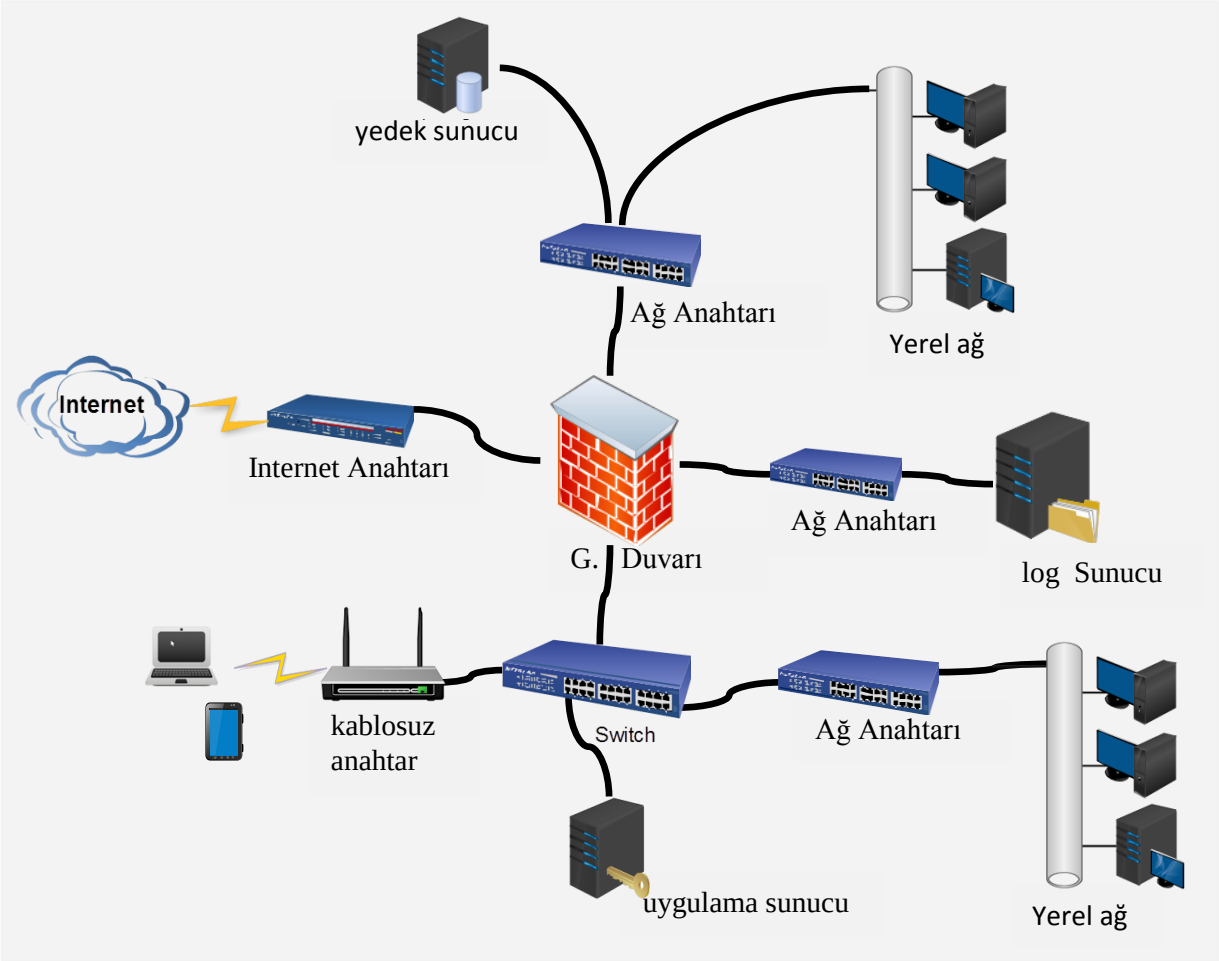
Dağıtılmış günlük altyapı modeli, günlük toplayıcılar ağı arasında dağıtılmış olmalıdır. Bu günlük toplayıcılar bir günlük sunucusu veya bazı durumlarda birkaç günlük sunucusu kadar döndürülmektedir. Bir hiyerarşik model olarak birden fazla günlük sunucusu merkezi bir log sunucusuna yuvarlanarak oluşturulabilir.



Şekil 4:3 Dağıtılmış altyapı günlük modeli

4.4.4. Bilgi Sistemlerinin Girişleri ve Çıkışları Kontrol Etmesi

Bazı durumlarda, özellikle hükümet tarafından ağımızdaki giriş ve çıkışları kontrol etmenin gerekliliği söz konusu olabilir ve bu durumda bu altyapının uygulanma zorunluluğu olabilir. Bu durumlarda, günlük olayları (kim ağ içine girer ve kim ağdan çıkar) oluşturmak için güvenlik duvarı yapılandırılmaktadır.



Şekil 4:4 Bilgi sistemlerin girişleri ve çıkışları kontrol etmesi altyapı günlük modeli

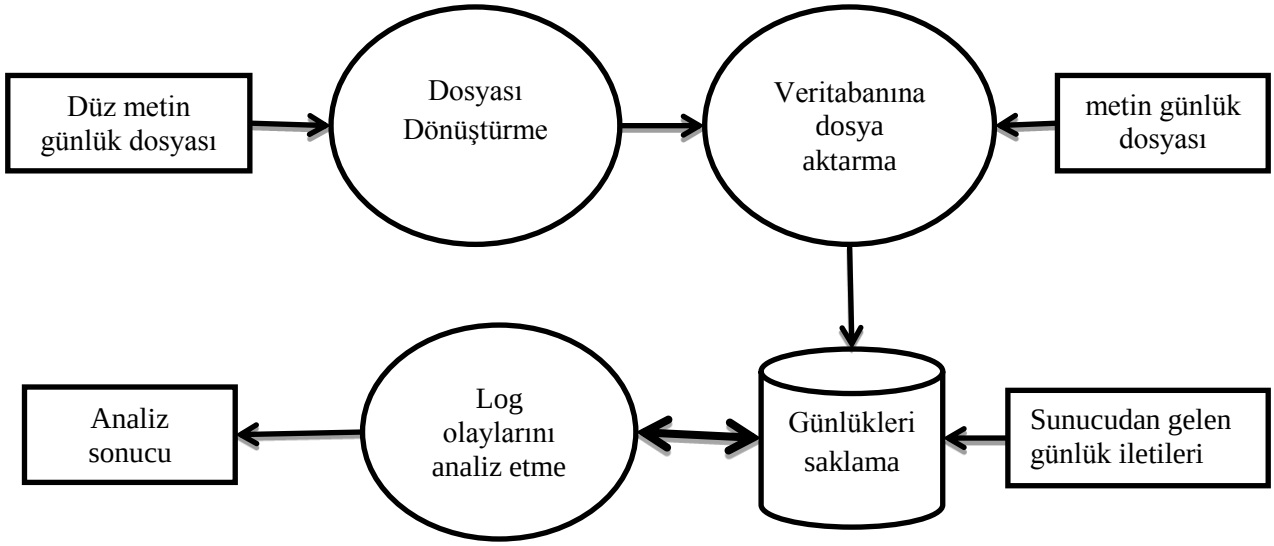
Özet olarak, farklı log yönetimi çözümleri mevcut olmasına rağmen, pek çok kuruluş çevresine ve ihtiyaçlarına özgü bir çözüm oluşturmayı ve ayarlamayı tercih eder. Birçok durumda bu yaklaşım, şirketlerin mevcut olan kaynaklardan faydalanarak ucuz bir maliyetle sistem kurması sağlanır. Bu yaklaşım, aşağıdaki avantajları beraberinde getirir:

- Bütün kuruluşun gereksinimlerinin çevre ile eşleşen bir bir çözüm elde etmesi daha fazla muhtemeldir.
- Ticari veya açık kaynak çözümleri bulunamayan olaylar gerçekleştirilebilir.
- Sistem için yeni bir platform, araç ve süreç seçilip tasarlanmaktadır.
- Sistemi elde etmek amacıyla peşin maliyet yoktur.

5. YENİ LOG ANALİZÖR SİSTEM

5.1. Sisteme Genel Bir Bakış

Bu bölümde, yeni log analyzer sistemine genel bir bakış verilerek, log mesajları çözümlemesi, logları veritabanına aktarma işlemleri, log mesajlarını analiz etme işlemi, sistemin arayüzü ve sistemi test etmek için bazı uygulamalar açıklanmaktadır. Şekil 5.1 önerilen Log File Analyzer Uygulama Sürecini ve farklı aşamalarda mimarinin bir üst düzey görünümünü göstermektedir.



Şekil 5:1 Log file analyzer genel bakış

Bu program, log mesajlar metin dosyasına kaydedildiğinde ya da log mesajlar gerçek zamanlı olarak veritabanına doğrudan gönderildiği anda, günlük mesajları üzerinde analiz yapabilir. Log mesajları veritabanına doğrudan yazılırken, dönüşüme gerek yoktur. Fakat bir dosyadan aktarma yapılacağı zaman, günlük iletileri analiz etmeden önce yapılması gereken bazı işlemler vardır.

İlk aşama, süreç günlükleri dizisi içeren bir düz metin günlük dosyasını ayrıştırma ve CSV'ye (Virgülle Ayrılmış Değerler) dönüştürmeyle başlar. CSV, yaygın olarak ticari ve bilimsel uygulamalar tarafından desteklenen ve nispeten basit bir dosya biçimidir. En yaygın kullanımlarından biri programlar arasında tablo verilerini dönüştürmektir. Bu çalışmada CSV kullanılmasının nedeni birçok program CSV'in bazı değişikliklerini desteklemektedir. Ayrıca

CSV dosyaları iki farklı mimarideki makineler arasında da veritabanı bilgilerinin değişimine ilişkin kullanılmaktadır.

İkinci aşama ise dönüştürülen CSV günlük dosyası ya da düz metin günlük dosyasının, program içine kolay bir biçimde aktarılmasıdır. CSV ya da düz metin dosyalar analiz etmeden önce bir veritabanıa aktarmak, log verileri okunmasaı ve analiz edilmesi kolaylaştırır.

Son aşamada içe aktarılan dosyaların analiz edilmesidir. Uygulama, bazı şartlara göre günlükler üzerinden arama yapabilmektedir. Aynı zamanda da gerekli sonuçları bulmak için günlük dosyasını kayıtlara filtre etmektedir. Son olarak program, raporlar oluşturmaktadır. Program Excel gibi üçüncü programa tablo verilerini aktarabilir ya da kendi içinde grafiksel olarak sonuçları gösterebilmektedir.

5.2. Log Mesajlarını Çözümleme

Bilgi sistemi tarafından oluşturulan günlük mesajları ya merkezi bir veritabanına doğrudan gönderilir ya da bir düz metin dosyasına yazılır. Log mesajları veritabanına doğrudan kaydedildiği zaman, program analiz işlemi ve raporlama için günlüklere kolayca erişebilir. Diğer taraftan, veritabanına aktarma için günlük mesajlarını dönüştürmek gerekmektedir.

Günlük iletilerini içeren dosyalar, milyarlarca ya da trilyonlarca satır ihtiva edebilir. Her satır tam bir günlük olayının kaydıdır ve bunun için, bir dosyada milyonlarca günlük kaydı bulunmaktadır. Bir günlük dosyasını analiz etmek için dosyanın veritabanına aktarılması gerekmektedir. Fakat dosya orijinal biçiminde kalırsa bu işlem yapılamamaktadır.

Günlük dosyasının veritabanına aktarılması için virgülle ile ayrılmış dosya biçimine dönüştürülmesi gerekir. CSV dosyası basit bir metin dosyasıdır. Genel olarak dosyadaki her satır ayrı bir kayıttır ve her kaydın sonu, genellikle bir satır kesici (satırbaşı / satır besleme çiftinin (0x0D, 0x0A)) gibi karakterler ile belirtilir. Her kayıt, bir set alanını kapsamaktadır. Alanlar virgül ile birbirinden ayrılmaktadır. Örneğin, günlük dosyasının tek bir satırı dönüştürülmeden önce aşağıdaki gibidir.

```
15-03-2015 10:16:34 Local0.Notice 10.81.1.2 fuhfw: NetScreen device_id=fuhfw [Root]system-notification-00257(traffic): start_time="2015-03-15 10:16:48"
```

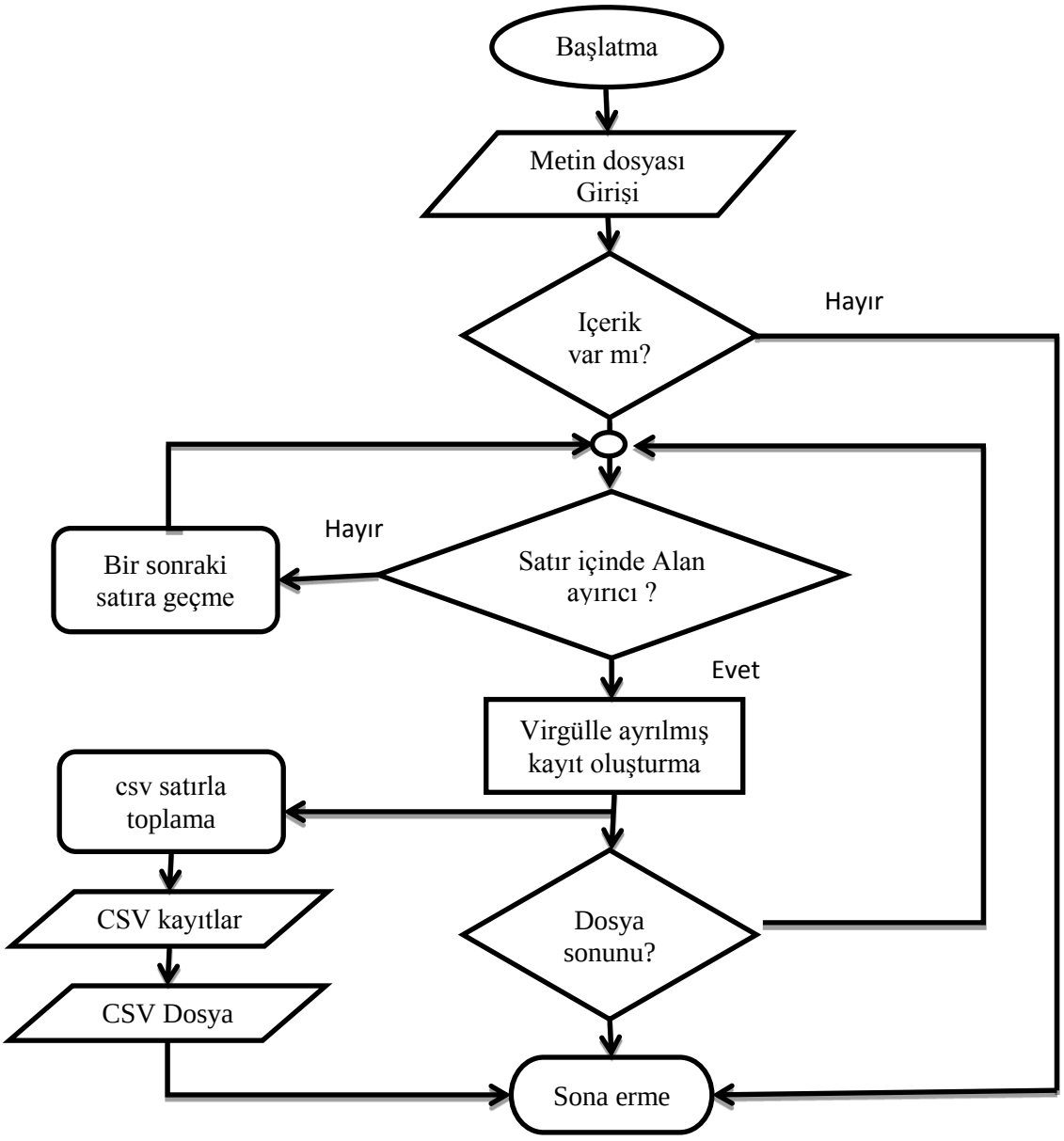
duration=0 policy_id=165 service=https proto=6 src zone=Trust dst zone=Untrust action=Permit sent=0 rcvd=0 src=10.8.12.118 dst=195.175.112.195 src_port=60415 dst_port=443 src-xlated ip=10.8.12.118 port=60415 dst-xlated ip=195.175.112.195 port=443 session_id=255089 reason=Creation<000>

Ama dönüştürme işleminden sonra aşağıdaki gibi olacaktır.

15-03-2015,10:16:34,Local0.Notice,10.81.1.2,NetScreen,start_time="2015-03-15 10:16:48",0,165,https,6,Trust,Untrust,Permit,0,0,10.8.12.118,195.175.112.195,src_port=60415 dst_port=443 src-xlated ip=10.8.12.118 port=60415 dst-xlated ip=195.175.112.195 port=443

Bu iki, örnekten kolayca anlaşılabildiği gibi, bu dönüşüm işlemi dosyadaki tüm gereksiz tekstleri kaldırıp CSV formatına dönüştürmektedir. Ayrıca dönüştürmeden sonra her satırda virgülle ayrılmış birden fazla alanı da ihtiva ettiği görülebilir. Şekil 5.2. günlük dosya dönüştürme sürecini açıklamaktadır. Günlük dosya dönüştürme algoritmasının aşamaları aşağıdaki gibidir:

- Günlük dosyasının içeriği satır satır okunmaktadır.
- Herhangi bir içerik yoksa işlemi sona erdirmekte, aksi takdirde de dosya dönüştürmesi devam etmektedir.
- Satır içinde sütun başlıklarını bulup kaldırdıktan sonra onların yerine virgül yerleştirilmektedir.
- Her satırın işlemini tamamladıktan sonra ayrı bir dosyada yeni oluşturulan satırları biriktirerek kaydetmektedir.
- Dosya sonuna ulaşıldığında süreç tamamlanır.

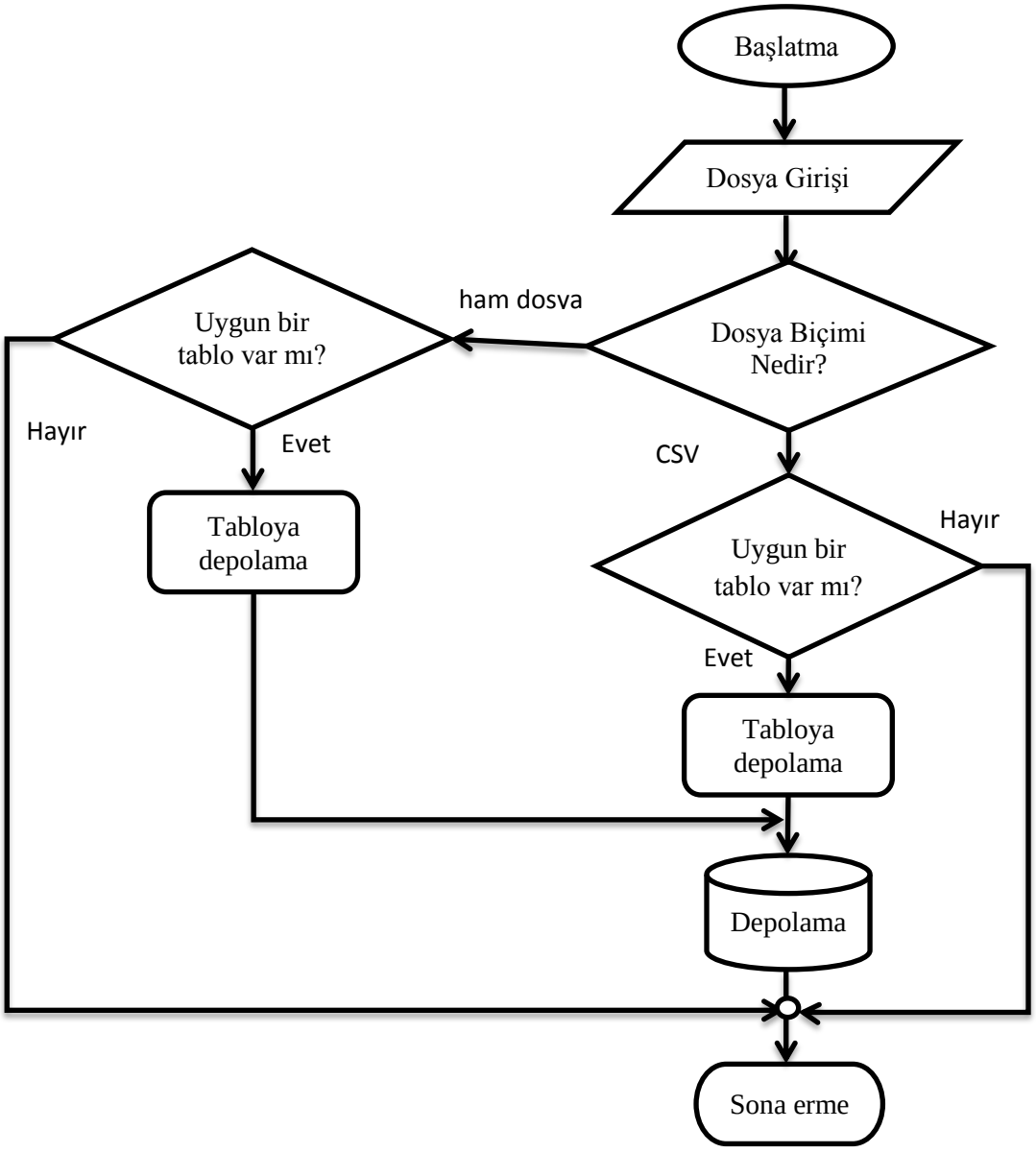


Şekil 5:2 Günlük dosyasını dönüştürme akış şeması

5.3. Çözümlenen Log Mesajlarının Veritabanına Aktarılması

Günlük dosya dönüştürme işleminden sonra veritabanında bir tabloya aktarılması gerekmektedir. Ayrıca günlüklerin tam bir analizini yapmak için program hem orijinal günlük dosyasını hem de dönüştürülen log dosyasını alması gereklidir. Ancak, en iyi analiz sonuçları CSV dosyasından çıkartılır. Dosyanın içe aktarılma süreci aşağıdaki gibidir.

- Log Dosyasını seçerek onun biçimini tespit edip uygun olan herhangi bir tablo olup olmadığının denetlenmesi.
- Herhangi bir uygun tablo olmadığı durumda işlem sona erecektir aksi halde dosya tabloya aktarılmaktadır.

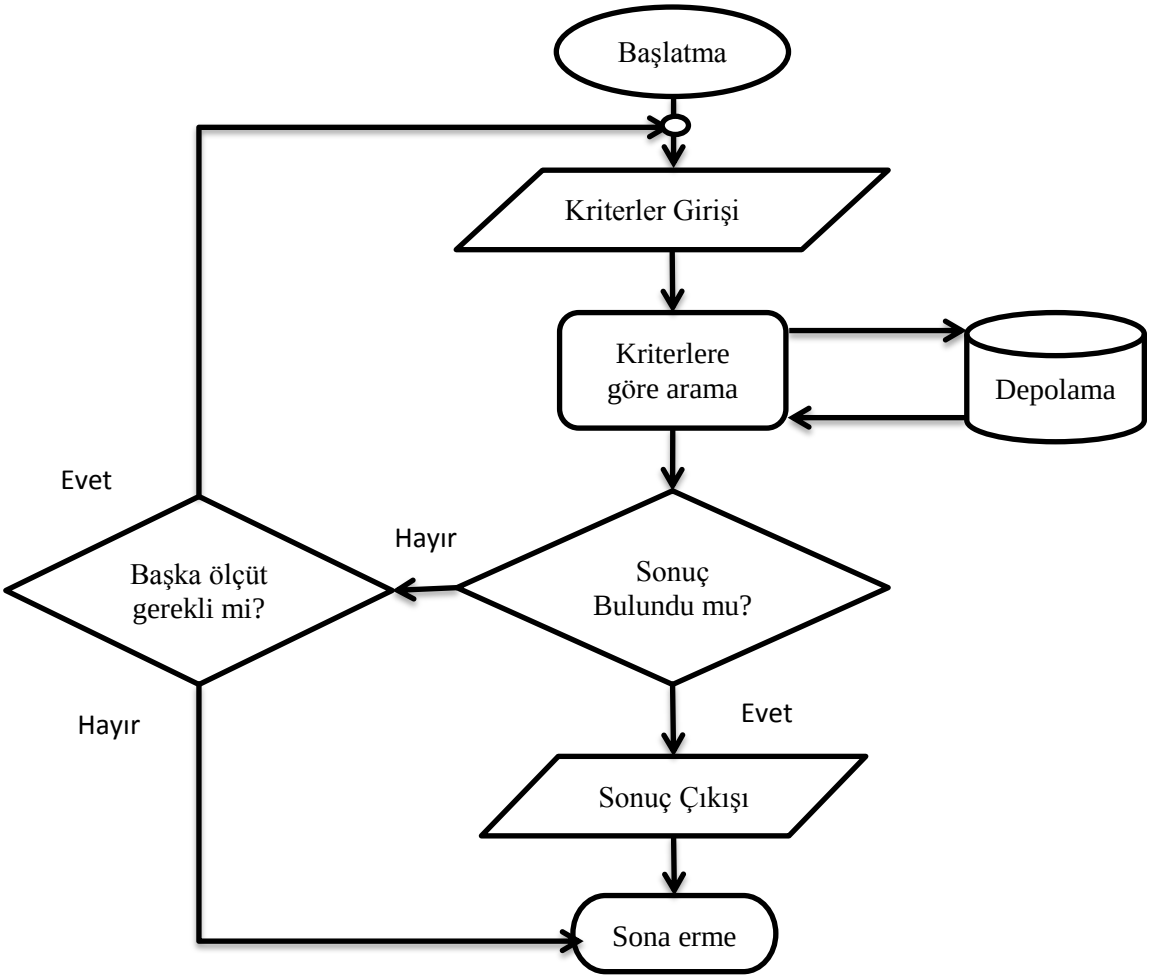


Şekil 5:3 Günlük dosyasını alma sürecinin akış şeması

5.4. Günlük Mesajlarının Analiz İşlemi

Günlük mesajları veritabanına kaydedildikten sonra, program günlük mesajlarını filtrelemek ve analiz etmek için geniş bir esneklik yelpazesi sunmaktadır. Günlük dosyasının içeriğini analiz etmek için dosyanın içeriğine göre kriterler ve ölçütler oluşturmaktadır. Şekil 5.4, akış çizelgesi sürecini göstermektedir.

- Ölçütler, günlük mesajlarını tablodan beklenen sonuçlara göre seçmektedir.
- Sonuçlar bulunmadığında, tüm tablonun aranacağı kadar ölçütler eklenir.
- Kullanılan ölçütlerin uygun olan bir sonuç veritabanı da yoksa program bir bildiri verir, aksi takdirde sonuç gösterir.



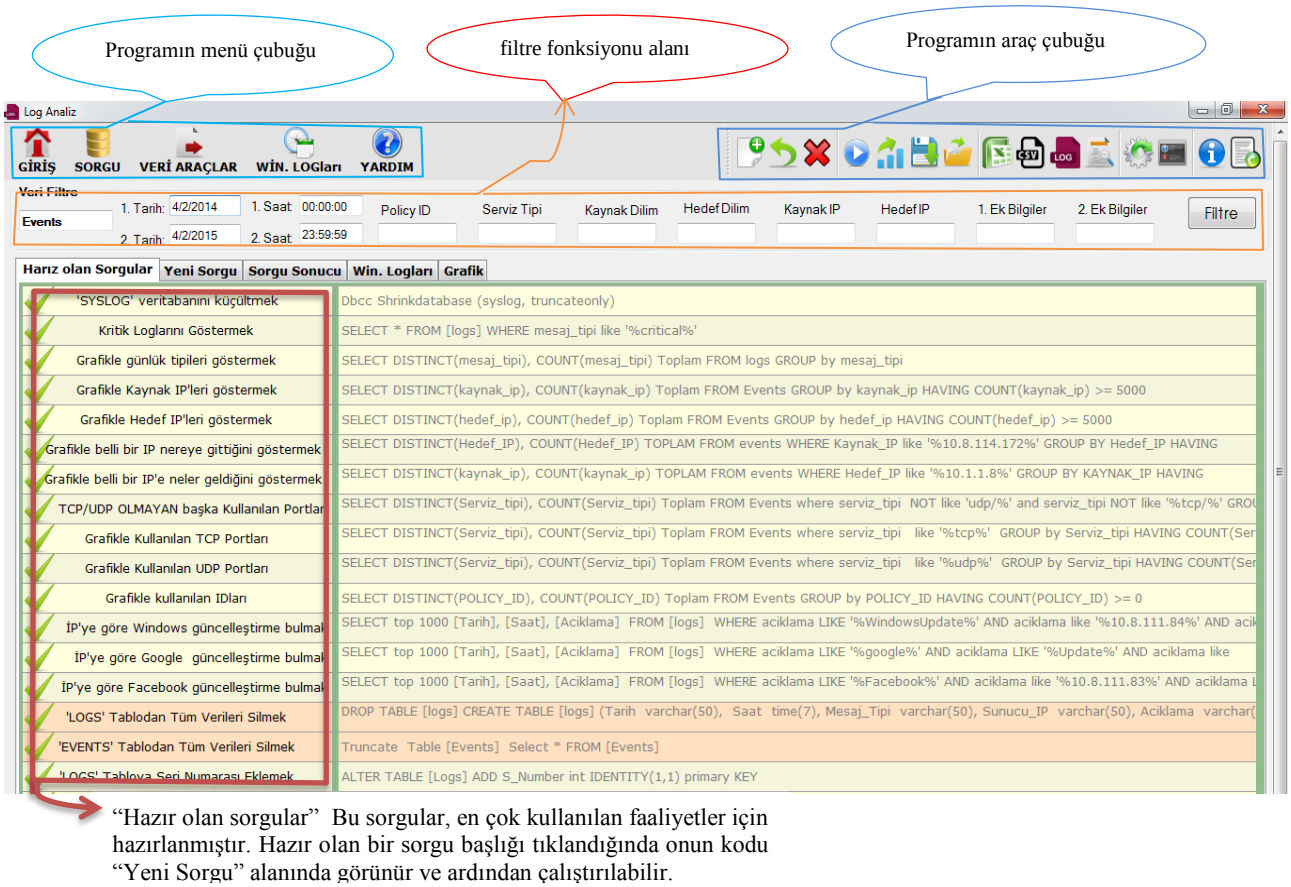
Şekil 5:4 Günlük dosyasının analiz işlemi akış şeması

5.5. Sistemin Arayüzü

Bu log analiz programı, Visual Basic .NET framework kullanılarak geliştirilen bir Windows platformu yazılım paketidir. Bu yazılım, günlük verileri depolamak ve aynı zamanda da analiz etmeyi kolaylaştırmak için SQL Server veritabanı kullanır. Program aşağıdaki özelliklere sahiptir.

- SQL veritabanını kullanarak sistemin büyük boyutlu olan log dosyalarını işlemesini kolaylaştırmak.
- Düz metin yerine tablo veya grafik formatıyla sonuçları görüntüleme.
- Günlük olaylar verilerinden alan başlıklarını ayırıp SQL veritabanında bir tabloda log verilerini yerleştirmesi.
- Çok iyi ve esnek bir filtre fonksiyonuna sahip olması.
- Bir filtre oluşturarak veya T-SQL komutlarını kullanarak kritik, uyarı ve hata gibi belirli ifadeler içeren günlük mesajlarını ya tabloyla ya da grafik ile görüntülemesi.
- Uygun bir kullanıcı arayüzü sunması.

Aşağıdaki ekran programın ana penceresini gösterir. Programın nasıl kullanılacağı hakkında daha fazla detay ekte verilmiştir.



Şekil 5:5 Sistemin Arayüzü

5.6. Uygulamalar

Sistemimiz bir arka-uç veritabanı olarak SQL kullanmaktadır. Bu sisteme aktarılan günlük verileri sorgulanarak kolayca analiz edilmesi sağlanır. Aynı zamanda veritabanı kümeleri aracılığıyla büyük günlük dosyaları için çok daha fazla bir ölçeklenebilirlik sağlanır. Bu bölümde, Transact-SQL kullanarak farklı durum analiz test sonuçları görüntülenmektedir.

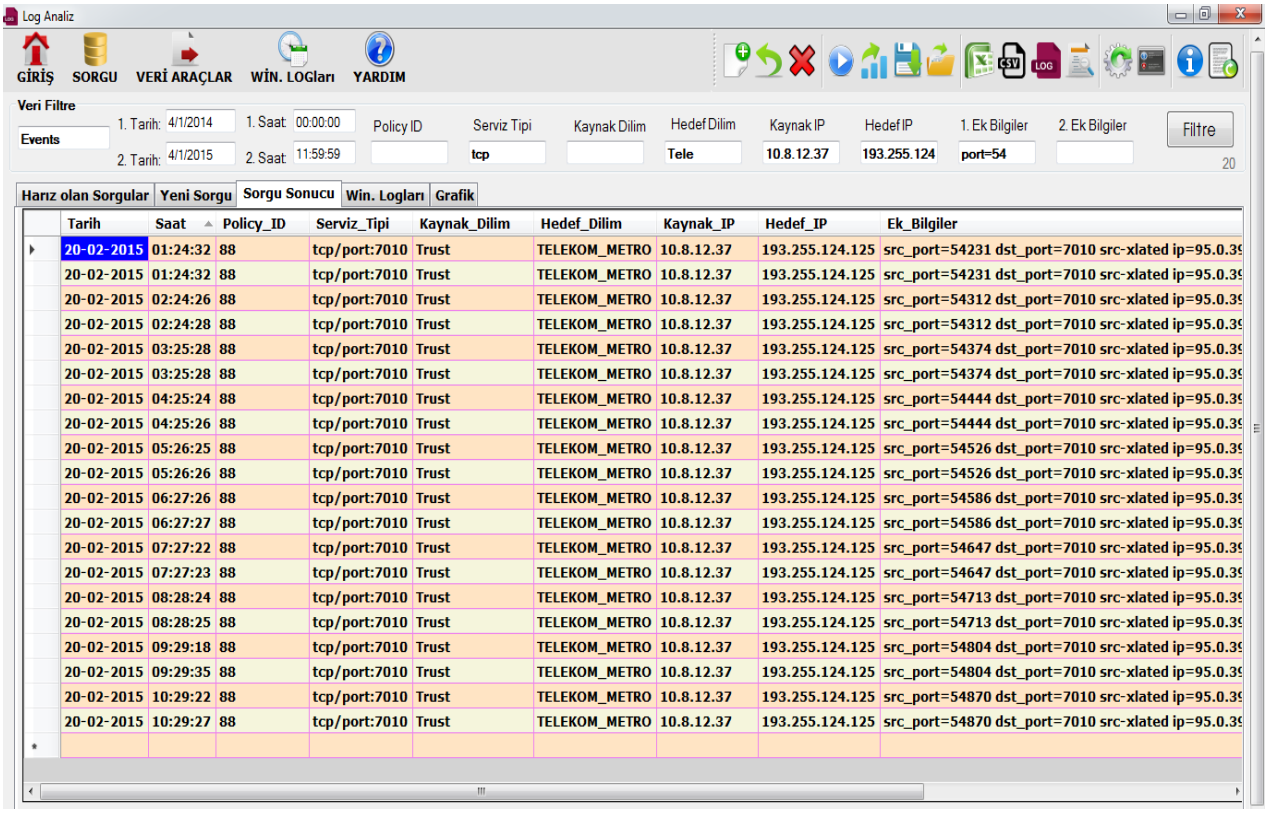
5.6.1. Uygulama 1 : Belirli bir IP adresi hareketlerinin bulunması

Bu testte, bizim sistemimizdeki belirli bir IP adresinin hareketlerini, özellikle belirli saatlerde sistemiz dışında nereye gittiğini ve hangi portları kullandığını bulmaya çalışıyoruz. Sonucu elde etmek için veritabanında bir sorgu çalıştırmanız gerekir. SQL komutlarını kullanarak sorgu yazabiliriz ancak sistem bize sorgu çalıştırmak için daha kolay bir yol da sağlar. Bu ikinci yöntemde biz sadece metin kutularına aradığımız kriterleri yazacağız ve

sistem buna göre sonuçları bulacaktır. Bu testte sonuçları bulmak için sistemin yeni bir sorgu alanına aşağıdaki Transact-SQL yazılıp çalıştırılablir.

```
SELECT [Tarih],[Saat],[Policy_ID],[Serviz_Tipi],[Kaynak_Dilim],[Hedef_Dilim],[Kaynak_IP],
[Hedef_IP],[Ek_Bilgiler] FROM events
WHERE [Saat] >= '00:00:00' AND [Saat] <= '11:59:59'
AND [Serviz_Tipi] LIKE '%tcp%'
AND [Hedef_Dilim] LIKE '%Tele%'
AND [Kaynak_IP] LIKE '%10.8.12.37%'
AND [Hedef_IP] LIKE '%193.255.124%'
AND [Ek_Bilgiler] LIKE '%port=54%'
```

Şekil 8.1'de görüldüğü gibi, sadece SQL komutu kullanılması yerine kriterleri metin kutularına yazarak da aynı sonuçları elde ettik.

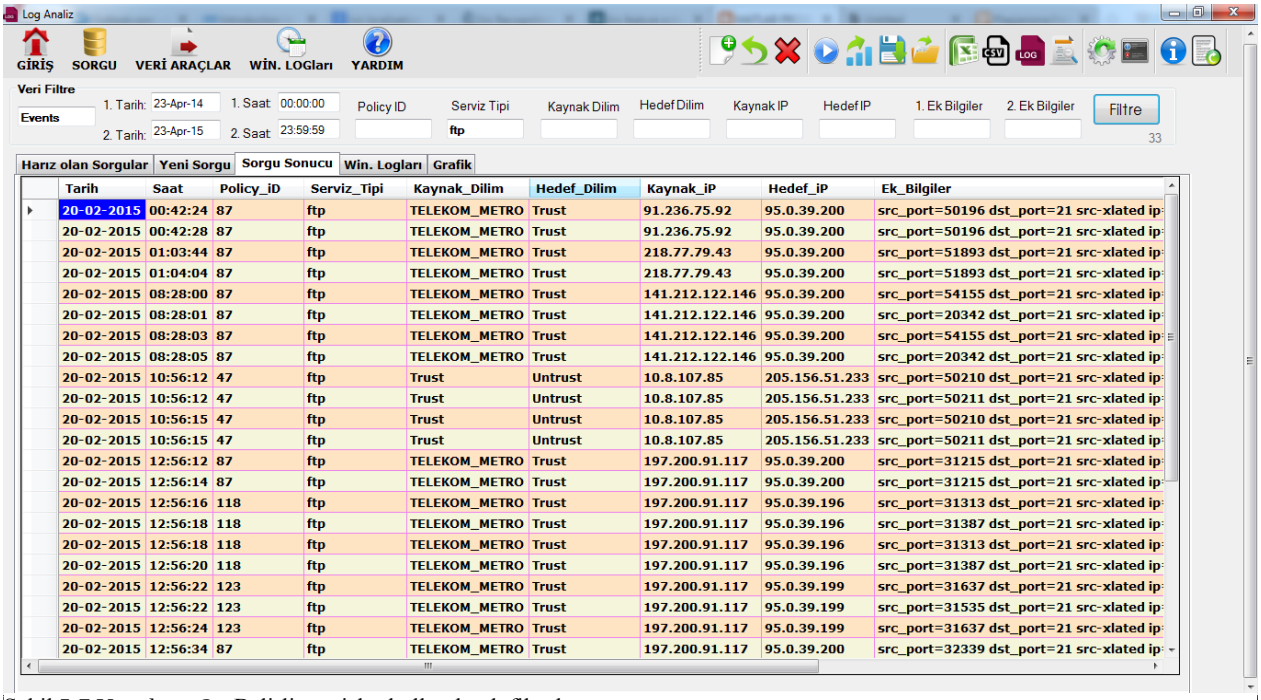


Tarih	Saat	Policy_ID	Serviz_Tipi	Kaynak_Dilim	Hedef_Dilim	Kaynak_IP	Hedef_IP	Ek_Bilgiler
20-02-2015	01:24:32	88	tcp/port:7010	Trust	TELEKOM_METRO	10.8.12.37	193.255.124.125	src_port=54231 dst_port=7010 src-xlated ip=95.0.39
20-02-2015	01:24:32	88	tcp/port:7010	Trust	TELEKOM_METRO	10.8.12.37	193.255.124.125	src_port=54231 dst_port=7010 src-xlated ip=95.0.39
20-02-2015	02:24:26	88	tcp/port:7010	Trust	TELEKOM_METRO	10.8.12.37	193.255.124.125	src_port=54312 dst_port=7010 src-xlated ip=95.0.39
20-02-2015	02:24:28	88	tcp/port:7010	Trust	TELEKOM_METRO	10.8.12.37	193.255.124.125	src_port=54312 dst_port=7010 src-xlated ip=95.0.39
20-02-2015	03:25:28	88	tcp/port:7010	Trust	TELEKOM_METRO	10.8.12.37	193.255.124.125	src_port=54374 dst_port=7010 src-xlated ip=95.0.39
20-02-2015	03:25:28	88	tcp/port:7010	Trust	TELEKOM_METRO	10.8.12.37	193.255.124.125	src_port=54374 dst_port=7010 src-xlated ip=95.0.39
20-02-2015	04:25:24	88	tcp/port:7010	Trust	TELEKOM_METRO	10.8.12.37	193.255.124.125	src_port=54444 dst_port=7010 src-xlated ip=95.0.39
20-02-2015	04:25:26	88	tcp/port:7010	Trust	TELEKOM_METRO	10.8.12.37	193.255.124.125	src_port=54444 dst_port=7010 src-xlated ip=95.0.39
20-02-2015	05:26:25	88	tcp/port:7010	Trust	TELEKOM_METRO	10.8.12.37	193.255.124.125	src_port=54526 dst_port=7010 src-xlated ip=95.0.39
20-02-2015	05:26:26	88	tcp/port:7010	Trust	TELEKOM_METRO	10.8.12.37	193.255.124.125	src_port=54526 dst_port=7010 src-xlated ip=95.0.39
20-02-2015	06:27:26	88	tcp/port:7010	Trust	TELEKOM_METRO	10.8.12.37	193.255.124.125	src_port=54586 dst_port=7010 src-xlated ip=95.0.39
20-02-2015	06:27:27	88	tcp/port:7010	Trust	TELEKOM_METRO	10.8.12.37	193.255.124.125	src_port=54586 dst_port=7010 src-xlated ip=95.0.39
20-02-2015	07:27:22	88	tcp/port:7010	Trust	TELEKOM_METRO	10.8.12.37	193.255.124.125	src_port=54647 dst_port=7010 src-xlated ip=95.0.39
20-02-2015	07:27:23	88	tcp/port:7010	Trust	TELEKOM_METRO	10.8.12.37	193.255.124.125	src_port=54647 dst_port=7010 src-xlated ip=95.0.39
20-02-2015	08:28:24	88	tcp/port:7010	Trust	TELEKOM_METRO	10.8.12.37	193.255.124.125	src_port=54713 dst_port=7010 src-xlated ip=95.0.39
20-02-2015	08:28:25	88	tcp/port:7010	Trust	TELEKOM_METRO	10.8.12.37	193.255.124.125	src_port=54713 dst_port=7010 src-xlated ip=95.0.39
20-02-2015	09:29:18	88	tcp/port:7010	Trust	TELEKOM_METRO	10.8.12.37	193.255.124.125	src_port=54804 dst_port=7010 src-xlated ip=95.0.39
20-02-2015	09:29:35	88	tcp/port:7010	Trust	TELEKOM_METRO	10.8.12.37	193.255.124.125	src_port=54804 dst_port=7010 src-xlated ip=95.0.39
20-02-2015	10:29:22	88	tcp/port:7010	Trust	TELEKOM_METRO	10.8.12.37	193.255.124.125	src_port=54870 dst_port=7010 src-xlated ip=95.0.39
20-02-2015	10:29:27	88	tcp/port:7010	Trust	TELEKOM_METRO	10.8.12.37	193.255.124.125	src_port=54870 dst_port=7010 src-xlated ip=95.0.39

Şekil 5:6 Uygulama 1 - Belirli bir IP adresi hareketleri

5.6.2. Uygulama 2: Servisler kullanılarak filtreleme

Bu ikinci test PC-Anywhere gibi belirli servisler kullanarak sistemimize erişim kuran kişileri araştırmaktadır. Bu uygulamada yine şekil 5.8 gösterildiği gibi herhangi bir T-SQL komutu yazmadık, bunun yerine metin kutusundaki kriterler yazılmıştır.

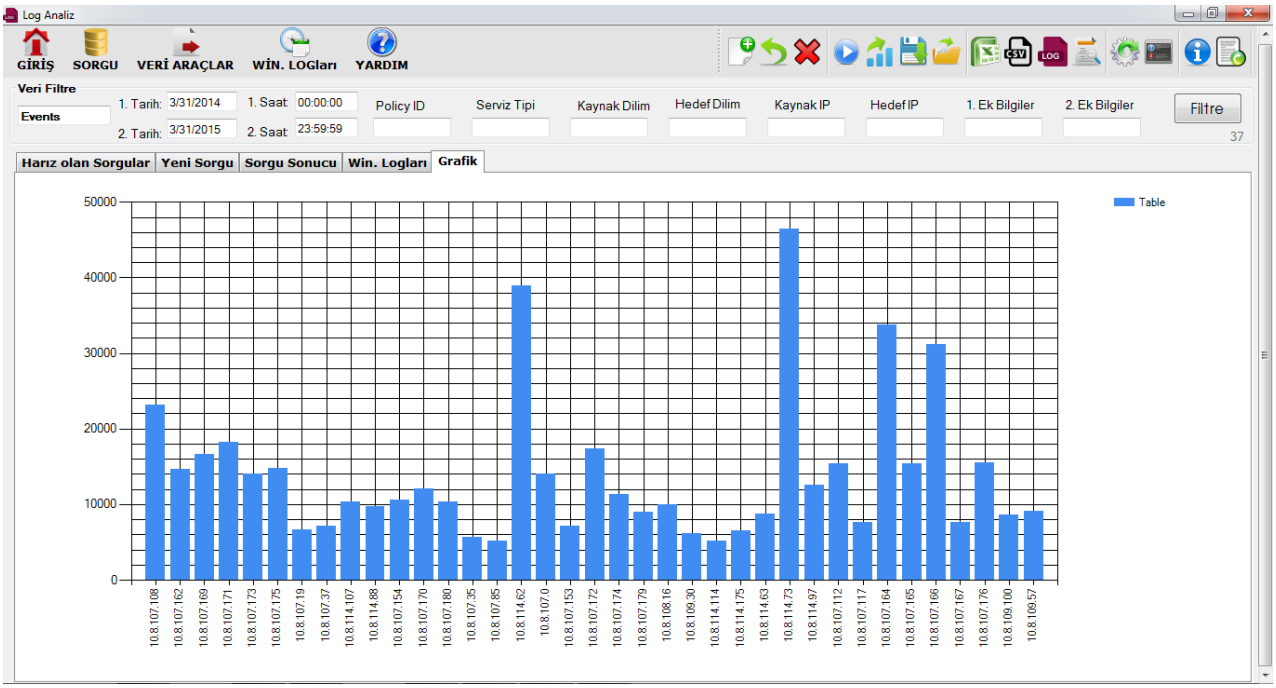


Tarih	Saat	Policy_iD	Serviz_Tipi	Kaynak_Dilim	Hedef_Dilim	Kaynak_iP	Hedef_iP	Ek_Bilgiler
20-02-2015	00:42:24	87	ftp	TELEKOM_METRO	Trust	91.236.75.92	95.0.39.200	src_port=50196 dst_port=21 src-xlated ip
20-02-2015	00:42:28	87	ftp	TELEKOM_METRO	Trust	91.236.75.92	95.0.39.200	src_port=50196 dst_port=21 src-xlated ip
20-02-2015	01:03:44	87	ftp	TELEKOM_METRO	Trust	218.77.79.43	95.0.39.200	src_port=51893 dst_port=21 src-xlated ip
20-02-2015	01:04:04	87	ftp	TELEKOM_METRO	Trust	218.77.79.43	95.0.39.200	src_port=51893 dst_port=21 src-xlated ip
20-02-2015	08:28:00	87	ftp	TELEKOM_METRO	Trust	141.212.122.146	95.0.39.200	src_port=54155 dst_port=21 src-xlated ip
20-02-2015	08:28:01	87	ftp	TELEKOM_METRO	Trust	141.212.122.146	95.0.39.200	src_port=20342 dst_port=21 src-xlated ip
20-02-2015	08:28:03	87	ftp	TELEKOM_METRO	Trust	141.212.122.146	95.0.39.200	src_port=54155 dst_port=21 src-xlated ip
20-02-2015	08:28:05	87	ftp	TELEKOM_METRO	Trust	141.212.122.146	95.0.39.200	src_port=20342 dst_port=21 src-xlated ip
20-02-2015	10:56:12	47	ftp	Trust	Untrust	10.8.107.85	205.156.51.233	src_port=50210 dst_port=21 src-xlated ip
20-02-2015	10:56:12	47	ftp	Trust	Untrust	10.8.107.85	205.156.51.233	src_port=50211 dst_port=21 src-xlated ip
20-02-2015	10:56:15	47	ftp	Trust	Untrust	10.8.107.85	205.156.51.233	src_port=50210 dst_port=21 src-xlated ip
20-02-2015	10:56:15	47	ftp	Trust	Untrust	10.8.107.85	205.156.51.233	src_port=50211 dst_port=21 src-xlated ip
20-02-2015	12:56:12	87	ftp	TELEKOM_METRO	Trust	197.200.91.117	95.0.39.200	src_port=31215 dst_port=21 src-xlated ip
20-02-2015	12:56:14	87	ftp	TELEKOM_METRO	Trust	197.200.91.117	95.0.39.200	src_port=31215 dst_port=21 src-xlated ip
20-02-2015	12:56:16	118	ftp	TELEKOM_METRO	Trust	197.200.91.117	95.0.39.196	src_port=31313 dst_port=21 src-xlated ip
20-02-2015	12:56:18	118	ftp	TELEKOM_METRO	Trust	197.200.91.117	95.0.39.196	src_port=31387 dst_port=21 src-xlated ip
20-02-2015	12:56:18	118	ftp	TELEKOM_METRO	Trust	197.200.91.117	95.0.39.196	src_port=31313 dst_port=21 src-xlated ip
20-02-2015	12:56:20	118	ftp	TELEKOM_METRO	Trust	197.200.91.117	95.0.39.196	src_port=31387 dst_port=21 src-xlated ip
20-02-2015	12:56:22	123	ftp	TELEKOM_METRO	Trust	197.200.91.117	95.0.39.199	src_port=31637 dst_port=21 src-xlated ip
20-02-2015	12:56:22	123	ftp	TELEKOM_METRO	Trust	197.200.91.117	95.0.39.199	src_port=31535 dst_port=21 src-xlated ip
20-02-2015	12:56:24	123	ftp	TELEKOM_METRO	Trust	197.200.91.117	95.0.39.199	src_port=31637 dst_port=21 src-xlated ip
20-02-2015	12:56:34	87	ftp	TELEKOM_METRO	Trust	197.200.91.117	95.0.39.200	src_port=32339 dst_port=21 src-xlated ip

Şekil 5:7 Uygulama 2 - Belirli servisler kullanılarak filtreleme

5.6.3. Uygulama 3: Dışarıdan giriş yapan İP adreslerinin grafik olarak gösterilmesi

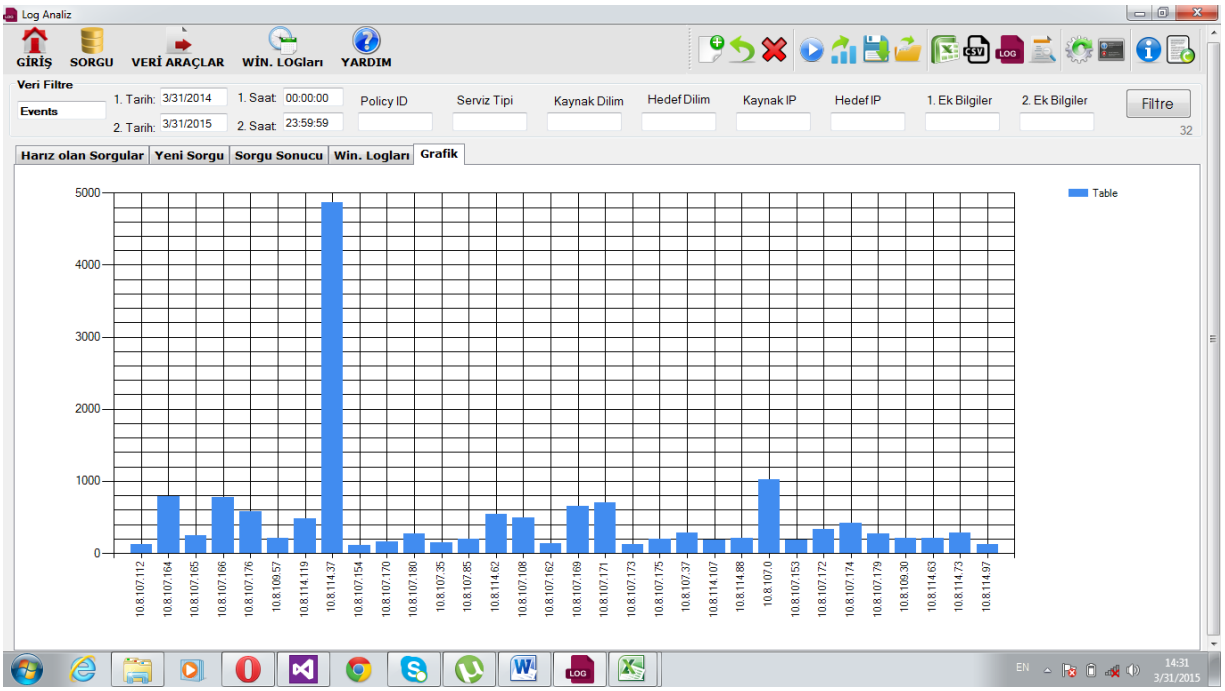
Üçüncü testimizin amacı bilgi sistemimize dışardan gelen İP adreslerini grafik olarak gösterilmesidir. Bu sorgulama filtre sistemimize internet üzerinde gelen İP adreslerinin hareketlerini ve hangisinin daha çok tehdit ihtiva ettiğini göstermektedir. Aşağıdaki şekil 5.8 sistemimize gelen başka İP'lerin rakamlarını ve her birisine toplamda kaç defa erişim yaptığını grafikle göstermektedir.



Şekil 5:8 Uygulama 3 - İP adreslerinin grafik olarak gösterilmesi

5.6.4. Uygulama 4: Bir İP adresinin hangi İP adreslerine erişim yaptığının grafikle gösterilmesi

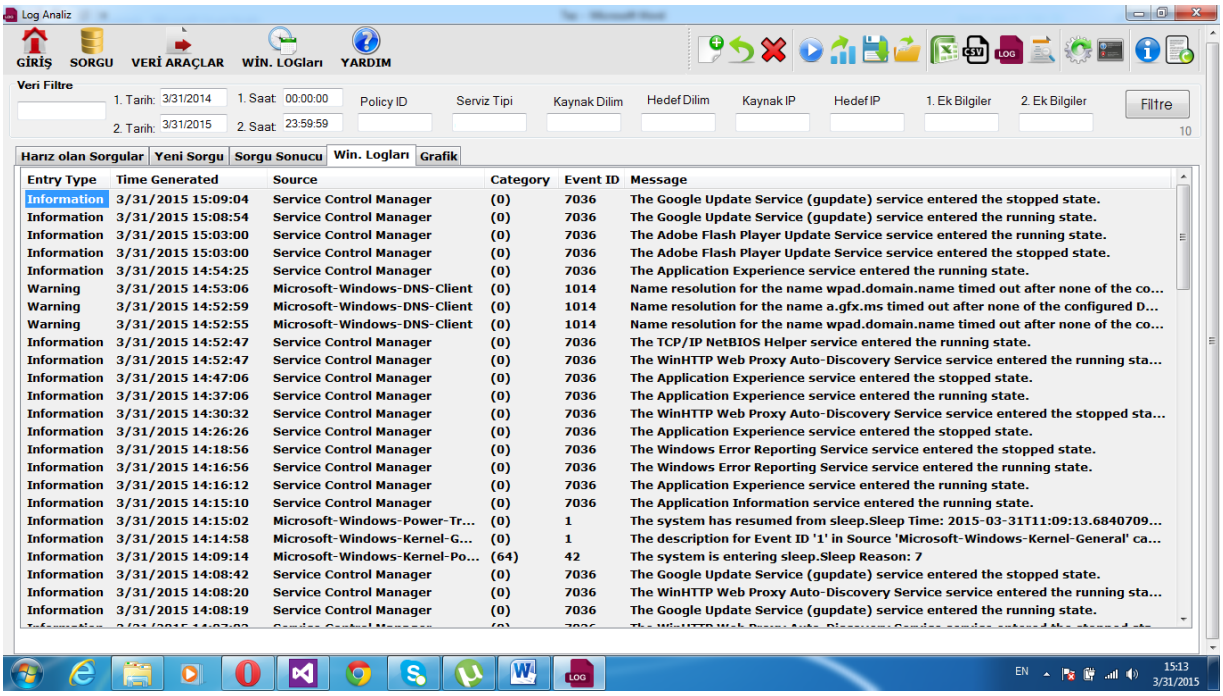
Bu test özel bir İP adresine hangi İP adreslerinin erişimde bulunduğunu ve iletişim yaptığını grafikle göstermek amacıyla verilmiştir. Bu sorgulamada belirli bir İP adresine sık sık gelen başka İP adreslerinin hareketleri ve hangi İP adresinin daha çok iletişime geçtiğini göstermektedir. Aşağıdaki şekil 5.9, bir İP adresine gelen başka İP'lerin rakamlarını ve her birisine toplam kaç defa erişim yaptığını grafikle göstermektedir.



Şekil 5:9 Uygulama 4 – Belirli bir İP adresinin hangi İP adreslerini erişim yaptığının grafikle gösterilmesi

5.6.5. Uygulama 5: Windows olay günlüklerinin görüntülenmesi

Bu testte de, Windows Olay günlüğünün aranması için sistemin komutlarından biri kullanılacaktır. Bu komut, Windows (sistem veya uygulama) olay günlüklerini görüntülemek için kullanılır. Windows Olay günlüğü önemli yazılım ve donanım olaylarını kaydetmek için uygulamalarda standart ve merkezi bir yol sağlar. Dolayısıyla Şekil 5.10 kişisel bir bilgisayardan yakalanan Windows günlük olaylarının listesini göstermektedir.



Şekil 5:10 Uygulama 5 Windows olay günlüklerinin görüntülenmesi

6. SONUÇ

Daha önceki bölümlerde de açıklandığı gibi log yönetimi ve analizi sistem yönetimi, sorun giderme, güvenlik saldırılarına karşı korunma, adli bilişim, standartlar ve kanun düzenlemeleri uygulaması yürütmeleri için önemli bir araçtır. Bu nedenle, bir uçağın kara kutusu ne kadar önemli ise çok benzer bir şekilde bilişim sistemleri için ayrıntılı log tutmak ve log yönetimi gerçekleştirmek aynı derecede önemlidir. Hiç şüphe yok ki sadece log tutmak tek başına pek birşey ifade etmez. Yani, nasıl tarladan toplanan hasat işlenmeden önce tüketici için bir anlam ifade etmiyorsa, toplanıp ve değerlendirilmeyen loglar için de aynı ifade geçerlidir. Bundan dolayı, toplanan loglara göre en uygun yazılımı kullanarak log verilerinin analizinin gerçekleştirilmesi ve log yönetim politikası ile birlikte yorumlanması gerekmektedir.

Daha önceden değinildiği gibi, log analizi yapmak amacıyla kullanılabilen iki tür çözüm vardır. Bunlardan birisi loglar oluşturulurken gerçek zamanlı log olaylarını izleme çözümleri ve diğeri de bir metin dosyasında depolanan log iletilerini sonradan analiz edebilen çözümlerdir. Bu tez çalışması da, bilgi sistemi üzerinde kullanılan sunucular tarafından ve ağ cihazları trafından üretilen günlük kayıtlarını ve metin dosyalarında bulunan günlük iletilerini alıp veritabanına kaydedilebilen ve aynı zamanda analiz edebilen bir log analiz programının tasarlamasını ve geliştirilmesini amaçlamaktadır.

Literatürde daha önceden verilen çözüm tekniklerinin eksik kalan bazı sorunlarının giderilmesi üzerinde çalışılmıştır. Aşağıda verilenler sistemimiz tarafından çözülen sorunları vermektedir.

- **Dosya Boyutu**: Milyonlarca log olayları içerdiğinden dolayı metin log dosyalarının boyutu çok büyüktür. Bu sorunu çözmek için SQL veritabanı kullanılarak sistemdeki büyük boyutlu olan log dosyaları işlenebilmektedir.
- **Satır Genişliği**: Log olaylarını içeren satırlar bazen çok uzun olabilmektedir. Ayrıca gereksiz tekstler veya tekrarlanan bir veri paketi olabilir. Uzun satırları azaltmak, gereksiz ve kopya verilerini ortadan kaldırmak için önerdiğimiz çözümler oldukça verimli çalışmaktadır.

- **Sütun başlığı**: Syslog sunucusu metin dosyasına günlük olayları kaydederken, her satır log olayınını tek bir kaydını temsil eder. Bu günlük olay kaydı birden fazla alan oluşturmaktadır. Ancak bu alanların başlıkları her satırda diğer veriler ile karıştırılır. Sistemimiz diğer verilerden alan başlıklarını ayırıp SQL veritabanındaki bir tabloda log verilerini yerleştirir. Bu da özel kriterlere göre tablo içerikleri sorgulanmasını ve filtrelenmesini kolaylaştırır. Ayrıca bu yöntem, düz metin yerine sekmeli biçimde sonuçları görüntüleme olanağı da vermektedir.
- **Grafik görüntüleme**: Metin dosyasından bir grafik görüntüsü oluşturmak kolay bir süreç değildir. Sistem tasarımcısı için önemli olan sonuçlara ulaşmak ve bu sonuçları elde etmek için sistemin, metin dosyasını tablo biçimine dönüştürdükten sonra grafik sonuçlarını da görüntüleme özelliği vardır.
- **Gerçek zaman analizi**: Bilgi sisteminin ağ içerisinde trafik sıkıntısına yol açmadığı durumlarda, log mesajlarını oluşturulurken logları alıp veritabanına kaydederek gerçek zamanlı bir günlük analizi gerçekleştirebilmektedir.
- **Windows olay günlükleri görüntüleme**: Windows, kendine göre sistemlerden ve uygulamalardan olay günlüklerini oluşturur. Bu program sayesinde Windows olay günlükleri de görüntülenebilmektedir.

Bu log analiz programını çok daha verimli hale getirmek için gelecekte programa eklenebilecek bazı özellikler şunlardır:

- Programanın birden fazla platformu (UNIX ve UNIX gibi platformlar) desteklemesinin sağlanması.
- Daha fazla arama kriterinin analizi için daha özel bir çözüm geliştirilebilir.

7. KAYNAKLAR

[1]. Radack, S. (2006), “log management: using computer and network records to improve information security”, Information Technology Laboratory.

[2]. Alert logic, Inc. (2011), “Log management best practices: the benefits of automated log management”

[3]. Chuvakin, A. (2011), “The Complete Guide to Log and Event Management”, [White Paper]

[4]. Anton A. Chuvakin, Kevin J. Schmidt, Christopher Phillips “Logging and Log Management: The Authoritative Guide to Understanding the concepts Surrounding Logging and Log Management”, 2013

[5]. Flowerfire (2013), “Sawmill Log Analyzer Best Practices” [White Paper]

[6]. Splunk Inc (2015), “Splunk Enterprise Overview”, Splunk Enterprise 6.2.3

[7]. http://www.retrospective.centeractive.com/content/library#whitepapers

[8]. Raab, H. (2011), “LogExpert Documentation”, CodePlex Project Hosting for Open Source Software

[9]. Postel, J., "Internet Protocol", STD 5, RFC 791, September 1981.

[10]. The CEE Editorial Board "Common Event Expression, Architecture Overview Version 0.5", May 2010

[11]. http://www.counterpane.com/log-analysis.html

[12]. Rehman, W., "Introduction to Syslog Protocol" March 2003.

[13]. http://www.linux.org/apps/all/Administration/Log_Analyzers

[14]. RFC 3164, The BSD Syslog Protocol

[15]. Gerhards R. "RFC 5424". The Syslog Protocol.

[16]. RFC 3195, Reliable Delivery for Syslog

[17]. "LXer: Patent jeopardizes IETF Syslog standard".

[18]. http://en.wikipedia.org/wiki/Syslog

[19]. http://www.w3.org/TR/WD-logfile.html

[20]. http://httpd.apache.org/docs/current/logs.html

[21]. http://www.cisco.com/en/US/docs/security/ips/specs/CIDEE_Specification.htm

[22]. Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", RFC 2234, November 1997.

[23]. Lockhart, A. "Ağ Güvenliği İpuçları", Windows, Linux, BSD için, Şubat 2006.

[24]. USA Standard Code for Information Interchange, USASI X3.4-1968.

[25]. Postel, J., "User Datagram Protocol", STD 6, RFC 768, August 1980.

[26]. Baker, F., "Requirements for IP Version 4 Routers", RFC 1812, June 1995.

[27]. http://www.rsyslog.com/module-Static_Docs-view-f-features.html.phtml

[28]. Karen Kent and Murugiah Souppaya (2006), "Guide to Computer Security Log Management", NIST Special Publication 800-92.

[29]. Marcus Ranum Logging Laws available at http://ranum.com/security/computer_security/archives/logging-notes.pdf (retrieved May 2012).

[30]. ÖNAL, H. (2009), "Standartlar ve Güvenlik Açısından Log Yönetimi", Beyazsapka dergisi

[31]. Mockapetris, P., "Domain Names - Concepts and Facilities", STD 13, RFC 1034, November 1987.

[32]. Mockapetris, P., "Domain names - Implementation and Specification", STD 13, RFC 1035, November 1987.

8. EKLER

8.1. Kullanıcı Kılavuzu

8.1.1. Yazılım ve Donanım Gereksinimleri

Programın tavsiye edilen donanım ve yazılım ihtiyacı:

- Intel I3 işlemci ve üstü
- 4 GB Ram ve üstü
- 256 MB Ram ekran kartı
- 1024x768 çözünürlüğü destekleyen ekran
- 10 GB boş hard disk alanı
- Windows XP, Windows XP Professional x64, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 ve Windows Server 2012 R2.
- Microsoft .NET Framework 4.5 (x86 and x64)
- Microsoft Excel (sonuçları aktarmak için)
- Microsoft SQL Server 2008 ve üstü (Veritabanı olarak)

8.1.2. Yazılım Kurulumu

Bu program, Windows işletim sistemi için hazırlanmıştır. Tüm 32, 64 ve 86 bit işletim sistemlerinde çalışabilir. Programı yüklemek için, kurulum dosyasını tıklayarak yerleştirme adımları tamamlanana kadar devam edin. Programın eski versiyonu sistemden kaldırmak istiyorsan, Control Panel→Add/Remove Programs ile kullanabilirsin.

Programı yüklemeden önce veya sonrasında, veritabanı tabloları oluşturulmaktadır. Program için üç temel tablolar Bulunmaktadır. “MSSQL Server Management Studio” kullanarak bu tablolar oluşturabilirsin. Kullanılan tablolarının yapısı Sekil 8-1’de verilmistir.

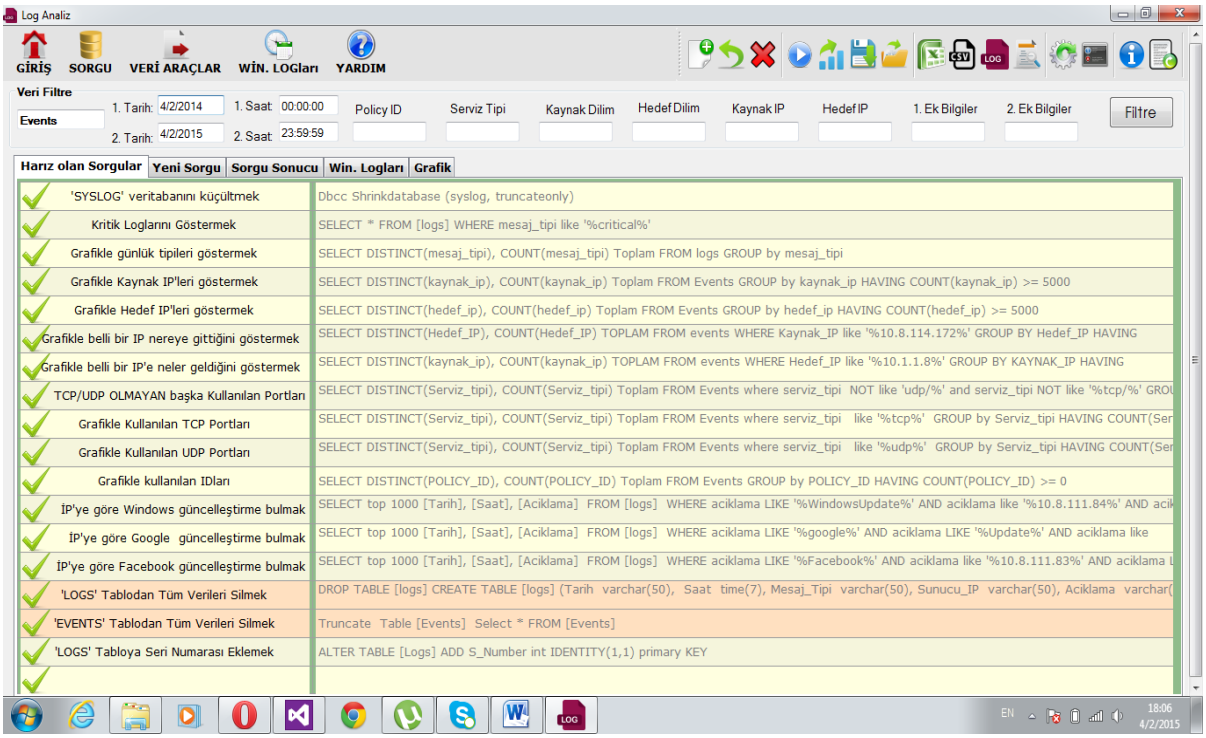
Şekil 8-1 Sistemin veritabanı yapısı

8.1.3. Giriş

Şekil 8-2 Programın giriş ekranı

Programa giriş yapılabilmesi için geçerli bir kullanıcı adı ve şifre olması gerekmektedir. Kullanıcı adı ve şifresi de program yönetici tarafından vermektedir.

8.1.4. Sistem Menüsü ve arayüzü



Şekil 8-3 programın ana ekranı

Sisteme giriş yaptıktan sonra 8.2 şekildeki gösterilen pencere ekranına gelmektedir. Bu pencere programın ana sayfasıdır. Ana sayfanın sol üst köşesinde programın komutları temsil eden farklı menüler bulunmaktadır.

Programın Menülerin düzeyi şöyledir.

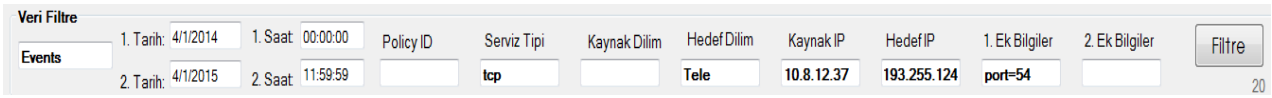
- GİRİŞ
  - *Yeni sorgu (Ctrl+N)*: yeni bir sorgu yazmak için "Yeni Sorgu" kod alanını açar.
  - *Kapat (Ctrl+K)* : ana sayfayı kapatıp program giriş sayfaya döner.
  - *Çıkış (Ctrl+F4) :* programı tamamen kapattır.
  - *Dosya Dönüştürme:* Metin dosyası CSV'a dönüştüren kodu çalıştırır.
- SORGU
  - *Sorguyu Çalıstrıma (F5):* veritabanından bir sorgu olarak "Yeni Sorgu" sekmesinde yazılan kodları çalıştırıp sonucu tabloyla gösterir.

- *Grafikle Gösterme (Ctrl+G):* veritabanından bir sorgu olarak "Yeni Sorgu" sekmesinde yazılan bazı kodları çalıştırıp sonucu grafikle gösterir.
- *Bir Sorgu Kaydetme (Ctrl+S):* daha sonra kullanılmak üzere "Yeni Sorgu" sekmesinde yazılmış sorgu bir metin dosyasına kaydeder.
- *Bir Sorgu Açma (Ctrl+O):* programda çalıştırmak için metin dosyaları sorguları açıp "Yeni Sorgu" sekmesinde yerleştirir.

- VERİ ARAÇLAR
  - *Excel'e Aktar:* "Sorgu Sonucu" sekmesinde bulunan sonuçları Excel'e Aktar.
  - *Bir (.CSV) Dosya İçeri Alın:* sistem içine CSV dosyasını aktar.
  - *Metin Bir Log Dosya İçeri Alın:* CSV dosya biçimine dönüştürülmemiş metin dosyaları sistem içine aktar.
  - *Uyarı Logları İnceleyin:* CSV dosya biçimine dönüştürülmemiş metin dosyaları inceleme sayfası açar.
- WİN. LOGLARI
  - *Sistem Logları*: "Win. logları" sekmesinde Windows sistem günlüğü olayları gösterir.
  - *Uygulama Logları*: "Win. logları" sekmesinde Windows uygulama günlüğü olayları gösterir.
- YARDIM
  - *Projeyle İlgili*: program hakkında kısa bir bilgi verir.
  - *Nasıl Kullanılır*: programın nasıl kullanıldığını içeren dosyayı açar.

Bu program aynı zamanda menülerdeki tüm komutları içeren bir araç çubuğu sağlamaktadır. Araç çubuğu ana pencerenin sağ üst kenarında yer almaktadır.

Ana menü altında farklı metin kutuları bulunmaktadır. Günlük iletilerini içeren tabloyu filtrelemek için kod yazma yerine bu metin kutular kullanılır.



Program ayrıca hazır olan sorgular da içerir. Bu sorgular, en çok kullanılan faaliyetler için yararlıdır. Bir hazır olan sorgu başlığını tıkladığınızda onun kodu "Yeni Sorgu" alanında görünür ve ardından çalıştırılabilir. Hazır olan sorgular, ana penceresinin orta sol tarafında özelikle "Hazır olan sorgular" sekmesinin altında bulunmaktadır.

8.1.5. Klavye Kısayolları

Tablo 8-1 Programın klavye kısayolları

Ctrl + N	Yeni bir sorgu penceresi gösterir.
Ctrl + K	Aktif pencereyi kapatır.
Alt + F4	Programından çıkış yapar.
F5	Sorguları çalıştırır
Ctrl + G	Sonuçları grafikle gösterir.
Ctrl + S	Sorgular metin dosyasına kaydet eder.
Ctrl + O	Sorgular metin dosyasından açar
Ctrl + T	Sonuçları Excel'e aktarır.

8.1.6. Bazı Önemli olan Kaynak Kodu

A. Programın Temel Tabloların Kodu

Kullanıcılar tablosu

```
Use Syslog
drop table users
CREATE TABLE Users
```

```
(
ID                  int IDENTITY(1,1) primary KEY,
Kullanici_Adi       varchar(50),
Parola              varchar(50),
Kullanici_Tipi      varchar(50),
)
```

Ham günlük dosyası tablosu

```
Use Syslog
Drop table logs
CREATE TABLE logs
(
Tarih           varchar(50),
Saat            time(7),
Mesaj_Tipi      varchar(50),
Sunucu_IP       varchar(50),
Aciklama        varchar(MAX)
)
```

Dönüştürülen günlük dosyası tablosu

```
use syslog
drop table Events
CREATE TABLE Events
(
Tarih           varchar(50),
Saat            time(7),
Mesaj_Tipi      varchar(50),
Sunucu_IP       varchar(50),
Sunucu_Adi      varchar(50),
Aciklama        varchar(MAX),
Süre            varchar(50),
Policy_id       varchar(50),
Serviz_Tipi     varchar(50),
Proto           varchar(50),
Kaynak_Dilim    varchar(50),
Hedef_Dilim     varchar(50),
Faaliyet        varchar(50),
goderildi       varchar(50),
```

RCVD	**varchar(50),**
Kaynak_ip	**varchar(50),**
Hedef_ip	**varchar(50),**
Ek_Bilgiler	**varchar(MAX))**

B. Csv Formatına Metin Dosyası Dönüştürme

```
use strict;
use warnings;
open my $in_fh, '<', 'd:/Syslogd/logs/logs' or die "failed to open 'd:/syslogd/logs/logs' <$!>";
open my $out_fh, '>', 'd:\logs\events.csv' or die "failed to open 'd:\logs\events.csv' <$!>";
while (my $line = <$in_fh>) {
   if ($line =~ /^
           (\S+) \s+
           (\S+) \s+
               (\S+) \s+
               (\S+) \s+
               fuhfw:\s (\S+) \s+
               .+: \s (.+?) \s+
               duration= (.+?) \s+
               policy_id= (.+?) \s+
               service= (.+?) \s+
               proto= (.+?) \s+
               src \s zone= (.+?) \s+
               dst \s zone= (.+?) \s+
               action= (.+?) \s+
               sent= (.+?) \s+
               rcvd= (.+?) \s+
               src= (.+?) \s+
               dst= (.+?) \s+
                    (.+) \s+
                    (session.+)(.+)
                    (reason.+)(.+)
              $/xi) {
     print {$out_fh} join(',',$1,$2,$3,$4,$5,$6,$7,$8,$9,$10,$11,$12,$13,$14,$15,$16,$17,$18 )
. "\n";
          }
```

}

C. Metin dosyası CSV'a dönüştürme

```
Try
        Dim TableName As String
        OpentxtFileD.FileName = "Dosya Alın"
        OpentxtFileD.Filter = "Tüm Dosyalar (*.*)|*.*"

        If OpentxtFileD.ShowDialog() = DialogResult.OK Then

          Dim Path = OpentxtFileD.FileName
          TableName = InputBox("Tablo Adını Girin:", "Dosya Bilgileri", "events")
          If TableName.Trim.Length <> 0 Then
            Me.Cursor = Cursors.WaitCursor

            ' Veritabanın tabloya veri ekleme
            SQL.Runquery("BEGIN TRANSACTION " & _
                         " BEGIN TRY " & _
                         " BULK INSERT " & TableName & _
                         " FROM '" & Path & "'" & _
                         " WITH " & _
                         "( " & _
                         " FIELDTERMINATOR = ',', " & _
                         " ROWTERMINATOR = '\n', " & _
                         " ROWS_PER_BATCH = 10000, " & _
                         " TABLOCK " & _
                         ")" & _
                         " COMMIT TRANSACTION " & _
                         " END TRY " & _
                         " BEGIN CATCH " & _
                         " ROLLBACK TRANSACTION " & _
                         " END CATCH ")
          Else
            MsgBox("Boş veya İptal edildi")
            Exit Sub
          End If
```

```
        End If
    Catch ex As Exception
        Me.Cursor = Cursors.Default
        MsgBox(ex.Message & vbNewLine & " Sıradışı bir durum, lütfen tekrar deneyin!")
        If SQL.SQLCon.State = ConnectionState.Open Then
            SQL.SQLCon.Close()
        End If
    End Try
```

D. Sorgu Sonuçları Excel'e Aktarma

```
Private Sub Export()
    Dim xlApp As New excel.Application
    Dim xlWorkBook As excel.Workbook
    Dim misValue As Object = System.Reflection.Missing.Value

    Try
        xlWorkBook = xlApp.Workbooks.Add(misValue)
        xlApp.Visible = True
        Dim xlWorkSheet = xlWorkBook.ActiveSheet

        ' Excel'e veri aktarımı
        With xlWorkSheet
            .Range("A1", misValue).EntireRow.Font.Bold = True

            ' Kopyalamaya modu ayarlamak
            DGQuery.ClipboardCopyMode =
DataGridViewClipboardCopyMode.EnableAlwaysIncludeHeaderText
            DGQuery.SelectAll()

            ' Panoya grid içeriği aktar
            Dim str As String = TryCast(DGQuery.GetClipboardContent().GetData(DataFormats.UnicodeText),
String)
            'Set the content to Clipboard
            Clipboard.SetText(str, TextDataFormat.UnicodeText)

            ' panoya verileri yapıştırmak için excel hücre aralığını belirlemek ve seçmek
```

```
            .Range("A1:" & ConvertToLetter(DGQuery.ColumnCount) & DGQuery.RowCount,
misValue).Select()
            ' Pano verilerini yapıştır
            .Paste()
            Clipboard.Clear()
        End With
        releaseObject(xlWorkSheet)

    Catch ex As Exception
        MsgBox(ex.Message)
    Finally
        releaseObject(xlWorkBook)
        releaseObject(xlApp)
    End Try
  End Sub
```

E. Windows günlük olayları gösterme

```
Private Sub WinReadEvents_Click(sender As Object, e As EventArgs) Handles WinReadEvents.Click
    ' Sistem günlüğünü okuma
    Dim Eventlogs As New System.Diagnostics.EventLog("System") ' , "OIRC-09"
    Dim LogEventEntry As System.Diagnostics.EventLogEntry

    SetupListView()

    ' Mevcut Sistem olaylar bilgileri döngüp ve EventEntry çağrarak AddEvents geç.
    For Each LogEventEntry In Eventlogs.Entries
        AddEvents(LogEventEntry)
    Next
    tabmainform.SelectedIndex = 3
    tabmainform.SelectedTab.Show()
    Eventlogs.Dispose()
    LogEventEntry.Dispose()
  End Sub

  Private Sub SetupListView()
    ' Temizle mevcut veriler ve sütunlar kurma
```

```
        With lvwEvents
            .Clear()
            .Columns.Clear()
            .View = View.Details
            .Columns.Add("Entry Type", 100, HorizontalAlignment.Left)
            .Columns.Add("Time Generated", 200, HorizontalAlignment.Left)
            .Columns.Add("Source", 250, HorizontalAlignment.Left)
            .Columns.Add("Category", 100, HorizontalAlignment.Left)
            .Columns.Add("Event ID", 80, HorizontalAlignment.Left)
            .Columns.Add("Message", 550, HorizontalAlignment.Left)
        End With
    End Sub
    Private Sub AddEvents(ByVal oEvEntry As System.Diagnostics.EventLogEntry)
        Dim li As New ListViewItem()
        With li
            .Text = oEvEntry.EntryType.ToString
            .SubItems.Add(oEvEntry.TimeGenerated.ToString)
            .SubItems.Add(oEvEntry.Source.ToString)
            .SubItems.Add(oEvEntry.Category.ToString)
            .SubItems.Add(oEvEntry.EventID.ToString)
            .SubItems.Add(oEvEntry.Message.ToString)
        End With
        lvwEvents.Items.Add(li)
    End Sub
```

ÖZGEÇMİŞ

Mohamed MOHAMUD 1981 yılında Somali'nin Mogadishu ilinde doğdu. Lisans öğrenimini 2007 yılında Somali Yönetim ve İdari Gelişim Enstitüsü'nde bilişim teknolojileri bölümünde tamamladı. 2007-2010 yılları arasında Somali Yönetim ve İdari Gelişim Enstitüsü'nde öğretim görevlisi olarak çalıştı. 2010-2012 yılları arasında Aaran International Şirketi'nde görev yaptı. 2012 yılından beri Fırat Üniversitesi Elektrik-Elektronik Mühendisliği Bölümü'nde yüksek lisans öğrenimine devam etmektedir.