T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SOSYAL AĞLARDA EMNİYET VERİLERİNİN İNCELENMESİ

YÜKSEK LİSANS TEZİ

Bil. Müh. Recep AKYÜZ

Enstitü Anabilim Dalı : BİLGİSAYAR VE BİLİŞİM MÜHENDİSLİĞİ

Tez Danışmanı : Yrd. Doç. Dr. Kürşat AYAN

Eylül 2009

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SOSYAL AĞLARDA EMNİYET VERİLERİNİN İNCELENMESİ

YÜKSEK LİSANS TEZİ

Bil. Müh. Recep AKYÜZ

Enstitü Anabilim Dalı : BİLGİSAYAR VE BİLİŞİM MÜHENDİSLİĞİ

Bu tez 08/09/2009 tarihinde aşağıdaki jüri tarafından Oybirliği ile kabul edilmiştir.

Yrd. Doç. Dr. Kürşat AYAN Jüri Başkanı	Yrd. Doç. Dr. Nilüfer YURTAY Üye	Yrd. Doç. Dr. Gültekin ÇAĞIL Üye

TEŞEKKÜR

Bu tez çalışmasında, bana rehberlik eden, kısıtlı zaman içerisinde yer ve mekan tanımadan okul dışında da desteğini esirgemeyen ve olumlu yaklaşımları ile sürekli teşvik eden tez danışmanım Sayın Yrd. Doç. Dr Kürşat AYAN' a içtenlikle teşekkür ederim.

Ayrıca çalışmalarımda kendisi ile geçirmem gereken zamanı feda edip çalışmalarımda her türlü maddi manevi desteğini esirgemeyip kendisini hep yanımda bulduğum sevgili eşim Zehra AKYÜZ'e, yavrumuza ve hayatımın her safhasında desteklerini esirgemeyen aileme sonsuz teşekkürlerimi sunarım.

İÇİNDEKİLER

TEŞEKKÜR ii
İÇİNDEKİLER iii
SİMGELER VE KISALTMALAR LİSTESİ vii
ŞEKİLLER LİSTESİ viii
TABLOLAR LİSTESİ..... x
ÖZET..... xi
SUMMARY..... xii

BÖLÜM 1.
GİRİŞ..... 1

BÖLÜM 2.
VERİ MADENCİLİĞİ ……..……..... 3
2.1. Veri Madenciliği ……..... 3
2.2. Veri Madenciliği, Veri Tabanı ve İstatistik 5
2.3. Veritabanlarında Bilgi Keşfi..... 5
2.3.1. Veri madenciliği süreci adımları 8
2.4. Veri Madenciliğinin Farklı Disiplinlerle İlişkisi ……..... 10
2.5. Veri Madenciliğinin Kullanım Alanları..... 11
2.5.1. Finans sektörü 11
2.5.2. Haberleşme sektörü 12
2.5.3. Sağlık sektörü 12
2.5.4. Devlet uygulamaları 13
2.6. Veri Madenciliğinde Karşılaşılan Zorluklar 17
2.6.1. Veri tabanı boyutu …..... 17
2.6.2. Gürültü 18

2.6.3. Eksik ve artık veriler..... 18
2.6.4. Dinamik veri yapısı..... 18

BÖLÜM 3.
SUÇ VERİ MADENCİLİĞİ……..… 20
3.1. Suç ve Suç Tipleri..... 20
3.2. Suç Veri Madenciliği……..... 21
3.3. Suç Veri Madenciliğini Önemli Kılan Faktörler 21
3.4. Suç Veri Madenciliği Yöntemleri..... 21
3.4.1. Yapı çıkarımı ……..…..... 21
3.4.2. Demetleme ……..... 22
3.4.3. İlişkilendirme kuralı ……..... 22
3.4.4. Sıralı örüntü madenciliği …….…….... 22
3.4.5. Sapma tespiti …….…..... 23
3.4.6. Sınıflandırma ……..... 23
3.4.7. Dizi karşılaştırıcı ……..... 23
3.4.8. Sosyal ağ analizi ……..... 23
3.5. Dünyadaki Suç Veri Madenciliği Örnekleri 25
3.5.1. Ricmond polis karakolu ……..……... 25
3.5.2. Amsterdam polis karakolu …….…… 25
3.6. Türkiye'deki Suç Veri Madenciliği Örnekleri ……. 26
3.6.1. Suç analiz merkezi işletim sistemi ..……..…….. 26
3.6.2. Asayiş uygulaması ……...……. 27
3.6.3. Benzer uygulamalar ……...……...……. 28
3.7. Suç Analizinde Kullanılan Veri Madenciliği Teknikleri ……. 29

BÖLÜM 4.
SOSYAL AĞ ANALİZİ ……..…….. ……..… 31
4.1. Sosyal Ağ Analizi ….……..…… 31
4.1.1. Derece merkeziliği ……....……..…… 35
4.1.2. Arasındalık merkeziliği ……...…..…… 35
4.1.3. Yakındalık merkeziliği …….……..…… 36

4.2. Sosyal Ağ Analiz'inin Gelişimi ……. 37
4.3. Sosyal Ağların Küresel Yapısı ……. 37
4.4. Sosyal Ağların Makro Yapısı ……. 38
4.4. Suç Örgütleriyle Mücadelede Sosyal Ağ Analizi ve Global Güvenlik ……. 40

BÖLÜM 5.
VERİ GÖRSELLEŞTİRME ……. 43
5.1. Ağ Diyagramından Yapısal Metne Geçiş ve Geri Dönüş…… 43
5.2. Görsel Ağ tipleri ……. 45
5.2.1. Merkezi, merkezisiz ……. 45
5.2.2. Dağıtık, ağaç ……. 46
5.2.3. Sık, seyrek ……. 46
5.2.4. Merkez-çevre, tüm bağlı ……. 47
5.2.5. Küçük dünya, scale-free ……. 47

BÖLÜM 6.
EMNİYET ASAYİŞ PROGRAMI ……. 48
6.1. Emniyet Asayiş Veri Görselleştirme ve Sosyal Ağ Analizi ……... 50
6.2. Veri Tabanı Yapısı ……. 53
6.2.1. AlisVerisTrafik tablosu ……. 53
6.2.2. BankaHesapTrafik tablosu ……. 54
6.2.3. DokumanTrafik tablosu ……. 55
6.2.4. EmailTrafik tablosu ……. 55
6.2.5. Il tablosu ……. 56
6.2.6. Ilce tablosu ……. 56
6.2.7. MsnTrafik tablosu ……. 57
6.2.8. SabikaKaydi tablosu ……. 57
6.2.9. SucTipi tablosu ……. 58
6.2.10. TelefonTrafik tablosu ……. 58
6.2.11. UrunCinsi tablosu ……. 59
6.2.12. Zanli tablosu ……. 59

6.2.13. ZanliEmail tablosu ……..…….....…… 60
6.2.14. ZanliHesapNo tablosu …..…….....…… 60
6.2.15. ZanliTelNo tablosu …..…….....…… 61
6.3. Kullanıcı Giriş Ekranı …….…… 61
6.4. Alış-Veriş Hareketleri Ekranı …….…… 62
6.5. Doküman Hareketleri Ekranı …….……..… 63
6.6. E-posta Hareketleri Ekranı …….……. 64
6.7. Hesap Hareketleri Ekranı ….…….……. 65
6.8. Msn Hareketleri Ekranı …….……. 66
6.9. Suç Tipi Ekranı …….…….……..… 67
6.10. Telefon Hareketleri Ekranı ..…….…… 68
6.11. Ürün Cinsi Ekranı …….…… 69
6.12. Zanlı Ekranı …….…….....…..… 70
6.13. Zanlı E-posta Ekranı …….…… 71
6.14. Zanlı Hesap Numarası …….…… 72
6.15. Zanlı Sabıka Kaydı ……..…….…… 73
6.16. Zanlı Telefon Ekranı …….…… 74
6.17. Alış-veriş Hareket İnceleme Ekranı …….…..…… 75
6.18. Doküman Hareket İnceleme Ekranı …….…… 77
6.19. E-posta Hareket İnceleme Ekranı …….…… 80
6.20. Hesap Hareket İnceleme Ekranı ..…….…… 83
6.21. Msn Hareket İnceleme Ekranı …….…… 85
6.22. Telefon Hareket İnceleme Ekranı …….…… 88

BÖLÜM 7.
SONUÇLAR VE ÖNERİLER……... 94

KAYNAKLAR …..…….. 95
ÖZGEÇMİŞ ……..…….. 97

SİMGELER VE KISALTMALAR LİSTESİ

A.B.D.	: Amerika Birleşik Devletleri
Ar-Ge	: Araştırma Geliştirme
CBS	: Coğrafi Bilgi Sistemi
CETS	: Child Exploitation Track System
CIA	: Central Intelligence Agency
FBI	: Federal Bureau of Investigation
MERNIS	: Merkezi Nüfus İdare Sistemi
Msn	: Messenger
OLAP	: Online analytical processing
PKI	: Public Key Infrastructure
POLNET	: Polis Network'ü
SAA	: Sosyal Ağ Analizi
SNA	: Social Network Analysis
SPSS	: Statistical Package for the Social Sciences
VM	: Veri Madenciliği
VTBK	: Veri Tabanı Bilgi Keşfi

ŞEKİLLER LİSTESİ

Şekil 2.1.	Veri madenciliği süreci …….….....	7
Şekil 2.2.	Veri madenciliğinin farklı disiplinlerle ilişkisi	11
Şekil 2.3.	Veri madenciliği uygulama alanları	16
Şekil 3.1.	Tucson polis birimindeki 164 çete mensubunun SNA yardımı ile çizilmesi…….....	24
Şekil 3.2.	Alt gruplar ve liderleri.....	25
Şekil 3.3.	VisaulLinks'ten örnek ekran görüntüsü	28
Şekil 4.1.	İlişki matrisi yardımı ile görselleştirilmesi	34
Şekil 4.2.	Derece merkeziliği	35
Şekil 4.3.	Arasındalık merkeziliği	36
Şekil 4.4.	Yakındalık merkeziliği	36
Şekil 4.5.	Merkeziliğin genel gösterimi	37
Şekil 4.6.	Yakınlığın 6 derecesi	38
Şekil 4.7.	Bilimsel bir topluluktaki işbirlikleri	39
Şekil 4.8.	HpLabs firmasındaki e-posta hareketlerinin SAA yardımı ile çizimi	40
Şekil 5.1.	Görselleştirilmiş veri örnekleri	43
Şekil 5.2.	Merkezi, merkezsiz ağ	45
Şekil 5.3.	Dağıtık ve ağaç ağ	46
Şekil 5.4.	Sık, seyrek ağ	46
Şekil 5.5.	Merkez-çevre, tüm bağlı ağ…….....	47
Şekil 5.6.	Küçük dünya, scale-free ağ…….…….....	47
Şekil 6.1.	Kullanıcı giriş ekranı	62
Şekil 6.2.	Alış-veriş hareketleri ekranı	63
Şekil 6.3.	Doküman hareketleri ekranı	64
Şekil 6.4.	E-posta hareketleri ekranı	65

Şekil 6.5. Hesap hareketleri ekranı 66
Şekil 6.6. Msn hareketleri ekranı 67
Şekil 6.7. Suç tipi ekranı 68
Şekil 6.8. Telefon hareketleri ekranı 69
Şekil 6.9. Ürün cinsi ekranı 70
Şekil 6.10. Zanlı ekranı 71
Şekil 6.11. Zanlı e-posta ekranı 72
Şekil 6.12. Zanlı hesap no ekranı ……..... 73
Şekil 6.13. Zanlı sabıka kaydı ekranı 74
Şekil 6.14. Zanlı telefon ekranı 75
Şekil 6.15. Alış-veriş hareketlerinin listelenmesi ekranı 76
Şekil 6.16. Alış-veriş hareketleri detayları inceleme ekranı 77
Şekil 6.17. Dokümanların listelenmesi ekranı 78
Şekil 6.18. Doküman detayları inceleme ekranı 79
Şekil 6.19. Doküman içeriği inceleme ekranı 80
Şekil 6.20. E-posta hareketleri listelenmesi ekranı 81
Şekil 6.21. E-posta detayları inceleme ekranı 82
Şekil 6.22. E-posta içeriği inceleme ekranı 82
Şekil 6.23. Hesap hareketleri listelenmesi ekranı 84
Şekil 6.24. Para transferi detayları inceleme ekranı 85
Şekil 6.25. Msn hareketleri listelenmesi ekranı 86
Şekil 6.26. Msn görüşmesi detayları inceleme ekranı 87
Şekil 6.27. Msn görüşmesi içeriği inceleme ekranı 88
Şekil 6.28. Telefon hareketleri listelenmesi ekranı 89
Şekil 6.29. Telefon görüşmesi detayları inceleme ekranı 90
Şekil 6.30. Telefon görüşmesi içeriği inceleme ekranı 90
Şekil 6.31. Kmz yardımı ile kullanıcıların coğrafi koordinatlarına bakılarak adreslerinin çizilmesi 91
Şekil 6.32. Fare üzerine getirilen zanlının detay bilgisinin listelenmesi 92
Şekil 6.33. Zanlıya ait listelene bilgiler 92
Şekil 6.34. GrapML yardımı ile örüntünün ortaya çıkarılması 93

TABLOLAR LİSTESİ

Tablo 2.1.	Veri madenciliği ve veritabanı arasındaki farklar	5
Tablo 2.2.	Veri madenciliğinin uygulandığı alanların dağılımı	17
Tablo 6.1.	AlisVerisTrafik tablosundaki sütunlar ve özellikler ……...	54
Tablo 6.2.	BankaHesapTrafik tablosundaki sütunlar ve özellikleri ..……...	54
Tablo 6.3.	DokumanTrafik tablosundaki sütunlar ve özellikleri ..……...	55
Tablo 6.4.	EmailTrafik tablosundaki sütunlar ve özellikler ….……	55
Tablo 6.5.	Il tablosundaki sütunlar ve özellikleri …….……	56
Tablo 6.6.	Ilce tablosundaki sütunlar ve özellikleri …….	56
Tablo 6.7.	MsnTrafik tablosundaki sütunlar ve özellikleri …….…….	57
Tablo 6.8.	SabikaKaydi tablosundaki sütunlar ve özellikleri …….…….	57
Tablo 6.9.	SucTipi tablosundaki sütunlar ve özellikleri …….…….	58
Tablo 6.10.	TelefonTrafik tablosundaki sütunlar ve özellikleri …….	59
Tablo 6.11.	UrunCinsi tablosundaki sütunlar ve özellikleri ……..	59
Tablo 6.12.	Zanli tablosundaki sütunlar ve özellikleri …….…….	59
Tablo 6.13.	ZanliEmail tablosundaki sütunlar ve özellikleri …….	60
Tablo 6.14.	ZanliHesapNo tablosundaki sütunlar ve özellikleri ……..….	61
Tablo 6.15.	ZanliTelNo tablosundaki sütunlar ve özellikleri …….....	61

ÖZET

Anahtar kelimeler: Emniyet Verileri, Kriminal Verilerin İncelenmesi, Sosyal Ağlarda Emniyet Verileri, Veri Madenciliği

Günümüzde teknolojiden sağlığa, eğitimden finansa ve daha birçok alanda ham verilerin artması bu veriler üzerinde çalışmalar yapılmasını gerekli kılmıştır. Ham verilerin incelenip üzerinde çalışmalar yapılmasıyla ortaya işlenmiş veriler çıkmaktadır. Emniyet alanında ortaya çıkan suç verilerinin çoğalması bu alanda ham suç verilerinin üzerinde incelemeler yapılmasını gerekli kılmıştır. Suç verilerinin incelenmesi yeni çıkacak suçları önlemeye yönelik çözümler sunacaktır. Bu alanda yapılacak çalışmalarla organize suç örgütlerinin yapısı, suç örgütünün lideri, suç örgütündeki alt gruplar ve daha birçok bilgiyi ortaya çıkarılabilecektir. Emniyet birimleri için suç istatistiklerine dair online raporlama, hangi profildeki insanların ne tür suçlara meyilli olduklarını belirleme, eş zamanlı suç engelleme politikaları oluşturmak büyük önem arz etmektedir. Bu da eldeki suç verilerin işlenmesi ile mümkündür. Son zamanlarda suç verileri üzerine yapılan çalışmaların popülerliği artmaktadır. Teknolojik imkanların gelişimine paralel olarak bu veriler üzerine yapılan çalışmalar artmakta ve kolay bir biçimde incelenebilmektedir.

CRIMINAL DATA ANALYSIS AT SOCIAL NETWORK

SUMMARY

Key Words: Criminal Data, Crimininal Data Analysis, Criminal Data At Social Network, Data Mining

Todays from tecnologies sectors to healty sectors, from educational activities to finance and also more sectors contains so many row datas. Increasing amounts of row data makes researchers to study on these datas. After studying and prosessing on row data information will be resulted.

Increasing amount of criminal on police department make resesearcher to study on row criminal datas at this department.

Studying row criminal data will represent solution to prevent new crimes. With studying on this area, organisational gang structure, the leader of the gang, subgroups of the gnag and so many information about gang will be appeared. Online reporting for Crime data statistics, which person can make what crime, prevent realtime crime are very important for police departmets. This can be done with with researching and processing holded crimes datas. Working on crime datas is being more popear atthe last times. Working on these crime datas is increasing and technologics development make it easy to resarch on these data.

BÖLÜM 1. GİRİŞ

Teknolojinin gelişimi ile birlikte bilgisayarlarda, bilgisayar ağlarında çok yüksek boyutlarda verilerin saklandığı günümüzde, kamu kurumları, bilişim sektöründe faaliyet gösteren kuruluşlar ve şirketler veri toplama, depolama ve işleme faaliyetleri için çok büyük miktarda paralar harcamaktadır. Bununla birlikte toplanan verilerin hacimlerinin çok büyük olması ve yapılarının da etkin bir veri analizi yapılmasına uygun olmaması bu verilerin ancak çok küçük bir kısmının kullanılabilmesine olanak sağlamaktadır.

Veri yoğunluğunun çok fazla olduğu alanlardan bir tanesi de emniyet alanıdır. Bu alanda çok miktarda işlenmemiş suç verisi bulunmaktadır. Bu veriler suç niteliği taşıyan veya gerçekleşmiş olan vakalarda olay yeri incelenmesi sonucu toplanan verilerdir. Bu verilerin çoğu gerçekleşmiş vakalardan toplanmış verilerden oluşmaktadır. Teknolojik imkânların gelişine paralel olarak bu veriler üzerinde yapılan çalışmalarla suçların önüne geçilmeye çalışılmakta, olayları gerçekleştiren suçlulara kısa sürede belirlenerek yakalanmaktadırlar. Son yıllarda suçların artması bu verileri daha önemli hale getirmiş ve bu veriler üzerine çalışmalar yapılmasını gerekli kılmıştır.

Emniyet alanında ortaya çıkan suç verilerinin çoğalması bu alanda ham suç verilerinin üzerinde incelemeler yapılmasını gerekli kılmıştır. Suç verilerinin incelenmesi yeni çıkacak suçları önlemeye yönelik çözümler sunacaktır. Bu alanda yapılacak çalışmalarla organize suç örgütlerinin yapısı, suç örgütünün lideri, suç örgütündeki alt gruplar ve daha birçok bilgiyi ortaya çıkarılabilecektir. Emniyet birimleri için suç istatistiklerine dair çevrimiçi raporlama, hangi profildeki insanların ne tür suçlara meyilli olduklarını belirleme, eş zamanlı suç engelleme politikaları oluşturmak büyük önem arz etmektedir. Bu da eldeki suç verilerin işlenmesi ile

mümkündür. Son zamanlarda suç verileri üzerine yapılan çalışmaların popülerliği artmaktadır.

Veri madenciliği; eldeki verilerden üstü kapalı, net olmayan, önceden bilinmeyen ancak potansiyel olarak kullanışlı bilginin çıkarılmasıdır[1]. Veri Madenciliği; veri ambarlarındaki tutulan, çok çeşitli ve çok miktarda veriye dayanarak daha önce keşfedilmemiş bilgileri ortaya çıkarmak, bunları karar verme ve eylem planını gerçekleştirmek için kullanma sürecidir. Büyük miktarda veri içinden, gelecekle ilgili tahmin yapmamızı sağlayacak bağıntı ve kuralların aranmasıdır. Veri Madenciliği, verilerin içerisindeki desenlerin, ilişkilerin, değişimlerin, düzensizliklerin, kuralların ve istatistiksel olarak önemli olan yapıların yarı otomatik olarak keşfedilmesidir. Veriler arasındaki ilişkiyi, kuralları ve özellikleri belirlemekten bilgisayar sorumludur. Amaç, daha önceden fark edilmemiş veri desenlerini tespit edebilmektir. Diğer bir deyişle veri madenciliği, büyük veri yığınlarından anlamlı bilgiler elde etmek için, bilgisayar destekli bir bilgi çözümleme işlemidir.

Bu çalışmada, emniyete ait suç verilerini barındıran veritabanları üzerine çalışmalar yapılarak verinin işlenmesi, görselleştirilmesi ve veri madenciliği konularını içeren emniyet mensupları tarafından kullanılabilecek bir uygulama geliştirilmeye çalışılmıştır

BÖLÜM 2. VERİ MADENCİLİĞİ

Gelişen ve değişen çevre koşulları, sınırların kalkması ile küreselleşen dünya, farklı pazarlama ve ar-ge(araştırma geliştirme) yöntemleri verinin değil bilginin önemini her geçen gün daha da artacak şekilde ortaya koymaktadır. İnternetin yaygınlaşması ve kolaylaşması ar-ge ekiplerinin bilgiye erişmelerini zorlaştırmaktadır. İnternette arama motorları kullanılarak yapılan araştırmalar çoğu zaman istenilenden farklı bir şekilde sonuçlanmaktadır. Tıbbi bir araştırma sonucunda elde edilen verilerin yorumlanıp analiz edilmesiyle bilgiye ulaşılabilmektedir. Büyük bir perakendecinin, fatura bilgilerinden müşteri eğilimlerini belirleyip ona göre pazarlama taktikleri üretebilmesi, rakiplerinin önüne geçmesini sağlayacaktır. Verilen örneklere dikkat edilirse, verinin bilgiye dönüşme işleminin vurgulandığı görülecektir. Bilginin kimi yöntemler ile analiz edilmesi ve çıkan sonuçların bir uzman gözüyle yorumlanmasıyla geçmiş verilerden gelecek tahminleri yapma işlemi veri madenciliği(data mining) olarak belirtilebilir

2.1.Veri Madenciliği

Veri madenciliği, eldeki verilerden üstü kapalı, çok net olmayan, önceden bilinmeyen ancak potansiyel olarak kullanışlı bilginin çıkarılmasıdır. Bu da; kümeleme, veri özetleme, değişikliklerin analizi, sapmaların tespiti gibi belirli sayıda teknik yaklaşımları içerir[2]. Başka bir deyişle, veri madenciliği, verilerin içerisindeki desenlerin, ilişkilerin, değişimlerin, düzensizliklerin, kuralların ve istatistiksel olarak önemli olan yapıların yarı otomatik olarak keşfedilmesidir.

Temel olarak veri madenciliği, veri setleri arasındaki desenlerin ya da düzenin, verinin analizi ve yazılım tekniklerinin kullanılması ile ilgilidir. Veriler arasındaki ilişkiyi, kuralları ve özellikleri belirlemekten bilgisayar sorumludur. Amaç, daha

önceden fark edilmemiş veri desenlerini tespit edebilmektir. Veri madenciliğini istatistiksel bir yöntemler serisi olarak görmek mümkün olabilir. Ancak veri madenciliği, geleneksel istatistikten birkaç yönde farklılık gösterir. Veri madenciliğinde amaç, kolaylıkla mantıksal kurallara ya da görsel sunumlara çevrilebilecek nitel modellerin çıkarılmasıdır. Bu bağlamda, veri madenciliği insan merkezlidir ve bazen insan – bilgisayar ara yüzü birleştirilir.

Veri madenciliği sahası, istatistik, makine bilgisi, veri tabanları ve yüksek performanslı işlem gibi temelleri de içerir.
Veri madenciliği konusunda bahsi geçen geniş verideki geniş kelimesi, tek bir iş istasyonunun belleğine sığamayacak kadar büyük veri kümelerini ifade etmektedir. Yüksek hacimli veri ise, tek bir iş istasyonundaki ya da bir grup iş istasyonundaki disklere sığamayacak kadar fazla veri anlamındadır. Dağıtık veri ise, farklı coğrafi konumlarda bulunan verileri anlatır.

Veri madenciliği, günlük yaşamda birçok şekilde kullanılabilmektedir. Bunlardan bazıları aşağıdaki gibi sıralanabilir:
- Emniyet birimleri için dinlemeye takılan telefon kayıtlarında, e-posta, para transferleri vb. verilerden örgütlerinin yapılarını ortaya çıkarmada, bu örgütlerin organize suç teşkil edip etmediği bilgisinin ortaya çıkarılmasında fayda sağlar.
- Hastanelere yapılan tedavi taleplerinin bölgelere, zamana ve ihtiyaca göre değerlendirmesi salgın hastalık riskinin ilk aşamada tespiti, kontrolü ve kaynak planlama açısından faydalı olur.
- Kaçak enerji kullananların profillerini tespit eden bir model, olası kaçak enerji kullanıcılarını tahmin etmeyi sağlayacak, düşük maliyet ile kaçaklarla etkin mücadele edilmesine olanak tanıyacaktır.
- Karayollarının bölgelere ve zamana göre yoğunluklarını öngörme amaçlı bir çalışma doğru zamanda doğru kaynak planlaması ile örneğin kaza oranlarının asgariye indirilmesini sağlayacaktır.
- Kamu kurumları destek programlarını uygularken, verilecek desteğin doğru miktarda ve doğru hedefleri olan kuruluşlara verilmesini sağlayacak kurumsal risk skorlaması yapılmasıyla uygulanan programların başarısı artar.

- Kredileri tahsis ederken ödememe riski olan profillerin tespit edilmiş olması batık kredi miktarlarını azaltır.

2.2. Veri Madenciliği, Veri Tabanı ve İstatistik

Veri madenciliği kendi başına bir çözüm değil çözüme ulaşmak için verilecek karar sürecini destekleyen, problemi çözmek için gerekli bilgileri sağlamaya yarayan bir araçtır.

Veri madenciliği basit istatistik yöntemi değildir. Veri madenciliği, analizi gerçekleyen kişiye, iş yapma aşamasında oluşan veriler arasındaki şablonları ve ilişkileri bulması konusunda yardım etmektedir.

Veri madenciliği, veri tabanları, istatistik ve yapay öğrenme konularının kavramlarına dayanır ve onların tekniklerini kullanır.

Veritabanı ve veri madenciliği birbirinin aynı olmamakla beraber, iç içe geçmiş kavramlardır. Veri madenciliğinin ve veritabanı arasındaki farklar Tablo 2.1'de verilmiştir.

Tablo 2.1 Veri madenciliği ve veritabanı arasındaki farklar

	Veri Tabanı	Veri Madenciliği
Sorgulama	Tanımlı SQL	Tam Tanımlı Değil Yaygın sorgulama dili yok
Veri	Hazır veri	Üzerinde işlem yapılmayan veri
Çıkış	Belirli	Belirli Değil

2.3. Veritabanlarında Bilgi Keşfi

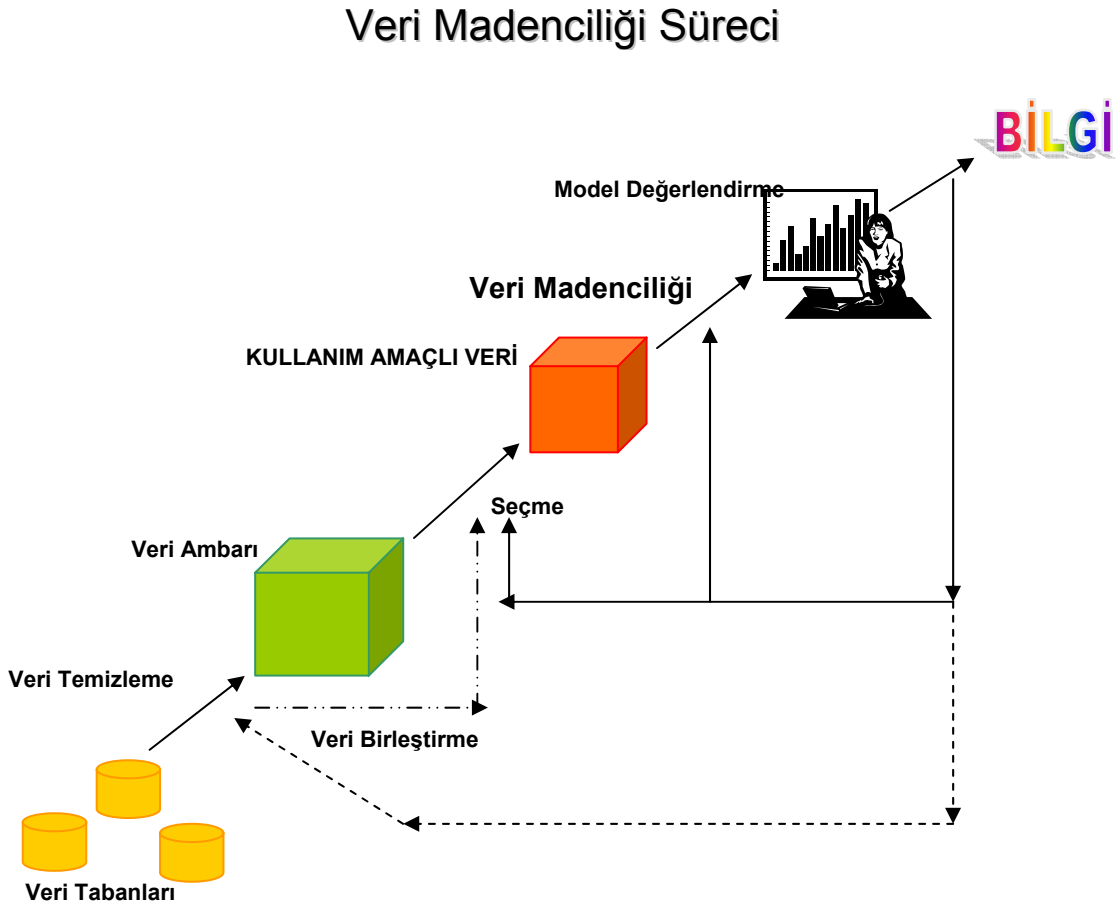
Veri kendi başına bir değer ifade etmez, bir gayeye yönelik olarak işlendiğinde bilgi meydana gelir. Veriyi bilgiye çevirme süreci veri analizi olarak nitelendirilir. Yakın geleceğin, günümüzden çok fazla farklı olmayacağı düşünüldüğünde, geçmiş ve

günümüzdeki verilerden çıkarılmış olan bilgiler yakın gelecekte de geçerli olacak ve gelecek için doğru tahmin yapmayı sağlayacaktır.

Kayıtlı verilerden anlamlı bilgilere ulaşım sürecine Veritabanlarında Bilgi Keşfi (VTBK) olarak nitelendirilmektedir. Veritabanlarında bilgi keşfi, depolanmış veri içerisindeki geçerli, yeni, faydalı ve sonuç olarak anlaşılabilir örüntülerin çıkarılması sürecidir. Bu sürecin ilk adımı, uygulama alanının öğrenilmesi ile başlar. Veritabanlarında bilgi keşfinin son basamağı ise, elde edilen bilginin görüntüleme ve bilgi gösterimi yöntemleri kullanılarak kullanıcıya sunulması şeklindedir. Bazı araştırmacılar veritabanlarında bilgi keşfi ile Veri Madenciliğini eşanlamlı olarak kabul etmelerine rağmen, genel görüş veri madenciliği VTBK sürecinin bir aşaması şeklindedir.

Veri madenciliği; eldeki verilerden üstü kapalı, net olmayan, önceden bilinmeyen ancak potansiyel olarak kullanışlı bilginin çıkarılmasıdır[1]. Diğer bir deyişle veri madenciliği, büyük veri yığınlarından anlamlı bilgiler elde etmek için, bilgisayar destekli bir bilgi çözümleme işlemidir.

Şekil 2.1 Veri madenciliği süreci özetlemektedir[3].



Şekil 2.1. Veri madenciliği süreci

Şekildeki veri madenciliği sürecinin adımları kısaca aşağıdaki gibi özetlenebilir;

Veri Seçimi: Bu adım birkaç veri kümesini birleştirerek, sorguya uygun örnekleme kümesini elde etmeyi gerektirir. Yapılacak işlemin amacına uygun veri kümesi seçme ve oluşturma adımıdır.

Veri Temizleme ve Önişleme: Seçilen örneklemde yer alan hatalı tutanakların çıkarıldığı ve eksik nitelik değerlerinin değiştirildiği aşamadır ve keşfedilen bilginin kalitesini artırır. Veri ayıklama ve önişleme adımı veri madenciliği sürecinin %70'lik bölümünü oluşturur.

Veri İndirgeme: Seçilen örneklemden ilgisiz niteliklerin atıldığı ve tekrarlı tutanakların ayıklandığı adımdır. Bu aşama ile seçilen veri madenciliği sorgusunun çalışma zamanını iyileştirir.

Veri Madenciliği: Verilen bir veri madenciliği sorgusunun (sınıflama, güdümsüz öbekleme, eşleştirme, vb.) işletilmesidir. Veri madenciliği tekniği seçme, sınıflandırma, eğri uydurma, bağıntı kurallarını bulma, demetleme, veri madenciliği algoritmasını seçme işlemleri bu adımda gerçekleştirilir.

Değerlendirme: Keşfedilen bilginin geçerlilik, yenilik, yararlılık ve basitlik kıstaslarına göre değerlendirilmesi ve bulunan bilginin yorumlanması aşamasıdır.

Veri madenciliği yapılabilmesi için, veritabanlarında bilgi keşfi süreçlerinin veritabanlarında tutulan verilere sıra ile uygulanması gerekmektedir. Her bir süreç tamamlandıktan sonra bir sonraki sürecin başlatılarak veri madenciliği aşamasına ulaşılmalıdır. Veri madenciliği aşamasında veri madenciliği tekniklerinden verilere ve elde edilmek istenen sonuca uygun olan teknik seçilerek uygulanır.

2.3.1. Veri madenciliği süreci adımları

Yukarıda anlatılan Veri Madenciliği Sürecinin adımları aşağıdaki gibidir:

Veri Seçimi: Bu aşamada birden fazla veri kümesi içerisinden, üzerinde sorgu yapılmasına uygun örnek bir veri kümesi oluşturma aşamasıdır. Veri toplama (data collection) ve farklı kümelerdeki verilerin birleştirilmesi işlemi de bu süreçte yer alır. Toplama, tanımlanan problem için gerekli olduğu düşünülen verilerin ve bu verilerin toplanacağı veri kaynaklarının belirlenmesi adımıdır. Veri seçimi aşamasında yapılması gerekenler;

1. Farklı ortamlardaki verilerin mevcut yapılarının incelenmesi ve tablo yapılarının ortaya çıkarılması,
2. Veri madenciliği ile hedeflenen sonuca ulaşmak için gerekli verilerin, uygulama için belirlenen veri depolama ortamına aktarılması olarak sıralanabilir.

Veri Önişleme: Veri seçimi ile elde edilen örnek veri kümesinde yer alan hatalı ve eksik değerlerin düzenlendiği ve çıkarıldığı aşamadır. Veri temizleme (data cleaning) ve veri dönüştürme (data transformation) veri önişleme işlemleridir. Veri temizlemenin amacı gürültülü ve ilgisiz verinin veri setinden çıkarmaktır. Veri dönüşümünün amacı ise, kaynak veri içindeki farklı biçimdeki veri tip ve değerlerini yapılacak veri madenciliği çalışması doğrultusunda değiştirmektir.

Modelde kullanılan veritabanının çok büyük olması durumunda örnekleme yapılması uygun olabilir. Günümüzde hesaplama olanakları ne kadar gelişmiş olursa olsun, çok büyük veritabanları üzerinde çok sayıda modelin denenmesi uzun zaman alması nedeni ile mümkün olamamaktadır. Bu nedenle tüm veritabanını kullanarak bir kaç model denemek yerine, rasgele örneklenmiş bir veritabanı parçası üzerinde birçok modelin denenmesi ve bunlar arasından en güvenilir ve güçlü modelin seçilmesi daha uygun olacaktır.

Veri tipi dönüşümü, basit olarak veri tipi değişimidir. Örnek olarak, integer tipteki bir veriyi boolean tipine dönüştürme işlemi verilebilir. Bu dönüşümün sonucunda, sorgulama yapılacak veri tabanı boyutu azaltılabilir ve sorgularda hız artışı sağlanabilir.

Bazı veritabanlarında bir kolon içinde sürekli tekrarlayan benzer veriler bulunmaktadır. Bu verileri bir kaç grup içine yerleştirme işlemi uygulanarak verinin kalitesi artırılır. Gruplama tekniği ile yorumlamanın daha kolay olması sağlanabilir. Farklı veritabanlarından gelen veriler tek bir tablo içinde birleştirildiğinde veri alanlarının bazıları boş kalabilir. Bu durumu düzeltmek için, kayıp değerler en çok kullanılan değerler ile doldurabilir, bir kayıtta çok fazla kayıp değer varsa kayıt tamamen silinebilir, en olası ortalama değer ile doldurulabilir.

Veri İndirgeme: Seçilen örnek veri kümesindeki ilgisiz nitelikte ve tekrarlı verilerin çıkarıldığı aşamadır. Bu işlem ile verinin boyutu indirgendiğinden veri madenciliği uygulanırken çalıştırılacak sorguların daha hızlı sonuç üretmeleri sağlanır.

Veri Madenciliği: Bu aşama veri madenciliği yöntemlerinin ve algoritmalarının uygulandığı adımdır. VM; veritabanı sistemleri, verilerin depolanması, istatistik, makine öğrenimi gibi alanların kombinasyonundan oluşan disiplinler arası bir yöntemdir. VM istatistikçiler için yeni bir konu değildir. İstatistik ve VM ortak amaçlara sahiptir, her ikisi de verilerin yapılarının keşfedilmesiyle ilgilidir. Her ne kadar VM istatistiğin bir alt kümesi olarak kabul edilse de VM, veritabanı teknolojisi ve makine öğrenimi gibi diğer alanlara ait fikirleri, araçları ve yöntemleri de kullanır[4].

Değerlendirme: Bilgi keşfi sürecinde bu aşamadan önceki aşamalar sonucunda elde edilen bilginin geç erlilik, yenilik, yararlılık ve basitlik kıstaslarına göre değerlendirilmesi aşamasıdır[5].

2.4. Veri Madenciliğinin Farklı Disiplinlerle İlişkisi

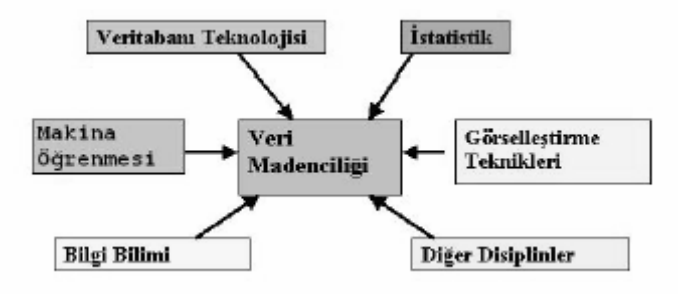
Veri madenciliği, önceden bilinmeyen ilişki ve trendlerin bulunması için bugünün endüstrisinde yaratılan büyük miktarlardaki veriyi analiz eden bir yoldur. Yüksek güçlü bilgisayarlara ve gereken yazılımlara kolay ve düşük fiyatlarla ulaşılabilmesi bu teknolojinin işlemesini olanaklı kılmıştır.

Gartner Grup tarafından yapılan tanımda veri madenciliği, istatistik ve matematik tekniklerle birlikte ilişki tanıma teknolojilerini kullanarak, depolama ortamlarında saklanmış bulunan veri yığınlarının elenmesi ile anlamlı yeni ilişki ve eğilimlerin keşfedilmesi sürecidir[6].

VM aracılığıyla, büyük veri kümelerinden oluşan veritabanı sistemleri içerisinde gizli kalmış bilgilerin çekilmesi sağlanır. Bu işlem, istatistik, matematik disiplinleri, modelleme teknikleri, veritabanı teknolojisi ve çeşitli bilgisayar programları kullanılarak yapılır.

Makine öğrenimi, istatistik ve VM arasındaki yakın bir bağ vardır. Bu üç disiplin veri içindeki örüntüleri bulmayı amaçlar. Makine öğrenimi yöntemleri, VM algoritmalarında kullanılan yöntemlerin çekirdeğini oluşturur. Makine öğreniminde kullanılan karar ağacı, kural çıkartımı pek çok VM algoritmasında kullanılmaktadır.

Makine öğrenimi ile VM arasında benzerliklerin yanı sıra farklılıklar da göze çarpmaktadır. Öncelikle VM algoritmalarında kullanılan örnekleme boyutu, makine öğreniminde kullanılan veri boyutuna nazaran çok büyüktür.



Şekil 2.2. Veri madenciliğinin farklı disiplinlerle ilişkisi

2.5. Veri Madenciliğinin Kullanım Alanları

Veri Madenciliği kullanım alanı olarak çok geniş bir yelpazeye sahiptir. Örnek uygulama alanları aşağıda belirtilmiştir.

2.5.1. Finans sektörü

Finans ve sigorta sektörü günümüzde sundukları hizmet, ürün ve servislerle bilgiye dayalı yönetime en fazla ihtiyaç duyan kuruluşlardır. Bu sektörde bilgiye dayalı yönetim özellikle ekonomik krizin yaşattığı sonuçlar göz önüne alındığında tartışmasız önemli ve zorunludur. Finans sektöründe en temel uygulamalar çapraz satış, risk derecelendirme, mevcut müşteriyi elde tutma, yeni müşteriler kazanma, maliyetleri azaltma, kayıp ve kaçakları engelleme, alternatif kanallar oluşturma, müşteri memnuniyetini sağlama olarak özetlenebilir. Hangi müşteri profilinin neyi, ne zaman ve neden tercih ettiğini anlayabilen bir kuruluş hem talep yaratma, hem de doğru zamanda doğru talebi karşılama ve sunma avantajına sahip olacaktır. Kuruluşun karlılığı artarken, müşterinin memnuniyeti de artacağından, aynı zamanda müşteri sadakati de sağlanmış olacaktır.

Ağ ekonomisinin en büyük korkusu mevcut müşteri kaybıdır. Çünkü mevcut müşteri kaybı, finans ve sigorta sektörlerinde en önemli problemi teşkil etmektedir. Yeni bir müşteri kazanmanın maliyetinin müşteriyi elde tutma maliyetinden daha yüksek olduğu, kaybedilen bir müşteriyi yeniden kazanma maliyetinin yeni müşteriler edinme maliyetinden daha fazla olduğu göz önüne alındığında şirketler müşteri odaklı gitmek ve mevcut müşteriyi ellerinde tutmak zorundadır. Bankalar, mevcut müşterilerden rakip bankaya geçme ihtimali olan müşterileri, profillerini ve kaybettikleri müşterilerin hangi sebepler yüzünden sistemden ayrıldıklarını tespit etmek istemektedir.

2.5.2. Haberleşme sektörü

Telekom sektöründe en önemli sorun müşteri kaybıdır. Kuruluşlar hangi müşterilerini kaybedebileceklerini önceden belirleyebildikleri takdirde bu müşterilerini elde tutma amaçlı stratejiler geliştirebilir, düşük maliyetli ve etkili kampanyalar düzenleyebilirler. Kaybetme olasılığı olmayan bir müşteriye kalıcılığını sağlama amaçlı bir mesaj göndermek hem müşterinin kendisine verilmek istenen mesajın ne olduğunu algılamasını zorlaştıracak hem de maliyetleri artıracaktır.

2.5.3. Sağlık sektörü

Doğru ve zamanında karar almanın hasta sağlığı üzerindeki etkisi tartışmasız çok önemlidir. Veri madenciliğinin sağlık sektörü uygulamalarında doktorlar tarafından bakıldığında, hastane bünyesinde toplanan operasyonel veriler, hasta verileri, uygulanan tedavi yöntemi ve tedavi sürecine dair veriler büyük önem arz etmektedir. Yöneticiler açısından bakıldığında, hastanedeki servislerin ve programların başarısının görüntülenmesi, kaynakların maliyetlerle göreceli olarak kullanımı, kaynak kullanımı ve hasta sayıları ile ilgili eğilimlerin tahmini, harcamalarla ilgili normal olmayan durumların anlık tespiti ve yolsuzlukların engellenmesi, hastanede uygulanan tedavi yöntemlerinin başarısının irdelenmesi açısından önemli bilgileri içermektedir. Bu veriler başarılı tedavi sonuçları almada etken faktörlerin belirlenmesi, ameliyatlarda yüksek risk faktörlerinin sınanması, hasta verilerinin yaş,

cinsiyet, ırk ve tedavi yöntemi gibi faktörlere göre sınıflanması, hasta sağlığı açısından geriye dönük faktörlerin sınanması, tedavi yöntemi geliştirme vb. amaçlarla kullanılmaktadır. Dünya çapında çok sayıda başarılı uygulama örneği mevcuttur.

2.5.4. Devlet uygulamaları

Kamu yöneticileri günümüzde verinin ve bilginin önemini kavramışlardır. Müşteriye özel hizmet sunan ticari kuruluşlarda olduğu gibi devlet kurumları da vatandaşlarının ihtiyaçlarına özel hizmet sunabilmenin önemini kavramışlardır. Kamu yöneticileri için en önemli uygulamalar kaynakların doğru olarak kullanımını sağlama ve planlamadır. Kamu güvenliğini sağlama amacı ile güvenlik problemlerini önceden tahmin etmek, rastlantısal olaylardaki sorunların çözümüne dair izleri keşfetme ve olası güvenlik sorunlarını eş zamanlı olarak tespit edebilme ve çözüm üretebilme kamu kurumlarında çalışan güvenlik işlerinden sorumlu yöneticiler için veri madenciliği yardımı ile önemli uygulamalar geliştirilmektedir. Ayrıca veri madenciliği kamu kurumları için vergi ile ilgili yolsuzlukları ve izlerini belirleme, yolsuzlukları eş zamanlı olarak belirleme, sağlık ödemeleri, programların uygulanması vb. konularda şüpheli durumların tespiti, suiistimal, israfları belirleme ve milyonlarca dolarlık zararı engelleme, gibi konularda da çok faydalı çözümler üretebilmektedir. Kamuda enformasyon ve bilgi ihtiyacı sonsuzdur. Emniyet birimleri için suç istatistiklerine dair online raporlama, hangi profildeki insanların ne tür suçlara meyilli olduklarını belirleme, suç örgütlerinin yapılarının ortaya çıkarılması, eş zamanlı suç engelleme politikaları oluşturmak ancak ileri analitik uygulamalar ile mümkündür.

Günümüzde e-devlet kavramı oldukça kritiktir. E-devlet uzmanlarının en önemli hedefi bilgiye eş zamanlı olarak ulaşmak ve daha iyi hizmet vermektir. E-devlet uygulaması gerçekleştirilen ülkelerde kamu kuruluşları ziyaretçilerin kamu sayfalarını nasıl kullandığı, ihtiyaç duyulan formlara kolayca ulaşılıp ulaşılamadığı, geçmişteki ziyaretçi davranışlarına göre kurumun web sayfasını vatandaşın ihtiyacına daha iyi yanıt verecek şekilde yeniden düzenlemek mümkündür.

Günümüzde VM teknikleri başta işletmeler olmak üzere çeşitli alanlarda başarı ile kullanılmaktadır. Aşağıda veri madenciliği kullanımı yapılabilecek birkaç örnek verilmiştir.

- İşletme kendi müşterisiyken rakibine giden müşterilerle ilgili analizler yaparak rakiplerini tercih eden müşterilerinin özelliklerini elde edebilir ve bundan yola çıkarak gelecek dönemlerde kaybetme olasılığı olan müşterilerin kimler olabileceği yolunda tahminlerde bulunarak onları kaybetmemek, kaybettiklerini geri kazanmak için strateji geliştirebilir.

- Ürün veya hizmette hangi özelliklerin ne derecede müşteri memnuniyetini etkilediği, hangi özelliklerinden dolayı müşterinin bunları tercih ettiği otaya çıkarılabilir.

- Kredi kartı ödemelerini aksatan, gecikmeli olarak yapan veya hiç yapmayanların özelliklerinden yola çıkılarak bundan sonra aynı duruma düşebilecek muhtemel kişiler saptanabilir.

- Bir ürün veya hizmetle ilgili bir kampanya programı oluşturmak için hedef kitlenin seçiminden başlayarak bunun hedef kitleye hangi kanallardan sunulacağı kararına kadar olan süreçte veri madenciliği kullanılabilir.
Veri madenciliğinin uygulama alanları konu başlıkları itibariyle aşağıdaki gibi sınıflandırılabilir[7].

Pazarlama
- Müşterilerin satın alma örüntülerinin belirlenmesi
- Müşterilerin demografik özellikleri arasındaki bağlantıların bulunması
- Posta kampanyalarında cevap verme oranının artırılması
- Pazar sepeti analizi
- Müşteri ilişkileri yönetimi
- Müşteri değerlendirme
- Satış tahmini
- Müşteri dağılımında

- Çeşitli pazarlama kampanyalarında
- Mevcut müşterilerin elde tutulması için geliştirilecek pazarlama stratejilerinin oluşturulmasında
- Çapraz satış analizleri
- Çeşitli müşteri analizlerinde

Bankacılık

- Farklı finanssal göstergeler arasında gizli korelasyonların bulunması
- Kredi kartı dolandırıcılıklarının tespiti
- Kredi kartı harcamalarına göre müşteri gruplarının belirlenmesi
- Kredi taleplerinin değerlendirilmesi
- Müşteri dağılımında
- Usulsüzlük tespiti
- Risk analizleri

Sigortacılık

- Yeni poliçe talep edecek müşterilerin tahmin edilmesi
- Sigorta dolandırıcılıklarının tespiti
- Riskli müşteri örüntülerinin belirlenmesi

Perakendecilik

- Satış noktası veri analizleri
- Alış-veriş sepeti analizleri
- Tedarik ve mağaza yerleşim optimizasyonu
- Hisse senedi fiyat tahmini
- Genel piyasa analizleri
- Alım-satım stratejilerinin optimizasyonu

Telekomünikasyon

- Kalite ve iyileştirme analizleri
- Hisse tespitleri
- Hatların yoğunluk tahminleri

Sağlık ve İlaç

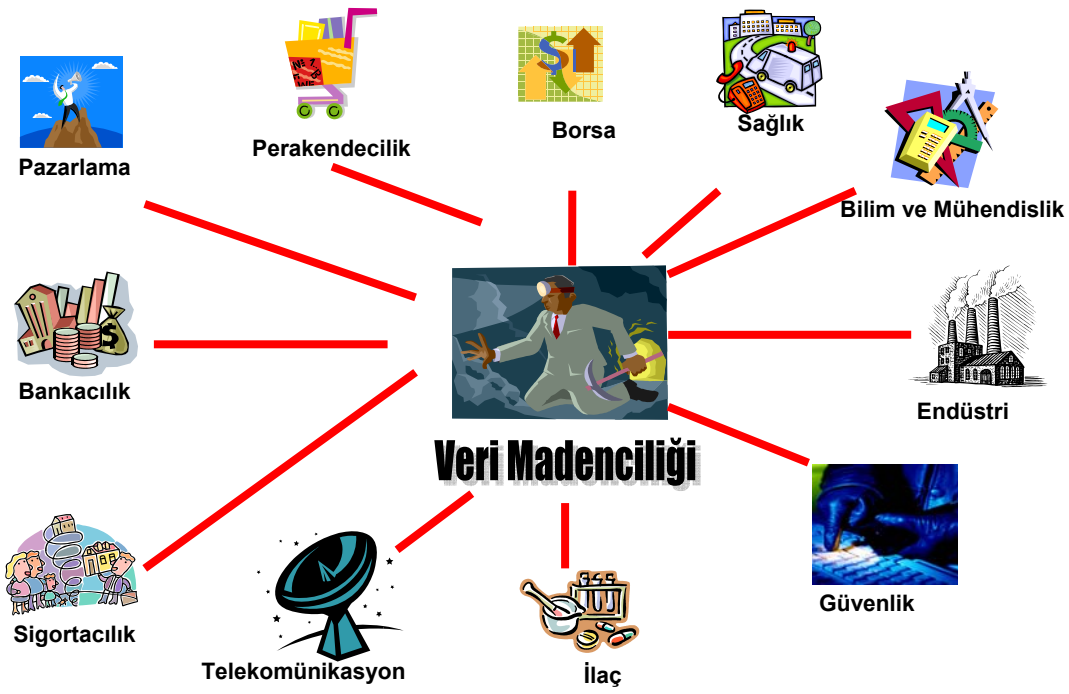
- Test sonuçlarının tahmini
- Ürün geliştirme
- Tıbbi teşhis
- Tedavi sürecinin belirlenmesi

- Semptomlara göre hastalık tespiti,

Endüstri

- Kalite kontrol analizleri
- Lojistik
- Üretim süreçlerinin optimizasyonu

Yukarıda geçen Veri Madenciliği uygulama alanlarını özetleyen şekil, Şekil 2.3'te verilmiştir.



Şekil 2.3. Veri madenciliği uygulama alanları

Tablo 2.2'de 2003 yılında veri madenciliğinin sektörler bazında kullanımına ilişkin bir araştırmanın sonuçları yer almaktadır[8].

Tablo 2.2. Veri madenciliğinin uygulandığı alanların dağılımı

Bankacılık (37)	13%
Bioteknoloji / Genetik (27)	10%
Pazarlama / Organizasyon (29)	10%
Web (15)	5%
Eğlence / Haber (4)	1%
Sahtekârlık Tespiti (24)	9%
Sigortacılık (23)	8%
Yatırım / Hisse Senedi (8)	3%
İmalat (5)	2%
Medikal (16)	6%
Perakende (17)	6%
Bilimsel Çalışmalar (24)	9%
Güvenlik (6)	2%
Tedarik Zinciri Analizi (3)	1%
Telekomünikasyon (21)	8%
Seyahat (5)	2%
Diğer (12)	4%
Bilinmeyen (3)	1%

2.6. Veri Madenciliğinde Karşılaşılan Zorluklar

Veri madenciliği girdi olarak kullanılacak ham veriyi veritabanlarından alır. Bu da veritabanlarının dinamik, eksiksiz, geniş ve net veri içermemesi durumunda sorunlar doğurur[9]. Küçük veri kümelerinde hızlı ve doğru bir biçimde çalışan bir sistem, çok büyük veri tabanlarına uygulandığında tamamen farklı davranabilir. Bir VM sistemi tutarlı veri üzerinde mükemmel çalışırken, aynı veriye gürültü eklendiğinde kayda değer bir biçimde kötüleşebilir. Günümüzde VM sistemlerinin karşılaştığı sorunlar şu şekildedir:

2.6.1. Veri tabanı boyutu

Veri tabanı boyutları inanılmaz bir hızla artmaktadır. Pek çok makine öğrenimi algoritması birkaç yüz tutanaklık oldukça küçük örneklemeleri ele alabilecek biçimde geliştirilmiştir. Örneklemenin büyük olması, örüntülerin gerçekten var olduğunu göstermesi açısından bir avantajdır ancak böyle bir örneklemeden elde edilebilecek olası örüntü sayısı da çok büyüktür. Bu yüzden VM sistemlerinin karşı karşıya olduğu en önemli sorunlardan biri veri tabanı boyutunun çok büyük olmasıdır. Dolayısıyla VM yöntemleri ya sezgisel bir yaklaşımla arama uzayını taramalıdır, ya da örneklemeyi yatay/dikey olarak indirgemelidir. Yatayda indirgeme

veri alanının örneklenmesi, dikeyde indirgeme ise özelliklerin bulunduğu kolonların azaltılma çalışmasıdır.

2.6.2. Gürültü

Büyük veri tabanlarında pek çok niteliğin değeri yanlış olabilir. Bu hata, veri girişi sırasında yapılan insan hataları veya girilen değerin yanlış ölçülmesinden kaynaklanır. Veri girişi veya veri toplanması sırasında oluşan sistem dışı hatalara gürültü adı verilir. Günümüzde kullanılan ticari ilişkisel veri tabanları, veri girişi sırasında oluşan hataları otomatik biçimde gidermek konusunda az bir destek sağlamaktadır. Hatalı veri gerçek dünya veri tabanlarında ciddi problem oluşturabilir. Bu durum, bir VM yönteminin kullanılan veri kümesinde bulunan gürültülü verilere karşı daha az duyarlı olmasını gerektirir[10].

2.6.3. Eksik ve artık veriler

Verilen veri kümesi, eldeki probleme uygun olmayan veya artık nitelikler içerebilir. Bir değer bilinmiyor ya da yanlışlıkla girilmemiş olabilir. Veri madenciliğindeki birçok yöntem, her veri nesnesi için sabit bir boyut (özellik sayısı) gerektirdiğinden, eksik veriler sorun yaratır. Artık veri oluşumunu engellemek için özellik seçimi yapılmalıdır. Özellik seçimi yalnızca arama uzayını küçültmekle kalmayıp, sınıflama işleminin kalitesini de artırır.

2.6.4. Dinamik veri yapısı

Çevrim içi veri tabanları dinamiktir, yani içeriği sürekli olarak değişir. Bu durum, bilgi keşfi metotları için önemli sakıncalar doğurmaktadır. İlk olarak sadece okuma yapan ve uzun süre çalışan bilgi keşfi metodu, bir veri tabanı uygulaması olarak mevcut veri tabanı ile birlikte çalıştırıldığında mevcut uygulamanın da performansı ciddi ölçüde düşer. Diğer bir sakınca ise, veri tabanında bulunan verilerin kalıcı olduğu varsayılıp, çevrim dışı veri üzerinde bilgi keşif metodu çalıştırıldığında, değişen verinin elde edilen örüntülere yansıması gerekmektedir. Burada kuralların hala aynı kalıp kalmadığı ve istikrarlılığı problemi ortaya çıkar. Öğrenme sistemi,

kimi verilerin zamanla değişmesine ve keşif sisteminin verinin zamansızlığına karşın zaman duyarlı olmalıdır[11].

BÖLÜM 3. SUÇ VERİ MADENCİLİĞİ

Suç veri madenciliği, kriminal araştırmacıların büyük veri tabanlarını veri analistleri gibi hızlı ve etkili bir şekilde inceleyerek çalışmalarını sağlayan güçlü bir araçtır. Bu teknikler, verimliliğin artırılması ve hataların azaltılmasıyla polisin çalışmasını ve dedektiflerin zamanlarını diğer önemli işlere ayırmasını kolaylaştırabilir.

Bilgisayarlar, binlerce işlemi saniyeler içinde yaparak zamandan çok büyük miktarda tasarruf sağlarlar. Bilgisayarlarla insanların iş gücü karşılaştırıldığında, bilgisayarlardaki programın kurulum ve çalıştırılması, personel tutma ve eğitiminden daha az oranlarda parasal güç gerektirmektedir. Ayrıca bilgisayarlar, özellikle uzun çalışma saatleri göze alındığında insanlara göre hataya daha az yatkındır.

3.1. Suç ve Suç Tipleri

Suç, yasak alanlara park etmekten uluslar arası örgütlü terör hareketlerine kadar geniş bir yelpazede tanımlanır. Topluma verdikleri zarara göre suçlar birkaç kategoriye ayrılabilir. Örneğin hırsızlık suçu suçun işlendiği şehirdeki polis birimlerini ilgilendirirken, tarihi eser kaçakçılığı uluslar arası boyutlardaki birimlerin çalışma alanıdır.

Çoğu suç, örneğin kitle imha silahları(biyolojik, kimyasal…) üretilmesi hem ulusal hem küresel suçlar tanımında yer alır. Uluslar arası dolandırıcılık ve çalıntı mal trafiği ticareti, iş dünyasını ve hükümeti etkileyen suçlardır. Yabancı kaynaklı uyuşturucu tacirliği yapan yerel çeteler, kamu sağlığını ve güvenliğini zarar vermekle birlikte finansal olarak büyük zarar vermektedir. Birçok saldırı suçu (cinayet, hırsızlık, taciz…) yerel polisin çalışma alanında olmasına rağmen, terörizm hükümetin bütün seviyelerden birimlerinin birlikte çalışmasını gerektiren küresel bir sorundur.

3.2. Suç Veri Madenciliği

Suç veri madenciliği, kriminal araştırmacıların büyük veri tabanlarını veri analistleri gibi hızlı ve etkili bir şekilde inceleyerek çalışmalarını sağlayan güçlü bir araçtır. Bu teknikler, verimliliğin artırılması ve hataların azaltılmasıyla polisin çalışmasını ve dedektiflerin zamanlarını diğer önemli işlere ayırmasını kolaylaştırabilir.

Değişik kaynaklı veriler, yoğun ağ trafiği sık çevrimiçi işlemler ve kural dışı bilgilerin de bulunduğu büyük boyutta veritabanı suçlar arasındaki ilişkiyi ortaya çıkarmayı zor hale getirmektedir. Siber suçları belirlemek zordur. Siber suçları belirlemenin zorluğu meşgul ağ trafiği, sık çevrimiçi işlemler kural dışı bilginin az yer aldığı büyük boyutta veri kümesi gibi nedenlere dayanmaktadır.

3.3. Suç Veri Madenciliği Önemli Kılan Faktörler

Verimliliği artan ve hataları azalan suç veri madencilik teknikleri, polislerin işlerini kolaylaştırır ve tetkikçilere kendi zamanlarını daha değerli işlerde kullanma imkanı yaratarak işleri kolaylaştırır. Büyük veritabanlarında çabuk ve verimli işlemleri gerçekleştiren veri analistliği konusunda az bilgiye sahip kriminal teftişleri için veri madenciliği çok güçlü bir araçtır. Bu sayede fazla çaba sarf etmeden zaman kazandırır.

3.4. Suç Veri Madenciliği Yöntemleri

Suç madenciliği yöntemlerini aşağıdaki başlıklar halinde toplamak mümkündür;

3.4.1. Yapı çıkarımı

Polislerin olay raporlarından aşağıdaki alanlarda veri toplanabilmektedir;
- İnsan
- Araç
- Adres
- Narkotik

- Menkul Mallar

Bu yöntem polislerin olay raporlarından insan, araç, adres, narkotik ve menkul malların otomatik olarak belirlenmesinde kullanılır. Varlık çıkarımı suç analizinde temel bilgileri verir fakat bunun performansı var olan güvenilir temiz giriş datasının varlığına bağlıdır

3.4.2. Demetleme

Suç veri madenciliğinde bu yöntem, suç kayıtlarından insan, organizasyon, araç vb. farklı nesneler arasındaki benzerlikleri veya farklılıkları ortaya çıkarır.

Bu yöntem sınıf içi benzerlikleri küçüklemek ya da büyüklemek için benzer karakteristikteki veri öğelerinin sınıflarda gruplanması işlemleri sağlamaktadır. Ayrıca bu yöntem suç kayıtlarından insan, organizasyon, araç vb farklı nesneler arasındaki ilişkileri kurar. Aynı yöntemleri kullanan ya da farklı çetelere ait gruplardaki şüphelilerin belirlenmesinde kullanılır.

3.4.3. İlişkilendirme kuralı

Saldırı tespit sisteminde kişiler arasındaki etkileşim kayıtlarından ilişkilendirme kurallarının çıkartılmasıdır. Veritabanında sıklıkla oluşan veri setlerini bulur ve örüntüyü bir kural olarak gösterir. Bu yöntem saldırı tespit sisteminde kişiler arasındaki etkileşim kayıtlarından ilişkilendirme kuralının çıkarımında kullanılmaktadır.

3.4.4. Sıralı örüntü madenciliği

Saldırı Tespit Sisteminde zaman damgalı veriler arasındaki saldırı örüntülerini belirlemede kullanılır. Farklı zamanlarda oluşan işlemler kümesi üzerinden sıklıkla oluşan sıralı olayların bulunmasıdır. Saldırı tespit sisteminde zaman damgalı veriler arasındaki saldırı örüntülerini belirlemede kullanılır.

3.4.5. Sapma tespiti

Var olan veriden daha farklı işaretlenmiş verileri bulmak için özel değerleri kullanır. Bu yöntem dolandırıcılık tespiti, saldırı tespiti ve diğer suç analizlerinin belirlenmesinde kullanılır.

3.4.6. Sınıflandırma

İstenmeyen maillerin kaynağını gönderenin dilsel örüntüsünden ve yapısal özelliklerinden belirlemede kullanılır. Farklı suç olayları arasındaki benzer özellikleri bulur ve daha önceden belirlenmiş sınıflarda bu verileri toplar. Bu yöntem istenmeyen maillerin kaynağını gönderenin dilsel örüntüsünden ve yapısal özelliklerinden belirlemede kullanılır. Sınıflandırma suç olaylarının belirlenmesinde gereken zamanı azaltır.

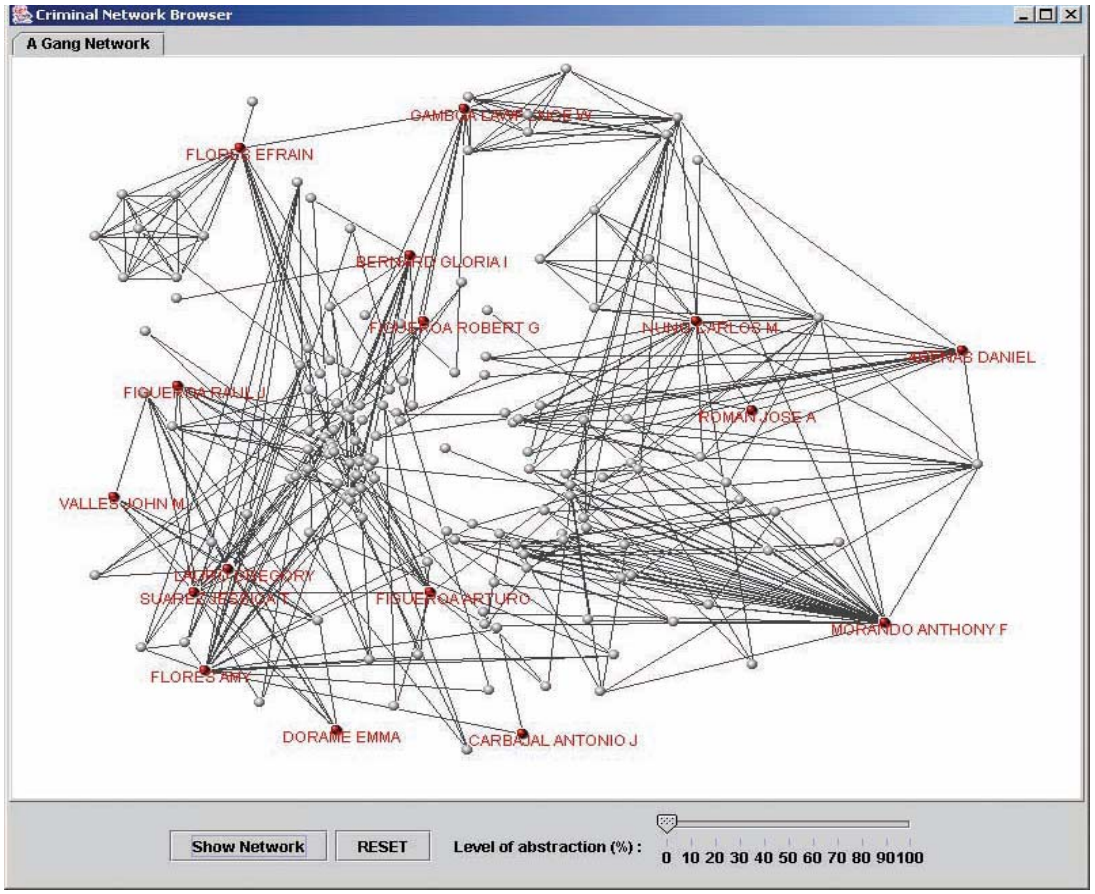
3.4.7. Dizi karşılaştırıcı

Suçlu kayıtlarından isim, adres, kimlik numarası gibi bilgilerde aldatıcı(yanıltıcı) bilgiyi belirler.

3.4.8. Sosyal ağ analizi

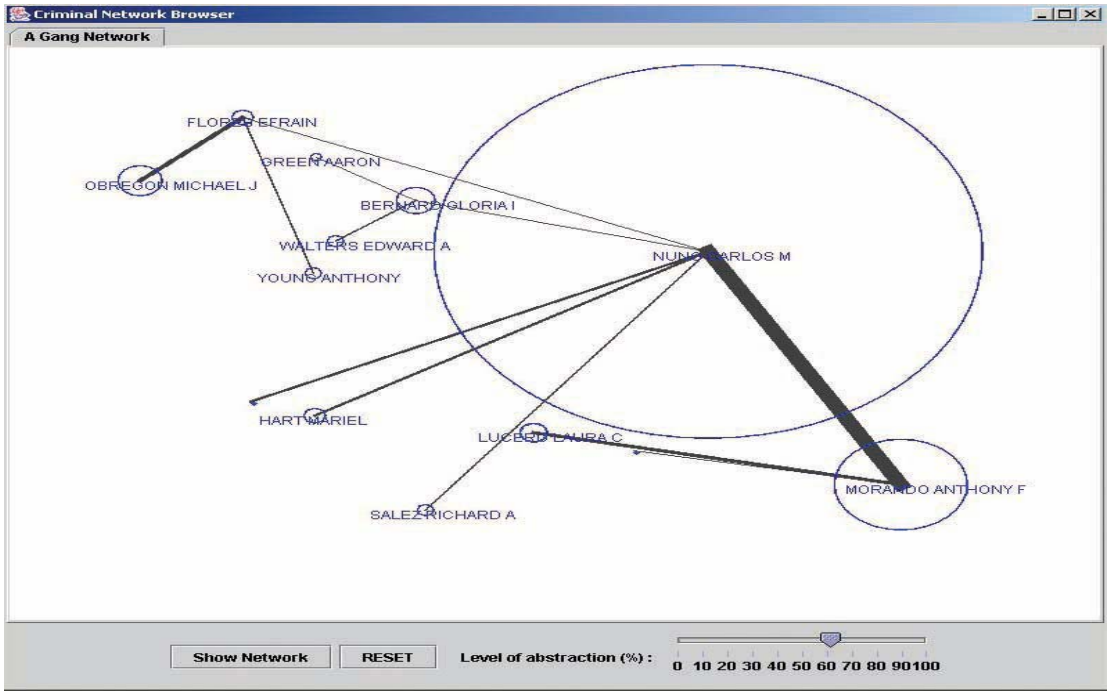
-Suçluların rollerine ait
-Bilgi akışına ait ve
-Bu olaylar arasındaki ilişkileri kuran bir ağ oluşturur.
(SNA) Kavramsal bir ağda uçların(node) rollerini ve aralarındaki ilişkileri tanımlar.

Şekil3.1’de Tucson polis biriminde veri tabanında kayıtlı 164 çete mensubu arasından 16 tanesi belli bir suç için şüpheli olarak belirlenmiştir



Şekil 3.1. Tucson polis birimindeki 164 çete mensubunun SNA yardımı ile çizilmesi

Şekil 3.2'de Şekil 3.1'deki alt gruplar ve liderleri daireler ile gösterilmiştir. Dairelerin büyüklüğü grup üyelerinin sayısına bağlıdır.



Şekil 3.2. Alt gruplar ve liderleri

3.5. Dünya'daki Suç Veri Madenciliği Örnekleri

3.5.1. Ricmond polis karakolu

Ricmond Polis Karakolu Suçları öngörmek ve önlemek için geliştirdiği veri madenciliği sistemi ile elde ettiği sonuçlar aşağıdaki gibidir:
%49 ateşli silah kullanımı şikayetlerinde azalma meydana gelmiş ve akabinde %246 silah ele geçirme artışı olmuştur.

Etkili personel kullanımı sayesinde daha önce başka işlerde çalışmak zorunda kalan yaklaşık 50 uzman personelin uzmanlık alanlarında konuşlandırılabilmesi sağlanmıştır. Sistemin çalışmaya başladığı ilk 8 saatte yapılan uygulamalar ve incelemeler sonucunda 15.000 dolarlık kazanç sağlanmıştır[12].

3.5.2. Amsterdam polis karakolu

Bilgiler arasındaki benzerlik ve ilişkileri bulan, terörizm alanında daha etkili, terör olaylarını önceden haber verecek olan bir sistem gerçekleştirildi. The LAPD Counter

Terrorism and Criminal Intelligence Bureau adı verilen sisteme 1 milyon dolar harcadı. Özellikle de 911 olayında eleştirilen emniyet güçleri ellerinde çok fazla bilgi olduğunu ancak gerekli olduğu anda bu bilgileri nasıl değerlendirmeleri gerektiğini bilmediklerini, geliştirilecek bu sistem sayesinde bilgiler arasındaki benzerlik ve ilişkileri bulup özellikle de terörizm alanında daha etkili ve önceden haber verecek bir bilgilendirme ortamı yaratmayı hedeflemektedir.

3.6. Türkiye'deki Suç Veri Madenciliği Örnekleri

3.6.1. Suç Analiz merkezi işletim sistemi

Suç Analiz Merkezi projesi kapsamında kullanılan sistem, asayiş uygulaması ve analiz yazılımları bileşenlerinden oluşmaktadır. Asayiş uygulaması ile olaya ve olaya karışan şahıs ve eşyaya ilişkin detaylı veri girişi yapılabilmektedir. Web servisleri sayesinde girilen veriler POLNET ve MERNIS veritabanları ile teyit edilmekte ve sistem kullanıcıyı yönlendirmektedir. Sistem veri girişini kolaylaştıran, kullanıcı hatalarını en aza indiren ara yüzlere sahip olduğu gibi adres girişlerinde coğrafi bilgi sistemleri ile entegre olarak harita tabanlı noktasal seçim veya bölgesel seçimler yapılabilmesini sağlamaktadır. Asayiş uygulaması ile suç analiz merkezi'nde toplanan veriler, proje kapsamında geliştirilen analiz yazılımları ve VisuaLinks ile detaylı analizler yapmak üzere kullanılmaktadır. SAMIS ve VisuaLinks sistemle entegre olarak çalışmakta ve görsel veri analizi için kullanılmakta olup; Suç Analiz Merkezi'nin ana hedeflerinden olan; verilerin birbirleriyle olan ilişkilerinin tanımlanabilmesi, suçlu profillerinin çıkarılabilmesi, suç dağılımlarının harita üzerinde gösterilmesi ve Türkiye'nin dijital suç haritasının oluşturulabilmesini sağlamaktadır. Sistem, ürettiği veri ve raporları diğer emniyet birimleri başta olmak üzere, Devlet İstatistik Enstitüsü, Adalet Bakanlığı gibi birçok devlet kurumuna güvenli bir biçimde aktarabilecek altyapıya sahiptir.

Tüm il ve ilçe teşkilatlarını kapsayan gelişmiş yetkilendirme mekanizmasına sahip olan sisteme kullanıcılar kendilerine verilen kullanıcı adı ve şifre ile erişebilmekte olup, kullanıcı giriş yaptıktan sonra kendisine atanan yetkiler kapsamında istediği tüm işlemleri sadece Internet Explorer kullanarak yerine getirebilmektedir.

Sistem kullanıcılarına kusursuz hizmet vermek üzere tasarlanmış olup, kesintisiz erişimi sağlamak üzere Suç Analiz Merkezinde yük dengelemeli (load-balance) çalışan kümeli (cluster) ve yedekli (fail-over) yapıda güçlü sunuculardan oluşmaktadır.

3.6.2. Asayiş uygulaması

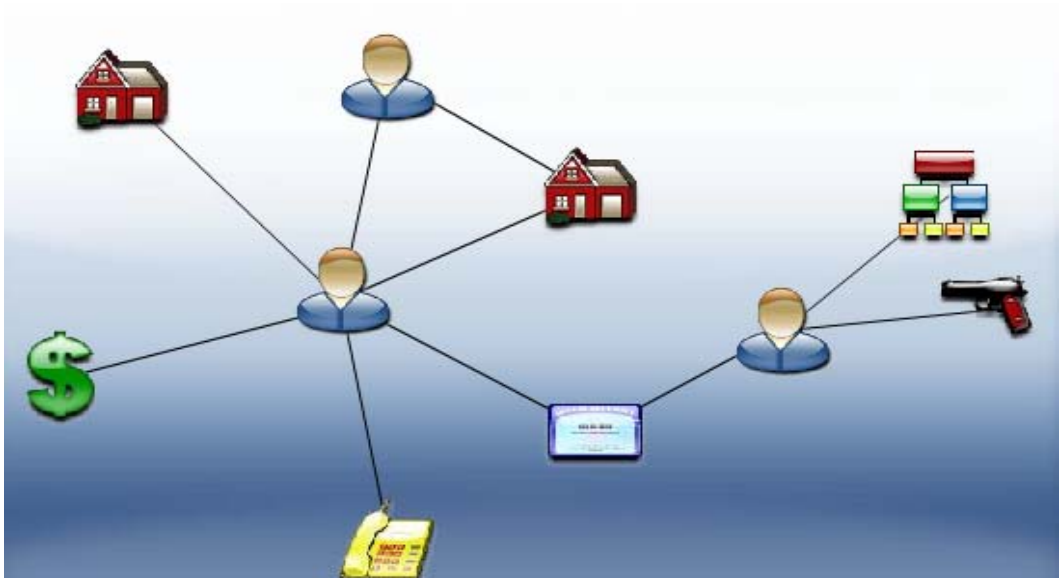
Genel olarak "Olay Giriş" ekranı ve alt fonksiyonları altında toplanmış olan Asayiş Uygulaması web tabanlı bir uygulama olup, tüm POLNET erişimi olan istemcilere, bir kurulum gerekmeksizin Web Browser aracılığıyla erişilebilir olacaktır. Uygulama aracılığı ile olayla ilgili kişi bilgilerinin girişi Mernis Web Servisleri ile entegre çalıştığından hatalı kişi bilgisi girişini engellemektedir. Aynı şekilde olaya karışan eşya (silah, araç, diğer) bilgisinin girişi ve POLNET veritabanındaki mevcut eşya bilgileri kullanıcıya sağlanmaktadır. Olay listesinden girişi yapılan olayı türü seçilebilmekte ya da sadece olayın kodu girilerek olayın türü çağrılabilmektedir. Her olaya özel otomatik olarak çıkan olay detayı giriş ekranı, kullanıcının sadece seçtiği olaylarla ilgili sorularla karşılaşmasını sağlayarak veri girişi rahatlığı sağlamaktadır. Coğrafi Bilgi Sistemi üzerinden alınan harita verileriyle entegre adres bilgisi girişi ile görselliği ve kullanım kolaylığı ön planda olan bir sistem oluşturulmuştur. Veri girişi yapılan tüm bu alanlar da sorgular yapılabilmekte, gelişmiş aramalarla son kullanıcının yetkisi bazında istediği veriye erişebilmesi mümkün olmaktadır. Sistem tutanak oluşturulması ve görevli savcı bilgisi girişi gibi işlemler yapılmasında kolay veri giriş ekranları sağlamakta ve ilgili birimlere iletilmek üzere PDF, Excel, XML, JPG vb. biçimlerde çıktılar üretebilmektedir.

Girilen veriler ışığında oluşturulan veritabanı, yapılacak detaylı analizlerde kullanılacak nitelikte tasarlanmıştır. Asayiş Uygulamasının en önemli görevlerinden biri olan analize esas data toplamanın ardından, Suç Analiz Merkezi İşletim Sistemi, verileri yapılacak analizler için kullanılacak analiz araçlarına uygun olarak hazırlar ve asayiş uygulaması haricinde sisteme dahil edilecek verilerin analiz uygulamalarına dahil edilmesini sağlar. Asayiş uygulaması ile veritabanında toplanan veriler ve SAMIS'ın veri aktarım modülleri kullanılarak sisteme aktarılan diğer harici veriler, sistemdeki analiz araçlarına uygun formatlarda aktarılarak detaylı

analizlere tabi tutulabilmektedir. Oluşturulan veritabanı üzerindeki tüm bilgiler oluşturulan ilişkilere bağlı olarak çok yönlü olarak sorgulanabilecek, raporlar oluşturulabilmektedir.

3.6.3. Benzer uygulamalar

Görsel analiz araçları ile veri alanları sürükle bırak yoluyla analiz edilerek veriler arasındaki ilişkileri görsel olarak modellenmektedir. Kişi bilgisinin başka bir kişi ile bir telefon numarası ya da banka hesabı ile bağlantısı görsel olarak tespit edilerek, ham veritabanı verisinin kullanışlı analiz raporları haline getirilmesi mümkün olmaktadır.



Şekil 3.3. VisaulLinks'ten örnek ekran görüntüsü

Bu sistemde kullanılan görsel analiz araçları, dünyada FBI, CIA gibi birçok büyük emniyet kuruluşu tarafından kullanılan, yetkinliği referansları ile kanıtlanmış bir veri madenciliği aracıdır. Sistemle, coğrafi bilgi sistemi'yle ve veritabanı yönetim sistemleriyle entegre çalışan bu araçlar, veri desenlerini ve ilişkilerini görsel olarak ortaya koyarak Türkiye'nin dijital suç haritasının ve suç trendinin oluşturulmasından anahtar görev almıştır. Sistemin ürettiği veriler, modellenerek detaylı sorgular yapılmak üzere hazır hale getirilebilmektedir. Benzer şekilde veriler SPSS analiz

programı tarafından kullanılmak üzere hazırlanacak ve istatistiksel analizler yapılabilmektedir. Sistem ürettiği raporlardan seçilen bazı önemli verileri görsel olarak, suç analiz merkezinden konumlandırılmış bir dev ekran üzerinden canlı olarak yayınlamaktadır. Bu vesileyle, ülkemizdeki suç trendi anlık değişimleri görsel grafiklerle ve harita üzerinde işaretlenmiş veri dağılımları ile izlenebilmektedir.

3.7. Suç Analizinde Kullanılan Veri Madenciliği Teknikleri

İlişkisel analiz, sınıflandırma ve tahmin, kümeleme(cluster) analizi ve outlier analizi suç analizinde kullanılan veri madenciliği teknikleridir. Yeni teknikler yapılandırılmış ve yapılandırılmamış veri şablonlarını açıklar.

Entitiy extraction, metin, resim ve ses gibi verilerden üretilen özel şablonları açıklar. Polis raporlarından otomatik olarak, kişileri, adresleri, araçları ve kişisel karakteristik özellikleri açıklar.

Clustering teknikleri benzer karakteristik özelliklerine göre gruplandırarak, sınıf içi benzerliği artırır ya da azaltır. Örneğin benzer yöntemlerle suç işleyen şüphelilerin bağlantılarını ve benzerliklerini gruplama gibidir.

Association rule mining veri tabanında sıkça görülen item set'lerini keşfeder ve şablonları kurallar olarak sunar. Bu teknik kullanıcıların hareketlerinin takip edilerek network saldırılarının tespit edilmesinde kullanılmaktadır. Araştırmacılar ayrıca network saldırganlarının profillerini oluşturmada bu tekniği kullanarak gelecekte olası saldırılarının tespit edilmesini sağlarlar.

Association rule mininge benzer olarak Sequential Pattern Mining farklı zamanlarda gerçekleşen ve sıklıkla karşılaşılan ardışık item set'leri bulur. Network saldırısı tespitinde bu yöntem zamana bağlı veride saldırı şablonlarını tanımlayabilir.

Deviation detection verinin tamamından ziyade geri kalanından açıkça ayrılan bir bölümüyle çalışmak için özel ölçümler kullanır.

Classification değişik suç tiplerinin ortak özelliklerini bularak bunları birlikte sınıflandırır. Bu teknik spam e-postaların kaynağının, dil özelliklerine bakılarak bulunmasında kullanılır.

Kelime karşılaştırıcı veri tabanı kayıtlarında metin alanlarını karşılaştırır ve kayıtlar arasındaki benzerlikleri bulur. Kriminal kayıtlarda yaş, adres, kimlik numarası bulunmasında kullanılır. Araştırmacılar kelime karşılaştırıcıyı metin tabanlı analizde kullanabilirler fakat çok yoğun işlem gerektirir.
Social network analysis kavramsal ağdaki düğümler arasında etkileşimleri ve bu düğümlerin işlevlerini tanımlar.

BÖLÜM 4. SOSYAL AĞ ANALİZİ

4.1. Sosyal Ağ Analizi

Sosyal ağlar insanlık tarihi kadar eski ilişkilerdir. İnsanlar arasındaki politik, resmi-gayri resmi, ailevi, coğrafi ya da herhangi başka bir şekildeki ilişkiler sosyal ağları oluşturur. Bu ağları analiz etmek için kullanılan bilgisayar teknolojilerinin artan miktardaki yazılımı ve kullanımı, sosyal ağ analizi yöntemini akademik ve diğer sahalar için erişilebilir konuma getirmiştir. Halen bu alanda geliştirilmiş birçok bilgisayar programı olması ve bir yenisinin her gün ortaya çıkması bu alanın gelecekte ne kadar gelişeceğinin de göstergesidir.

Sosyal ağ analizi(SAA) bir grup aktörün sosyal ilişkileri üzerine yapılan çalışmaya denir. Ağ analizi ve sosyal bilimlerdeki diğer yaklaşımlar arasındaki temel fark, aktörlerin kişisel özelliklerinden çok, aktörler arasındaki ilişkilere odaklanılmasıdır. Ağ analizi yaklaşımına göre bireysel bağlantılıklardan ötürü ortaya çıkan ilişki türleri ve örüntülerinin varlığı ya da yokluğunun ağ ve ağın bileşenleri üzerinde etkisi vardır. Örnek olarak, bilimsel bir topluluktaki bir kişinin performansını değerlendirirken geleneksel bir sosyal bilimsel yaklaşım araştırmacının yaşı, yayın sayısı vs. gibi kişisel özellikleri ile ilgilenir. Daha sonrasında toplanan bu veriler üzerinde istatistiksel analizler yapılır. Ağ analizinde ise bilimsel topluluk içindeki bağlantı ve ilişkilere odaklanılır. Örneğin, bu topluluktaki araştırmacıların ilişkilerine ve bu ilişkilerin çalışma üzerindeki potansiyel avantaj ve dezavantajları üzerinde durulur.

Bireyler arası ilişkilerin sayısallaştırılıp bilimsel hale getirilmesi de demek olan sosyal ağ analizi, önemli olaylar karşısında çeşitli organizasyonların, ya da bu organizasyonların oluşturduğu ağların da ilişkilerini rakama dökmek için kullanılmaktadır. Bilgisayar programlarına girilen verilere göre alınacak olan çıktının

niteliği de değişmekte ve bu esneklik organizasyonlardaki verimliliği test etmek için kullanılabilecek yeni bir olanak sağlamaktadır. Eski Irak kralı Saddam Hüseyin'in yakalanmasında bireysel ağ ilişkilerini etkili bir biçimde ortaya koyan UCI-NET isimli programın Amerikan ordusu tarafından kullanıldığı ve yine başka bir terör ağının SNA yardımıyla ortaya çıkarıldığı bilinmektedir.

Batı Avrupa'da SNA, ekonomik ilişkileri ortaya koymak amacıyla kar amacı güden organizasyonların bağlantılarını işlemek üzere kullanılırken, ABD'de her türlü ikili ya da daha çoklu ilişkiyi ortaya çıkarmak için kullanılmaktadır. Özellikle sosyal ilişki kurma amacıyla kurulmuş internet sitelerinde bireylerin diğerleriyle kurdukları kontakların bilimsel dilde anlaşılabilmesi için SNA'lar yoğun bir şekilde kullanılmaktadır. Yine bu amaçla Facebook, MySpace, Linked-in vb. sitelerde sosyal ağ grupları kurulmakta ve bilginin bireyler arasında ne yönde taşındığı konusunda araştırmalar ortaya konmaktadır.

Geniş bant internet bağlantısı kullanan her beş internet kullanıcısının dördünün Facebook, MySpace, Linked-in ya da diğer bir sosyal ağa üye olduğu Parks Associates adlı şirket tarafından yapılan bir araştırma ile ortaya konulmuştur. Hedef odaklı ve geri dönüşü yüksek olarak nitelendirilen sosyal ağlar günlük yaşamda olduğu kadar, iş hayatındaki yerini de almış durumdadır.

Sosyal ağları bu kadar çekici kılan etken, bu ağlar üzerinden hedef kitle analizinin yapılabilmesi ve bu analiz doğrultusunda tam da hedefe yönelik pazarlama modellerinin oluşturulabilmesi ve binlerce kategori arasından firmanın hizmet alanına uygun hedef kitleyi belirleme imkânına sahip olunabilmesidir.
Sosyal ağlar bu kadar yaygınlaşıp hayatımızın bir parçası olunca, normal olarak pazarlama dünyasının da ilgisini çekmiştir. Bu ilgi sosyal ağlarda, sosyal ağ analizinin yapılmasını zorunlu kılmıştır. Peki, bu sosyal ağlarda SAA nasıl yapılmaktadır.

Sosyal ağ analizinde en önemli faktör güçlü bir veri kaynağıdır. Bu veri kaynağı milyonlarca üyeyi barındıran sosyal ağlarda bolca bulunmaktadır. Bu platformlar, kişilerin internete bağlanma alışkanlıklarını ve diğer kişilerle kurdukları bağları

ortaya koyan ham veri için bulunmaz bir kaynak oluşturmaktadır. Sosyal ağları bu kadar değerli kılan, milyon dolarlık fiyatlara ulaşmalarını sağlayan içerdikleri büyük çaplı verilerdir. Sosyal ağlar aracılığı ile bulunan verilerin düzgün şekilde işlenerek doğru yorumlanması gerekmektedir. Analiz ve yorumlama safhasında dikkat edilecek nokta, topluluk içerisinde etkisi yüksek ve çevresi geniş kitlelerin, diğer bir değişle fikir liderlerinin belirlenmesi işlemidir. Lider konumda olan kişilere yönelik yapılan kampanyalar şirket verimliliğinde yüzde yirmilere varan bir oranda artış sağlamaktadır. Popüler kişilerin davranış tarzını, eğilimlerini, tercihlerini benimseyen diğer kullanıcılar, fikir lideri olarak gördükleri bu kişilerin izinden giderek her biri hedef kitlenin bir halkasını oluşturan potansiyel müşteri durumuna gelmektedirler. Böylelikle rekabetçi ortamda hedef kitlesini iyi tanıyan ve kitlesine yönelik pazarlama faaliyetleri geliştiren firmalar bir adım öne çıkarak diğer firmalar arasından sıyrılabilmektedirler. Sosyal ağlar üzerinde yapılan kampanyalar bir çığ etkisi ile büyüme göstermektedir. Örneğin x sosyal ağında aktif rol oynayan bir kişiyi yaptığınız pazarlama faaliyeti ile etkilediniz ve bu kişi sizin ürününüzün veya markanızın bir sözcüsü haline geldi. Doğal olarak günlük hayatında olduğu gibi sosyal ağ üzerinden temas kurduğu kişileri de sizin lehinizde etkileyecektir. Etkilenen kişiler de temas ettikleri diğer kişileri etkileyecek ve bu bir zincir şeklinde sürüp gidecektir.

Ülkemizde gerek akademik, gerekse iş dünyasından yeterli ilgiyi görmeyen SNA hakkındaki az miktardaki çalışmaların da büyük bölümü ekonomik ilişkiler, şirketler arası ağlar ve bu şirketlerin yönetim problemlerinin çözümü hakkındadır. Güncel anlamda sosyal ağ analizi, Ülkemizde SAA, SAA'yı bir yöntem olarak içinde barındıran Microsoft tarafından geliştirilen CETS programı ile duyuldu. Çocuk istismarı suçuyla mücadelede başarıyla kullanıldı ve kamuoyu tarafından olumlu karşılandı. Fakat yine de ABD'de gerek akademik, gerek iş dünyasının, gerekse hükümet dairelerinin yoğun şekilde kullandığı bu metot, bundan daha fazla ilgiyi hak etmektedir.

Sosyal analizinde kullanılan başlıca programlar; UCI-NET, NetMiner, Pajek, ORA, Stat-Net, SocNet-V, InFlow ve Keyhubs'tır. UCI-NET, NetMiner yazılımları ABD'de yoğun bir şekilde kullanılmaktadır. Bu programlar genelde ücretsiz olup,

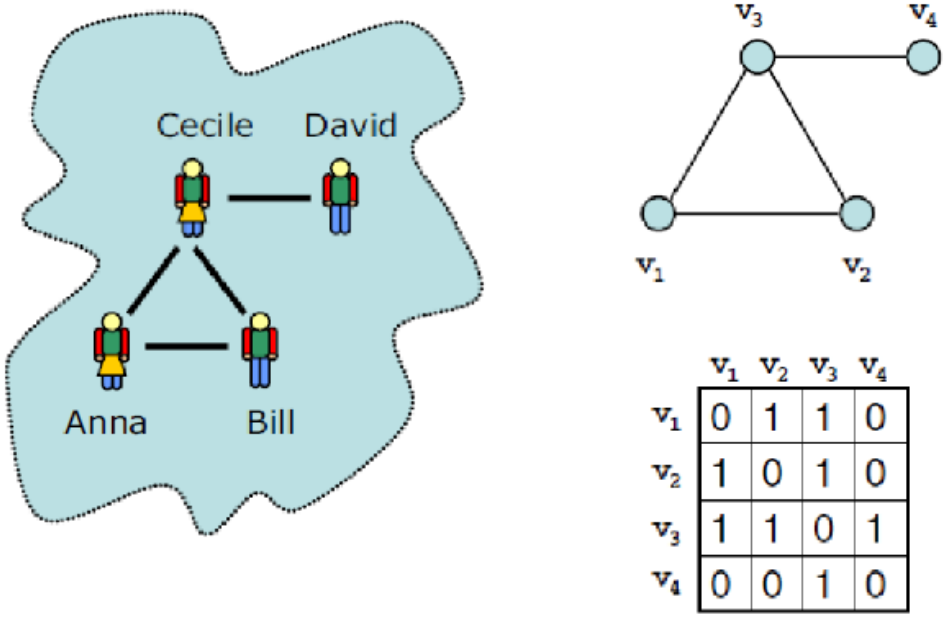
ayrıca bir kullanma kılavuzu da bulundurmaktadırlar. Türkçe bir SNA maalesef henüz piyasada bulunmamaktadır.

Bu yazılımlar genelde ağ aktörleriyle (nodes) ilgili belli bir içerikte bulunan karşılıklı iki yönlü ya da direk tek yönlü ilişkileri bir matris tablosunda inceleyerek ilişkilerin yönü ve konumu konusunda bilgi sağlar. Dolayısıyla içerik, ağ aktörleri ve incelenen ilişki cinsi çok önemlidir. İçerik; gazete haberleri, resmi raporlar, bireysel anketler ya da ilişki sorgulayan diğer materyaller olabilir. İçeriğin objektif olması sonuçların da objektif olmasını sağlar.

Sosyal ağ analizi yapılarak aşağıdaki soruların yanıtlarını almak mümkündür:

-Ağ üzerinde en sıkı bağlı varlık veya üye nedir ya da kimdir?
-Ağın tamamında en önemli varlık veya üye nedir ya da kimdir?
-Bir ağın merkezideki kilit konumundaki varlık veya üye nedir ya da kimdir?
-Ağ içerisindeki bilgi akışı nasıl ilerlemektedir?

SNA yazılımları, içerikten oluşturulan ilişki matrisinden aldığı bilgiyi grafikler veya artan-azalan veri tabloları yoluyla kullanıcıya geri bildirir (Şekil 4.1).



	v1	v2	v3	v4
v1	0	1	1	0
v2	1	0	1	0
v3	1	1	0	1
v4	0	0	1	0

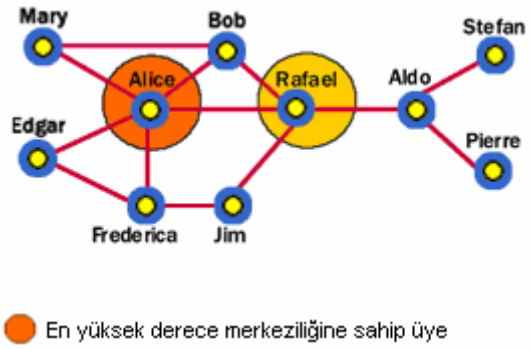
Şekil 4.1. Kişi bağlantılarının ilişki matrisi yardımı ile görselleştirilmesi

Bunlara kısaca değinmek gerekirse derece merkeziliği bir üyenin (node) diğerleri arasında ilişki olsun ya da olmasın bunlarla ilişkili olmayı, arasındalık merkeziliği iki ya da daha farklı üye grubu arasındaki kilit üyeliği, yakındalık merkeziliği kilit konumdaki üyelere daha yakın olmayı betimler. Bir üyenin ağın kilit üyesi olup olmamasını derece merkeziliği veya arasındalık merkeziliği belirler.

4.1.1. Derece merkeziliği

Derece merkeziliği bir üyenin diğerleri arasında olan direk bağlantı sayısıdır. Derece merkeziliğinde bağlantı sayısı en fazla olan üyenin özellikleri aşağıdaki gibi olabilir:

-Genellikle ağdaki en aktif kişidir.
-Bilgisayar ağları olarak düşünüldüğünde bu ağdaki bir hub cihazı olabilir.
-Ağdaki en avantajlı pozisyona sahip olan üye olabilir.



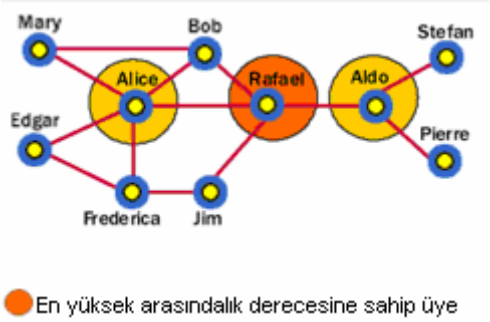
Şekil 4.2. Derece merkeziliği

4.1.2. Arasındalık merkeziliği

İki ya da daha farklı üye grubu arasındaki kilit üyeliği tanımlar. Arasındalık merkeziliği en fazla olan üyenin özellikleri aşağıdaki gibi olabilir:

-Ağ üzerindeki en güçlü ve en iyi pozisyonu belirtir.

-Ağ üzerinde ne olduğundan haberdar olan ve en büyük etkiye sahip olan üyeyi belirtir.

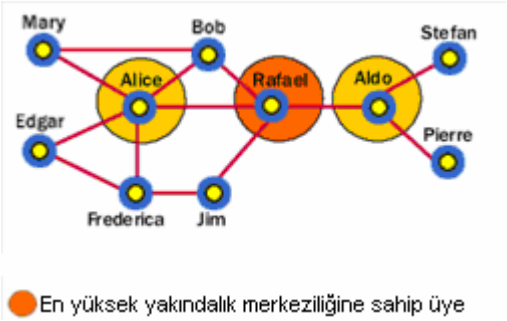


Şekil 4.3. Arasındalık merkeziliği

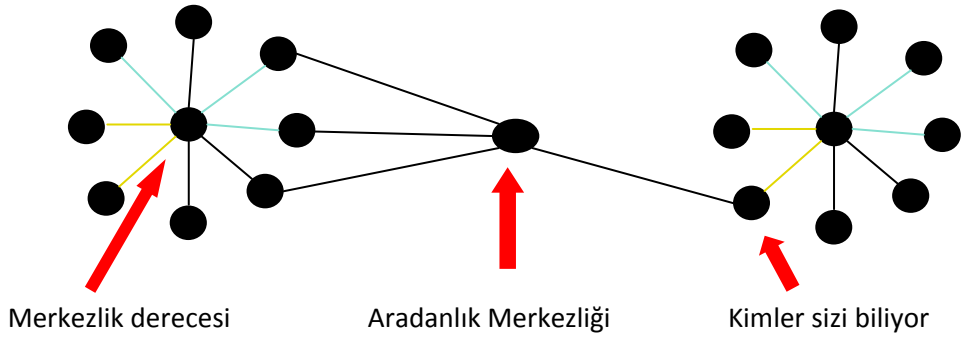
4.1.3. Yakındalık merkeziliği

Kilit konumdaki üyelere daha yakın olmayı betimler. Bir üyenin diğer üyelere ne kadar uzaklıkta olduğunun bir ölçüsü de yakındalık merkeziliğidir. Yakındalık merkeziliği en fazla olan üyenin özellikleri aşağıdaki gibi olabilir:

-Ağ üzerindeki diğer üyeler en hızlı şekilde ulaşabilir.
-Diğer üyelere erişirken en kısa yola sahiptir.
-Diğer üyelere en yakın elamandır.
-Ağ üzerinde neler olduğu en fazla görebilen üyedir.



Şekil 4.4. Yakındalık merkeziliği



Şekil 4.5. Merkeziliğin genel gösterimi

4.2. Sosyal Ağ Analiz'inin Gelişimi

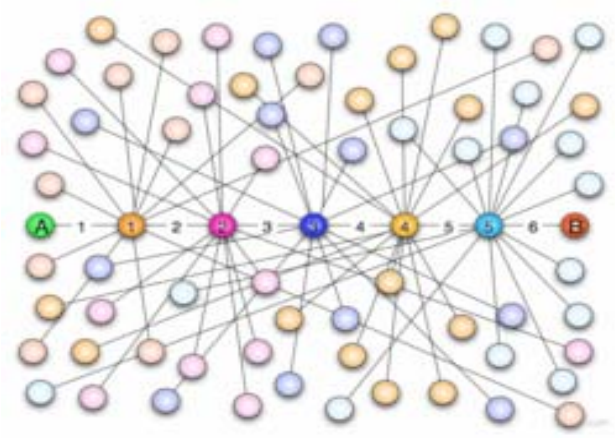
Sosyal ağ analizi sosyoloji, sosyal psikoloji ve antropoloji alanlarında yapılan bir dizi çalışmanın ortak ürünü olarak ortay çıkmıştır. 1950'lerden itibaren ağ analizi sosyolojik araştırmalara yapılan diğer yaklaşımlardan kendisini ayırmıştır. "Sosyal ağ" terimi ilk kez 1954 yılında Barnes tarafından kullanılmıştır.
Sosyal ağların genişlemesinde etkili olan en önemli gelişme ise son 20 yılda enformasyon teknolojilerindeki gelişmeler olmuştur.

4.3. Sosyal ağların küresel yapısı

Sosyal ağ analizi sosyal ağların analizine özgü bir dizi kavram ve yöntem geliştirmiştir. Bir sosyal ağ G=(V,E) grafiğinden oluşur ve E $\subset$ VxV'dir.
Amerikalı psikolog Stanley Milgram sosyal ağların yapısı hakkında önemli bir araştırma yapmıştır. Milgram, nerede yaşarsak yaşayalım, dünyanın bize çok küçük göründüğü ve karşılaştığımız insanları tanımasak da arkadaşımızın arkadaşı çıktığı gözleminden yola çıkmıştır. Milgram yalnızca gerçekten de hepimizin bağlantılı olup olmadığını test etmek istememiş, aynı zamanda amerikan toplumunun sosyal ağında herhangi iki birey arasındaki ortalama mesafenin ne olduğunu da araştırmak istemiştir.

Bu amaçla Milgram Boston, Massachusetts ve Omaha, Nebraska'dan rasgele seçilmiş birkaç yüz kişiye mektuplar verir. Katılımcılara bu mektupları Sharon,

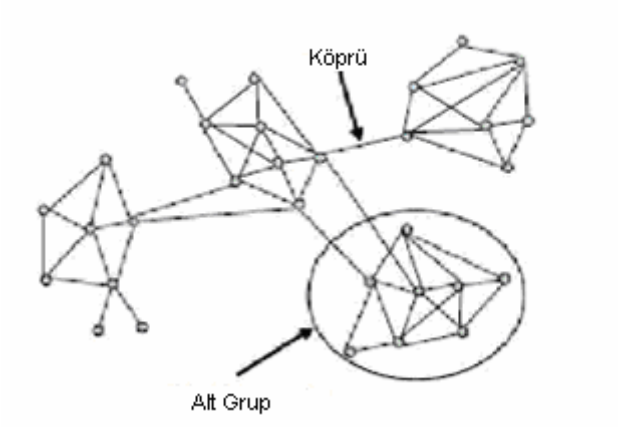
Massachusetts'teki bir borsacıya vermelerini ister. Ancak mektupları doğrudan hedef kişiye göndermelerine izin verilmez. Bunu yerine hedef kişiyi tanıyabilecek kişilere ileterek mektubu sahibine iletmeleri istenir. İlettikleri kişi de aynı kurala uyarak hedef kişiye mektubu ulaştırmaya çalışacaktır. Sonunda mektup hedef kişiyi tanıyan birisine ulaşacak ve ona elden verecektir. Araştırma sonucunda Milgram Amerikalıların birbirlerine en fazla 6 adım uzakta olduklarını hesaplamıştır (Şekil 4.6)[13]. Milgram'ın örneklemi küçük ve mektup toplamın sadece %20'ne ulaştığı için bu ortalama uzaklık daha fazla olabileceği gibi, daha büyük bir örneklemde mektup daha büyük bir oranda sahibine ulaşabileceğinden bu ortalama uzaklık daha da kısa olabilir.



Şekil 4.6. Yakınlığın 6 derecesi

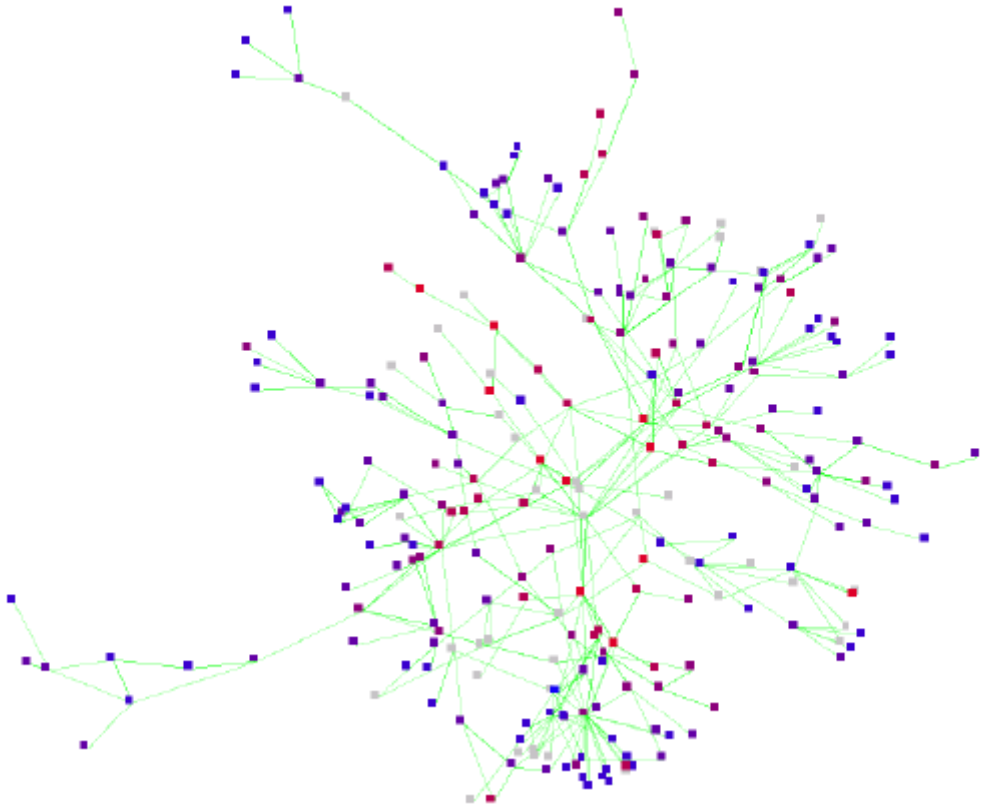
4.4. Sosyal Ağların Makro Yapısı

Yoğun kümeler veya sosyal gruplar birbirleri ile birkaç bağ ile bağlanmışlardır. Örneğin Şekil 4.7'de bilimsel bir topluluktaki işbirliklerini göstermektedir. Aynı kurumdaki bilim insanları birbirleriyle daha yoğun ilişki içindeyken farklı kurum ve ülkelerden bilim insanları da çeşitli yollarla birbirleriyle bağlantı kurmaktadırlar. Bu bağlantılar birkaç kısa adımla bilim insanlarının birbirleriyle ilişki kurmalarını sağlamaktadır.



Şekil 4.7. Bilimsel bir topluluktaki işbirlikleri

Tyler, Wilkinson ve Huberman kendi çalıştıkları laboratuarda şirket e-posta arşivini inceleyerek çalışanlar arasındaki iletişimi analiz etmişlerdir[14]. Belirli bir dönemde en az bir kez birbirlerine e-posta gönderen çalışanlar arasında bağlantı kurarak bir tartışma ağı oluşturmuşlardır. Tyler ve arkadaşları bu çalışma sonucunda bir örgüt içindeki liderlik rolünü, organize ve organize olmayan toplulukları belirlemede e-posta ağının faydalı olduğunu bulmuşlardır. Araştırmacılar bulgularını daha sonra çalışanlarla yapmış oldukları görüşmelerle doğrulamışlardır.



Şekil 4.8. HpLabs firmasındaki e-posta hareketlerinin SAA yardımı ile çizimi

4.5. Suç Örgütleriyle Mücadelede Sosyal Ağ Analizi ve Global Güvenlik

Örgütlerle mücadele (terör veya organize suç) ülke güvenliğini ilgilendirdiği kadar küresel güvenliğin de temel taşlarındandır. Sınır aşan örgütlü suçlarla mücadele bir ülke ne kadar güçlü olursa olsun tek başına başarılı olması pek mümkün değildir. Başarının ülkelerin ve kurumlarının işbirliğine bağlı olduğu bir mücadelede kullanılacak yöntemler de dünya düzenine uyum sağlamalıdır.

Teknolojinin en büyük faydalarından biri de iletişimi kolaylaştırmasıdır. Ama aynı zamanda iletişimin kayıt altında tutabilmesi insanlar arasındaki irtibatların tespitinin kayıt altına alınmasına sebep oldu. Önceleri örgütler iletişim içeriklerini gizli tutmaya çalışmaktaydılar. Analizler içerikten ziyade örgüt üyelerinin kimlerle irtibatlı olduğu, ne tür faaliyetler içersinde bulunduğunu delillendirmeye yetmektedir. Ağ tipi yapılanma örgüt içi ve örgütler arası irtibatları kontrol altında tutmaya yaramaktadır. Yakalanan alt birimler kolayca tasfiye edilmekte ve alt birimdekilerin üst birimleri deşifre etmesi zorlaştırılmaktadır[15]. Yıllar önce

kurulduğu tespit edilen birçok örgütün hücre tipinde yapılandığını yakın zamandaki soruşturmalarda görülmektedir. Ülkemizde Hizbullah veya Ergenekon gibi terör örgütlerinde görülen bu yapılanma El Kaide gibi uluslararası terör örgütlerinin yapılarında da ortaya çıktı[16].

Bu örgütlerin eylemleri, stratejileri ve kısmen üyeleri deşifre edilebilmektedir. Fakat klasik polis yöntemleriyle kişiler arasındaki en üst bağları çözmekte yeterli olmadığı gözlemlenmektedir. Halen Ergenekon davasında da görülen en büyük problem örgütün liderinin kim olduğu, kararların kimler tarafından alındığı, eylemlerin kimlere yaptırıldığı, yakalanmayan kişilerin rolünün ne olduğu ve kimler olduğudur. Bu bilgiler olmadan örgütlerin çökertilmesi mümkün değildir. Bu bağlar çözülmezse davanın tutarlılığı azalmakta, kimlerin hangi suçtan yargılanacağı belirsizlik göstermekte ve örgütün kendisi değil alt birimleri tasfiye edilmektedir. İleri düzey bir analiz olamadan peyderpey yakalanan kişilerin örgüt içindeki yerini ve örgütün yapısını tespit etmek çok zordur.

Polis tarafından ağ analizi anlamında kullanılan en yaygın yöntem I2 türü programlardır. Fakat bu programlar polisin elindeki verilerden birisi olan telefon kayıtları üzerinden yapılmaktadır. Günümüzdeki örgütler artık doğrudan telefon görüşmesi yapmayacak kadar gelişmiştir. Polisin klasik anlamda yaptığı bu analizden ortaya çıkacak ağ telefon kayıtlarından ve itiraf bilgilerinden öteye gitmeyecektir. Bu mevcut bilgiler örgütlerin analizi için yeterli değildir. Daha ileri düzey bir analiz ise sosyal ağ analizi ile mümkün olmaktadır.

Sosyal ağ analizi çalışmaları yeni yeni suç örgütlerini analiz etmek amacıyla kullanılmaktadır. Yeni bir terminoloji gerektiren araştırmalarda ağ için kullanılan temel prensipler de gelişmektedir. Bu çalışmalar teorik olarak karanlık network (dark network) adı altında yapılmaktadır[17]. Karanlık isminin kullanılmasının sebepleri bu örgütlerinin faaliyetlerinin bilinmemesi ve öngörülen hipotezlerin bilimsel olarak test edilmesinin zorluğundandır.

Bu metodun kullanılması için telefon kayıtları, internet üzerinden veya yüz yüze yapılan iletişim kayıtları, polis takip raporlar ve sorgulama sonrası sanıklardan elde

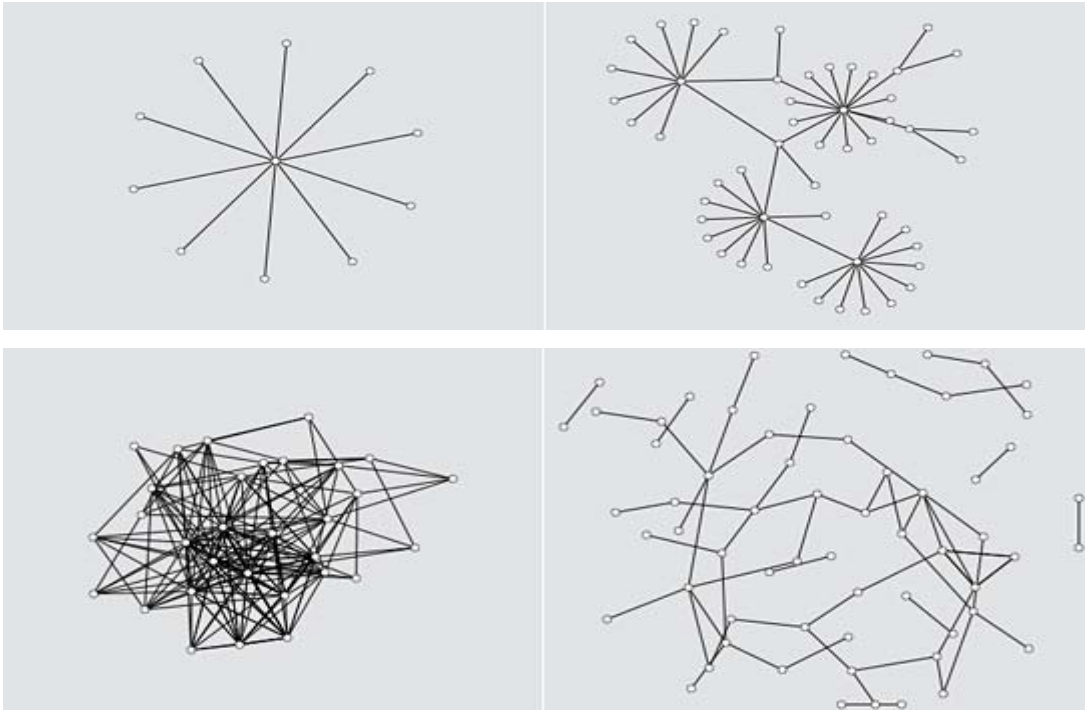
edilen bilgiler toplanmakta ve hepsi aynı anda analiz edilmektedir. Örgüt üyelerinin bütün iletişim bilgilerinin analiz edilmesi karanlıkta kalan birçok noktayı aydınlatmaktadır. Bu analizde en önemli unsur ise klasik sosyal ağ analizinden farklı bir metodun incelenmesi gerekliliğidir. Çünkü karanlık ağların işleyişleri normal hayattaki insanların kuracağı iletişimden farklıdır. Mesela örgütlerin hiyerarşik yapıları ağ analizi açısından farklı bir yaklaşım gerektirmektedir. Klasik yaklaşımda bir kişiden diğer kişiye giden yol ne kadar kısa ise kişinin networktaki rolü o kadar güçlüdür ama bu suç örgütlerinde irtibatların kısa ve ulaşılır olması değil güvenli olması daha önemlidir. Lider herkesin ulaşabildiği değil hatta kimsenin ulaşamadığı kişi olmalıdır. Klasik telefon kayıtlarında bu bağın ortaya çıkması çok zordur hatta mümkün değildir. Bu önemli nokta sadece örgütün içyapısını değil diğer örgütlerle irtibatını da ortaya koymaktadır. Çünkü diğer örgütlerle ilişkileri karşılıklılık esasına dayanmaktadır ve aynı hiyerarşik seviyedeki kişiler birbirleriyle görüşmektedirler [18]. Ergenekon davasında sözü edilen Hizbullah ve PKK bağlantıları örgütlerin operasyonel düzeyde mi irtibatlı oldukları yoksa fikirsel düzeyde mi oldukları bu tür analizler ile ortaya çıkabilmektedir. Eğer irtibatlar operasyonel düzeyinde ise PKK'nın bazı eylemleri PKK'ya rağmen yapıldığını gösterebilir.

Sosyal ağ analizi sadece güvenlik güçlerinin etkisini arttırmamakta, küresel güvenliğe de katkı sağlamaktadır. Özellikle sınır aşan suçlarda birçok ülkeden toplanacak veriler tek bir sistemde analiz edilebilir. Bu sayede El Kaide gibi örgütlerin hangi ülkede nasıl yapılandığı, hangi ülkelerde ne tür eylemler yaptığı, hangi ülkelere eylem planlarının gittiği ve hangi ülke vatandaşlarının kullanıldığı gibi bilgileri kolaylıkla analiz etmek mümkündür.

BÖLÜM 5. VERİ GÖRSELLEŞTİRME

5.1. Ağ Diyagramından Yapısal Metne Geçiş ve Geri Dönüş

Sanatta biçim ve metin arasındaki gerginlik veya ortam ile kavram arasındaki ilişki bugün bir şekilde bilgisayar kodu ile veri arasında mevcuttur. İşlemsel sanat dediğimiz alan bu ilişkiyle yakından ilgilenmektedir. Aslında bir ağ diyagramı metin olarak yazılabilir. Belli bir yapıda yazmak mümkün olursa bilgisayarlar tarafından da okunabilir. Bir ağ, düğüm ve bağlantı denilen elemanlardan oluşmaktadır. Düğüm nokta, bağlantı çizgi olarak gösterilebilir. Ağ yapısı genelde fizik, matematik, sosyoloji ve bilgisayar bilimlerinde kullanılan bir modeldir. Son zamanlarda da pek çok görselleştirme projesinin bel kemiğini oluşturmaktadır. Aşağıdaki Şekil 5.1'de bazı ağ örnekleri görülmektedir.



Şekil 5.1. Görselleştirilmiş veri örnekleri

Bir ağ basitçe şöyle yazılabilir:

ali -> elif
elif -> dara
dara -> ali

Yukarıdaki yazım basitçe bir sosyal üçgen belirtmektedir. Bu sözdizimi Graphviz denilen bir ağ görselleştirme yazılımından alıntıdır. Graphviz yazılımı ağı ifade etmek için dot dili denilen bir yapı kullanmaktadır. Normalde çok basit olmakla birlikte, daha karmaşık ağ özelliklerine girildiğinde dil de karmaşıklaşmaktadır.

Çizilen diyagramları metne çeviri amacımız bilgisayar tarafından okunabilmesini ve tekrar ekranda çizebilmesini sağlamaktır. Yukarıda yazılan metni görselleştirmek için GraphML, bir XML formatı kullanacağız. GraphML kullanılmasının amacı uyumlu, standart haline gelmiş ve XML benzeri bir yazıma benzemiş olmasıdır. XML dili hem insan hem makine tarafından okunabilen en nihai veri düzenidir.

GraphML ağ tanımlamak içim kullanması çok kolay bir XML yapısıdır. Oldukça esnek yapılacak uygulamaya göre genişletebilir. Yönlü yönsüz hiyerarşik ağ yapılarını destekleyebilen bir yapıya sahiptir. Ayrıca GraphML formatına ekstra veri yapıları da ekleyebilmektedir. Düğüm ve bağlantı içine ayrı ayrı veri yapıları eklenebilmektedir. Yukarıda yazılan ağ basit bir GraphML ile şöyle yazabilir;

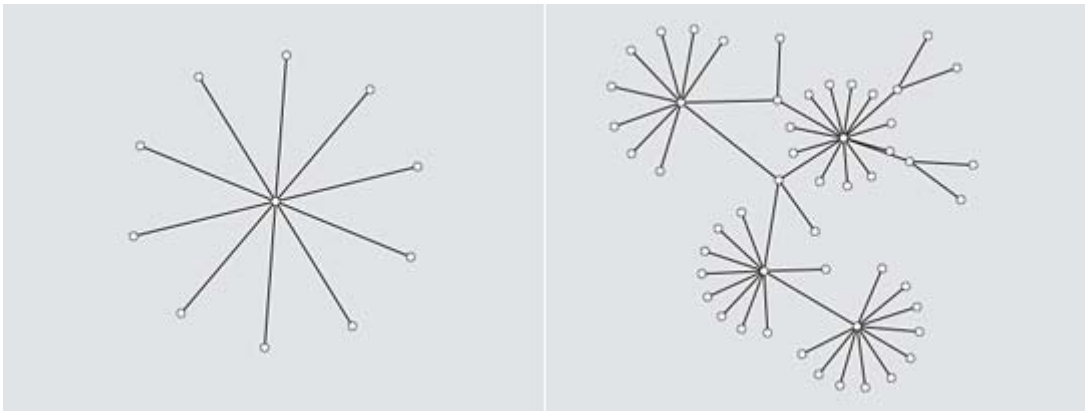
```
<graph id="G">
   <edge source="ali" target="elif">
   <edge source="elif" target="dara">
   <edge source="dara" target="ali">
</graph>
```

GraphML Primer ve GraphML Specification sayfalarında GraphML hakkında daha ayrıntılı bilgiler bulunmaktadır.

Veri görselleştirme işlemi ağ topolojileri ile çok yakından ilgilidir. Topoloji Türkçede biçimleri ya da boyutları değişmeyen geometrik cisimlerin incelenmesi bilimi anlamına gelmektedir. Ağ topolojileri ağ bağlamında düğümlerin ve bağlantıların nasıl konumlandırıldığını çalışan bir bilimdir. Bu yüzden ağ topolojileri GraphML formatında yazılabilir.

5.2.Görsel Ağ Tipleri

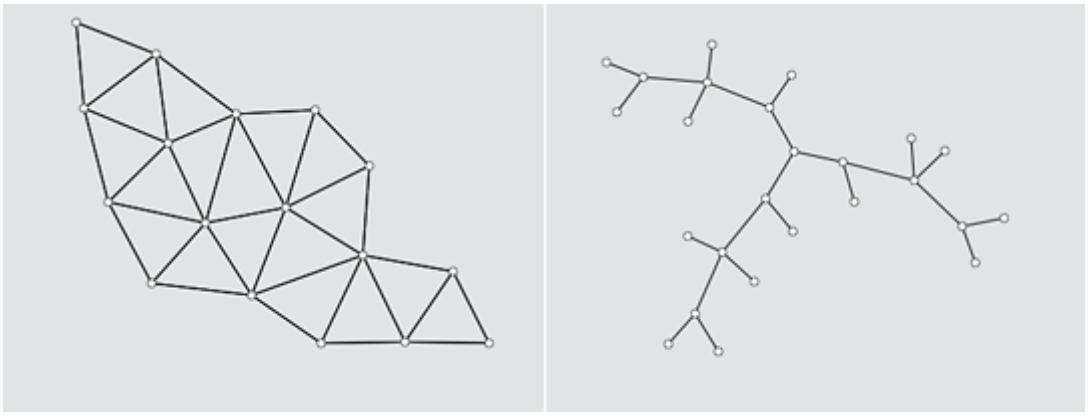
5.2.1.Merkezi, Merkezsiz



Şekil 5.2. Merkezi, merkezsiz ağ

Merkezi ağ yapısında tüm düğümler tek bir düğüme bağlıdır. Hiyerarşik yapıdadır. Tek bir otorite bulunmakta ve dallar arasında bağlantı bulunmamaktadır. Merkezsiz ağ ise merkezi ağın çoğaltılmış halidir. Pek çok merkez bir birine bağlı bulunmaktadır.

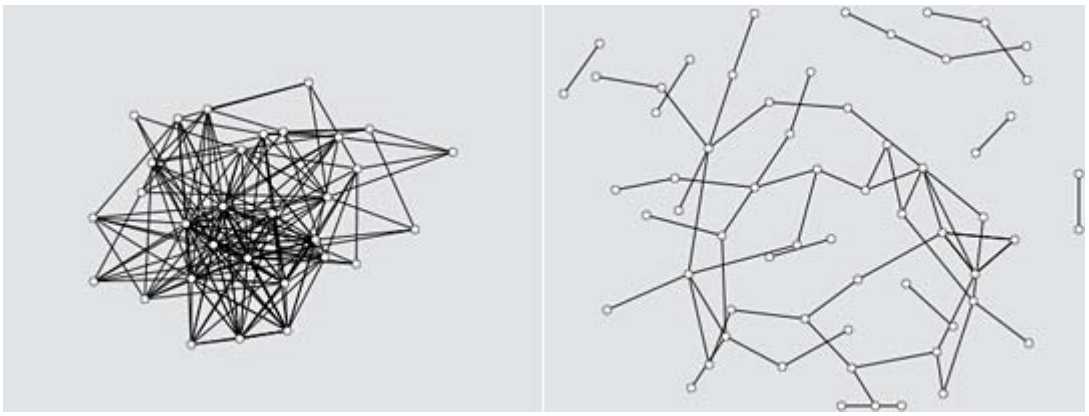
5.2.2.Dağıtık, Ağaç



Şekil 5.3. Dağıtık ve ağaç ağ

Bir dağıtık ağın merkezi yoktur. Her düğüm bağımsızdır. Bir düğümden diğer düğüme pek çok yoldan gidilebilir. Bir ağaç yapısı ismi üstünde hiyerarşiktir.

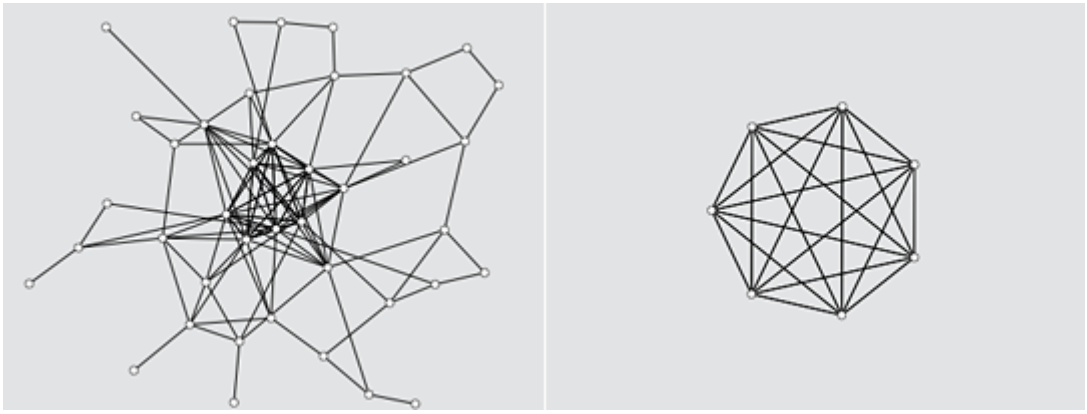
5.2.3. Sık, seyrek



Şekil 5.4. Sık, seyrek ağ

Bu tip ağlarda ağarın elemanları ya birbirine çok sık bağlı veya seyrek bağlıdır.

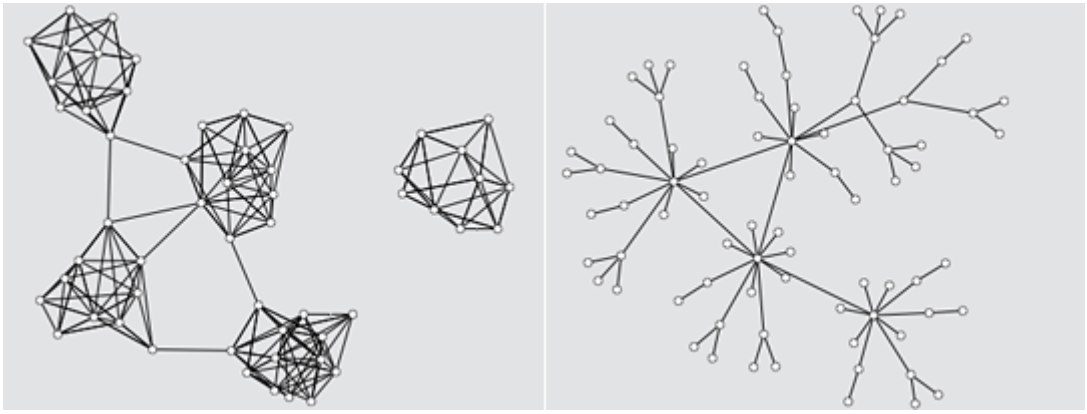
5.2.4. Merkez-çevre, Tüm Bağlı



Şekil 5.5. Merkez-çevre, tüm bağlı ağ

Merkez-çevre ağın merkezinde sık bağlantılı çevreye doğru seyrek bağlantılı ağlardır. Tüm bağlı ağların tüm elemanları diğer tüm elemanlara bağlıdır. Aslında bu tip ağların elemanları arasındaki ilişki futbol takımının 11 oyuncusu arasındaki ilişkiye çok benzemektedir.

5.2.5. Küçük dünya, Scale-free



Şekil 5.6. Küçük dünya, scale-free ağ

Sosyolog Stanley Milgram'ın bulduğu Küçük Dünya kavramı birbirine sadece bir kaç köprüyle bağlı kümeleri tarif eder. Bu tür ağlarda sadece bir kaç düğüm en çok bağlantıya sahiptir, bazı düğümler orta derecede bağlantıya sahip, çoğu düğüm bir kaç bağlantıya sahiptir. Buna aynı zamanda uzun kuyruk da denilmektedir.

BÖLÜM 6. EMNİYET ASAYİŞ PROGRAMI

Suçla ilgili ağ analizi, birçok (multiple) suç olaylarından veya çeşitli kaynaklardan bilgileri tümleştirilmesi ve suç/suçlu ağındaki bilgi akışı, operasyon, organizasyon ve yapı hakkında düzenli örüntülerin ortaya çıkarılmasıdır.

Suçla ilgili bir ağı çözmek ve ortaya çıkarmak için güvenilir veriyle beraber ileri tekniklerin geliştirilmesi kaçınılmazdır. Bununla beraber polis teşkilatları, çok fazla veriye sahip olmalarına karşın çok az değer ifade etmesi ikilemi ile karşı karşıyadırlar. Telefon kayıtları, banka hesapları ve hareketleri, araç satışları, gözaltı raporları gibi değişik kaynaklardan elde edilen büyük hacimli ham verilere sahip olmaları bir diğer problemdir. Diğer yandan veriyi ektin ve verimli bir şekilde değerlendirmek için gelişmiş ağ analiz araçları ve teknikleri yoktur.

Günümüzde suçla ilgili ağ analizi, çok fazla zaman ve emek isteyen elle yapılan bir işlemdir. Böylece, suç incelemek için uygulanabilirliği sınırlı kalmaktadır. Emniyet birimlerine eldeki suçla ilgili verileri analiz etmesi amacıyla sosyal ağ analizi (SAA) önerilmektedir. SAA veri madenciliği tekniği olarak geleneksel olmamasına rağmen, suçla ilgili ağlarda gizli yapısal örüntüleri keşfetmek amacıyla büyük hacimli ilişkili verinin incelenmesi için özellikle uygundur[19-21].

Literatürde var olan suçla ilgili ağ analizi yaklaşımları ve araçları üç nesil halinde gruplanmıştır[22]:

-İlk nesil olan manüel yaklaşım, anacapa şematik gösterimidir. Bu yaklaşımda analist, ilk olarak ham veriden suç ya da suçlu ilişkilerini tanımlayan bir ilişki matrisi oluşturmaktadır. Suçla ilgili ağ analizi için bu tür bir manüel yaklaşım, suçu ya da suçluyu incelemede yardımcı olmasına rağmen, veri kümesi çok büyük olduğu zaman son derece etkin olmayan ve verimsiz bir yöntemdir.

- İkinci nesil yaklaşım, grafik tabanlı yaklaşımdır. Bu tür araçlar, otomatik olarak suç/suçlu ağlarının grafiksel gösterimini üretmektedirler. Mevcut ağ analiz araçlarının çoğu bu nesil olanlardır. Analyst's Notebook, Netmap ve XANALYS Link Explorer bunların en popüler olanıdır. Bunlara ek olarak son dönemde Coplink sistemi altında iki tane ikinci nesil ağ analizi yaklaşımı geliştirilmiştir. Birinci yaklaşım suçla ilgili ilişkileri görselleştirmek için hiperbolik ağaç yapısını kullanmaktadır. Bu yaklaşım, büyük hacimli ilişkili verilerin görselleştirilmesi için kullanılmaktadır. İkinci yaklaşım ise ağın çok gürültülü verileri göstermesini engelleyecek şekilde otomatik olarak düğümlerin pozisyonunu ayarlamak için sezgisel bir çizge algoritması (spring embedder algorithm) kullanmaktadır.

İkinci nesil yöntemler, suçla ilgili ağların görselleştirilmesi için değişik yöntemler kullanmalarına rağmen, çok fazla analitik işlevselliği olmadığından sadece grafiksel gösterim yaptıkları için gelişmişlik seviyesi beklentilerin bir miktar altında kalmaktadır. Bu yöntemlere dayanan araçlar, ağın yapısal özelliklerinin bulunduğunu haber veren grafiklerin incelenmesi için analistlere ihtiyaç duymaktadırlar.

-Üçüncü nesil ise SAA tabanlı yaklaşımdır. Bu yaklaşımın suç analistine yardımcı olacak daha fazla analitik işlevsellik sağlaması beklenilmektedir. Gelişmiş yapısal analiz araçlarının, yalnızca ağları göstermesi değil aynı zamanda suçla ilgili ağların organizasyonu ve yapısı hakkında kullanışlı bilgiyi bulmak amacıyla büyük hacimli verinin madenciliğini yapmasına gereksinim vardır.

Polis teşkilatları çoğunlukla suçla ilgili ağların aşağıdaki yapısal özelliklerinin bulunmasıyla ilgilenmektedirler[23]:

-Ağdaki mevcut alt gruplar nedir?
-Bu alt gruplar birbiriyle nasıl etkileşim içindedirler?
-Ağın kapsamı ya da genel yapısı nedir?
-Ağ üyelerinin rolleri (merkezi, ikincil vb.) nedir?

Bu yapısal özelliklerin açık bir şekilde anlaşılması, ifade alma, gözaltına alma vb. için hedef kritik ağ üyelerinin analizine ve bozucu aksiyonların etkili olacağı, ağın

savunmasız ve kırılgan notalarının belirlenmesine yardımcı olabilir. Bu nedenle, suçla ilgili ağların veri madenciliği ve bu problemlerin iç yüzünü kavramak için uygun ağ analizi tekniklerine ihtiyaç vardır.

SAA teknikleri sosyal ağlarda sosyal aktörler arasındaki etkileşime ait örüntüleri ortaya çıkarmak için tasarlanmıştır[24]. Bu nedenle suçla ilgili ağları incelemek için özellikle uygundur. SAA, özellikle alt grupların tespitini yapacak, onların etkileşimine ait örüntüleri bulacak, merkezi bireylerin tanımlamasını yapacak ve ağ organizasyonu ile yapısını ortaya çıkarabilecek yetenektedir.

6.1. Emniyet Asayiş Veri Görselleştirme ve Sosyal Ağ Analizi

Bitirme projesi kapsamında suç örgütlerinin yapısını ortaya çıkarmakla görevli kullanıcılara web ara yüzünden kullanılan bir program geliştirilmiştir.

Program sayesinde kullanıcılar sisteme internet bağlantısı olan her yerden suç örgütüne üye olan olması ihtimali olan suçlu veya zanlıları sisteme kaydedebilmektedir. Bu kişilerin bilgilerini sisteme ekleyip aynı zamanda sistemden çıkarabilme işlemini gerçekleştirebilmektedir. Gerektiğinde suçlu veya zanlı kişinin bilgilerini güncelleyebilmektedir.

Geliştirilen programın kullanıcıları suç örgütünün elemanları arasındaki yapılan telefon görüşmelerini sisteme kaydedebilmekte bu görüşmeleri güncelleyebilmekte ve sisteme hatalı bir görüşme girdiyse silebilmektedir.

Telefon görüşmelerinin hareketleri daha sonra sorgulanabilmekte ve bu hareketler görsel hale getirilmektedir. Görsel hale getirilen görüşmelerin detaylarına ulaşılabilmektedir. Telefon trafiğinin hangi tarihte ne kadar sıklıkta yapıldığına ait tarih bazında grafik çizimi yapılabilmektedir. Bu sayede grafikten hangi tarihte görüşme sayılarındaki hareketliliğin arttığı bilgisine ulaşılabilmektedir.

Programın kullanıcıları, suç örgütünün elemanları arasındaki gönderilen e-postaları sisteme kaydedebilmekte bu e-posta bilgilerini güncelleyebilmekte ve sisteme hatalı bir e-posta kaydı girdiyse silebilmektedir.

E-posta gönderme hareketleri daha sonra sorgulanabilmekte ve bu trafik hareketler görsel hale getirilmektedir. Görsel hale getirilen e-posta hareketlerinin detaylarına ulaşılabilmektedir. E-posta trafiğinin hangi tarihte ne kadar sıklıkta yapıldığına ait tarih bazında grafik çizimi yapılabilmektedir. Bu sayede grafikten daha çok hangi tarihlerde hareketliğin arttığı bilgisine ulaşılabilmektedir.

Programın kullanıcıları, suç örgütünün elemanları arasındaki yapılan msn kayıtlarını sisteme kaydedebilmekte bu msn kayıtları güncelleyebilmekte ve sisteme hatalı bir msn kaydı girdiyse silebilmektedir.

Msn görüşmeleri daha sonra sorgulanabilmekte ve bu görüşmeler görsel hale getirilmektedir. Görsel hale getirilen msn görüşmelerinin detaylarına ulaşılabilmektedir. Msn görüşmesi trafiğinin hangi tarihte ne kadar sıklıkta yapıldığına ait tarih bazında grafik çizimi yapılabilmektedir. Bu sayede grafikten hangi tarihlerde hareketliğin arttığı bilgisine ulaşılabilmektedir.

Programın kullanıcıları suç örgütünün elemanları arasındaki banka üzerinden yapılan para transferi işlemlerini sisteme kaydedebilmekte bu hesap hareketi bilgilerini güncelleyebilmekte ve sisteme hatalı bir hesap hareketi kaydı girdiyse silebilmektedir.

Banka üzerinden gönderilen para trafiği daha sonra sorgulanabilmekte ve bu trafik görsel hale getirilmektedir. Görsel hale getirilen para trafiğinin detaylarına ulaşılabilmektedir. Para trafiğinin hangi tarihte ne kadar sıklıkta yapıldığına ait tarih bazında grafik çizimi yapılabilmektedir. Bu sayede grafikten hangi tarihlerde para transferindeki hareketliğin arttığı bilgisine ulaşılabilmektedir

Programın kullanıcıları suç örgütünün elemanları arasında gönderilen dokümanları sisteme kaydedebilmekte bu doküman bilgilerini güncelleyebilmekte ve sisteme hatalı bir doküman kaydı girdiyse silebilmektedir.

Suç örgütünün elemanları arasında gönderilen dokümanların trafiği daha sonra sorgulanabilmekte ve bu trafik görsel hale getirilmektedir. Kim kime dokuman göndermiş. Kaç defa göndermiş. Şüpheli sözcükleri içeren dokuman trafiği kimler arasında gerçekleşmiş. Bu bilgiler kullanıcılar görsel olarak sunulmaktadır.

Programın kullanıcıları suç örgütünün elemanları arasında yapılan alışveriş işlemlerini sisteme kaydedebilmekte bu alışveriş bilgilerini güncelleyebilmekte ve sisteme hatalı bir alışveriş kaydı girdiyse silebilmektedir.

Suç örgütünün elemanları arasında yapılan alışveriş trafiği daha sonra sorgulanabilmekte ve bu trafik görsel hale getirilmektedir. “Kim kimden ne almış?”, “Kaç defa alışveriş işlemi gerçekleşmiş?”, “Şüpheli alışveriş işlemlerinin trafiği kimler arasında gerçekleşmiş?” sorularının yanıtları kullanıcılara görsel olarak sunulmaktadır.

Program kullanıcılara incelemek istedikleri suçlu veya zanlıların daha önceki sabıka kaydını getirmektedir. Program kullanıcılara bu suçlu veya zanlı daha önce hangi tarihler de ne gibi suçlara karışmış bilgisini sunacaktır.

Ayrıca program kullanıcılara suçluların veya zanlıların sitemdeki kayıtlı adres bilgisinden hareketle suç örgütünde bulunan elemanların harita üzerindeki adres dağılımlarının görselleştirilmesi işlemini gerçekleştirmektedir.

Eldeki e-posta, telefon kayıtları, msn görüşmeleri vb. verilerin görselleştirme işlemi sonucu yapılacak olan sosyal ağ analizi, aşağıdaki maddeler halinde sunulan soruların cevabını ortaya çıkarmada uzman personele yardım sağlamakta ve yapılacak programın gerekliliğini biraz daha ortaya çıkarmaktadır. Ayrıca aşağıdaki sorular suç örgütlerinin analiz edilerek görselleştirilmesinde suçu araştıranların odaklandığı noktaları da belirtmektedir[19,20];

-Örgütün merkezinde kim var?
-Örgütün içinde alt yapılanmalar var mı?
-Alt grupların birbirleri arasındaki iletişim şekli nasıldır?
-Örgütlerin ayrıntılı kapsamlı yapısı nasıldır?
-Hangi üyenin bu örgütten ayrılması örgütün yapısının bozulması, örgütün parçalanması örgütteki ilişkilerin bozulması ile sonuçlanacaktır.
-Örgütteki bilgi ve iş, eşya, mal akışı nasıl gerçekleşmektedir.

6.2. Veri Tabanı Yapısı

Bitirme projesi kapsamında geliştirilen program, veritabanı aracı olarak Microsoft SQL Server 2005 veri tabanı programını kullanmaktadır. Programın verilerini saklaması amacı ile oluşturulan tablolar ilişkisel veritabanı yapısına sahiptir. İlişkisel veritabanı yapısı, verilerin tablolarda satır ve sütunlar halinde tutulduğu ve yüksek bir veri tutarlılığına sahip veri depolama yapısıdır. İlişkisel veri tabanını çeşitli tablolar arasında organize edilmiş verilerden oluşan veri tabanı olarak açıklayabiliriz. Farklı tablolar arasındaki veriler, çeşitli anahtarlar vasıtası ile birbirlerine bağlanırlar. İlgili tablolarda, sütunlar arasında bir anahtar sütun yer alır. Bu anahtar sütun aracılığı ile birden çok tablo verileri birbiriyle bağlantı sağlayabilir ve herhangi bir sorgulamada birlikte görüntülenebilir.

Aşağıda programda kullanılan verileri içinde barındıran tablolar ve bu tablolardaki veri yapısı açıklanmaktadır.

6.2.1. AlisVerisTrafik tablosu

AlisVerisTrafik tablosu, zanlıların kendi aralarında yapmış oldukları alış-veriş hareketlerini tutmaktadır. Bu tablodaki veriler kullanılarak zanlılar arasındaki alış-veriş hareketleri görselleştirilmektedir. Bu görselleştirme işlemi sayesinde ortaya bir örüntü çıkmaktadır. Alış-veriş hareketlerinde ortaya çıkan bu örüntü emniyet teşkilatındaki uzman personele zanlılar arasında alış-verişe bağlı organizasyonel bir çete yapısı olup olmadığı hakkında bilgi vermektedir.

Tablo 6.1. AlisVerisTrafik tablosundaki sütunlar ve özellikleri

PK	Adı	Tip	Boş Olamaz	Tekil	Uzunluk
Evet	AlisVerisID	int	Evet	Evet	
Hayır	AlanTcNo	bigint	Evet	Hayır	
Hayır	SatanTcNo	bigint	Evet	Hayır	
Hayır	Tutar	money	Evet	Hayır	
Hayır	Cinsi	nvarchar	Evet	Hayır	300
Hayır	Tarih	datetime	Evet	Hayır	

6.2.2. BankaHesapTrafik tablosu

BankaHesapTrafik tablosu, zanlıların kendi aralarında yapmış oldukları para transferi hareketlerini tutmaktadır. Bu tablodaki veriler kullanılarak zanlılar arasındaki para transferi hareketleri görselleştirilmektedir. Bu görselleştirme işlemi sayesinde ortaya bir örüntü çıkmaktadır. Para transferi hareketlerinde ortaya çıkan bu örüntü emniyet teşkilatındaki uzman personele zanlılar arasında banka hesap kayıtlarına bağlı organizasyonel bir çete yapısı olup olmadığı hakkında bilgi vermektedir.

Tablo 6.2. BankaHesapTrafik tablosundaki sütunlar ve özellikleri

PK	Adı	Tip	Boş Olamaz	Tekil	Uzunluk
Evet	HeTrafikID	int	Evet	Evet	
Hayır	Gonderen	nvarchar	Evet	Hayır	50
Hayır	Alan	nvarchar	Evet	Hayır	50
Hayır	Miktar	money	Evet	Hayır	
Hayır	Aciklama	nvarchar	Evet	Hayır	300
Hayır	Tarih	datetime	Evet	Hayır	

6.2.3. DokumanTrafik tablosu

DokumanTrafik tablosunda, zanlılarından ele geçirilen dosyalar tutulmaktadır. Bu tablodaki veriler kullanılarak zanlılar arasındaki dosyaların içerikleri incelenebilmektedir. Bu tablodaki veriler emniyet teşkilatındaki uzman personele zanlılardan ele geçirilen dokümanların içeriğini analiz etmede yardım etmektedir.

Tablo 6.3. DokumanTrafik tablosundaki sütunlar ve özellikleri

PK	Adı	Tip	Boş Olamaz	Tekil	Uzunluk
Evet	DokumanID	int	Evet	Evet	
Hayır	TcNo	bigint	Evet	Hayır	
Hayır	Icerik	text	Evet	Hayır	
Hayır	Tarih	datetime	Hayır	Hayır	

6.2.4. EmailTrafik tablosu

EmailTrafik tablosu, zanlıların kendi aralarında yapmış oldukları e-posta hareketlerini tutmaktadır. Bu tablodaki veriler kullanılarak zanlılar arasındaki e-posta hareketleri görselleştirilmektedir. Bu görselleştirme işlemi sayesinde ortaya bir örüntü çıkmaktadır. Para transferi hareketlerinde ortaya çıkan bu örüntü emniyet teşkilatındaki uzman personele zanlılar arasında e-posta kayıtlarına bağlı organizasyonel bir çete yapısı olup olmadığı hakkında bilgi vermektedir.

Tablo 6.4. EmailTrafik tablosundaki sütunlar ve özellikleri

PK	Adı	Tip	Boş Olamaz	Tekil	Uzunluk
Evet	EmailID	int	Evet	Evet	
Hayır	Kimden	nvarchar	Evet	Hayır	300
Hayır	Kime	nvarchar	Evet	Hayır	300
Hayır	Konu	nvarchar	Hayır	Hayır	250

Tablo 6.4. (Devamı)

Hayır	Icerik	text	Evet	Hayır	
Hayır	Tarih	datetime	Evet	Hayır	

6.2.5. Il tablosu

Il tablosu, veritabanındaki diğer tablolar tarafından kullanılmaktadır. Türkiye'deki 81 ili plaka kodları ve isimleri ile barındırmaktadır.Sabıka kaydı, zanlı vb. adres bilgisinin kullanıldığı tablolarda kullanılmaktadır.

Tablo 6.5. Il tablosundaki sütunlar ve özellikleri

PK	**Adı**	**Tip**	**Boş Olamaz**	**Tekil**	**Uzunluk**
Evet	PlakaKodu	int	Evet	Evet	
Hayır	IlAdi	nvarchar	Hayır	Hayır	50

6.2.6. Ilce tablosu

Ilce tablosu, veritabanındaki diğer tablolar tarafından kullanılmaktadır. Türkiye'deki 81 ile bağlı ilçelerin isimlerini tutmaktadır.Sabıka kaydı, zanlı vb. adres bilgisinin kullanıldığı tablolarda kullanılmaktadır.

Tablo 6.6. Ilce tablosundaki sütunlar ve özellikleri

PK	**Adı**	**Tip**	**Boş Olamaz**	**Tekil**	**Uzunluk**
Evet	IlceID	int	Evet	Evet	
Hayır	IlceAdi	nvarchar	Evet	Hayır	50
Hayır	SehirID	int	Evet	Hayır	

6.2.7. MsnTrafik tablosu

MsnTrafik tablosu, zanlıların kendi aralarında yapmış oldukları msn görüşmelerini tutmaktadır. Bu tablodaki veriler kullanılarak zanlılar arasındaki msn görüşmeleri görselleştirilmektedir. Bu görselleştirme işlemi sayesinde ortaya bir örüntü çıkmaktadır. Msn görüşmelerinde ortaya çıkan bu örüntü emniyet teşkilatındaki uzman personele zanlılar arasında msn görüşmelerine bağlı organizasyonel bir çete yapısı olup olmadığı hakkında bilgi vermektedir.

Tablo 6.7. MsnTrafik tablosundaki sütunlar ve özellikleri

PK	Adı	Tip	Boş Olamaz	Tekil	Uzunluk
Evet	MsnTrafikID	int	Evet	Evet	
Hayır	Kimden	nvarchar	Evet	Hayır	300
Hayır	Kime	nvarchar	Evet	Hayır	300
Hayır	Icerik	text	Evet	Hayır	
Hayır	Tarih	datetime	Evet	Hayır	

6.2.8. SabikaKaydi tablosu

SabikaKaydi tablosu, zanlıların daha önce işlemiş oldukları suçlara ait sabıka kaydı bilgilerini tutmaktadır. Emniyet teşkilatındaki yetkili personeller ortaya çıkan örüntülerde şüphelendikleri kişilere ait sabıka kayıtlarını bu tablodaki veriler yardımı ile görüntüleyebilmektedir.

Tablo 6.8. SabikaKaydi tablosundaki sütunlar ve özellikleri

PK	Adı	Tip	Boş Olamaz	Tekil	Uzunluk
Evet	SabikaKaydiID	int	Evet	Evet	
Hayır	TcNo	bigint	Evet	Hayır	

Tablo 6.8. (Devamı)

Hayır	SucID	int	Evet	Hayır	
Hayır	IlID	int	Evet	Hayır	
Hayır	IlceID	int	Evet	Hayır	
Hayır	Tarih	datetime	Evet	Hayır	

6.2.9. SucTipi tablosu

SabikaKaydi tablosunda, zanlıların daha önce işlemiş oldukları suç adlarını içeren tablodur. SabikaKaydi tablosu ilişkisel veritabanı mantığına göre bu tablodan suç adlarına bağlı olan suç kodunu tutmaktadır.

Tablo 6.9. SucTipi tablosundaki sütunlar ve özellikleri

PK	**Adı**	**Tip**	**Boş Olamaz**	**Tekil**	**Uzunluk**
Evet	SucID	int	Evet	Evet	
Hayır	SucAdi	nvarchar	Evet	Hayır	250

6.2.10. TelefonTrafik tablosu

TelefonTrafik tablosu, zanlıların kendi aralarında yapmış oldukları telefon görüşmelerini tutmaktadır. Bu tablodaki veriler kullanılarak zanlılar arasındaki telefon görüşmesi hareketleri görselleştirilmektedir. Bu görselleştirme işlemi sayesinde ortaya bir örüntü çıkmaktadır. Telefon görüşmesi hareketlerinde ortaya çıkan bu örüntü emniyet teşkilatındaki uzman personele zanlılar arasında telefon görüşmelerine bağlı organizasyonel bir çete yapısı olup olmadığı hakkında bilgi vermektedir.

Tablo 6.10. TelefonTrafik tablosundaki sütunlar ve özellikleri

PK	Adı	Tip	Boş Olamaz	Tekil	Uzunluk
Evet	TelTrafilID	int	Evet	Evet	
Hayır	Kimden	nvarchar	Evet	Hayır	20
Hayır	Kime	nvarchar	Evet	Hayır	20
Hayır	Icerik	text	Hayır	Hayır	
Hayır	Tarih	datetime	Evet	Hayır	

6.2.11. UrunCinsi tablosu

AlisVerisTrafik tablosunda, zanlıların birbirleri arasında yapmış oldukları alış-veriş hareketlerindeki alış-verişe konu olan malın cinsini tutan tablodur. AlisVerisTrafik tablosu ilişkisel veritabanı mantığına göre bu tablodan malın cinsine bağlı olan ürün kodunu tutmaktadır.

Tablo 6.11. UrunCinsi tablosundaki sütunlar ve özellikleri

PK	Adı	Tip	Boş Olamaz	Tekil	Uzunluk
Evet	UrunID	int	Evet	Evet	
Hayır	UrunAdi	nvarchar	Evet	Hayır	250

6.2.12. Zanli tablosu

Zanli tablosu üzerinde çete araştırması yapılan şahısların ad, soy ad, adres, TcNo vb. bilgilerinin tutulduğu tablodur. Diğer tablolar bu tablodaki TcNo bilgisini kullanarak incelemeye konu olan verileri saklamaktadır.

Tablo 6.12. Zanli tablosundaki sütunlar ve özellikleri

PK	Adı	Tip	Boş Olamaz	Tekil	Uzunluk
Evet	TcNo	bigint	Evet	Evet	

Tablo 6.12. (Devamı)

Hayır	Ad	nvarchar	Hayır	Hayır	100
Hayır	Soyad	nvarchar	Hayır	Hayır	100
Hayır	Adres	nvarchar	Hayır	Hayır	250
Hayır	IlID	int	Evet	Hayır	
Hayır	IlceID	int	Evet	Hayır	
Hayır	Cinsiyeti	bit	Evet	Hayır	
Hayır	XKoordinat	decimal	Hayır	Hayır	
Hayır	YKoordinat	decimal	Hayır	Hayır	

6.2.13. ZanliEmail tablosu

ZanliEmail tablosu üzerinde çete araştırması yapılan zanlıların e-posta bilgilerinin tutulduğu tablodur. Bir zanlı birden fazla e-posta bilgisine sahip olabilmektedir. Zanlılar farklı internet adreslerinden değişik isimlerde birçok e-posta adresi almış olabilirler.

Tablo 6.13. ZanliEmail tablosundaki sütunlar ve özellikleri

PK	Adı	Tip	Boş Olamaz	Tekil	Uzunluk
Evet	EmailID	int	Evet	Evet	
Hayır	TcNo	bigint	Evet	Hayır	
Hayır	Email	nvarchar	Evet	Hayır	300

6.2.14. ZanliHesapNo tablosu

ZanliHesapNo tablosu üzerinde çete araştırması yapılan zanlıların hesap numarası bilgilerinin tutulduğu tablodur. Bir zanlı birden fazla hesap numarası bilgisine sahip olabilmektedir. Zanlılar farklı bankalardan veya aynı bankadan birden fazla hesap numarası almış olabilirler.

Tablo 6.14. ZanliHesapNo tablosundaki sütunlar ve özellikleri

PK	Adı	Tip	Boş Olamaz	Tekil	Uzunluk
Evet	HesapNoID	int	Evet	Evet	
Hayır	TcNo	bigint	Evet	Hayır	
Hayır	HesapNo	nvarchar	Evet	Hayır	50

6.2.15. ZanliTelNo tablosu

ZanliTelNo tablosu üzerinde çete araştırması yapılan zanlıların telefon numaralarının tutulduğu tablodur. Bir zanlı birden fazla telefon numarasına sahip olabilmektedir. Zanlılar farklı operatörlerden veya aynı operatörden birden fazla telefon numarası almış olabilirler.

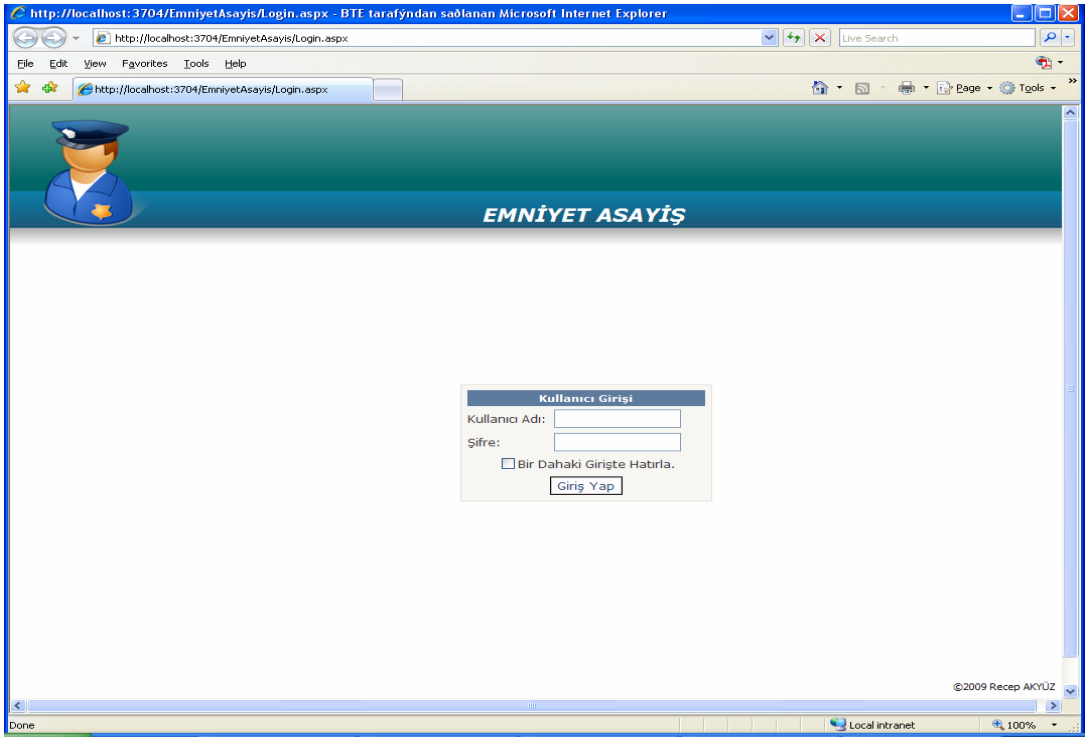
Tablo 6.15. ZanliTelNo tablosundaki sütunlar ve özellikleri

PK	Adı	Tip	Boş Olamaz	Tekil	Uzunluk
Evet	TelNoID	int	Evet	Evet	
Hayır	TcNo	bigint	Evet	Hayır	
Hayır	TelNo	nvarchar	Evet	Hayır	20

6.3. Kullanıcı Giriş Ekranı

Sistem kullanıcıları(organize suçlar müdürlüğünde bulunan programı kullanan polisler) bu ekran yardımı ile sahip oldukları kullanıcı adı ve şifre bilgileri ile sisteme giriş yapabilmektedirler. Sistemde 2 tip kullanıcı bulunmaktadır.Birinci tip kullanıcı kriminalkullanıcı olarak adlandırılan kullanıcıdır. Bu kullanıcı sisteme veri girişinden sorumlu kullanıcıdır. Teknik takip sonucu incelemeye alınan tüm kayıtları bu kullanıcı sisteme girmektedir. İkinci tip kullanıcı kriminaladmin olarak adlandırılan veri analizini gerçekleştiren kullanıcıdır. Kriminalkullanıcı tarafından sisteme girilen verileri analiz eden, sorgulayan ve bu verileri program yardımı ile görselleştiren kullanıcıdır. Bütün kullanıcılar şekil 6.1'deki ekranı kullanarak sisteme giriş

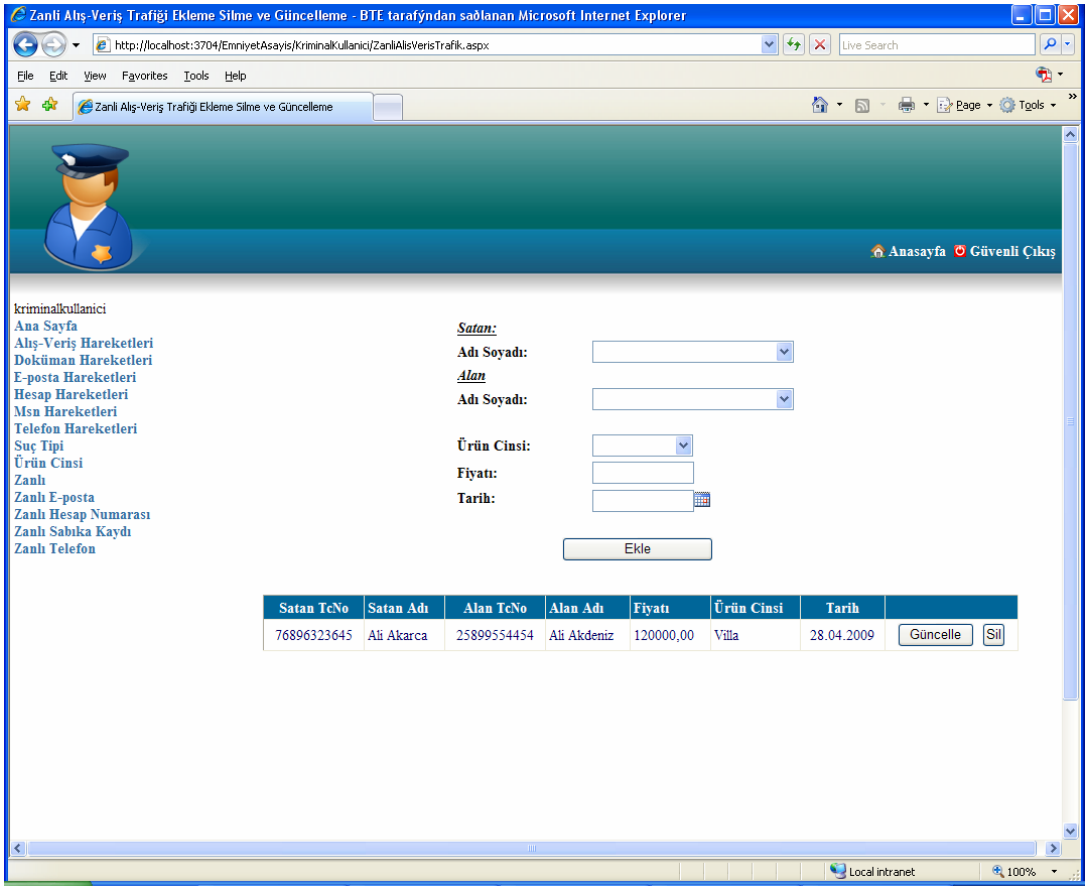
yapmaktadırlar. Kullanıcının tipine göre ekran özelleşerek kullanıcının yapabileceği işlemleri sunan bir yapıya dönüşmektedir.



Şekil 6.1. Kullanıcı giriş ekranı

6.4. Alış-Veriş Hareketleri Ekranı

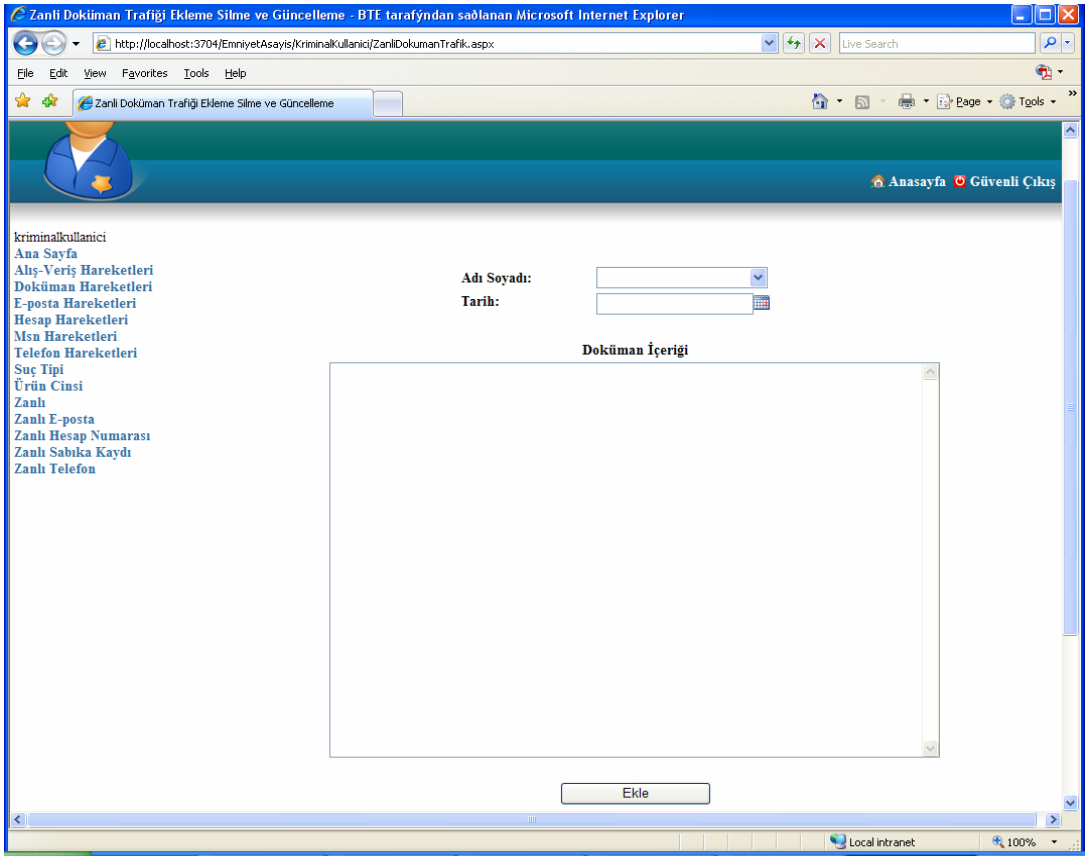
Sistem kullanıcıları(organize suçlar müdürlüğünde bulunan programı kullanan polisler) bu ekran yardımı ile suç örgütü ilişkisi olduğu düşünülen zanlılar arasındaki geçen alış-veriş hareketlerinin kayıtlarını sisteme ekleyebilmekte, eklediği bu kayıtları güncelleyebilmekte ve silebilmektedir. Bu kayıtlardan oluşan alış-veriş hareketleri geliştirilen program yardımı ile analiz edilip görsel hale getirilmektedir. Bu görselleştirme işlemi sayesinde ortaya bir örüntü çıkmaktadır. Alış-veriş hareketlerinde ortaya çıkan bu örüntü emniyet teşkilatındaki uzman personele zanlılar arasında alış-veriş hareketlerine bağlı organizasyonel bir çete yapısı olup olmadığı hakkında bilgi vermektedir.



Şekil 6.2. Alış-veriş hareketleri ekranı

6.5. Doküman Hareketleri Ekranı

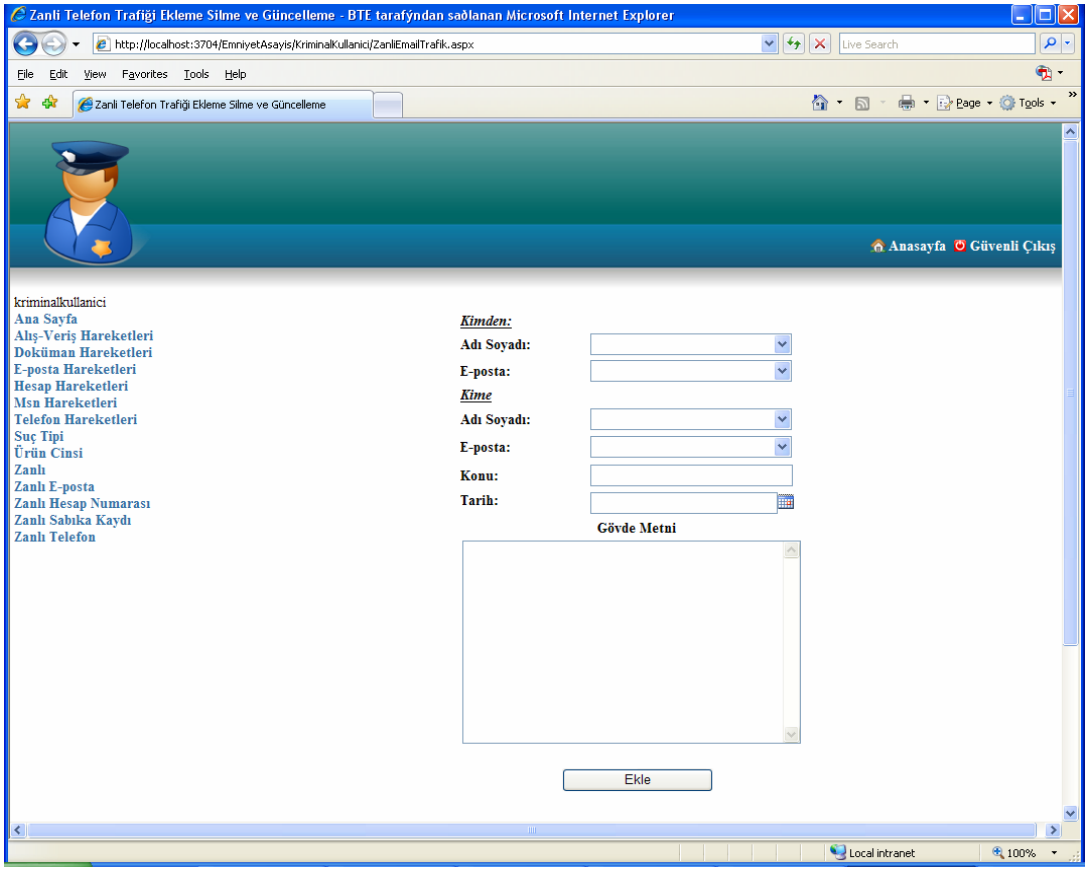
Sistem kullanıcıları(organize suçlar müdürlüğünde bulunan programı kullanan polisler) bu ekran yardımı ile suç örgütü ilişkisi olduğu düşünülen zanlılardan ele geçirilen dokümanları sisteme ekleyebilmekte, eklediği bu dokümanları güncelleyebilmekte ve silebilmektedir.



Şekil 6.3. Doküman hareketleri ekranı

6.6. E-posta Hareketleri Ekranı

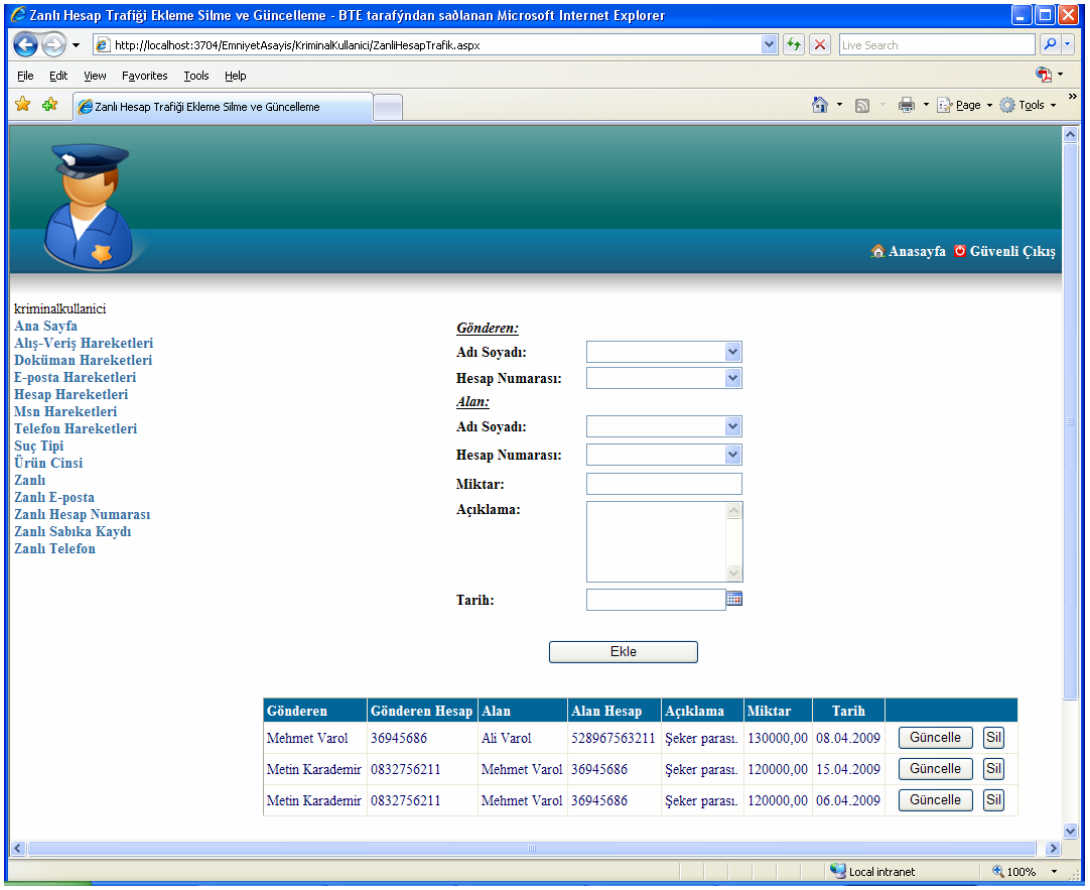
Sistem kullanıcıları(organize suçlar müdürlüğünde bulunan programı kullanan polisler) bu ekran yardımı ile suç örgütü ilişkisi olduğu düşünülen zanlılar arasındaki geçen e-posta hareketlerinin kayıtlarını sisteme ekleyebilmekte, eklediği bu kayıtları güncelleyebilmekte ve silebilmektedir. Bu kayıtlardan oluşan e-posta hareketleri geliştirilen program yardımı ile analiz edilip görsel hale getirilmektedir. Bu görselleştirme işlemi sayesinde ortaya bir örüntü çıkmaktadır. E-posta hareketlerinde ortaya çıkan bu örüntü emniyet teşkilatındaki uzman personele zanlılar arasında e-posta hareketlerine bağlı organizasyonel bir çete yapısı olup olmadığı hakkında bilgi vermektedir.



Şekil 6.4. E-posta hareketleri ekranı

6.7. Hesap Hareketleri Ekranı

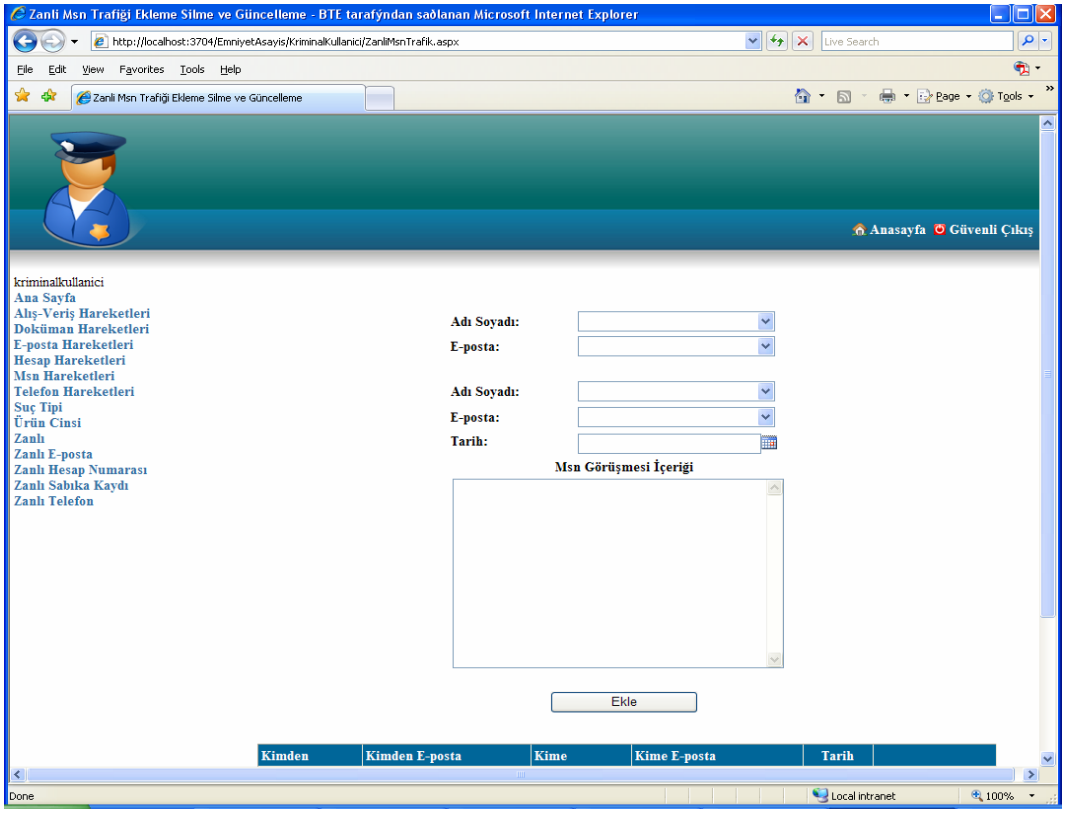
Sistem kullanıcıları(organize suçlar müdürlüğünde bulunan programı kullanan polisler) bu ekran yardımı ile suç örgütü ilişkisi olduğu düşünülen zanlılar arasındaki yapılan para transferlerinin kayıtlarını sisteme ekleyebilmekte, eklediği bu kayıtları güncelleyebilmekte ve silebilmektedir. Bu kayıtlardan oluşan para transferleri hareketleri geliştirilen program yardımı ile analiz edilip görsel hale getirilmektedir. Bu görselleştirme işlemi sayesinde ortaya bir örüntü çıkmaktadır. Para transferi hareketlerinde ortaya çıkan bu örüntü emniyet teşkilatındaki uzman personele zanlılar arasında para transferine bağlı organizasyonel bir çete yapısı olup olmadığı hakkında bilgi vermektedir.



Şekil 6.5. Hesap hareketleri ekranı

6.8. Msn Hareketleri Ekranı

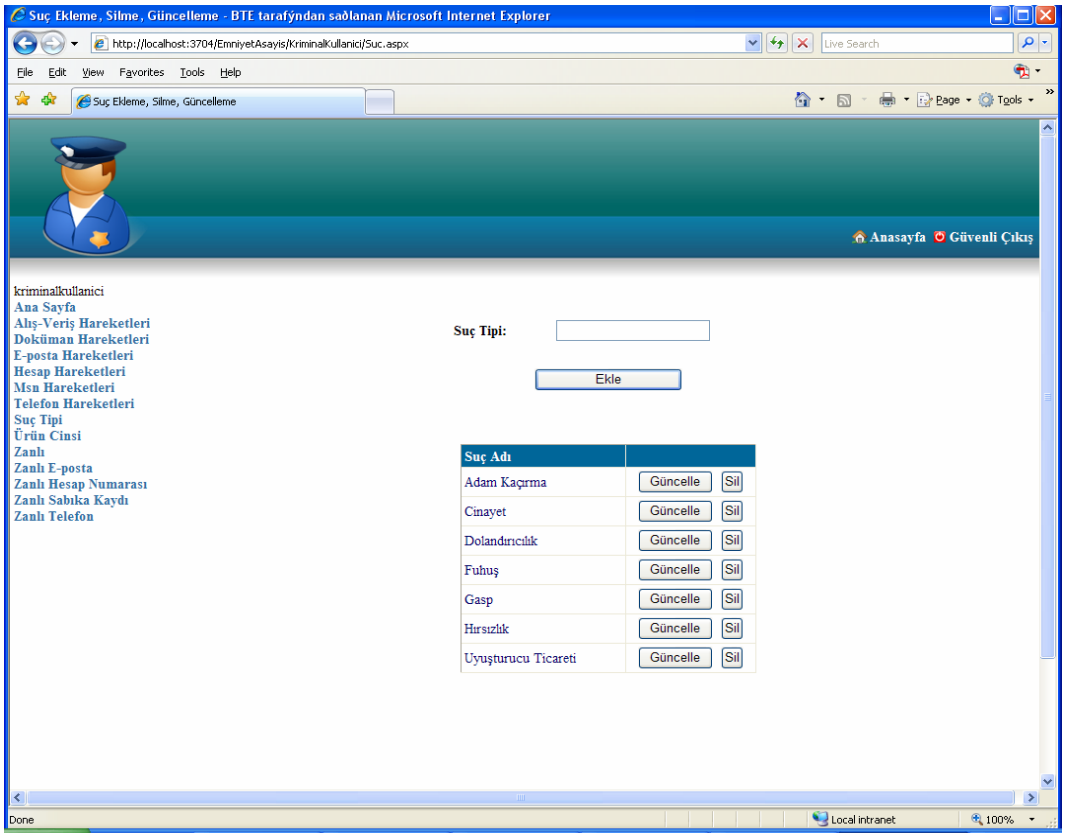
Sistem kullanıcıları(organize suçlar müdürlüğünde bulunan programı kullanan polisler) bu ekran yardımı ile suç örgütü ilişkisi olduğu düşünülen zanlılar arasındaki geçen msn görüşmelerinin kayıtlarını sisteme ekleyebilmekte, eklediği bu kayıtları güncelleyebilmekte ve silebilmektedir. Bu kayıtlardan oluşan msn görüşmeleri hareketleri geliştirilen program yardımı ile analiz edilip görsel hale getirilmektedir. Bu görselleştirme işlemi sayesinde ortaya bir örüntü çıkmaktadır. Msn görüşmelerinde ortaya çıkan bu örüntü emniyet teşkilatındaki uzman personele zanlılar arasında msn görüşmelerine bağlı organizasyonel bir çete yapısı olup olmadığı hakkında bilgi vermektedir.



Şekil 6.6. Msn hareketleri ekranı

6.9. Suç Tipi Ekranı

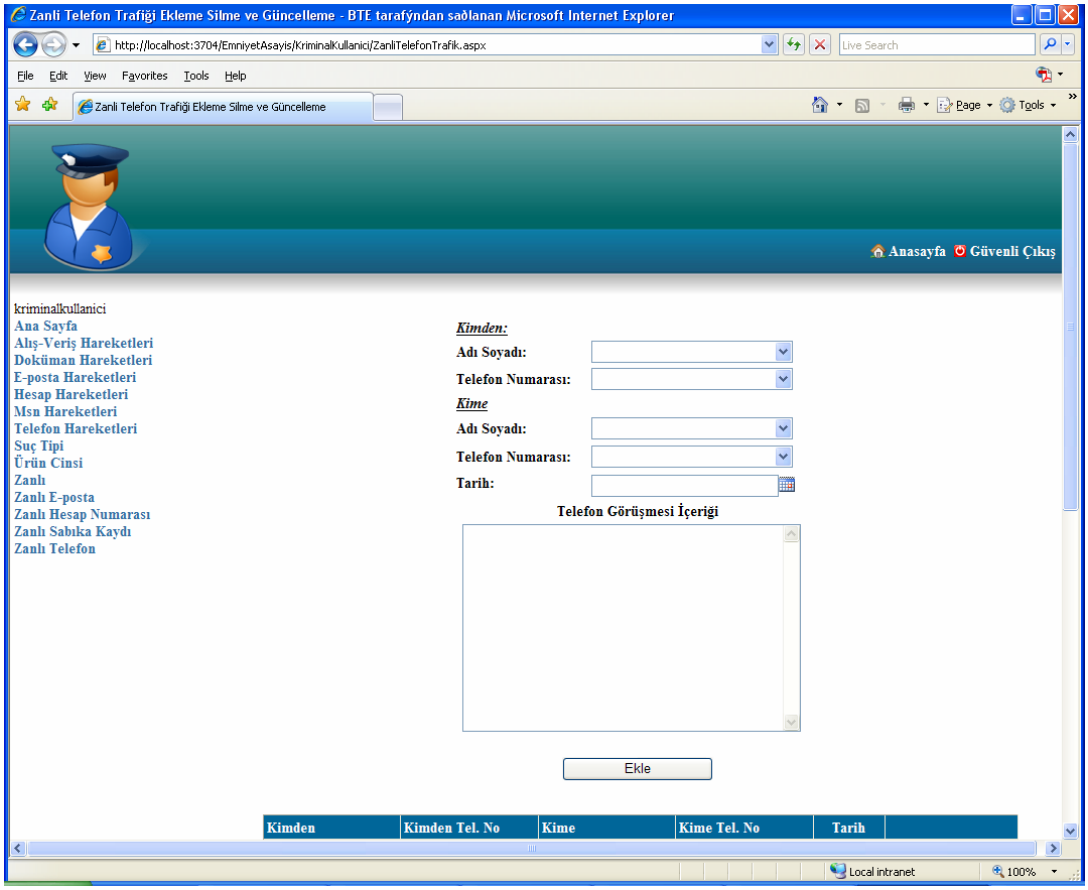
Sistem kullanıcıları bu ekran yardımı ile suç tiplerini sisteme ekleyebilmekte, eklediği bu suç tiplerini güncelleyebilmekte ve silebilmektedir. Suç tipleri zanlıların sabıka kayıtlarını sisteme kaydetme esnasında sistemdeki mevcut suçları listelerken kullanılmaktadır. Eğer listede zanlıların sabıka kaydına işlenmek istenen suç tipi listede yoksa bu ekran arcılığı ile istenilen suç tipi sisteme eklenebilmektedir.



Şekil 6.7. Suç tipi ekranı

6.10. Telefon Hareketleri Ekranı

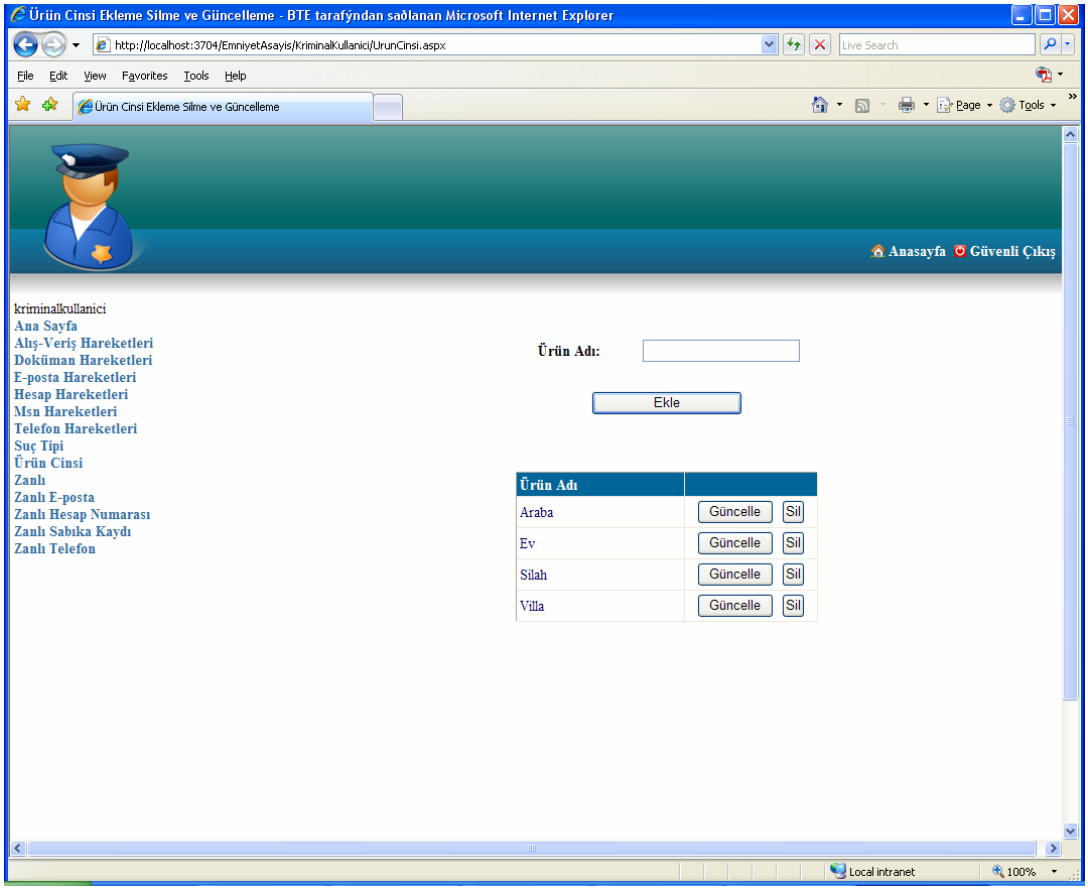
Sistem kullanıcıları(organize suçlar müdürlüğünde bulunan programı kullanan polisler) bu ekran yardımı ile suç örgütü ilişkisi olduğu düşünülen zanlılar arasındaki geçen telefon görüşmelerinin kayıtlarını sisteme ekleyebilmekte, eklediği bu kayıtları güncelleyebilmekte ve silebilmektedir. Bu kayıtlardan oluşan telefon görüşmeleri hareketleri geliştirilen program yardımı ile analiz edilip görsel hale getirilmektedir. Bu görselleştirme işlemi sayesinde ortaya bir örüntü çıkmaktadır. Telefon görüşmelerinde ortaya çıkan bu örüntü emniyet teşkilatındaki uzman personele zanlılar arasında telefon görüşmelerine bağlı organizasyonel bir çete yapısı olup olmadığı hakkında bilgi vermektedir.



Şekil 6.8. Telefon hareketleri ekranı

6.11. Ürün Cinsi Ekranı

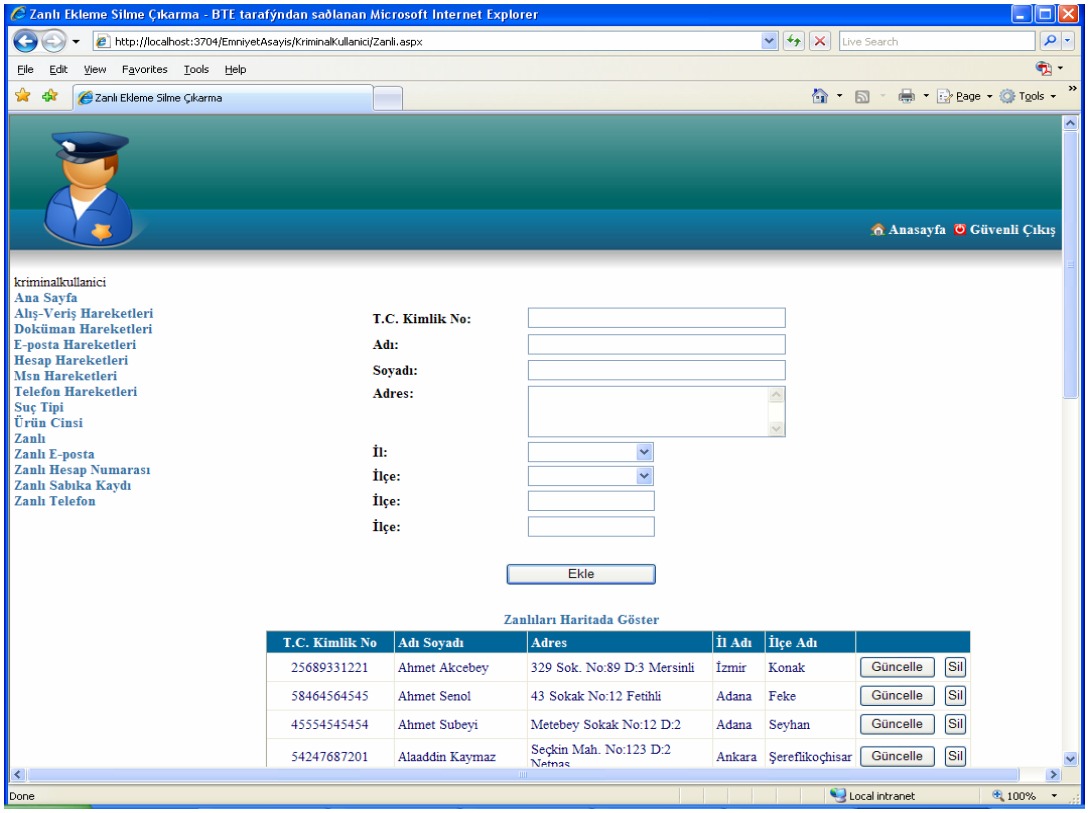
Sistem kullanıcıları bu ekran yardımı ile alış-veriş hareketlerinde kullanılan ürün cinsleri sisteme ekleyebilmekte, eklediği bu ürün cinsleri güncelleyebilmekte ve silebilmektedir. Ürün cinsleri zanlılar arasında yapılan alış-veriş işlemlerini sisteme kaydetme esnasında sistemdeki ürün cinslerini listelerken kullanılmaktadır. Eğer eklenmek istenen ürün cinsi listede yoksa bu ekran arcılığı ile istenilen ürün cinsi sisteme eklenebilmektedir.



Şekil 6.9. Ürün cinsi ekranı

6.12. Zanlı Ekranı

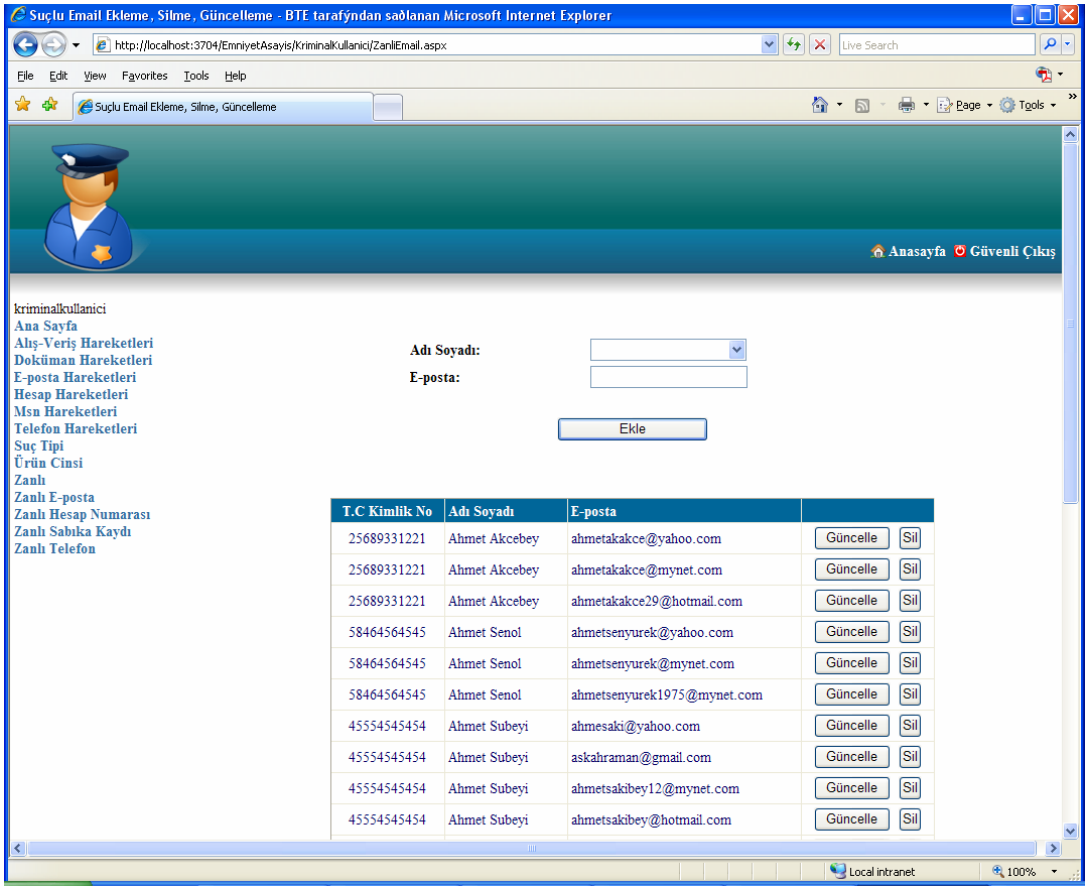
Sistem kullanıcıları bu ekran yardımı ile suç örgütü oluşturdukları düşünülen zanlıları sisteme ekleyebilmekte, eklediği bu zanlıları güncelleyebilmekte ve silebilmektedir. Sisteme zanlılara ait e-posta hesap numarası gibi bilgileri kaydetme esnasında sistemdeki zanlıları listelerken bu ekran yardımı ile eklenen zanlı isimleri kullanılmaktadır. Herhangi bir zanlıya ait herhangi bir kayıt sisteme eklenmek istendiğinde listede kaydı eklenmek istenen zanlı yoksa bu ekran aracılığı ile istenilen zanlı sisteme eklenebilmektedir.



Şekil 6.10. Zanlı ekranı

6.13. Zanlı E-posta Ekranı

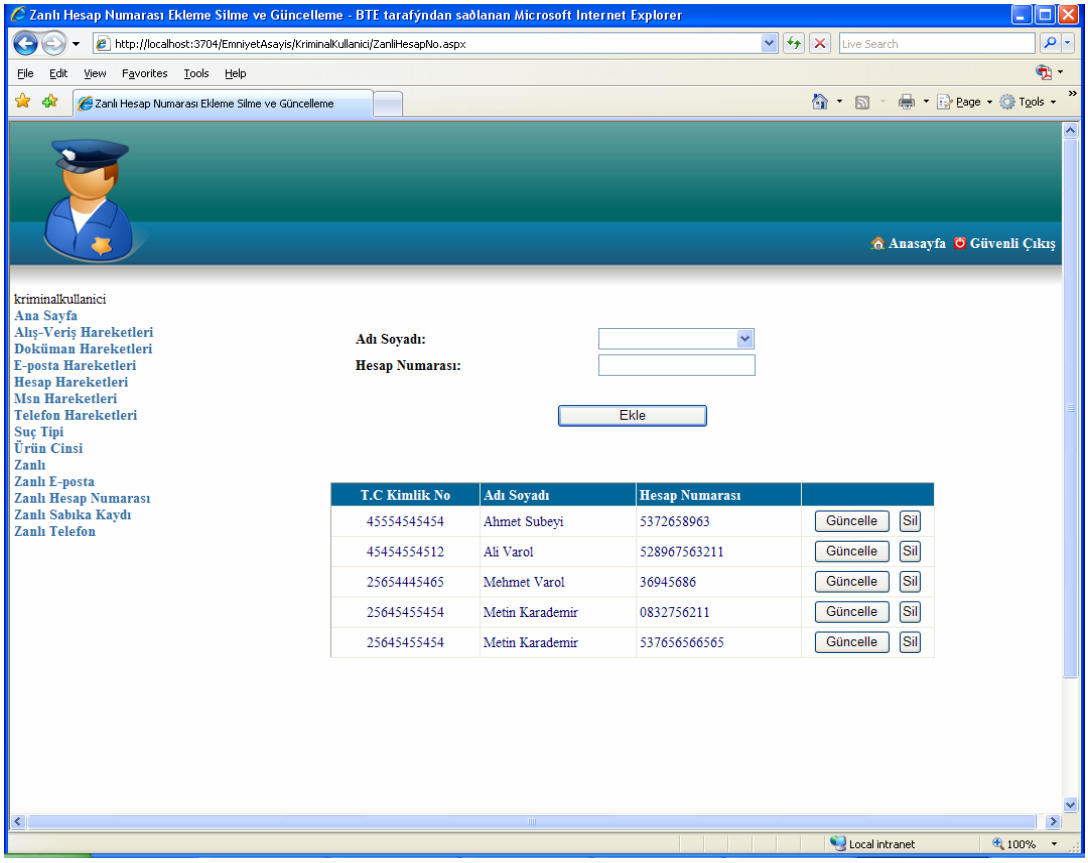
Sistem kullanıcıları bu ekran yardımı ile suç örgütü oluşturdukları düşünülen zanlılara ait e-posta bilgilerini sisteme ekleyebilmekte, eklediği bu e-posta bilgilerini güncelleyebilmekte ve silebilmektedir. E-posta bilgileri, zanlıların e-posta trafiğini sisteme kaydetme esnasında sistemdeki mevcut zanlılara ait e-posta bilgileri listelenirken kullanılmaktadır. Eğer listede e-posta detayı eklenmek istenen zanlıya ait e-posta bilgisi yoksa bu ekran arcılığı ile istenilen zanlıya ait e-posta bilgisi sisteme eklenebilmektedir.



Şekil 6.11. Zanlı e-posta ekranı

6.14. Zanlı Hesap Numarası

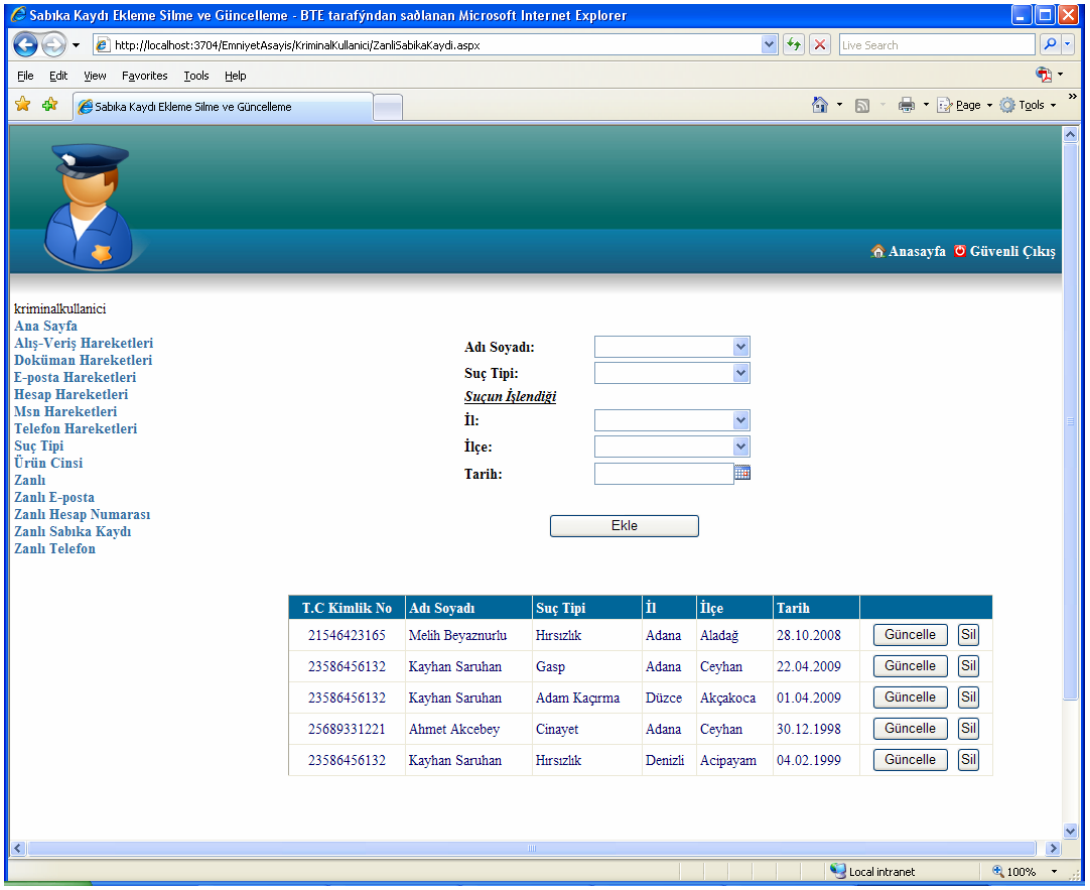
Sistem kullanıcıları bu ekran yardımı ile suç örgütü oluşturdukları düşünülen zanlılara ait banka hesap numarası bilgilerini sisteme ekleyebilmekte, eklediği bu banka hesap numarası bilgilerini güncelleyebilmekte ve silebilmektedir. Banka hesap numarası bilgileri zanlıların banka hesap trafiğini sisteme kaydetme esnasında sistemdeki mevcut zanlılara ait banka hesap numarası bilgileri listelenirken kullanılmaktadır. Eğer listede banka hesap numarası detayı eklenmek istenen zanlıya ait banka hesap numarası bilgisi yoksa bu ekran arcılığı ile istenilen zanlıya ait banka hesap numarası bilgisi sisteme eklenebilmektedir.



Şekil 6.12. Zanlı hesap no ekranı

6.15. Zanlı Sabıka Kaydı

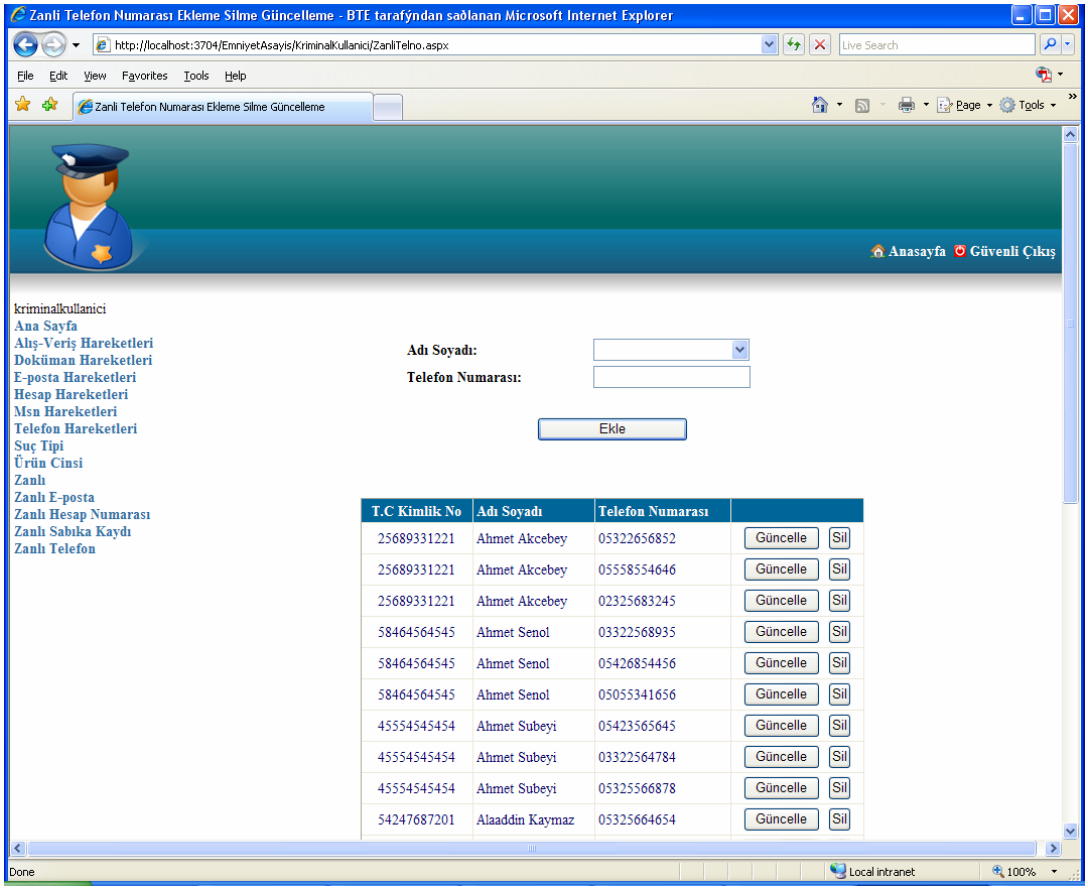
Sistem kullanıcıları bu ekran yardımı ile suç örgütü oluşturdukları düşünülen zanlılara ait varsa daha önceki suçlardan oluşmuş sabıka kaydı bilgisini sisteme ekleyebilmekte, eklediği bu sabıka kaydı bilgisini güncelleyebilmekte ve silebilmektedir. Sabıka kaydı bilgisi zanlıların geçmiş dönemlerde işledikleri suçlar listelenmek istendiğinde kullanılmaktadır. Sistem kullanıcıları zanlı daha önce ne gibi suçlar işlemiş bilgisine bu ekran aracılığı ile ulaşabilmektedir.



Şekil 6.13. Zanlı sabıka kaydı ekranı

6.16. Zanlı Telefon Ekranı

Sistem kullanıcıları bu ekran yardımı ile suç örgütü oluşturdukları düşünülen zanlılara ait telefon numarası bilgilerini sisteme ekleyebilmekte, eklediği bu telefon numarası bilgilerini güncelleyebilmekte ve silebilmektedir. Telefon numarası bilgileri zanlıların telefon trafiğini sisteme kaydetme esnasında sistemdeki mevcut zanlılara ait telefon numarası bilgileri listelenirken kullanılmaktadır. Eğer listede telefon numarası detayı eklenmek istenen zanlıya ait telefon numarası bilgisi yoksa bu ekran arcılığı ile istenilen zanlıya ait telefon numarası bilgisi sisteme eklenebilmektedir.



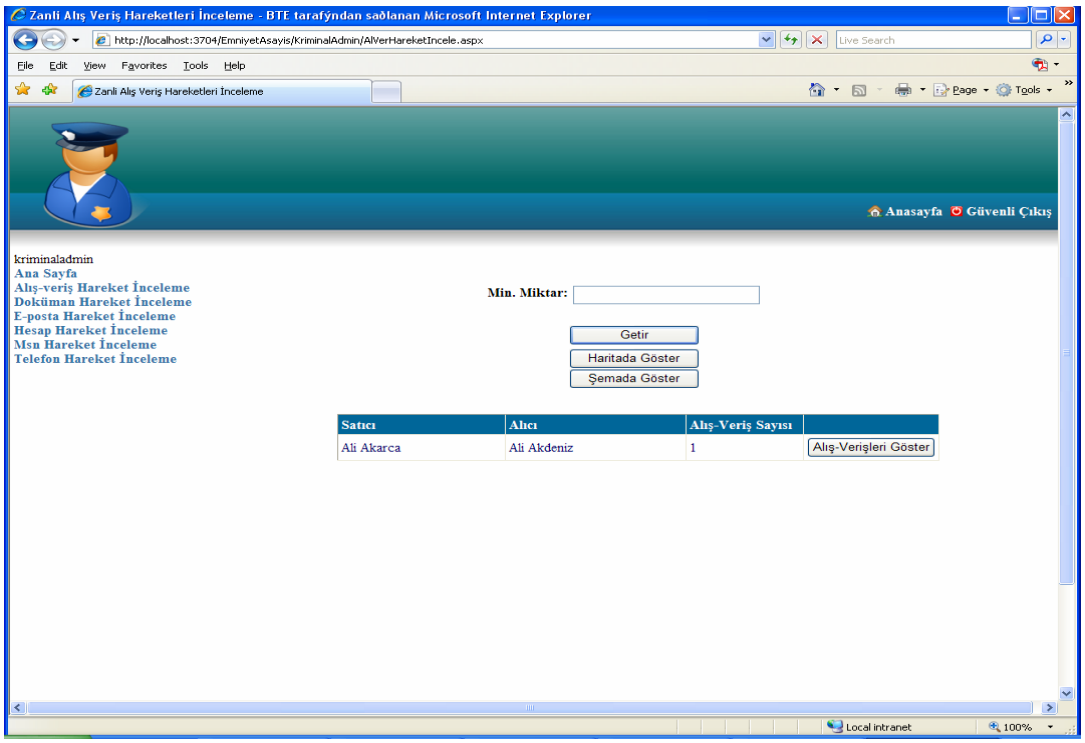
Şekil 6.14. Zanlı telefon ekranı

6.17. Alış-veriş Hareket İnceleme Ekranı

Veri girişinden sorumlu kullanıcılar tarafından sisteme girilen zanlılar arasında yapılan alış-veriş hareketleri bu ekran yardımı ile veri analizinden sorumlu kullanıcılar tarafından detaylı bir şekilde incelenebilmektedir. Alış-veriş hareketlerini analiz etmek isteyen kullanıcı, en az kaç paralık hareketlerin incelenmesini istiyorsa minimum miktar alanına o miktarı girer. Daha sonra "Getir" tuşuna basarak analiz etmek istediği alış-veriş hareketlerini listeler (Şekil 6.15).

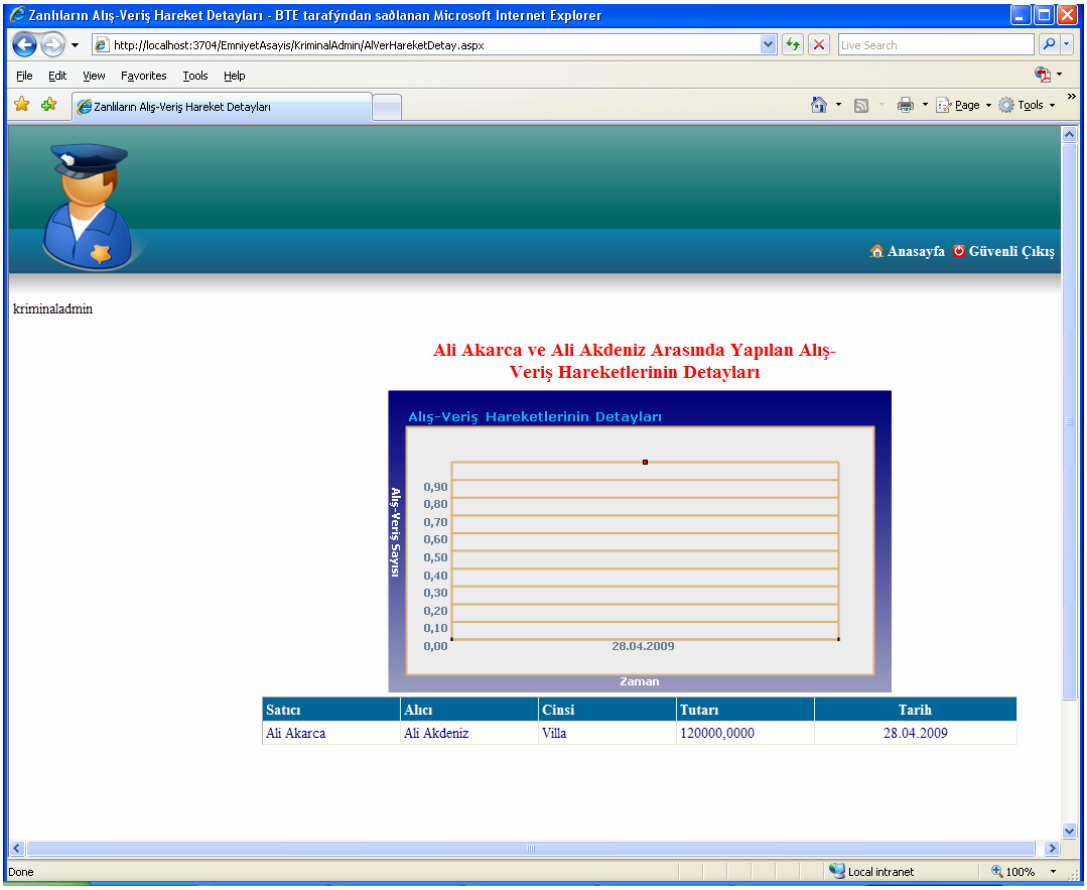
Listelenen alış-veriş hareketlerindeki zanlılar "Haritada Göster" tuşuna basılarak geliştirilen program yardımı ile adres bilgileri ve coğrafi koordinat bilgileri dikkate alınıp KMZ formatına dönüştürülüp coğrafi koordinat sisteminde googleeart programında gösterilmektedir. Bu sayede zanlıların coğrafi olarak nasıl bir dağılım gösterdiği bilgisine rahatlıkla ulaşılabilir.

Listelenen alış-veriş hareketleri "Şemada Göster" tuşuna basılarak geliştirilen program yardımı ile GrapML formatına dönüştürülüp görsel hale getirilmektedir. Bu görselleştirme işlemi sayesinde ortaya bir örüntü çıkmaktadır. Alış-veriş hareketlerinde ortaya çıkan bu örüntü emniyet teşkilatındaki uzman personele zanlılar arasında alış-veriş hareketlerine bağlı organizasyonel bir çete yapısı olup olmadığı hakkında bilgi vermektedir.



Şekil 6.15. Alış-veriş hareketlerinin listelenmesi ekranı

Listelenen alış-veriş hareketlerinin her birinde bulunan "Alış-veriş Göster" tuşuna basılarak iki zanlı arasında geçen alış-veriş hareketlerinin detayları incelenebilmektedir. Ayrıca alış-veriş hareketleri grafik üzerinde çizilerek hangi tarihlerde kaç defa alış-veriş hareketi gerçekleştirildi bilgisine çizilen grafik yardımı ile kolayca erişilebilmektedir (Şekil 6.16).

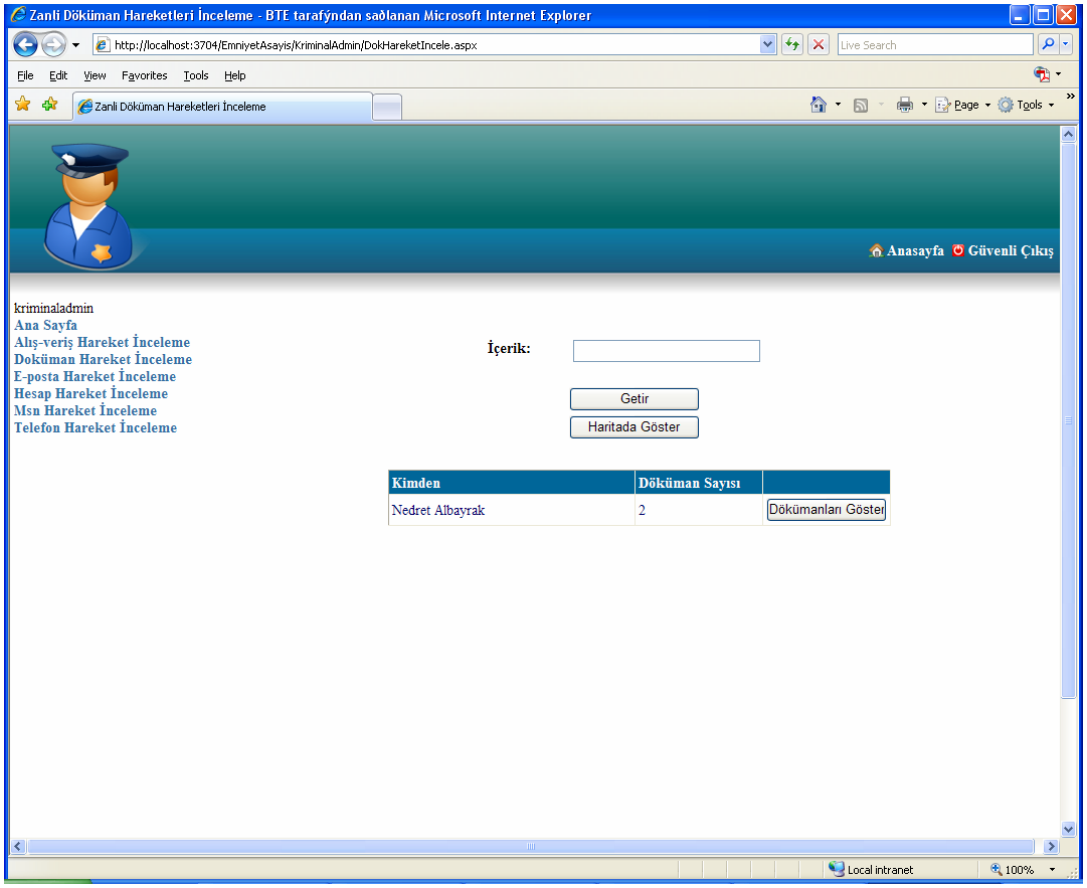


Şekil 6.16. Alış-veriş hareketleri detayları inceleme ekranı

6.18.Doküman Hareket İnceleme Ekranı

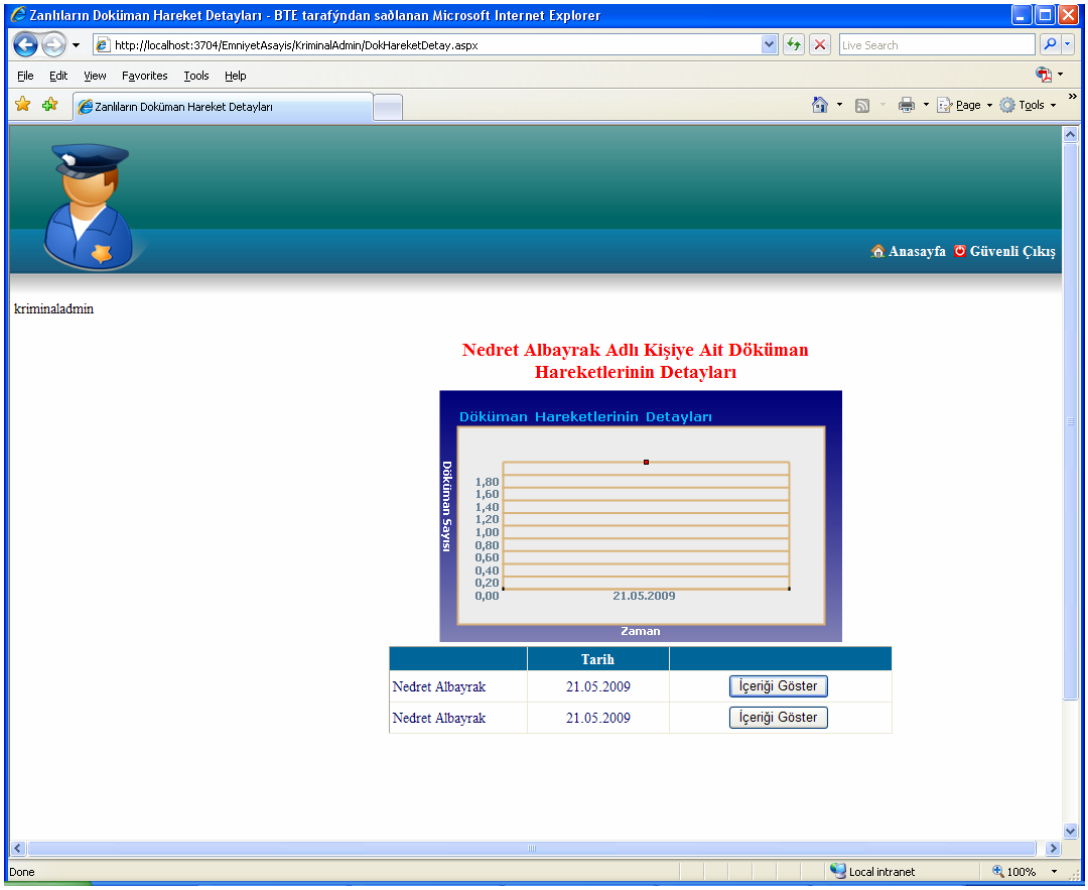
Veri girişinden sorumlu kullanıcılar tarafından sisteme girilen zanlılardan ele geçirilen dokümanlar bu ekran yardımı ile veri analizinden sorumlu kullanıcılar tarafından detaylı bir şekilde incelenebilmektedir. Ele geçirilen dokümanları analiz etmek isteyen kullanıcı, doküman içeriğinde şifre kelimeleri yada filtrelemek istediği kelimeleri içerik alanına girer. Daha sonra "Getir" tuşuna basarak analiz etmek istediği dokümanları listeler (Şekil 6.17).

Listelenen dokümanlara sahip olan zanlılar, "Haritada Göster" tuşuna basılarak geliştirilen program yardımı ile adres bilgileri ve coğrafi koordinat bilgileri dikkate alınıp KMZ formatına dönüştürülüp coğrafi koordinat sisteminde googleeart programında gösterilmektedir. Bu sayede zanlıların coğrafi olarak nasıl bir dağılım gösterdiği bilgisine rahatlıkla ulaşılabilir.



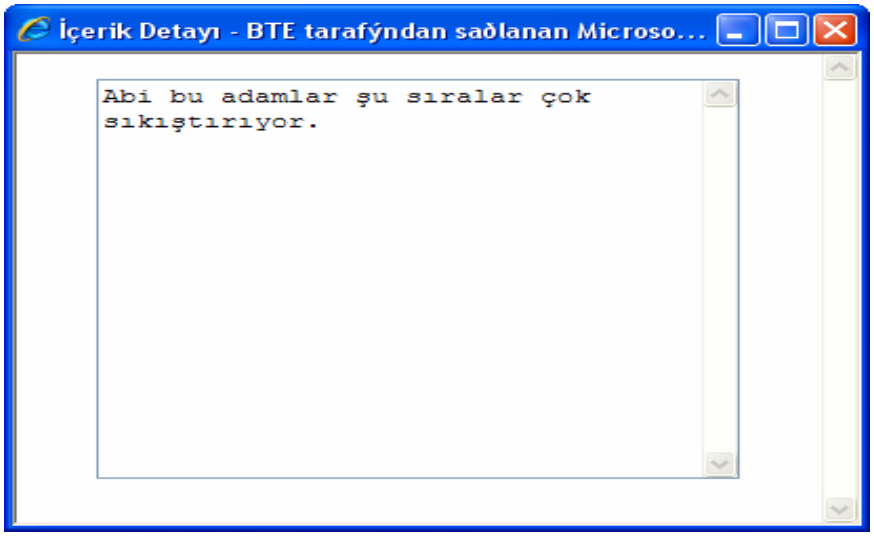
Şekil 6.17. Dokümanların listelenmesi ekranı

Listelenen dokümanların her birinde bulunan “Dokümanları Göster” tuşuna basılarak iki zanlılardan ele geçirilen dokümanların detayları incelenebilmektedir. Ayrıca ele geçirilen dokümanlar grafik üzerinde çizilerek hangi tarihlerde kaç tane doküman ele geçirildi bilgisine çizilen grafik yardımı ile kolayca erişilebilmektedir (Şekil 6.18).



Şekil 6.18. Doküman detayları inceleme ekranı

Dokümanların detaylarının incelendiği ekranda listelenen dokümanların her birinde bulunan "İçeriği Göster" tuşuna basılarak ele geçirilen dokümanın içeriği incelebilmektedir (Şekil 6.19).



Şekil 6.19. Doküman içeriği inceleme ekranı

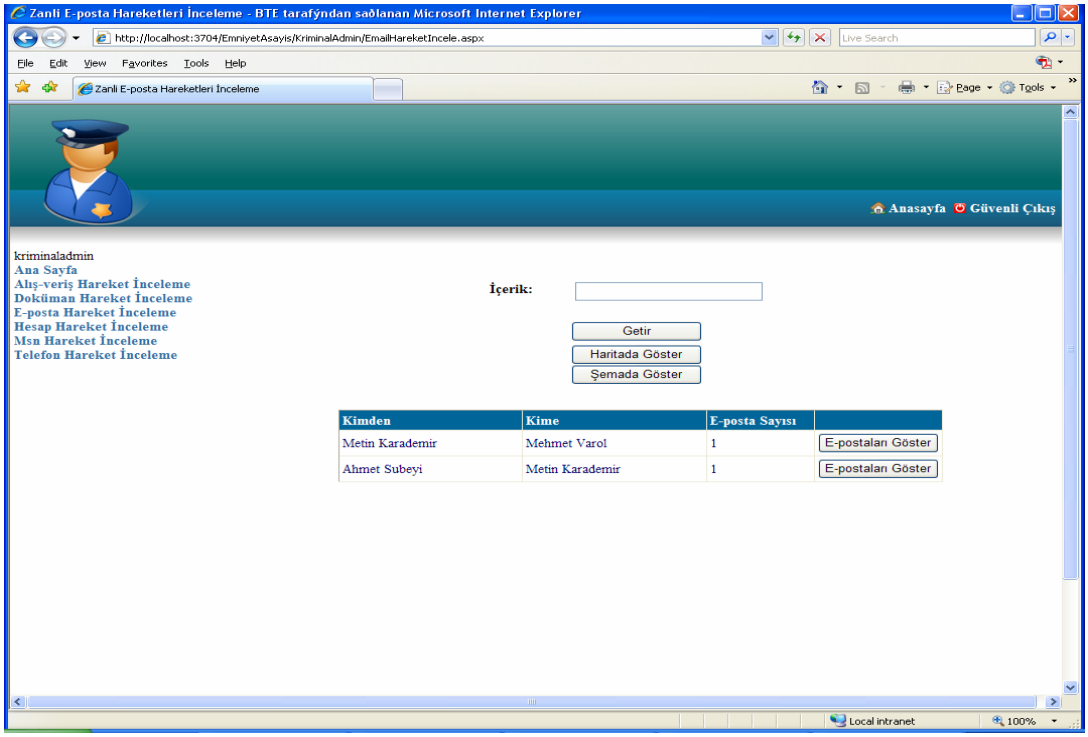
6.19. E-posta Hareket İnceleme Ekranı

Veri girişinden sorumlu kullanıcılar tarafından sisteme girilen zanlılar arasında yapılan e-posta hareketleri bu ekran yardımı ile veri analizinden sorumlu kullanıcılar tarafından detaylı bir şekilde incelenebilmektedir. E-posta hareketlerini analiz etmek isteyen kullanıcı, e-posta içeriğinde şifre kelimeleri yada filtrelemek istediği kelimeleri içerik alanına girer. Daha sonra "Getir" tuşuna basarak analiz etmek istediği e-posta hareketlerini listeler (Şekil 6.20).

Listelenen e-posta hareketlerindeki zanlılar "Haritada Göster" tuşuna basılarak geliştirilen program yardımı ile adres bilgileri ve coğrafi koordinat bilgileri dikkate alınıp KMZ formatına dönüştürülüp coğrafi koordinat sisteminde googleeart programında gösterilmektedir. Bu sayede zanlıların coğrafi olarak nasıl bir dağılım gösterdiği bilgisine rahatlıkla ulaşılabilir.

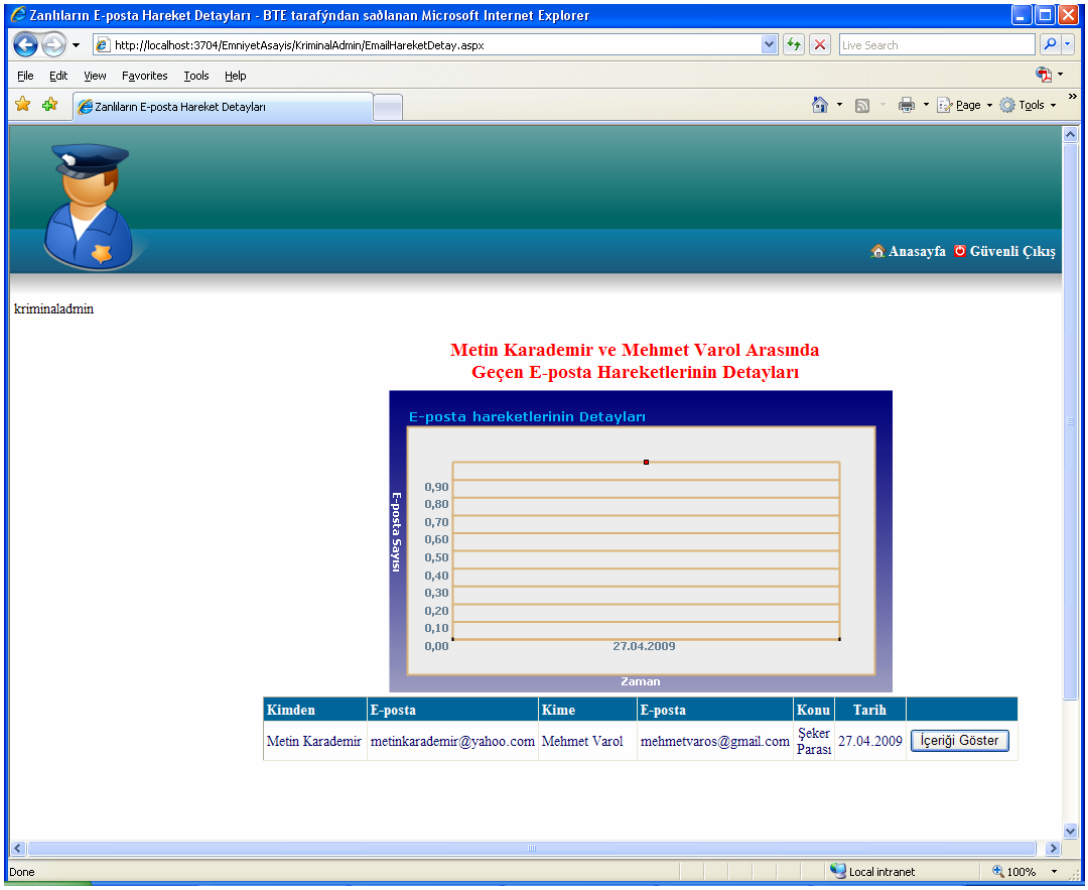
Listelenen e-posta hareketleri "Şemada Göster" tuşuna basılarak geliştirilen program yardımı ile GrapML formatına dönüştürülüp görsel hale getirilmektedir. Bu görselleştirme işlemi sayesinde ortaya bir örüntü çıkmaktadır. E-posta hareketlerinde ortaya çıkan bu örüntü emniyet teşkilatındaki uzman personele zanlılar arasında e-

posta hareketlerine bağlı organizasyonel bir çete yapısı olup olmadığı hakkında bilgi vermektedir.



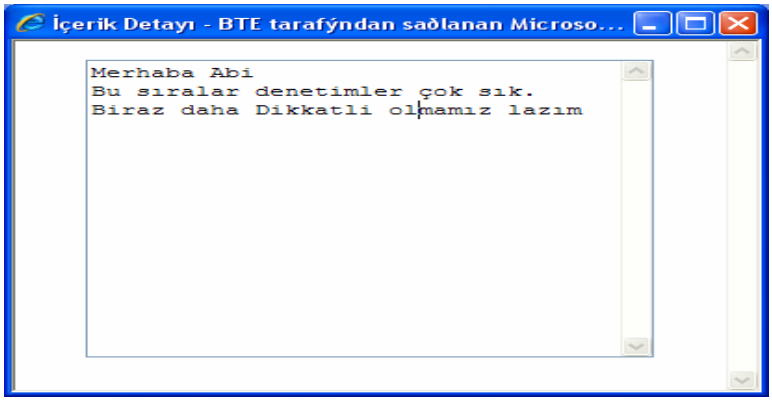
Şekil 6.20. E-posta hareketleri listelenmesi ekranı

Listelenen e-posta hareketlerinin her birinde bulunan “E-postaları Göster” tuşuna basılarak iki zanlı arasında geçen e-posta hareketlerinin detayları incelenebilmektedir. Ayrıca e-posta hareketleri grafik üzerinde çizilerek hangi tarihlerde kaç defa e-posta hareketi gerçekleştirildi bilgisine çizilen grafik yardımı ile kolayca erişilebilmektedir (Şekil 6.21).



Şekil 6.21. E-posta detayları inceleme ekranı

E-posta detaylarının incelendiği ekranda listelenen e-posta hareketlerinin her birinde bulunan "İçeriği Göster" tuşuna basılarak istenen e-posta hareketinin içeriği incelebilmektedir (Şekil 6.22).



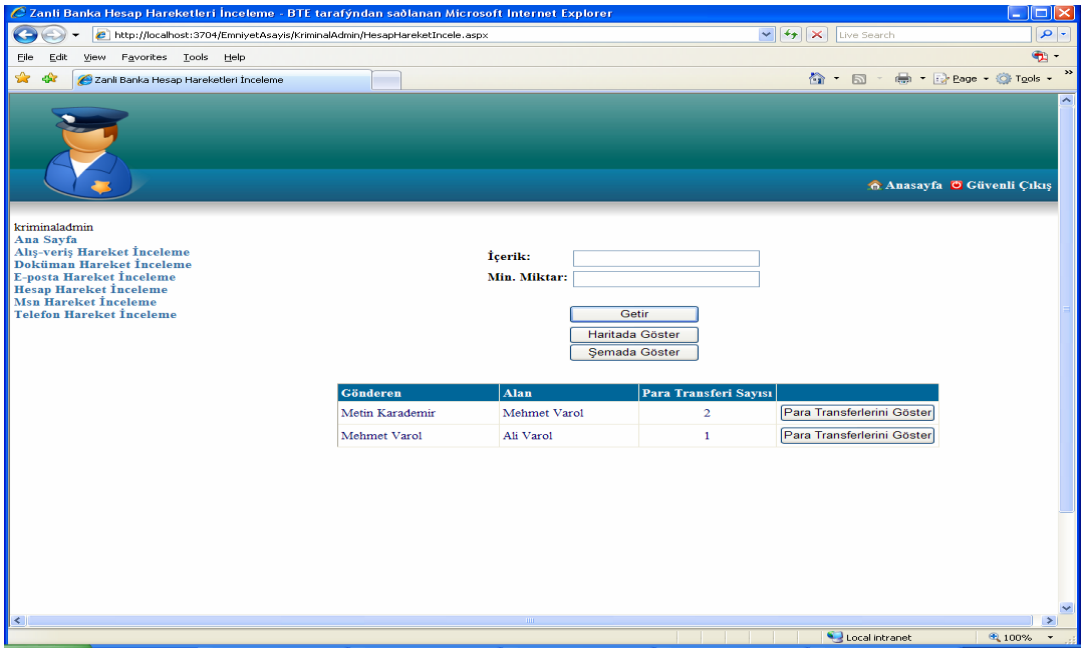
Şekil 6.22. E-posta içeriği inceleme ekranı

6.20. Hesap Hareket İnceleme Ekranı

Veri girişinden sorumlu kullanıcılar tarafından sisteme girilen zanlılar arasında yapılan para transferleri bu ekran yardımı ile veri analizinden sorumlu kullanıcılar tarafından detaylı bir şekilde incelenebilmektedir. Para transferlerini analiz etmek isteyen kullanıcı, en az kaç paralık transferin incelenmesini istiyorsa minimum miktar alanına o miktarı girer ve para transferinin açıklama kısmında aramak istediği şifre kelimeleri yada filtrelemek istediği kelimeleri de içerik alanına girer. Daha sonra "Getir" tuşuna basarak analiz etmek istediği para transferlerini listeler (Şekil 6.23).

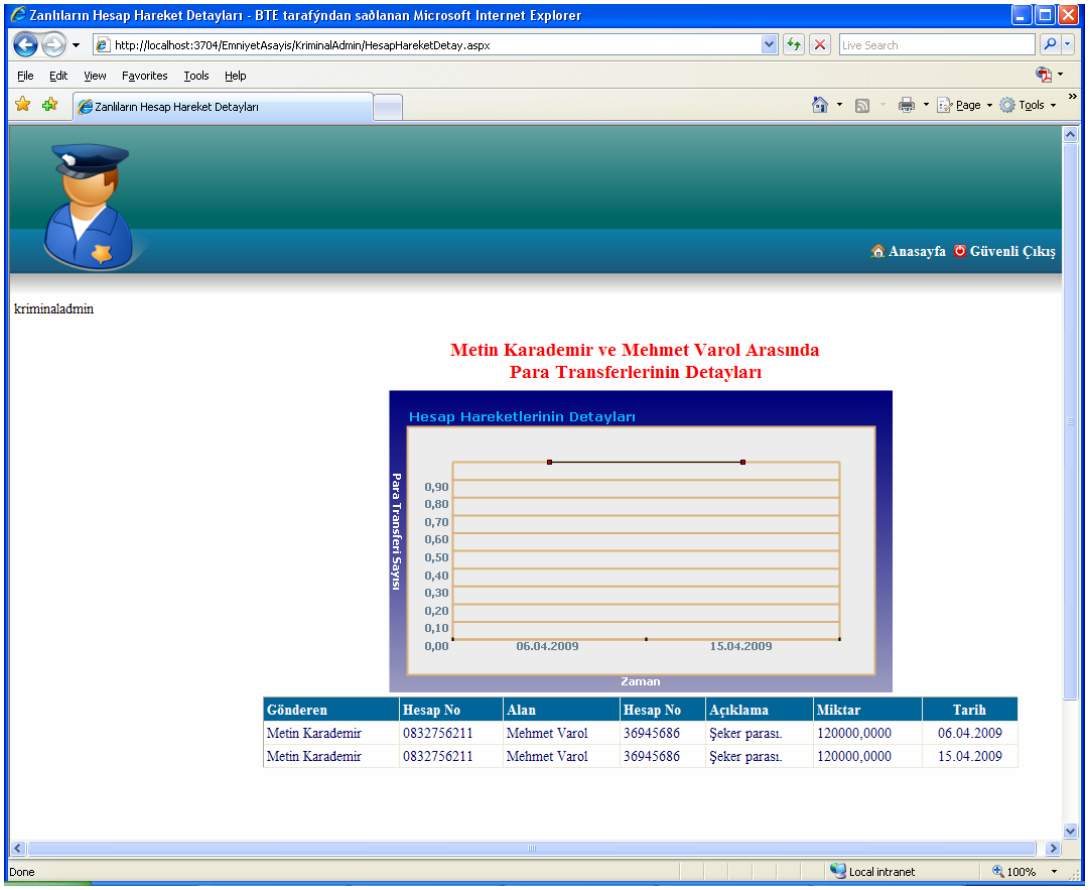
Listelenen para transferlerindeki zanlılar "Haritada Göster" tuşuna basılarak geliştirilen program yardımı ile adres bilgileri ve coğrafi koordinat bilgileri dikkate alınıp KMZ formatına dönüştürülüp coğrafi koordinat sisteminde googleeart programında gösterilmektedir. Bu sayede zanlıların coğrafi olarak nasıl bir dağılım gösterdiği bilgisine rahatlıkla ulaşılabilir.

Listelenen para transferleri "Şemada Göster" tuşuna basılarak geliştirilen program yardımı ile GrapML formatına dönüştürülüp görsel hale getirilmektedir. Bu görselleştirme işlemi sayesinde ortaya bir örüntü çıkmaktadır. Para transferlerinde ortaya çıkan bu örüntü emniyet teşkilatındaki uzman personele zanlılar arasında para transferlerine bağlı organizasyonel bir çete yapısı olup olmadığı hakkında bilgi vermektedir.



Şekil 6.23. Hesap hareketleri listelenmesi ekranı

Listelenen para transferlerinin her birinde bulunan “Para Transferlerini Göster” tuşuna basılarak iki zanlı arasında geçen para transferlerinin detayları incelenebilmektedir. Ayrıca para transferleri grafik üzerinde çizilerek hangi tarihlerde kaç defa para transferi gerçekleştirildi bilgisine çizilen grafik yardımı ile kolayca erişilebilmektedir (Şekil 6.24).



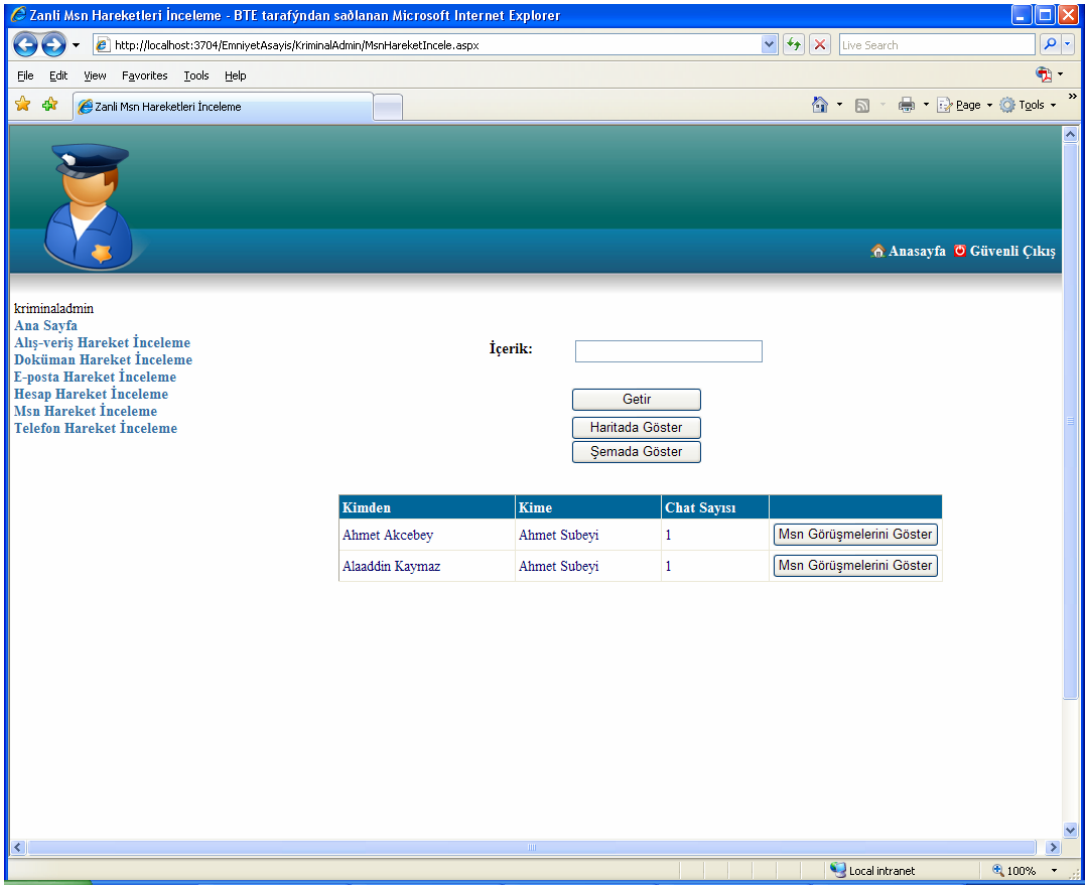
Şekil 6.24. Para transferi detayları inceleme ekranı

6.21. Msn Hareket İnceleme Ekranı

Veri girişinden sorumlu kullanıcılar tarafından sisteme girilen zanlılar arasında yapılan msn görüşmeleri bu ekran yardımı ile veri analizinden sorumlu kullanıcılar tarafından detaylı bir şekilde incelenebilmektedir. Msn görüşmelerini analiz etmek isteyen kullanıcı, msn görüşmesi içeriğinde şifre kelimeleri yada filtrelemek istediği kelimeleri içerik alanına girer. Daha sonra "Getir" tuşuna basarak analiz etmek istediği msn görüşmelerini listeler (Şekil 6.25).

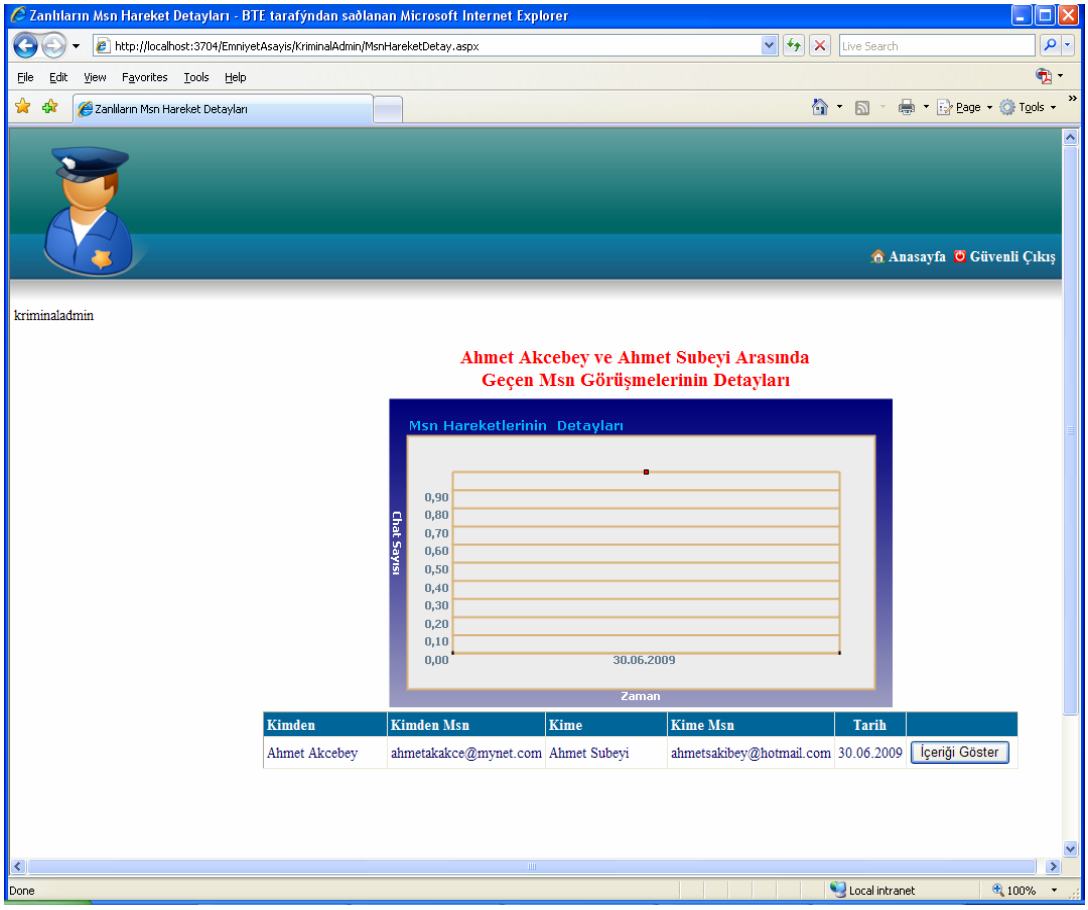
Listelenen msn görüşmelerindeki zanlılar "Haritada Göster" tuşuna basılarak geliştirilen program yardımı ile adres bilgileri ve coğrafi koordinat bilgileri dikkate alınıp KMZ formatına dönüştürülüp coğrafi koordinat sisteminde googleeart programında gösterilmektedir. Bu sayede zanlıların coğrafi olarak nasıl bir dağılım gösterdiği bilgisine rahatlıkla ulaşılabilir.

Listelenen msn görüşmeleri “Şemada Göster” tuşuna basılarak geliştirilen program yardımı ile GrapML formatına dönüştürülüp görsel hale getirilmektedir. Bu görselleştirme işlemi sayesinde ortaya bir örüntü çıkmaktadır. Msn görüşmelerinde ortaya çıkan bu örüntü emniyet teşkilatındaki uzman personele zanlılar arasında msn görüşmelerine bağlı organizasyonel bir çete yapısı olup olmadığı hakkında bilgi vermektedir.



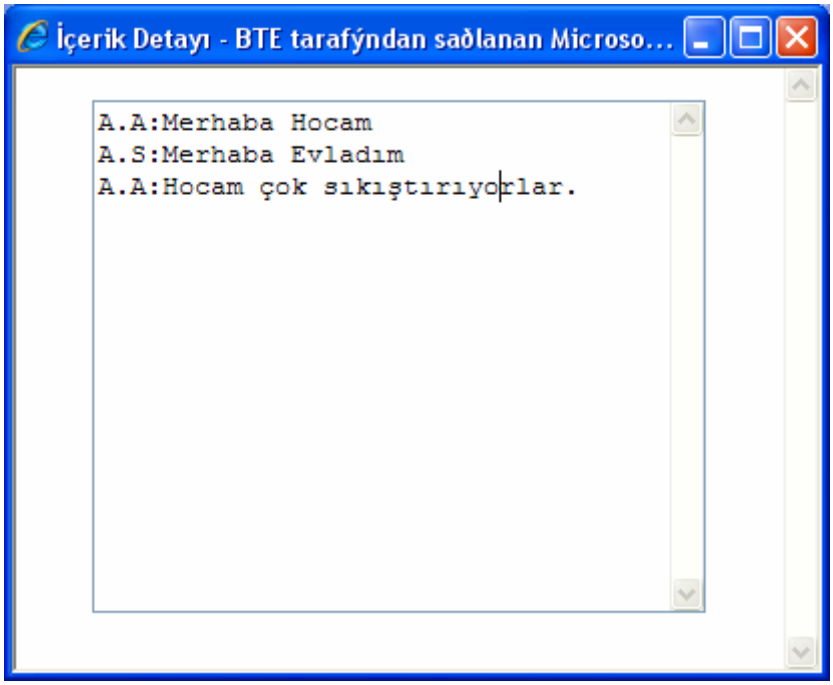
Şekil 6.25. Msn hareketleri listelenmesi ekranı

Listelenen msn görüşmelerinin her birinde bulunan “Msn Görüşmelerini Göster” tuşuna basılarak iki zanlı arasında geçen msn görüşmelerinin detayları incelenebilmektedir. Ayrıca msn görüşmeleri grafik üzerinde çizilerek hangi tarihlerde kaç defa msn görüşmesi gerçekleştirildi bilgisine çizilen grafik yardımı ile kolayca erişilebilmektedir (Şekil 6.26).



Şekil 6.26. Msn görüşmesi detayları inceleme ekranı

Msn görüşmesi detaylarının incelendiği ekranda listelenen msn görüşmelerinin her birinde bulunan “İçeriği Göster” tuşuna basılarak istenen msn görüşmesinin içeriği incelebilmektedir (Şekil 6.27).



Şekil 6.27. Msn görüşmesi içeriği inceleme ekranı

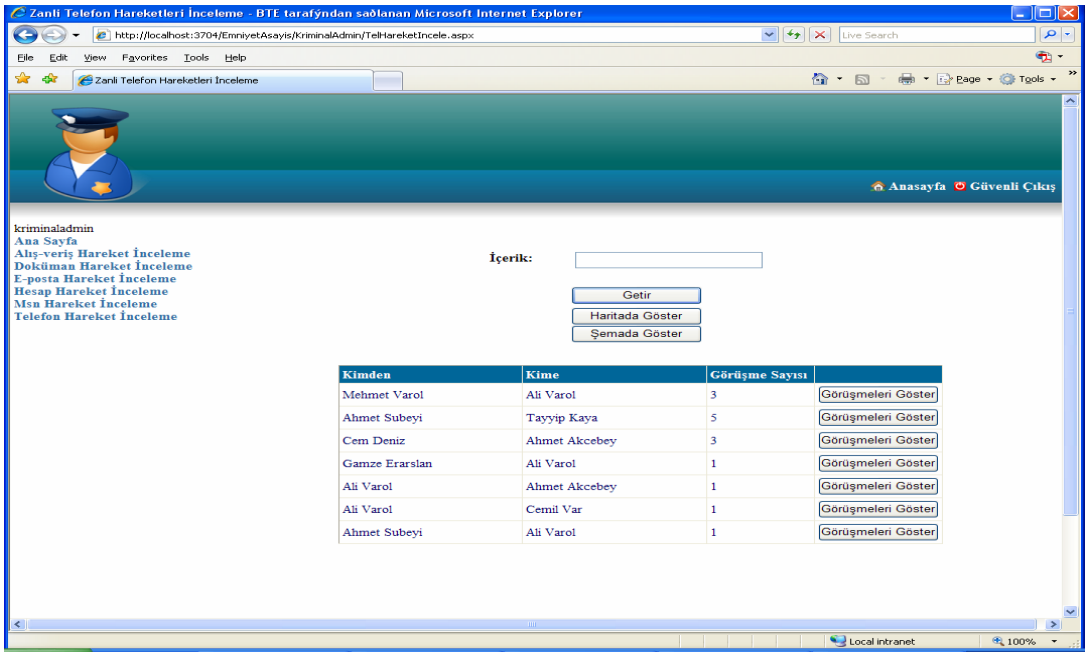
6.22. Telefon Hareket İnceleme Ekranı

Veri girişinden sorumlu kullanıcılar tarafından sisteme girilen zanlılar arasında yapılan telefon görüşmeleri bu ekran yardımı ile veri analizinden sorumlu kullanıcılar tarafından detaylı bir şekilde incelenebilmektedir. Telefon görüşmelerini analiz etmek isteyen kullanıcı, telefon görüşmesi içeriğinde şifre kelimeleri yada filtrelemek istediği kelimeleri içerik alanına girer. Daha sonra "Getir" tuşuna basarak analiz etmek istediği telefon görüşmelerini listeler (Şekil 6.28).

Listelenen telefon görüşmelerindeki zanlılar "Haritada Göster" tuşuna basılarak geliştirilen program yardımı ile adres bilgileri ve coğrafi koordinat bilgileri dikkate alınıp KMZ formatına dönüştürülüp coğrafi koordinat sisteminde googleeart programında gösterilmektedir. Bu sayede zanlıların coğrafi olarak nasıl bir dağılım gösterdiği bilgisine rahatlıkla ulaşılabilir.

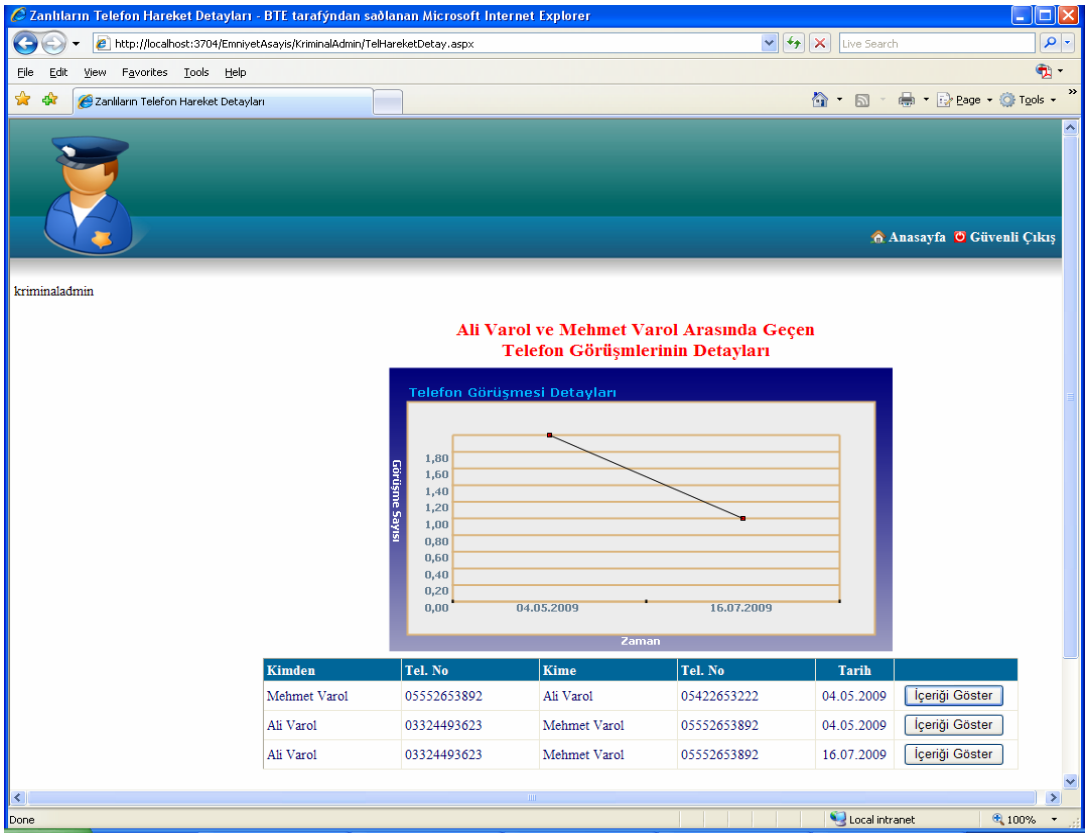
Listelenen telefon görüşmeleri "Şemada Göster" tuşuna basılarak geliştirilen program yardımı ile GrapML formatına dönüştürülüp görsel hale getirilmektedir. Bu görselleştirme işlemi sayesinde ortaya bir örüntü çıkmaktadır. Telefon

görüşmelerinde ortaya çıkan bu örüntü emniyet teşkilatındaki uzman personele zanlılar arasında telefon görüşmelerine bağlı organizasyonel bir çete yapısı olup olmadığı hakkında bilgi vermektedir.



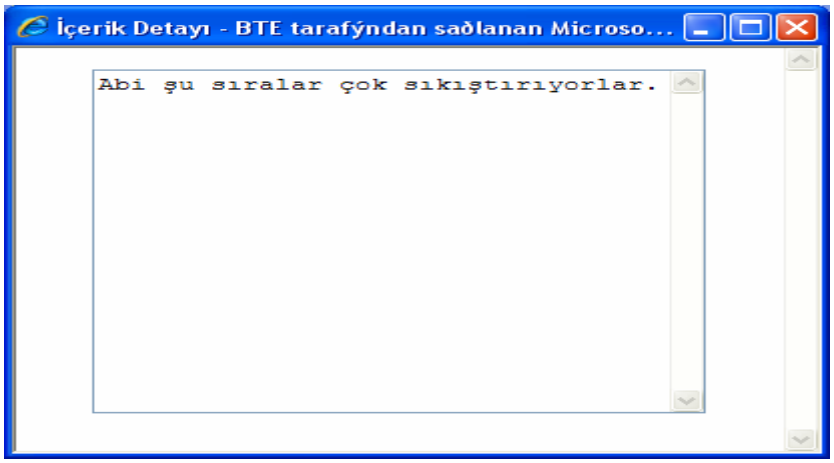
Şekil 6.28. Telefon hareketleri listelenmesi ekranı

Listelenen telefon görüşmelerinin her birinde bulunan “Görüşmeleri Göster” tuşuna basılarak iki zanlı arasında geçen telefon görüşmelerinin detayları incelenebilmektedir. Ayrıca telefon görüşmeleri grafik üzerinde çizilerek hangi tarihlerde kaç defa telefon görüşmesi gerçekleştirildi bilgisine çizilen grafik yardımı ile kolayca erişilebilmektedir (Şekil 6.26).



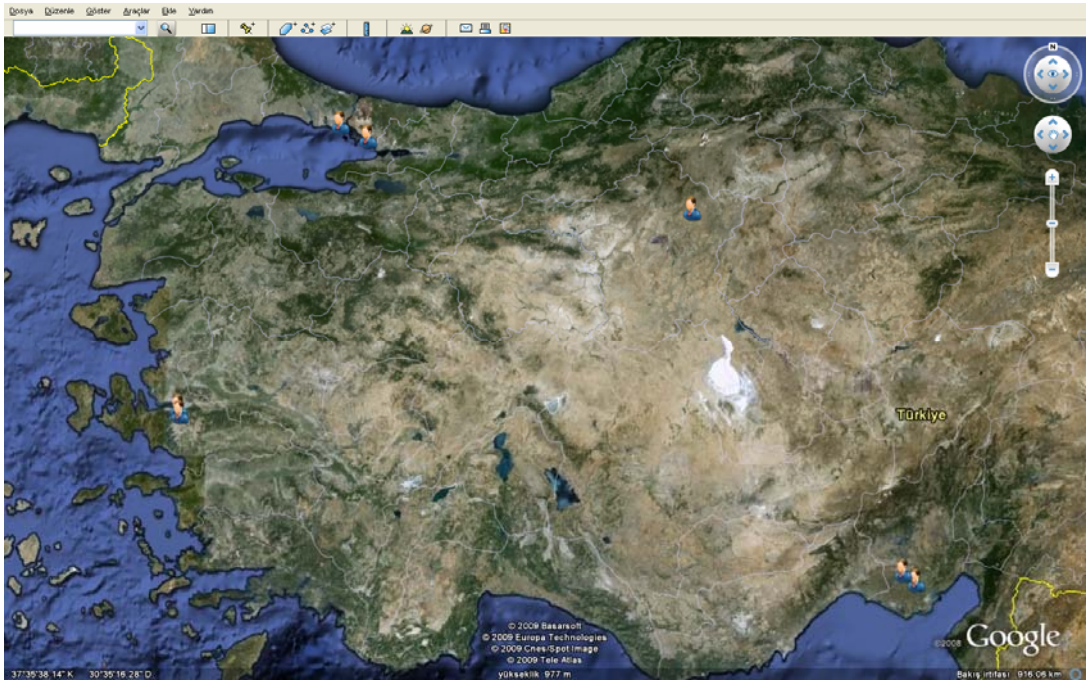
Şekil 6.29. Telefon görüşmesi detayları inceleme ekranı

Telefon görüşmesi detaylarının incelendiği ekranda listelenen telefon görüşmelerinin her birinde bulunan "İçeriği Göster" tuşuna basılarak istenen telefon görüşmesinin içeriği incelebilmektedir (Şekil 6.22).



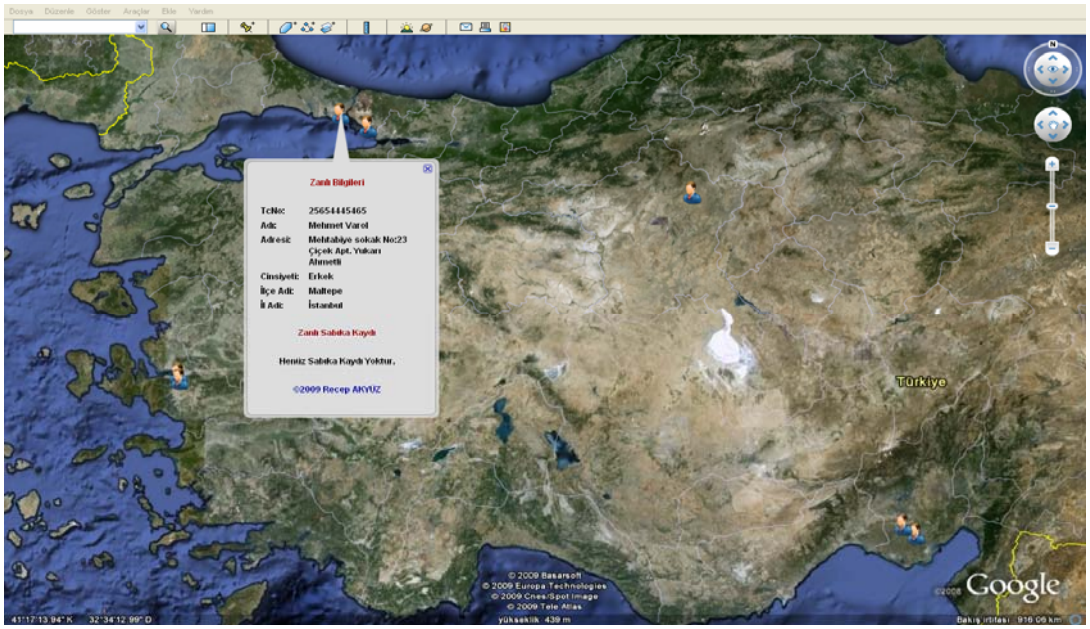
Şekil 6.30. Telefon görüşmesi içeriği inceleme ekranı

Listelenen bütün hareketlerdeki zanlılar “Haritada Göster” tuşuna basılarak geliştirilen program yardımı ile adres bilgileri ve coğrafi koordinat bilgileri dikkate alınıp KMZ formatına dönüştürülüp Şekil 6.31’deki gibi googleeart programında gösterilmektedir. Bu sayede zanlıların coğrafi olarak nasıl bir dağılım gösterdiği bilgisine rahatlıkla ulaşılabilir.



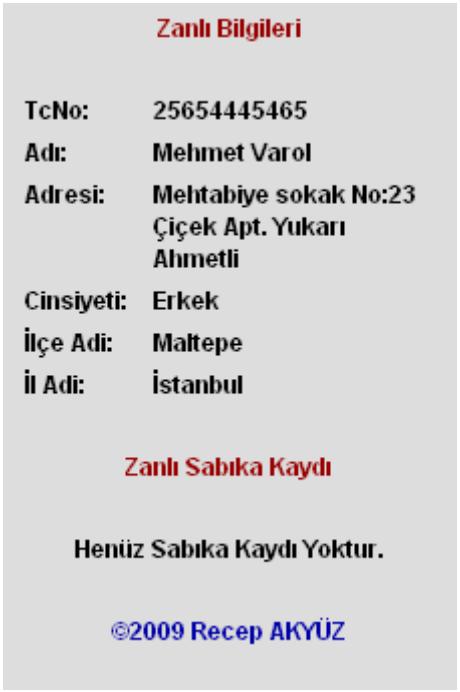
Şekil 6.31. Kmz yardımı ile kullanıcıların coğrafi koordinatlarına bakılarak adreslerinin çizilmesi

Fare, detay bilgisine ulaşılmak istenen zanlının üzerine getirildiğinde zanlıya ait ad, soy ad, adres vb bilgiler tablo yapısında listelenmektedir.



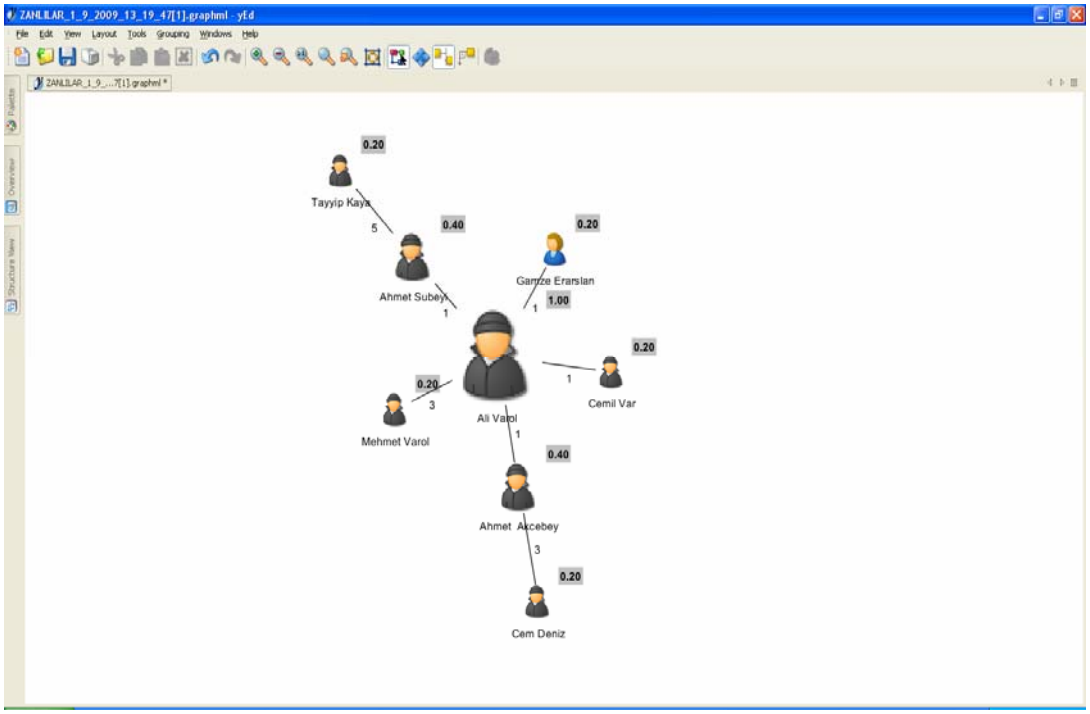
Şekil 6.32. Fare üzerine getirilen zanlının detay bilgisinin listelenmesi

Fare'nin üzerine gelmesi ve çift tıklanması sonucu zanlıya ait listelenen bilgiler aşağıdaki gibidir.



Şekil 6.33. Zanlıya ait listelene bilgiler

Listelenen hareketler "Şemada Göster" tuşuna basılarak geliştirilen program yardımı ile GrapML formatına dönüştürülüp görsel hale getirilmektedir. Bu görselleştirme işlemi sayesinde ortaya bir örüntü çıkmaktadır. Şekil 6.35'te ortaya çıkan örüntülerden biri gözükmektedir. Merkeze yakın olan kullanıcılar daha belirgindir



Şekil 6.34. GrapML yardımı ile örüntünün ortaya çıkarılması

BÖLÜM 7. SONUÇLAR VE ÖNERİLER

Emniyet verilerinin incelenmesinde karşılaşılan zorluklar bu alanlarda yapılan çalışmaları zorlaştırmakta ve yavaşlatmaktadır. Ülkemizde özel yaşamın gizliliğine ait kanunların sertliği sebebiyle bu verilere ulaşım bazen ya hiç ya da yok denecek az miktarda olabilmektedir. Yurtdışında bu alanda yapılan uygulamaların çokluğuna rağmen ülkemizde yok denecek kadar az olması, yukarıda bahsi geçen sebeplerden kaynaklanmaktadır.

Bu çalışmada suç verileri derinlemesine incelenmiş ve suç veriler incelenmesi sonucu ortaya örüntülerden suç örgütlerinin yapıları ortaya çıkarılmaya çalışılmıştır. Veri görselleştirme için kullanılan araçların GraphML formatının esnekliğinden faydalanılmıştır.

Türkiye'de suç verilerine ulaşılmasının önündeki zorluklar kaldırılarak daha güzel sonuçlar üreten araştırmalar yapılmalıdır. Gerçek veriye ulaşmanın zor olmasından dolayı yapılan çalışma örnek veriler üzerine gerçekleştirilmiştir. Daha önceki bölümlerde yurtdışında yapılan çalışmalar ve bu çalışmaların olumlu sonuçları aktarılmıştır. Yapılan çalışmalarda elde edilen başarılı sonuçlara rağmen ülkemizde bu alanda atılan adımlar yavaş ilerlemektedir. Yasalar ve emniyet teşkilatı üniversitelerin suç verileri üzerine araştırmalar yapmasını kolaylaştırmalı ve bu bilgilere erişimin önündeki engelleri kaldırmalıdır.

KAYNAKLAR

[1] ALATAŞ, B., AKIN, E., "Veri Madenciliğinde Yeni Yaklaşımlar", YA/EM'2004 - Yöneylem Araştırması /Endüstri Mühendisliği - XXIV Ulusal Kongresi, Gaziantep – Adana, 15-18 Haziran 2004.

[2] WILLIAM, F., GREGORY, S., CRHRISTOPER, J., "Knowledge discovery in databases - an overview"

[3] THUARISINGHAM, M., "Web Data Mining and Applications in Business Intelligence and counter Terrorism", Auerbach Publishers, incorporated, 2003.

[4] YALÇINTAŞ, G., "Veri Madenciliği", Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara, 2003.

[5] FAYYAD, U., PIATETSKY-SHAPIRO, G., SMITH, P., "The KDD process for extracting useful knowledge from volumes of data.", Communications of ACM, 39(11), 27-34, 1996.

[6] LARSE, D.T., Discovering Knowledge in Data: An Introduction at Data Mining, Jhn Wiley & Sns Inc., 2005.

[7] AKPINAR, H., "Veritabanlarında bilgi keşfi ve veri madenciliği", İstanbul Üniversitesi İşletme Fakültesi Dergisi, 2000.

[8] http://www.kdnuggets.com/polls/2003/data_mining_applications_industries.html, Nisan 2005.

[9] AYDOĞAN, F., "E-ticarette veri madenciliği yaklaşımlarıyla müşteriye hizmet sunan akıllı modüllerin tasarımı ve gerçekleştirimi", Yüksek Lisans Tezi, Hacettepe Üniversitesi Fen Bilimleri Enstitüsü, Ankara, 2003.

[10] QUINLAN, J.R., The effect of noise on concept learning, San Mateo, CA: Morgan Kauffmann Inc., 1986

[11] HULTEN, G., SPENCER, L., DOMINGOS, P., "Mining time-changing data streams", 7th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, San Fransisco, CA: ACM Pres, 2001.

[12] http://www.spss.com/dirvideo/richmond.htm?source=dmpage&zone=rtsidebar, "The results demonstrated a 49% reduction in the number of random gunfire complaints, with a concomitant", Mayıs 2007.

[13] STANLEY, M., "The Small World Problem", Psychology Today, 1967.

[14] TYLER, J., WILKINSON, D., HUBERMAN B., Email as spectroscopy: automated discovery of community structure within organizations. In M. Huysman, E. Wenger, and V. Wulf, editors, Communities and Technologies, 2003.

[15] MALTZ, M., Defining Organized Crime. Westport, CT and London: Greenwood, 1994.

[16] http://www.turkishdailynews.com.tr/article.php?enewsid=110985, Ekim 2008.

[17] RAAB, J., MILWARD, H.B., Dark Networks as Problems. Journal of Public Administration Research and Theory, 2003.

[18] RAAB, J., Milward, H.B., Dark Network as an Organizational Problem: Elements of a Theory. International Public Management Journal, 2006.

[19] MCANDREW, D., The structural analysis of criminal networks. In The Social Psychology of Crime: Groups, Teams, and Networks. D. Canter and L. Alison, Eds. Dartmouth Publishing, Aldershot, UK, 1999.

[20] SPARROW, M.K. The application of network analysis to criminal intelligence: An assessment of the prospects. Soc. Netw. 13, 1991.

[21] CHEN, H.X., “Criminal Network Analysis and Visualization”, Communications of The ACM, Haziran 2005.

[22] KLERKS, P. The network paradigm applied to criminal organizations: Theoretical nitpicking or a relevant doctrine for investigators? Recent developments in the Netherlands. Connections, 2001.

[23] MCANDREW, D., The structural analysis of criminal networks. The Social Psychology of Crime: Groups, Teams, and Networks, Offender Profiling Series, III. D. Canter and L. Alison (Eds.). Aldershot, Dartmouth, 1999.

[24] WASSERMAN, S., FAUST, K., Social Network Analysis: Methods and Applications. Cambridge University Press, Cambridge, MA, 1994.

ÖZGEÇMİŞ

Recep AKYÜZ, 07.05.1983 de İzmir' de doğdu. İlk ve orta eğitimini İzmir Konak'ta, lise eğitimini Aydın Ortaklar'da tamamladı. 2001 yılında Aydın Ortaklar Anadolu Öğretmen Lisesi, Fen Bilimleri Bölümünden mezun oldu. 2002 yılında başladığı EGE Bilgisayar Mühendisliği bölümünü 2006 yılında bitirdi. 2007 yılında Sakarya Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar ve Bilişim Mühendisliği Bölümüne girdi. 2007 yılından beri TÜBİTAK Marmara Araştırma Merkezi'nde araştırmacı bilgisayar mühendisi olarak çalışmaktadır. Bu süre içerisinde TÜBİTAK Marmara Araştırma Merkezi'nde yürütülen yazılım, internet programlama, veritabanı tasarımı ve yönetimi konularını içeren Ar-Ge projelerinde aktif rol aldı. Şu anda TÜBİTAK Marmara Araştırma Merkezi'nde yazılım uzmanı olarak görev yapmaktadır.