Adli Bilişim ve Etmen Tabanlı Sistemler

A. Emekci, E. Kuğu

***Özet*—Bu çalışmada, adli bilişim ile etmen tabanlı sistemler alanlarının entegrasyonu incelenmiştir. Adli bilişim; teknoloji ve teknolojik ürünlerin hayatımızdaki yerinin giderek genişlemesi ve çeşitlenmesine paralel olarak gelişen ve kullanılan yöntem, teknik ve ürünlerin sürekli yenilenmesini gerektiren çok dinamik bir alandır. Özellikle bilgisayar ve iletişim sistemlerinin baş döndürücü bir hızla geliştikleri günümüz dünyasında, depolama kapasitelerindeki artış, sistemlerin dağıtık bir yapıda genişlemesi ve mobilitenin sınır tanımazlığı adli bilişim alanında kullanılacak yeni yöntem, teknik ve ürünlere ihtiyaç duyulduğunun habercisidir. Bu noktada, ortaya çıkan yeni ihtiyaç ve problemlerle başa çıkılmasında, etmen tabanlı sistemlerin adli bilişim alanına büyük katkı yapacağı değerlendirilmektedir. Çalışmada, etmen tabanlı sistemlerin adli bilişim alanındaki uygulamaları etraflıca incelenmiş, bu doğrultuda halihazırda ve gelecek dönemde etmen tabanlı sistemlerin adli bilişim alanında daha etkin kullanılmasına dönük değerlendirmeler yapılmıştır.**

***Anahtar Kelimeler*— Adli bilişim, Akıllı sistemler, Etmen, Etmen tabanlı sistemler**

***Abstract*—The subject of this paper is a research on the integration of digital forensics and agent-based systems fields. Digital forensics is a very dynamic field that necessitates modernized and upgraded methods, techniques and tools in parallel with the expansion of technology and its products in our lives. Especially, the incredibly fast progress in computer and telecommunication systems in todays world, increasing capacity of data storage, distributed structure of the systems and no-boundaries in mobility are the harbingers of some new methods, techniques and tools needed in digital forensics. At this point, it is estimated that agent-based systems can well contribute to digital forensics field to cope with the emerging needs and challenges. In this study, a wide range of the applications of agent-based systems on digital forensics field has been examined, and in this direction, some inferences has been made for the more effective usage of agent-based systems on the field of digital forensics.**

***Index Terms*—Agent, Agent-based systems, Digital forensics, Intelligent systems**

I. GİRİŞ

GÜNÜMÜZDE her alanda olduğu gibi, belki çok daha fazlaca, bilgisayar ve iletişim alanlarında en belirleyici ve önemli unsurlardan bir tanesi hızdır. Buna paralel olarak, adalete ilişkin yapılan işlemlerle ilgili olarak "Gecikmiş adalet, adalet değildir" sözünü duymayanımız sanıyorum yoktur. Özellikle teknojik imkânlara çok az maliyetle ve hemen herkesçe çok kolay erişilebilir olması, üretilen her türlü verinin de kahir ekseriyetle elektronik ortamda üretilmesi ve tutulması sonucunu doğurmuştur. Bu kadar çok elektronik verinin üretildiği bir ortamda, suç örgütleri ya da bireylerce işlenen suçlarda, işlenen suçlara ilişkin elde edilen deliller arasında elektronik verilerin oranının artması da olağan bir sonuçtur.

1965 yılında Intel firmasının kurucularından Gordon Moore'un, yapacağı bir konuşmaya hazırlık yaptığı süreçte gözlemlediği bir durum bilişim dünyasının geleceğini çizmiş gibidir. Moore Kanunu olarak bilinen bu gözleme göre, ortalama her 18-24 aylık dönemlerle yonga kapasitesi, işlemci hızı ve veri depolama kapasitesi iki katına çıkmaktadır [1]. Günümüzde de büyük oranda doğruluğunu sürdüren bu çıkarım, maalesef adli bilişim alanı için incelenmesi gereken verilerin giderek artıyor olması gibi bir sorun oluşturmaktadır. Bilişim sistemlerinin ve teknolojik ürünlerin artık çok yaygın olarak kullanılıyor, sistemlerin karmaşık ve dağıtık bir yapı gösteriyor olması adli bilişim alanının ilgilenmesi gereken diğer sorunlar olarak göze çarpmaktadır.

Adli bilişim alanındaki yukarıda bahsedilen problem sahalarının hafifletilmesi noktasında, etmen tabanlı sistemlerin katkısının büyük olacağı düşünülmektedir. Çalışmanın diğer bölümleri ve ele alınacak konular şöyle olacaktır: Bölüm 2'de adli bilişim ve uygulama alanları, Bölüm 3'te etmen tabanlı sistemler, Bölüm 4'te etmen tabanlı sistemlerin adli bilişim alanındaki uygulamaları ele alınacak, Bölüm 5'te iki alan arasındaki entegrasyonun geliştirilmesi üzerine bir değerlendirme yapılacak ve Bölüm 6'da da sonuç ile çalışma tamamlanacaktır.

II. ADLİ BİLİŞİM VE UYGULAMA ALANLARI

Adli bilişim kavramının ortaya çıkması, bilişim ve bilgisayar teknolojilerinin gelişmesine ve suç işlemede bir unsur olmaya başlamasına paralel olarak 1980'li yılların sonlarına dayanmaktadır. Ancak adli bilişim uygulamalarından biri olan veri kurtarma işlemini de dikkate aldığımızda, aslında 1970'lerin ilk dönemlerine kadar gitmemiz gerekir [2]-[3].

Adli bilişim, herhangi bir suça konu olarak elde edilmiş bulunan elektromanyetik/elektro-optik ortamlarda muhafaza edilen, taşınan, iletilen vb. verilerin hukuk kurallarına uygun olarak tespiti, elde edilmesi, toplanması, saklanması,

Adem Emekci, Hava Harp Okulu, Havacılık ve Uzay Teknolojileri Enstitüsü, İstanbul, Türkiye. (e-posta: adem.emekci@gmail.com)
Emin Kuğu, Hava Harp Okulu, Bilgisayar Mühendisliği Bölümü, İstanbul, Türkiye. (e-posta: e.kugu@hho.edu.tr)

derlenmesi ve yine uygun teknikler kullanılmak suretiyle analiz edilmesi sonucu elde edilecek suça ilişkin kanıtların adli makamlara sunulması işlemleri bütünüdür [4]-[5]. Uygulamada intihar gibi çok basit bir olaydan, uyuşturucu tacirlerinin iletişimlerinin ortaya çıkarılmasına, sosyal medya ortamında bir şahsa yönelik hakâretten, çok sayıda müşterisi bulunan bir bankanın veri tabanındaki tüm bilgilerin saldırganlarca ele geçirilmesine ve hatta siber saldırı yöntemleriyle bir ülkenin, diğer bir ülkenin bilgisayar sistemlerini çökertmesine kadar çok geniş bir yelpazeyi ilgilendirmektedir.

Adli bilişim uygulamalarında yapılan işlemler birbirlerine çok yakın olmakla birlikte, işlenen suçun türü, söz konusu elektronik ortam, elektronik ortamın yapısı, delillerin kalıcı-uçucu olması, suç şüphelilerinin uyguladıkları karartma teknikleri ve yapılan işlemlerin zamanı gibi faktörlere bağlı olarak bazı adli bilişim türlerinden bahsetmek mümkündür [5]-[6].

Şekil 1. Elektronik delil ortamları

A. Geleneksel Anlamda Adli Bilişim (Disk Forensics)

Adli bilişimin ilk uygulamaları kalıcı veriler üzerindeki işlemler olmuştur. Bilgisayar sabit diski, USB bellek, hafıza kartları, CD/DVD/Bluray gibi elektronik ortamlardaki işlemleri kapsar. İnceleme yapılan alanları; dosya türleri, işletim sistemleri, işletim sistemi kayıtları, veri kurtarma, şifre çözme, ayrılmamış bölümlerin incelenmesi şeklinde sıralayabiliriz.

B. Canlı Adli Bilişim (Live Forensics)

Bir siber suçun araştırılmasında ya da şifreli bir dosyanın şifresini elde etmek amacıyla bazı durumlarda ilgili bilgisayarın belleğindeki (RAM) verilere ulaşmak gerekebilir. Bu sayede, bir siber saldırıda o an bilgisayarda hangi işleçlerin çalıştığı, hangi portların açık olduğu gibi bilgilere ya da örneğin PGP şifreleme programını kullanan bir şüphelinin uzak bağlantı yaptığı sunucuya bağlanırken kullandığı parolaya erişmek mümkün olabilecektir.

C. Ağlarda Adli Bilişim (Network Forensics)

Özellikle siber suçların soruşturulmasında, bir bilgisayar sabit diski ya da şüpheliden ele geçirilen bir USB bellek üzerinde yapılacak incelemeler yeterli olmayacaktır. Örneğin, önemli bir bankanın veri tabanlarına saldırganlarca sızma girişimlerinin yapıldığı bir durumu ele alalım. Burada uygulanacak adli bilişim işlemlerinin konusunu bilgisayar ağları ve bu ağlara bağlı sistemler, cihazlar oluşturacaktır. İlgili bankanın bilgisayar ağ yapısı, saldırıların türü, ateş duvarı, saldırı tespit ve önleme sistemleri, günlük kayıtlar ve belki de yönlendirici/anahtarlama cihazları, ağ/e-posta/dosya sunucusularının tamamının incelenmesinin gerektiği bir inceleme söz konusu olacaktır. Ağlarda adli bilişimin uygulama alanları kablolu, kablosuz ve mimarisi itibariyle bulut bilişim ağ yapılarıdır. Belki kullanımının ve etkilerinin yoğun olması nedeniyle sosyal ağ incelemelerini de bu bölüme dahil etmek mümkündür.

D. Mobil Cihazlarda Adli Bilişim (Mobile Device Forensics)

Günümüzde hemen hemen herkes bir cep telefonu sahibidir. Artık cep telefonları sadece ses iletişimi için değil, akıllı telefonların yaygınlaşması ile belki daha çok veri iletişimi için kullanılmaktadır. Bu adli bilişim türünün ayrı tutulmasının nedenleri, ilk olarak GSM mimarisinin ve SIM kart teknolojisinin kullanılıyor olması, ikinci olarak ise bilgisayarlarda kullanılan standartlardan çok daha geniş bir yelpazede standartların kullanılmasıdır (özellikle verilerin kopyalanmasında cihazlar üzerindeki bağlantı kapılarının çok farklılık göstermesi).

III. ETMEN TABANLI SİSTEMLER

Öncelikle etmen sistemlerin temelini oluşturan yapay zeka ve etmen kavramlarından bahsetmek doğru olacaktır. Yapay zeka (artificial intelligence), normal bir insanın zekice kabul edebileceği şekilde davranan bir bilgisayar işleci oluşturulmasıdır [7]. Etmen (agent) ise, algılayıcıları sayesinde çevresini algılayan ve hareket organlarıyla çevresine katkı sağlayan, kullanıcısının kendisine verdiği hedefler doğrultusunda çalışan, bu hedeflerin gerçekleştirilmesinde otonom (kendi kendine karar verebilen) ve çevresinde başka etmenler varsa onlarla iletişim ve etkileşim halinde, sosyal bir program parçasıdır [8]-[9]-[10]. Etmenlerin özelliklerini; otonom, reaktif, proaktif, uyumlu, süreklilik gösteren, sosyal, esnek, işbirliği ve iş paylaşımına açık olarak sıralayabiliriz [9]. Bu iki kavramdaki özelliklerden akıllı etmen (intelligent agent), akıllı etmenlerden de etmen tabanlı sistemler geliştirilmiştir.

Adli bilişim alanının, her geçen gün artan elektronik ortamdaki verilerin adli açıdan analizinde ihtiyaç duyduğu tam da böyle bir araçtır. Alanın yoğunluğunu hafifletecek reçete; yığınla elektronik ortamdaki veri içerisinden öncelikle konu ile

ilgili olanları tespit etmek, bunları uygun yöntemlerle elde etmek, gerekiyorsa farklı elektronik ortamlar arasında bir örüntü ortaya çıkarmak, kısacası gerekli ile gereksizi ayırt etmek ve bu işlemleri bir adli bilişim uzmanının klasik yöntem ve araçları kullanarak gerçekleştirebileceğinden çok daha süratli ve hatasız bir şekilde yerine getirmektir. İşte adli bilişim alanında ihtiyaç duyulan ve kaldıraç etkisi oluşturacak böyle bir değişimi, içinde barındırdığı özellikler sayesinde etmen tabanlı sistemler yardımıyla gerçekleştirmek mümkün olabilecektir. Bu bağlamda, çalışmanın bir sonraki bölümünde, bahsedilen adli bilişim alanı ihtiyaçlarından bir kısmını karşılama noktasında akıllı etmen veya etmen tabanlı sistemler yapıları üzerinden geliştirilmiş uygulamalar incelenmiştir.

IV. ETMEN TABANLI SİSTEMLERİN ADLİ BİLİŞİM ALANINDAKİ UYGULAMALARI

Literatür taramasında etmen tabanlı sistemler ile adli bilişim alanlarının entegrasyonu adına bir çok çalışma yapıldığı görülmüştür. Gerçekleştirilen çalışmalar ve ortaya çıkan ürünlere bakıldığında; etmen tabanlı sistemlerin, yapılan işlem ve incelemelerin daha hızlı ve verimli hale getirilmesi doğrultusunda temel adli bilişim işlemlerinden, fiziki delillere ilgili kolluk uzmanlarınca erişiminin zor olması ya da ilgili sistemin bir RAID yapısı ya da bulut bilişim mimarisinde olması nedeniyle sistemin çalışmasını sekteye uğratmadan uzak bağlantı yoluyla elektronik delillerin toplanmasına, suç şüphelilerinden ele geçen cep telefonlarının veri tabanlarının kopyalanmasından, gerçekleşmiş ya da devam etmekte olan bir siber saldırının tespiti, ilgili delillerin elde edilmesi ve analizinin yapılmasına kadar bir çok uygulamaya rastlanmıştır. Bu uygulamaları aşağıdaki alt başlıklarda ele alacağız.

A. Temel Adli Bilişim İşlemlerine İlişkin Uygulamalar

İlk olarak temel adli bilişim uzmanlarının işlerini kolaylaştıran ve zamanı daha etkin kullanmalarına imkân sağlayan MADIK uygulamasına değineceğiz. MADIK (Multi-Agent Digital Investigation ToolKit), aslında temel adli bilişim incelemelerinin uygulandığı bir çok etmenli sistem yaklaşımıdır [11]-[12]. Bu kısımda sadece temel incelemeye ilişkin özelliklerini ele alacağız. MADIK uygulaması içerisinde altı adet etmen geliştirilmiştir. Bu etmenler ve işlevleri şöyledir:

--HashSetAgent: Elektronik ortamdaki tüm dosyaların MD5 özetlerini (hash) çıkaran ve bu özetleri kendi veri tabanındaki bilinen sistem dosyaları (örneğin Windows işletim sistemlerindeki System32 klasöründeki dosyalar) ile incelemeye gerek duyulmayacak yazılım dosyalarının (örneğin Java kurulum dosyaları) özetleri ile karşılaştırarak örtüşenleri incelelenecek dosyalar arasından eleyen etmendir.

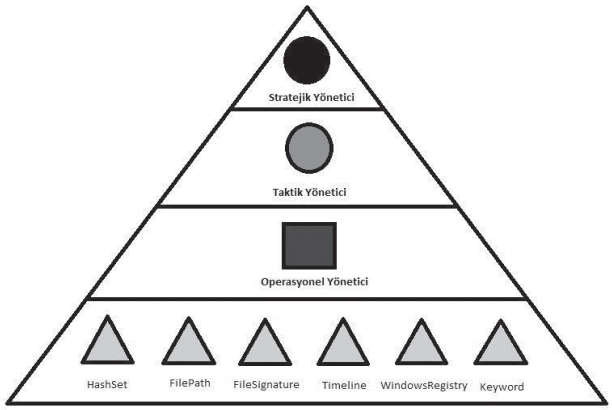
--FilePathAgent: Elektronik ortamdaki kurulu bulunan yazılımların varsayılan klasör/dosya yollarını veri tabanında tutan ve incelemeyi kolaylaştıran etmendir.

--FileSignatureAgent: İncelenen dosya uzantılarının, dosya başlıkları (file header) ile uyumlu olup olmadığını inceleyen etmendir.

--TimelineAgent: Dosyaların oluşturulma, son erişim ve değiştirilme zamanlarını çıkaran etmendir. Yazılımların kurulum zamanları, yedeklemeler, internet tarayıcısı üzerindeki işlemlerin incelenmesinde yardımcı olur.

--WindowsRegistryAgent: Windows tabanlı işletim sistemlerinde sistemin kurulum zamanı, bilgisayar zaman ayarlaması, taşınabilir ortam bilgilerinin tespitinde yardımcı olan etmendir.

--KeywordAgent: Elektronik ortamdaki e-posta adresleri, URL bilgileri, kredi kartı bilgileri gibi standartlık içeren verilerin tespitine yardımcı olan etmendir.



Şekil 2. MADIK mimarisi

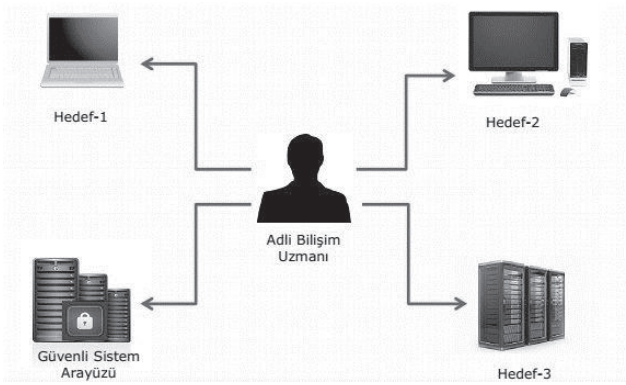
Diğer bir uygulama ise adli bilişim kapsamında spam e-posta incelemelerine yardımcı olmak amacıyla, yapay zeka ve veri madenciliği teknikleri kullanılarak geliştirilmiş olan EMADIK uygulamasıdır [13]. MADIK içerisindeki etmenler ile aynı isim ve işlevlere sahip etmenlerin e-posta incelemerinde kullanıldığı bir yapıdır.

B. Ağlarda Adli Bilişime İlişkin Uygulamalar

Günümüzde artık işlemlerin büyük çoğunluğunu bilgisayar, akıllı cep telefonları kullanılarak internet üzerinden ya da örneğin iç ağa sahip bir firma için bilgisayar ağları üzerinden gerçekleştirilmektedir. Örneğin, bir kolluk görevlisinin bir suç kapsamındaki soruşturmayı yürüten savcı tarafından bir firmaya ait ağa bağlı bazı çalışanların kullandıkları bilgisayarları kopyalamak ve incelemek üzere ya da bir sistem güvenlik yöneticisinin firma güvenlik müdürü tarafından firmanın iç ağına bağlı bilgisayarlara zararlı bir yazılım bulaşması üzerine problemin giderilmesi için görevlendirildiğini düşünelim. Devam eden bölümde, bahsedilen bu gibi durumlarda yapılacak işlemlerin yasal çerçevede ve sağlıklı bir şekilde yapılabilmesi için geliştirilmiş iki ticari uygulama ele alınmıştır.

Aynı amaçla geliştirilmiş bu iki uygulama, Guidance Software firmasının ürünü EnCase® Enterprise (EE) [14] ve AccessData firmasının ürünü AccessData® Enterprise'dır [15]. Her iki uygulama da, bir ağ içerisinde gerekli delillere güvenli

bir altyapı bağlantısı üzerinden erişim sağlayarak, ilgili bilgisayar üzerinde adli bilişim kurallarına bağlı kalarak ön inceleme yapmaya, ilgili bilgisayar diskinin ya da RAM'inin kopyasını almaya ve RAM'de bulunan canlı bilgileri incelemeye imkan vermektedir. Yine her iki uygulama da sunucu-istemci mimari yapısı içerisinde; delillere erişecek bir inceleme bilgisayarı, hedef bilgisayara yüklenecek bir etmen (EE için servlet, AccessData Enterprise için agent) ile sistemin güvenliğinin (bağlantı ve yetkilendirme güvenliği) ve yapılan işlemlerin adli bilişim açısından sağlıklı olmasının sağlanması (işlemin kim tarafından, ne zaman, ne şekilde yapıldığı ve hangi işlemlerin gerçekleştirildiği) amaçlarıyla kullanılan bir güvenli sistem arayüzünden oluşmaktadır. Bu uygulamalar kullanılarak, merkezî olarak yürütülen bir soruşturmada ya da bir firmanın farklı yerlerde bulunan birimlerinin ağına bulaşmış bir zararlı yazılımın incelenmesinde, şayet yapılan işlemler bir suç soruşturması kapsamında ise gizlilik ve sistemin çalışmaya devam etmesi sağlanacak, eğer konu bir zararlı yazılım incelemesi ise sistemlerin çalışması sekteye uğratılmayacak, yapılacak işlemler de hem bilgi güvenliği ve hem de adli bilişim noktasında yasal ve sağlıklı bir şekilde gerçekleştirilebilecektir.



Şekil 3. Bilgisayar ağlarında adli bilişim uygulaması

Bilgisayar ağlarının çok dinamik bir yapıda olması, ağ üzerindeki trafiğe ilişkin; kim, nerede, ne zaman, ne amaçla, hangi yetkiyle, ne yapmış gibi sorulara cevap verebilecek şekilde tüm verilerin kaydının tutulmasını zorunlu hale getirmiştir. Bir sisteme bir saldırı gerçekleştiğinde, öncelikle saldırı esnasında tespiti ve engellenmesi, eğer saldırı gerçekleşmiş ve sonlanmışsa da bu saldırının izlerinin tespiti ve kaynağının ortaya çıkarılmasında bizi sonuca ulaştırmada yardımcı olacak işte az önce sözü edilen kayıtlardır. Ancak gerek bu kayıtların standart olmayışı ve karmaşık yapıda olmaları, gerekse kayıtların çok fazla ve insan gözüyle incelenmesinin mümkün olmayışı bazı pratik çözümleri gerektirmiştir. Bu noktada etmen tabanlı sistemlerin ağ üzerindeki işlemlerin analizinde kullanılmasına ilişkin bazı çalışmalar yapıldığı görülmüştür.

Bu kısımda ilk olarak JADE (Java Agent DEvelopment Framework) platformu [16] üzerinde geliştirilmiş etmen tabanlı bir uygulama ele alınmıştır [17]. Uygulamanın amacı, dağıtık mobil etmen yapısı üzerinden ağ trafiğinin ve ağ kayıtlarının elde edilerek, bu verilerin analizinin yapılmasında incelemeyi yapan adli bilişim personeline bir arayüz yordamıyla yardımcı olmaktır. Uygulama bir merkezi ve üç adet de mobil olmak üzere dört bölümden oluşmaktadır. Uygulamada; ağ trafiği, sızma tespit sistemi ve bir ağ sunucusu üzerindeki işlemlerin kayıtları geliştirilmiş etmenler ile elde edilerek bu kayıtlar üzerinden merkezi ağ adli bilişim etmeni kontrol ve koordinesinde analizler yapılmaktadır. Merkezdeki adli bilişim etmeni üzerinden tüm veriler tek noktadan bir arayüz vasıtasıyla takip edilebilmekte ve gerekli analizler gerçekleştirilebilmektedir.

İkinci olarak ise, ateş duvarı (firewall) üzerindeki kayıtların incelenmesini konu alan bir uygulama ele alınmıştır [18]. Bir bilgisayar ağı üzerindeki ateş duvarı kayıtlarının çoklu etmen mimarisi yordamıyla elde edilmesi ve incelenmesi konu edilmiştir. Uygulamada üç etmenli bir yapı öngörülmüştür. Bir etmen tarafından (collector agent) ateş duvarı üzerindeki kayıtların bir kopyası elde edilerek kayıt numarası, kaydın tarihi, zamanı, kaynak-hedef IP adresleri ve port numaraları ile kullanılan protokol bilgileri bir veri tabanına aktarılmaktadır. Bir diğer etmen (inspector agent) tarafından veri tabanındaki kayıtlar incelenerek, bilgi tabanındaki kurallara göre normal ya da zararlı işlem olarak belirlenmektedir. Zararlı olarak belirlenen işlemler, bir sonraki adımdaki etmene (investigator agent) ay, gün ve işlem numarası tabloları şeklinde yapılandırılarak aktarılmaktadır. Buradan sonraki aşamada ise, sağlanan bir arayüz yordamıyla adli bilişim personeli ya da ağ güvenlik birimi tarafından bu tablolar incelenerek istenen sonuçlara ulaşılabilmektedir.

C. Mobil Cihazlarda Adli Bilişime İlişkin Uygulamalar

Bu kısımda benzer mantıkla çalışan üç uygulama ele alınmıştır. Her üç uygulamada da, cihazın veri tabanları cihaza yüklenen bir etmen yardımıyla kopyalanır ve istemci-sunucu mimari yapısında analiz bilgisayarına aktarılır. Cihaza yüklenen etmen, kopyalama işleminin bitiminde kendiliğinden cihazın belleğinden silinmekte ve böylece cihazdaki verilerin orijinalliğinin bozulmasının önüne geçilmiş olmaktadır.

Bu uygulamalardan ilki, ticari bir uygulama olan ve birçok telefon modeli ve işletim sistemi ile uyumlu çalışabilen Oxygen Forensic® Suite ürünüdür [19]. Bir diğeri, Blackberry marka cep telefonlarının veri tabanlarındaki verilerin kopyalanması ve analizine ilişkin BAAT (Blackberry Acquisition and Analysis Tool) uygulamasıdır [20]. Son uygulamamız da, Android tabanlı cep telefonlarının kopyalanmasında ve veri tabanlarının analizinde kullanılan SAFT uygulamasıdır [21].

D. Adli Bilişim Sistemlerine İlişkin Uygulamalar

Bu kısımda, ilk olarak daha önce bahsettiğimiz MADIK uygulamasının sistem tarafını ele alacağız [11]-[12].

MADIK'te dört katmanlı bir yapı düşünülmüştür. Yukarıdan aşağı olacak şekilde; *Stratejik, Taktik, Operasyonel Yönetici* katmanları ile *Uzman* katmanlarından oluşmaktadır. Bu şekilde bir hiyerarşik yapı oluşturulmak suretiyle; incelenecek elektronik deliller, bir ön inceleme sayesinde değerlerine göre sınıflandırılmakta, rutin ve tekrar mahiyetindeki işlemler azaltılmakta, deliller arasında bir korelasyon oluşturulmakta ve iş paylaşımı sağlanmaktadır. En son aşamada MADIK sisteminden geçen elektronik deliller, insan adli bilişim uzmanlarının kontrolünde değerlendirilerek nihâi kararlar verilmektedir.

Ele alacağımız diğer bir sistem, adli bilişim işlemlerinin gerçekleştirileceği bir ortam olarak bulut bilişim mimarisini kullanan CUFF (Collaborative Forensic Framework) sistemidir [22]. CUFF sistemi; *CUFF Link* adı verilen ve sistemin diğer unsurları arasındaki iletişimi sağlayan bir haberleşme platformu, *Analysis Block* adı verilen ve iş paylaşımını koordine eden bir analiz merkezi, delillerin muhafaza edildiği ve ilgililerce paylaşımının sağlandığı bir veri deposu ve tüm bu işlemlerin adli bilişim uzmanlarınca takibine imkân veren bir arayüzden oluşmaktadır. CUFF sayesinde, çok farklı problemlerle karşılaşan uzmanlar arasında fikir ve tecrübe alış verişi sağlanmakta ve ayrıca iş dağılımı yapılarak işlemlerin daha kısa sürede tamamlanması imkânı elde edilmektedir.

V. DEĞERLENDİRME

Önceki bölümlerde, adli bilişim ve etmen tabanlı sistem kavramları ile bu iki alan arasında bir entegrasyon sağlanması noktasında yapılan çalışmalar incelenmiştir. Bilişim ve iletişim sektörlerindeki gelişmelere paralel olarak ilgi yelpazesi genişleyen adli bilişim alanı, artık klasik yöntem, teknik ve ürünlerin yetersiz kaldığı bir zaman dilimine girmiştir. Yapılan bazı çalışmalarda, adli bilişim alanının çıkmaza girmesi muhtemel konular şöyle sıralanmıştır [2]-[22]:

--Veri depolama kapasitelerindeki ve dolayısıyla elektronik delil ortam kapasitelerindeki artış

--Özellikle cep telefonu teknolojisindeki gelişmelere paralel olarak gömülü sistemlerdeki artış ve donanım arayüzlerindeki çeşitlilik

--İşletim sistemlerindeki ve dosyalama sistem formatlarındaki gelişmeler

--Bir davaya ilişkin elde edilen elektronik ortamlardaki deliller arasındaki korelasyonun ortaya çıkarılması gerekliliği

--Yaygın kriptografik uygulamalar

--Zararlı yazılımlardaki artış ve çeşitlilik bağlamında geçici bellek incelemelerinde yaşanan zorluklar

--Belki de en önemlisi bulut bilişim mimarisinin giderek yaygınlaştığı bir ortamda klasik adli bilişim uygulamalarının neredeyse tamamen geçersiz/yetersiz kalması

--Bilişim ve iletişim dünyasını takip etmekte çok yavaş kalan yasal düzenlemeler ve yaşanan problemler

Problem sahasının giderek yoğunlaştığı bir alan olarak, içine düştüğü/düşeceği çıkmazların telafisinde adli bilişim alanı, birçok alandan olduğu gibi etmen tabanlı sistemlerden de pekala faydalanabilir. Bu bağlamda; veri depolama teknolojisindeki kapasite artışı ve düşük maliyetlerle orantılı olarak elektronik delil korelasyonunun ortaya çıkarılması, internete bağlanan cihaz çeşit ve sayısındaki artış dikkate alındığında internet ve sosyal ağ incelemeleri, bulut bilişim teknolojisinin getirdiği sorunlar, kriptanaliz yeteneklerinin artırılması, siber saldırıların artık profesyonel anlamda siber ordulara dönüşümünün yaşandığı günümüz dünyasında saldırı tespit, önleme ve analiz yeteneklerinin artırılmasında etmen tabanlı sistem uygulamalarının adli bilişim alanına çok katkı sağlayabileceği öngörülmektedir.

VI. SONUÇ

Bu çalışmada, adli bilişim ile etmen tabanlı sistemler alanlarının entegrasyonu incelenmiştir. Adli bilişim kavramı ve türleri açıklanmış, etmen tabanlı sistemler ve özellikleri ele alınmış, etmen tabanlı sistemlerin temel adli bilişim işlemleri, ağlarda adli bilişim, mobil cihazlarda adli bilişim ve adli bilişim sistemlerine ilişkin uygulama örnekleri incelenmiş ve hâlihazırdaki katkı alanları ile günümüzde ve gelecekte adli bilişim alanın yaşaması muhtemel problem alanlarına yönelik etmen tabanlı sistem uygulamalarının yapabileceği katkı ve girdiler değerlendirilmiştir.

KAYNAKLAR

[1] S. Mueller, *Upgrading and Repairing PCs*. Pearson Education, Inc., USA, 20th edition, 2012, p.16.

[2] S. L. Garfinkel, "Digital forensics research: The next 10 years", *Digital Investigation,* 7:64-73, 2010. The Proceedings of the Tenth Annual DFRWS Conference.

[3] I. Khoury and E. Caushaj, "Computer Forensic", [Online]. Available: http://www.secs.oakland.edu/~iskhoury/Computer_Forensic_final.pdf

[4] F. Gallegos, "Computer Forensics: An Overview", *Information Systems Control Journal,* Vol.6, 2005.

[5] H. Önal, "Bilişim Sistemlerinde Adli Bilişim Analizi ve Bilgisayar Olayları İnceleme - 101", *Bilgi Güvenliği Akademisi,* [Online]. Erişilebilir: http://www.bga.com.tr/calismalar/computer_forensic101.pdf

[6] J. Sammons, *The Basics of Digital Forensics.* Elsevier Inc., USA, 2012, pp.2-3.

[7] F. Mitchell, "The Use of Artificial Intelligence in Digital Forensics: An Introduction", *Digital Evidence and Electronic Signature Law Review*, 7:35-41, 2010.

[8] M. Wooldridge, *An Introduction to Multiagent Systems.* John Wiley & Sons Ltd., Sussex, England, 2002, p.15.

[9] I. Ademu, C. Imafidon, and D. Preston, "Intelligent Software Agent Applied to Digital Forensic and its Usefulness", 2012, [Online]. Available: http://interscience.in/IJCSI_Vol2Iss1/IJCSI_Paper_21.pdf

[10] I. Ademu and C. Imafidon, "Agent-Based Computing Application and its Importance to Digital Forensic Domain", [Online]. Available: http://world-comp.org/p2012/ICA7716.pdf

[11] Bruno W. P. Hoelz, G. Ralha Celia, Rajiv Geeverghese, and Hugo C. Junior, "A Cooperative Multi-Agent Approach to Computer Forensics", *IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology*, 2:477–483, 2008.

[12] Bruno W. P. Hoelz, G. Ralha Celia, Rajiv Geeverghese, "Artificial İntelligence Applied to Computer Forensics", *24th Annual ACM Symposium on Applied Computing, SAC'09, Computer Forensics Track,* 211-217, Honolulu, Hawaii, USA, ACM Press, 2009.

[13] S. B. Bandgar, M. Sale and B. B. Meshram, "Artificial Intelligence Applied to Digital Email for Forensic Application", ISSN: 2249-0558, 2012.
[14] S. Bunting, *EnCase Computer Forensics The Official EnCE: EnCase Certified Examiner Study Guide.* John Wiley & Sons Inc., USA, 3rd edition, 2012, pp.176-180.
[15] AccessData, AD Enterprise, [Online]. Available: http://www.accessdata.com/solutions/digital-forensics/ad-enterprise
[16] T. Italia Lab (TILAB). Java Agent DEvelopment Framework - JADE, [Online]. Available: http://jade.tilab.com
[17] A. Nagesh, "Distributed Network Forensics Using JADE Mobile Agent Framework", [Online]. Available: https://technology.asu.edu/files/documents/tradeshow/Dec06/asha_nagesh_report.pdf
[18] H. Bensefia and N. Ghoualmi, "A Mutli-Agent System for Firewall Forensics Analysis" International Journal on New Computer Architectures and Their Applications (IJNCAA) 1(1): 25-33, *The Society of Digital Information and Wireless Communications*, ISSN: 2220-9085, 2011.
[19] Oxygen Forensics, Oxygen Forensic® Suite, [Online]. Available: http://www.oxygen-forensic.com/
[20] [18] S. K. Sasidharan and K. L. Thomas, "BlackBerry Forensics: An Agent Based Approach for Database Acquisition", *Advances in Computing and Communications, Communications in Computer and Information Science Vol.190, 2011, pp. 552-561.*
[21] SAFT Mobile Foresics, [Online]. Available: http://www.signalsec.com/saft/
[22] M. Mabey and G. J. Ahn, "Towards Collaborative Forensics: Preliminary Framework", *IEEE International Conference on Information Reuse and Integration (IRI), 2011, pp.94-99.*