TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ

SOSYAL MEDYA ÜZERİNDEN İŞLENEN SUÇLARDA TWİTTER ÖRNEK OLAYLARININ ADLİ OLARAK İNCELEMESİ

Ahmet SALUK

DİSİPLİNLERARASI ADLİ BİLİMLER ANABİLİM DALI
DOKTORA TEZİ

DANIŞMAN
Doç. Dr. Recep ERYİĞİT

Ankara
2022

TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ

SOSYAL MEDYA ÜZERİNDEN İŞLENEN SUÇLARDA TWİTTER ÖRNEK OLAYLARININ ADLİ OLARAK İNCELEMESİ

Ahmet SALUK

DİSİPLİNLERARASI ADLİ BİLİMLER ANABİLİM DALI
DOKTORA TEZİ

DANIŞMAN
Doç. Dr. Recep ERYİĞİT

ANKARA
2022

Ankara Üniversitesi
Sağlık Bilimleri Enstitüsü Müdürlüğü'ne,

Doktora tezi olarak hazırlayıp sunduğum "SOSYAL MEDYA ÜZERİNDEN İŞLENEN SUÇLARDA TWİTTER ÖRNEK OLAYLARININ ADLİ OLARAK İNCELEMESİ" başlıklı tez; bilimsel ahlak ve değerlere uygun olarak tarafımdan yazılmıştır. Tezimin fikir/hipotezi tümüyle tez danışmanım ve bana aittir. Tezde yer alan deneysel çalışma/araştırma tarafımdan yapılmış olup, tüm cümleler, yorumlar bana aittir.
Yukarıda belirtilen hususların doğruluğunu beyan ederim.

Öğrencinin Adı Soyadı: Ahmet SALUK
Tarih:
İmza:

Ankara Üniversitesi Sağlık Bilimleri Enstitüsü

Disiplinlerarası Adli Bilimler Anabilim Dalında

Ahmet SALUK tarafından hazırlanan

"SOSYAL MEDYA ÜZERİNDEN İŞLENEN SUÇLARDA TWİTTER ÖRNEK OLAYLARININ ADLİ OLARAK İNCELEMESİ" adlı tez çalışması aşağıdaki jüri tarafından DOKTORA TEZİ olarak

OY BİRLİĞİ / OY ÇOKLUĞU ile kabul/ret edilmiştir.

Tez Savunma Tarihi:

İmza
Prof. Dr. H.Sinan SÜZEN
Ankara Üniversitesi
Jüri Başkanı

İmza
Prof. Dr. Rukiye TIPIRDAMAZ
Hacettepe Üniversitesi
Raportör

İmza
Doç. Dr. Recep ERYİĞİT
Ankara Üniversitesi
Danışman Üye

İmza
Doç. Dr. Cahit DOĞAN
Hacettepe Üniversitesi
Raportör

İmza
Dr. Öğr. Üyesi Bülent TUĞRUL
Ankara Üniversitesi
Üye

Tez hakkında alınan Jüri kararı Ankara Üniversitesi Sağlık Bilimleri Enstitüsü Yönetim Kurulu Kararı tarafından onaylanmıştır.

İmza
Prof. Dr. Fügen AKTAN
Sağlık Bilimleri Enstitü Müdürü

İÇİNDEKİLER

ÖNSÖZ

Teknolojinin gelişmesi, sosyal hayatın her alanına etki etmiş ve hayatı kolaylaştırmıştır. Teknolojinin bu kadar hızlı gelişimi hayatı kolaylaştırmanın yanında suç işlemeyi kolaylaştırdığı gibi suçların aydınlatılması veya suçluların yakalanmasını da zorlaştırmaya başlamıştır. Suç ile başarılı bir mücadelenin temeli, işlenmesi muhtemel bilişim vasıtasıyla işlenen/işlenebilecek suçlara yönelik çeşitli hazırlıklar yapılması gerekmektedir. Bilişim teknolojilerinin hızlı gelişimine hukuk sistemleri hızlı reaksiyon verememektedir. Suç ve suçlulukla mücadele eden birimler konuya daha sınırlı çerçevelerden bakmaktadırlar. Ortak bir bakış sağlayamamışlardır. Sınır tanımayan, bir kaba sığmayan ve kontrol altına alınamayan yeni teknolojiler, hukukun uygulanması ve hukuk sistemleri açısından zorluklar ortaya çıkarmakta ve çözülemeyen havada kalan olaylar bulunmaktadır.

Mobil cihazların ve internetin yaygınlaşması ile fiyatların geçmiş yıllara göre ucuzlaması, sosyal medya kullanıcı sayısının hızlı artışına neden olmuştur. Hızla artan bu sosyal medya kullanımı bireylerin iletişim kurma biçimlerini de değiştirmiştir. Sosyal medya uygulamaları yüz yüze iletişimin önüne geçecek kadar tehlikeli boyutlara ulaşmıştır. Sosyal medyanın yaygın kullanılması maalesef suçluların da rahat hareket etmesini sağlamıştır. Günümüz sosyal medya ortamları, suçluların suç mahalli olarak yaygınlaşmıştır.

Sosyal medya, suç işleme düşüncesinde olan kişi/kişiler tarafından daha yaygın kullanılmaya başlanmıştır. Özellikle sahte hesaplar oluşturularak hakaret, tehdit, cinsel taciz, özel hayatın gizliliği, kişisel verilerin hukuka aykırı şekilde

yayınlanması, dolandırıcılık, müstehcenlik, terör propagandası gibi suçlar için kullanılabilmektedir.

Bir kullanıcı kendi ismi ile hesap oluşturması ve iddia edilen suçu kabul etmesi durumunda soruşturma dosyalarında şüpheliye ulaşmak ve sonuç almak mümkün olabilirken, ancak kimliklerini gizleyenler veya sahte hesap kullananlar, twitter üzerinde kimliklerinin tespit edilemeyeceğini bilmenin rahatlığıyla hareket etmektedirler.

Çalışmam esnasında sunduğu kapsamlı bilgi ve tecrübesinden yararlandığım ve çalışmam boyunca bana gösterdiği sevgi ve anlayış için Sayın Doç. Dr. Recep ERYİĞİT'e, bize derslerimizde çok önemli katkılar sağlayan hocalarımız Sayın Prof. Dr. H.Sinan SÜZEN'e, Sayın Prof. Dr. İ. Nergis CANTÜRK'e, Sayın Doç.Dr.Cahit DOĞAN'a, tüm değerli hocalarımıza, Adli Bilişim Uzmanı ve Eğitmeni Murat GÖKALP'e ve yıllardır maddi ve manevi desteğini hiçbir zaman esirgemeyen sevgili aileme,

Ankara Üniversitesi Disiplinlerarası Adli Bilimler Enstitüsü'nün her aşamasında görev alan tüm personellerine, çalışmalarımda destek veren, yol gösteren, zaman ayıran, her türlü desteği sağlayan arkadaşlarıma sonsuz saygı ve teşekkürlerimi sunarım.

Ahmet SALUK

SİMGELER VE KISALTMALAR

ABD	Amerika Birleşik Devletleri
Bitmap	Windows işletim sistemi tarafından sektörlerin kullanılıp kullanılmadığının kaydını tutan dosyadır.
CMK	Ceza Muhakemesi Kanunu
HMK	Hukuk Muhakemeleri Kanunu
LogFile	Windows işletim sisteminde dosya günlüklerinin tutulduğu dosyadır
MFT	Ntfs dosya sistemi içerisinde kullanılan dosyaya ait bilgilerin tutulduğu sistem dosyasıdır.
Ntfs	Windows işletim sisteminde kullanılan yeni teknoloji dosyalama sistemidir
PCI	Intel tarafından geliştirilen yerel veriyolu standartıdır.
RAM	Memory, Rastgele erişimli bellek
SQL	Yapılandırılmış sorgu dilidir.
TCK	Türk Ceza Kanunu

ŞEKİLLER

1. GİRİŞ

İnsanlar doğaları gereği kendilerini ifade etme ihtiyacı duyar. Bazen ihtiyaçlarını bazen de duygu ve düşüncelerini ifade ederler. Bireysel ifade etme ihtiyacı zamanla gelişmiş ve teknolojinin de etkisi ile çeşitlenerek çok yaygınlaşmıştır. Bu ihtiyaçlar içerisinde bilgi alma ve iletişim ihtiyacı da bulunmaktadır. Bireyler ihtiyaçlarını, duygu ve düşüncelerini ifade etmek iletmek ile birlikte başkalarını da dikkate almakta ve kendi dışındaki insanlarda nasıl bir etki bıraktıklarını da merak etmektedirler. Şirketlerin geri bildirim süreci gibi kimlerin kendisini takip ettiğini, mesajlarını kimlerin okuduğunu, paylaşımlarının kimler tarafından görüldüğünü öğrenmek istemektedirler. Teknolojik gelişmeler iletişim alanında her geçen gün yeni yeni özellikler ortaya koymakta ve ortaya çıkan bu özellikleri de bireyler kullanmaktadır. Bireylerin iletişim ve etkileşimi için çeşitli aletler ve cihazlar geliştirilmiştir.

1.1. Medya

Teknolojinin ve dolayısı ile iletişim araçlarının hızlı gelişmesi neticesinde medya hızlı bir şekilde yaygınlaşmıştır. Dünyanın herhangi bir yerinde hazırlanan ve internet ortamına yüklenen bir video dosyası aynı zaman diliminde dünyanın dört bir yanındaki kullanıcılar tarafından izlenebilmektedir. Teknolojik cihazların

hayatımızda yaygın kullanılması bir anda dünyanın öbür ucuna ulaşmaya ve veri paylaşmaya olanak sağlamıştır. Teknolojik gelişmeler kıtalar arası seyahat sürelerini azaltmış ve kıtalar arası dolaşımı artırmıştır. Teknolojik gelişmelerin kısa sürede hızlı gelişimi ülkeler arasındaki sınırların önemini azaltmış, insanların artık istedikleri her şeye erişebilir hale gelmiştir.

İletişim için medya kavramının ortaya çıkmasında haber alma ve aktarma ihtiyacı etkili olmuştur. Medya, ifadesi altında iletişim kaynağı ve iletişim mecraları genel olarak toplanmaktadır(Medya 2019). Medya, iletişim için kullanılan alan ve olanakların tamamı olarak değerlendirilebilir. Basit düşünürsek iletişim araç ve gereçleri ile kitlelerin etkileşimi diyebiliriz. Bu etkileşim yazılı, sesli veya görsel herhangi bir vasıta ile olabilir.

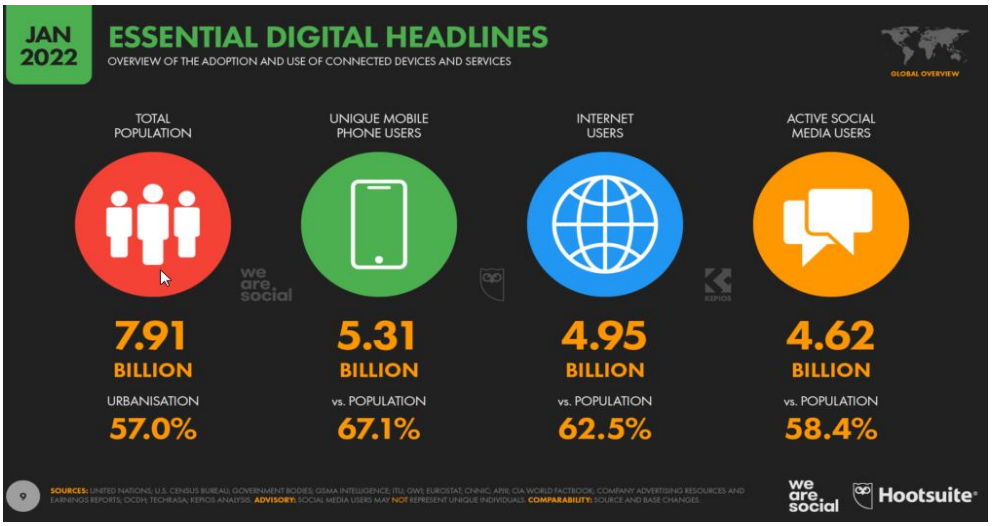
Medya kitleleri harekete geçirme potansiyeli olan devasa bir sektördür. Algı yönetiminde kullanılan en kuvveti argümandır. Sadece bilgi aktarmamakta, insanların düşünceleri etkilemekte ve duygu paylaşımı için de kullanılmaktadır. Eğer medya kötü niyetler için kullanılırsa, suç işleme niyetindeki birisinin elindeki silah gibi bir işlev görecektir. Medyanın kötü kullanılması neticesinde masum bir insan suçlu, suçlu insanları da masum olarak da gösterebilir. Bu nedenle günümüzde medya faaliyetleri kitleleri hareket ettirmede en etkili yöntemlerden birisi olarak kullanılmaktadır. Ulusal veya uluslar arası bir medya endüstrisini takip eden bir kişi farkında olmadan zamanla medyanın bir ürünü haline gelebilmektedir.

Günümüzde en büyük medya internettir. İnternet, ilk Amerika'da ortaya çıkmıştır ve askeri temellere dayanmaktadır. Araştırma ve geliştirmeler neticesinde genel kullanıma sunularak yaygınlaştırılmıştır(İnternet 2019). Ülkemizde hızla internet ile tanışmış ve internet ülkemizde de zamanla yaygınlaşmıştır. İnternet bağlantısı sonrasında, hayatımızı etkileyen ve değişikliklere yol açan bir zorunluluk

olmuştur. Internet, ulaşmak istediğimiz veriye erişmenin ve paylaşmak istediğimiz verinin paylaşmanın en pratik yoludur.

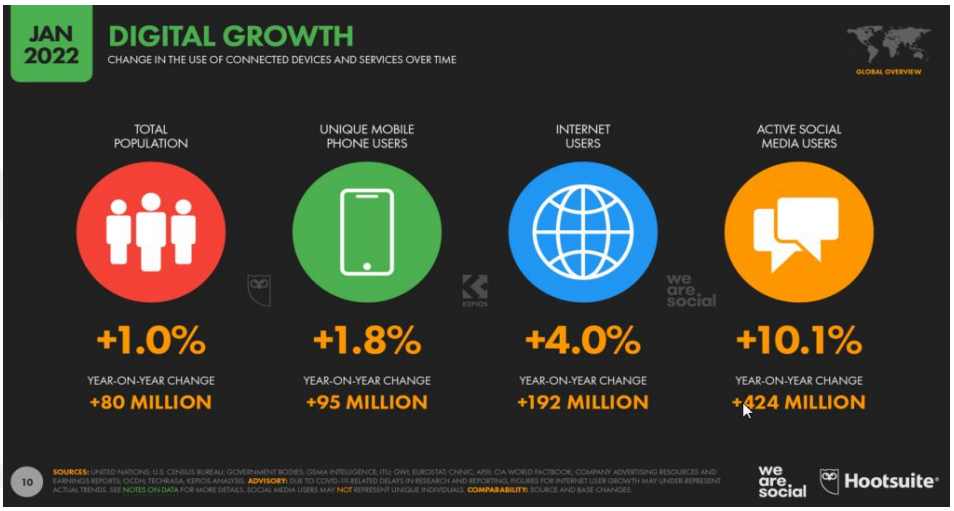
Bilgiye erişim ve kullanımı için hemen hemen her alanda internet kullanımı günden güne artarak devam etmektedir. İnsanlar bilgilenmek için artık yazılı basın yerine sosyal medyayı tercih etmesi nedeniyle sosyal medya uygulamalarının kullanımında patlama yaşanmıştır.

We are social tarafından hazırlanan bilgilendirme raporuna göre, dünya nüfusunun Ocak 2022'de 7,91 milyar olduğu, nüfusun yarısından fazlasının (yüzde 57,0) artık kentsel alanlarda yaşadığı, mobil kullanıcı sayısının, dünya nüfusunun çoğu kısmının (% 67) bir mobil telefonu kullandığı, kullanıcı sayısının 2022 yılının ocak ayında 5,31 milyar kişi olduğu, internet kullanıcı sayısının, 2022 yılı ocak ayında 4,95 milyar kişiye yükseldiği ve ağ kullanımının şu anda dünya üzerinde yaşayan insanların sayısının yüzde 62,5'ini oluşturduğu, sosyal medya kullanıcı sayısının ise 4,62 milyar olduğu belirtilmiştir(Social 2022). İnternet ve sosyal medya kullanım sayıları Şekil 1.1'de gösterilmiştir.



Şekil 1.1. İnternet ve Sosyal Medya Kullanımı (Social-1 2022)

Mobil cihaz kullanımının geçen yıla göre yüzde 1,8 arttığı, 95 milyon yeni mobil kullanıcının geçen seneden bu zamana katıldığı, genel ağ kullanıcılarının bir önceki yıl 192 milyon artış ile yüzde dört arttığı, sosyal medya kullanımının toplam nüfusunun yüzde 58,4'ü olduğu, 2021 yılında'da 424 milyon kişinin sosyal medya hesabı almasıyla son bir yılda yüzde 10'dan fazla büyüdüğü görülmektedir. Sosyal medya kullanımındaki artış giderek devam etmektedir . Şekil 1.2'de gösterilmiştir.



Şekil 1.2. Sosyal Medya Kullanımı Yıllık Artışı (Social-2 2022)

1.2. Sosyal Medya

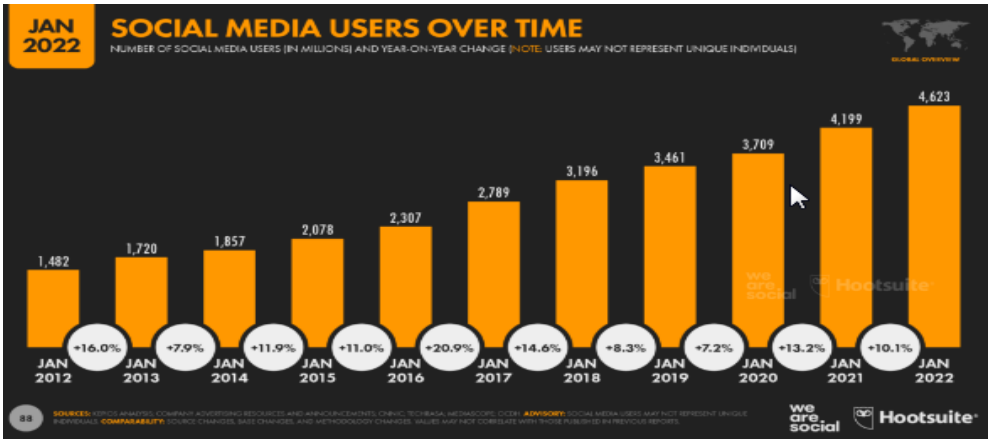
Sosyal medya, kullanıcıların oluşturduğu verileri, sade, kısa sürede ve karşılıklı paylaşılmasını sağlayan iletişim şeklidir. Sosyal medya insan odaklı olması nedeniyle insanlar aralarındaki bilgi paylaşımını arttırmaktadır. İnsanlar, gün geçtikçe dijital ortamlarda daha fazla zaman geçirmektedirler. Dijital dünyayı çok yoğun kullananlar gerçek yaşam ihtiyaçlarını karşılamakta ve sanal bir dünya kurarak yaşamaktadır.

Artık normal hayatta yapılması gereken çoğu sosyal faaliyetler sanal alemde yapılmakta ve ciddi kararlar alınabilmektedir. Çoğunlukla gençler arasında kullanımı hızla yükselen sosyal medya, geleneksel medyanın yerini almaktadır. Öyle ki bazı insanlar haberleri bile sosyal medya üzerinden takip etmektedirler.

Sosyal medya, kullanıcı sayısının çok olması, paylaşıma olanak tanıması ve sürekli yeniliklerle güncellenmesi sebebiyle yaygın iletişim aracı olarak kullanılmaktadır. İnsanlar, düşüncelerini sosyal medya ortamında paylaştıkları yazı, fotoğraflar, videolar ile yapmakta, bu paylaşımlar neticesinde medya üzerinde çeşitli tartışmalar yaşanmakta ve yeni fikirler ortaya çıkmaktadır.

Sosyal medya aynı zamanda iş arayan insanların da yoğun kullanımında olup, etkili kullanım ve paylaşımlar neticesinde iş arayanlar kısa sürede iş bulabilmekte veya işveren de kendilerine uygun çalışan bulabilmektedirler.

Sosyal medya kullanıcı sayısı son 12 ayda da yüzde 10,1'lik çift haneli bir oranda artmıştır. 2021 ile 2022 arasındaki büyüme oranının pandeminin de etkisi olduğu değerlendirilmektedir. Geçen yıl 424 milyon kullanıcının sosyal medyaya katıldığı ve bu sayının da günde ortalama 1 milyondan fazla yeni kullanıcıya ve her saniyede yaklaşık 13.5 yeni kullanıcıya eşit olduğunu anlaşılmaktadır. Sosyal medya kullanımın sürekli arttığı Şekil 1.3.'de gösterilmiştir.



Şekil 1.3. Sosyal Medya Kullanımı(Social-3 2022)

1.3. Twitter

Twitter uygulamasının en önemli özelliği anlık ve kısa içerik mesajları diğer twitter kullanıcıları ve kamuoyu ile paylaşılmasına olanak veren cep telefonu ve bilgisayar ile kullanılabilen popüler bir uygulamadır. Jack Dorsey tarafından geliştirildiği bilinmektedir ancak bir grup tarafından geliştirilmiştir(DALKIRAN D. 2017).

Twitter uygulaması ile aynı anda milyonlarca insana ulaşmaya imkan vermesi neticesinde, dünya liderlerinin %83'ü ve resmi kurumların tamamı twitter kullanmaya başlamışlardır(İstatistik Twitter 2022). Resmi kurumların iletişim adreslerinin başında twitter adresleri gelmektedir.

Twitter'ın kısa sürede anlık paylaşım özelliği sayesinde bazen devlet başkanları kamuoyunu bilgilendirmek için resmi twitter hesabından, kendi fikirlerini açıklamak içinse özel twitter hesaplarını kullanmaktadırlar. Twitterın kullanıcı sayısındaki bu artış nedeni ile resmi kurumlar kamuoyuna yapacakları resmi açıklamalar için twitteri kullanmaya başlamışlardır. Hatta kullanıcılar yine twitter

üzerinden ilgili resmi kurum veya şirketlere daha rahat ve hızlı ulaşabilmektedirler. Twitter resmi kurumlar başta olmak üzere bu kadar çok tercih edilmesi ve kullanılmasının sebebi, paylaşılan bir mesajın diğer kullanıcılar tarafından re-twit edilerek çok kısa sürede daha fazla aboneye ulaşmasına imkan vermesidir. Yani özellik arz eden bir mesaj bir saatten daha kısa sürede dünya geneline yayılabilmektedir.

Tabi özellik art niyetli veya kötü düşüncelere sahip kullanıcıların yalan-yanlış bilgileri paylaşması neticesinde de hedef kişi veya kurumlar hakkında da olumsuz görüşlerin hızla yayılmasına imkan vermektedir. Bu gibi durumlarda hedef durumdaki kişi veya kurumların sıcağı sıcağına twitter help desk itiraz ederek bu twitterların kaldırılmasını, ilgili mahkeme kararları ile erişime yasaklanması ve son aşamada ise twiti atan kişi/kişiler hakkında adli makamlara başvurulması gerekmektedir.

Twitter uygulamasının diğer sosyal medya uygulamalarından farkı arkadaşlık sistemi ile değil de takipçi sistemi ile çalışmasıdır. Sizinle arkadaş olmayan ve hatta tanımayan herhangi bir yerdeki bir twitter kullanıcısı sizinle arkadaş olmadan sizin attığınız veya paylaştığınız bütün twitleri görebilir, altına yorum yazabilir ve hatta bunları kendi takipçileri ile paylaşabilmektedir. Ancak twitter abonesi olmadan veya hedef şahsın takipçisi olmadan da kısıtlı olarak bir abonenin paylaştığı bilgileri de görmek mümkündür. Twitter bütün özelliğini kullanabilmek için ücretsiz olarak üye olunması gerekmektedir.

Twitter uygulamasına üye olunması ile birlikte kime ait bilgisayarda hesap alındığı, hangi kullanıcı hesabı üzerinden hesap alındığı ve kullanıcıya ait hesaba giriş yapılıp yapılmadığı adli incelemeler açısından önemlidir. Hesaba giriş yapıp, paylaşım yapmak, suç işlemek amacıyla kullanılabilmektedir. Hesaba giriş yapıldığının bilgisi, suçlular tarafından kullanılabildiğinden dolayı inceleme ve

analiz için önemlidir. Türkiye'de twitter kullanıcı sayısı 16,1 milyondur ve Dünya genelinde kullnım sıralamasında yedinci sıradayız(Teknoloji 2022).

1.4. Bilişim

İnsanoğlunun, teknik kullanarak elektronik makineleri işlemesini bilişim olarak tanımlayabiliriz. Bilişim, her türlü verinin elektronik araçlarla işlenmesini ve değerlendirmesini konu alan bir bilim dalı olup, en basit şekilde teknoloji kullanılarak üretilen sonuçlar olarak da ifade edilebilmektedir. Bilişim delilleri içerisinde akıllı her türlü cihaz bulunmaktadır. Bilişim, iletişim anlamında düşünülürse etkileşim olarak da değerlendirilebilir. Bilgisayar ve yazılımlar insanların ihtiyaçlarına göre düzenlenmektedir.

1.5. Adli Bilişim

Adli bilişim kavramı, "bilgisayar adli bilimi" olarak kullanılmak yerine teknolojik ürünlere karşılık gelen bilişimin baz alınması nedeniyle "adli bilişim" olarak kullanılmıştır. Adli sözcüğü İngilizce'de "forensics" sözcüğünün karşılığı olarak kullanılmaktadır. Tam bir çeviri olmadığından "adli" sözcüğü Türkçe'de insanlara doğrudan adli işlemleri aklına getirmektedir.

İngilizce "forensics" sözcüğü genellikle adli amaçlı incelemeler için kullanılırken, adli olmayan bir durumla alakalı bilgi sağlayan teknik incelemeleri de kapsayabilmektedir. Adli bilişim, bir kişinin suçlu veya suçsuz olduğunun belirlenmesi için bilişim cihazı üzerinde teknik incelemeler yapılmasıdır.

Adli incelemeler, gerek duyulduğunda yasal sürece katkıda bulunur ve suçun aydınlatılabilmesi veya suçluların tespit için bilimsel yöntemler kullanılır. Adli bilişimin esası, hedef durumundaki dijital delillerin toplanmasından inceleme aşamasına kadar bozulmadan ve zarar görmeden muhafaza edilmesi ve içerisindeki bilgilerin basit ve anlaşılabilir bir şekilde adalet makamına sunulmasıdır.

Uluslararası alanda adli bilişim için çeşitli terimler kullanılmaktadır. "Digital, Computer, Cyber gibi farklı terimler yanında forensics birleştirilerek çeşitli isimlendirmeler kullanılmaktadır. Adli bilişim faaliyeti, hedef durumundaki dijital cihazlar (deliller) üzerinde imaj alma, inceleme-araştırma ve raporlama uygulamasını barındırır.

1.6. Bilişim suçu

Bilişim suçları, klasik anlamda suç işleyenlere nazaran yakalanma riski daha az ve getirisi daha fazla olması nedeniyle suç işleme düşüncesinde olan kişi/kişilerin klasik suç işleme düşüncesinden bilişim suçu veya bilişim vasıtasıyla işlenen suçları tercih etmeye başlamışlardır. Bilişimin gelişmeye başladığı yıllarda salam taktiği ile banka hesaplarından cent'ler toplanırken günümüzde kamuoyu artarak devamlı bilişim suçları türleri ile tanışmaya başlamıştır. Bilişim suçu, bilişim sistemleri aracılığıyla yazılı hukukta belirlenen suçların işlenmesidir.

Türk Ceza Kanununda bilişim ile ilgili işlenebilecek suçlar tanımlanmıştır. TCK'da Topluma karşı işlenen suçlar bölümünde bulunması nedeniyle, bu maddelere uygun bir suçu haber alan Cumhuriyet Savcıları şikayet olunmasa bile doğrudan soruşturma başlatmak zorundadırlar.

Klasik suçlar olarak adlandırılan hırsızlık, dolandırıcılık, sahtecilik gibi suçların işlenmesinde bilişim sistemleri kullanılmışsa bu tür suçlar bilişim vasıtasıyla işlenen suçlar olarak ifade edilmektedir. Yine bu tür suçlar klasik suçlara göre riskleri az ancak getirileri diğerlerine göre daha fazladır.

İlgili kanun maddeleri ve yönetmeliklerden kaynaklı eksiklikler, insanların ilgisizliği ve bilgisizliği nedeniyle son dönemde bilişim sistemleri vasıtasıyla işlenen en çok suçların başında telefon dolandırıcılığı gelmektedir. Bu suç sistemini kuran kişi/kişiler işlerini o kadar profesyonel yapmaya başlamışlardır ki, hedef konumuna aldıkları sanatçılar, tanınmış kişiler ve hatta emekli kolluk kuvvetlerini dahi dolandırabilmektedirler.

1.6.1. Sisteme Giriş-Md. 243

İzinsiz bir internet sitesine giren ve sistemde kalan kişiye yasalarda belirlenen 12 aya kadar hapis veya adli para cezası verilir. Yapılan siteye girme işleminin hukuka aykırı olması gerekmektedir.

İnternet sitesine girdikten sonra siteye ait veriler değişir veya kaybolursa altı aydan iki yıla kadar hapis cezası verilebilir. İnternet sitesine girmeden hukuka aykırı olarak özel cihazlarla internet trafiğini izleyenlere 12 aydan 36 aya kadar hapis cezası verilebilir.

1.6.2. Sistemde Değişiklik-Md. 244

Bir internet sitesinin çalışmasını bozan veya engelleyen kişiye 12 aydan 60 aya kadar hapis cezası verilebilir.

Bir internet sitesindeki bilgileri değiştiren, yok eden, bozan veya ulaşılmasına engel olan, siteye dosya kopyalayan, mevcut kayıtları başka bir yere yollayan kişiye altı aydan üç yıla kadar hapis cezası verilebilir.

Bu suçlar resmi kurum veya kuruluşa ait bilişim sitemi üzerinden işlenmesi kredi kurumuna veya bir bankaya karşı da işlenmesi halinde ceza yarı oranında artırılmaktadır. Çıkar sağlamak için bu suçları işlemesi durumunda 24 aydan 72 aya kadar hapis cezası ve beş bin güne kadar adlî para cezası verilebilir. Ayrıca başka bir suç işlemişse farklı değerlendirilmektedir.

1.6.3. Kötü Kullanım-Md. 245

Kart kullanım hakkı olan kişinin rızası olmadan kredi kartı veya bankamatik kartını bulunduran ve bu kartı çıkar sağlamak için kullananlara 36 aydan 72 aya kadar hapis cezası ve beş bin güne kadar adli para cezası verilebilir. Gerçek olmayan

kredi kartı veya bankamatik kartını başkalarının banka hesapları ile irtibatlandırılıp kullanıma sunan kişilere 36 aydan 84 aya kadar hapis cezası ve on bin güne kadar adli para cezası verilebilir. Çıkar sağlamak için bu suçları işlemesi durumunda başka bir suç işlemişse 48 aydan 96 aya kadar hapis cezası ve beş bin güne kadar adlî para cezası verilebilir.

1.6.4. Cihaz Kullanımı-Md. 245/A

Sadece suç işlemek amacıyla üretilen bilişim cihazlarının tedarik zincirinde bulunan kişilere 12 aydan 36 aya kadar hapis cezası ve beş bin güne kadar adlî para cezası verilebilir. Papağan ismiyle anılan kart kopyalama cihazı bunlara örnek gösterilebilir. Otomobillerin uzaktan kumandalı kilitlerini açmak ve hırsızlık yapmak için üretilen cihazları da örnek gösterebiliriz.

Suçluların suç işleme şekilleri benzerlik göstermekle beraber bilişim cihazları kimi zaman suçluların işlerini kolaylaştırmaktadır. Ülkemizde en yaygın bilişim suçları; kredi kartı yolsuzlukları, sahtecilik, hakaret, küfür, kişisel veya kurumsal verilerin çalınması olup, bunlarla sınırlı olmayıp, sürekli değişiklikler göstermektedir. Türk Ceza Kanununda, belirtilen suçların kitle iletişim araçlarıyla işlenmesi halinde cezalar ağırlaştırılmıştır.

1.7. Avrupa Konseyi Siber Suç Sözleşmesi

Bilişim suçlularının sınır tanımadan suç işlemeleri uluslararası işbirliğini ve yardımlaşmayı zorunlu kılmıştır. Uluslararası işbirliği için birçok kuruluş çalışma yürütmüştür. En kapsamlısı Avrupa Konseyi Siber Suç Sözleşmesi'dir.

İsmi Avrupa Konseyi Siber Suç Sözleşmesi olmasına rağmen Avrupa dışında ülkelerinde üye olması ile uluslararası bir özellik kazanmıştır. Amerika, Avusturalya, Japonya, İsrail ve Kanada gibi ülkeler de imzalamıştır. Sözleşmeyi imzalayan devletler sözleşme maddelerini kendi iç hukuklarında uygulamayı üstlenmişlerdir. Sözleşmeye taraf devletler uluslararası işbirliğini de kendi menfaatleri doğrultusunda üslenmişlerdir. Bilişim suçluları ileri düzey bilgisayar kullanım bilgisi ve ileri düzey internet kullanım bilgisine sahip oldukları için uluslararası koordinasyon aslında her ülkenin kendi çıkarınadır. Bu konuda öncü ülkelerden de esinlenip kendi yasalarına bilişim suçları ile mücadele için gerekli düzenlemeleri yapmak diğer ülkeler için de bir fırsat olmuştur.

Avrupa Konseyi'nin alt çalışma gruplarından Avrupa Suç Sorunları Komitesi'nin 1996 yılında siber suçlarla ilgilenecek bir uzmanlar komitesi kurulmasını teklif etmesi ilk icraatı olmuştur. Teklif karşılık bulmuş Avrupa Konseyi Bakanlar Kurulu 1997 yılında siber suçlara karşı uzmanlar komitesini kurmuştur. Kurulan uzmanlar komitesinden ilk iş olarak uluslararası işbirliği için metin hazırlanması istenmiştir(Konsey 2022).

Sözleşme, Macaristan Budapeşte'de 2001 yılı Kasım ayında imzaya açılmıştır. Türkiye, 2010 yılı Kasım ayında imzalamıştır. Avrupa Konseyi Siber Suç Sözleşmesini, Türkiye 2014 yılı Eylül ayında onaylamıştır. Sözleşme, 2015 yılından

itibaren iç hukukumuzda geçerlilik kazanmıştır. Yasa ile kabul edilmiştir. Yasa ile kabul edilene kadar TCK ve CMK'da benzer kurallar konmuştur.

Uluslararası sözleşme dört bölümden oluşmakta ve 48 maddedir. Kapsamlı bir düzenlemedir. Ülkelerarası işbirliği ve yardımlaşma hükümlerinin etkin bir şekilde yürütülmesi suç ve suçlulukla mücadele için gereklidir.

1.8. Bilirkişilik

Bilişim sistemleri içerisinde bulunan veriler iz bırakılmadan istenilen şekilde değiştirilebilecek özellikte bulunduklarından bunlara yapılacak işlemler klasik delillerden farklılık arz etmektedir. Dijital materyallerin mahkemelerde hakimler tarafından delil olarak kabul edilebilmesi için, materyallerin ilgili kanunlar kapsamında ve adli bilişim prosedürlere uygun olarak bu alanda uzman personel tarafından toplanması, imajlarının alınması ve incelenmesine bağlıdır.

Bilişimin gelişme başlangıcında sadece bir forensic uzmanlık alanı bütün bilişim faaliyetleri ile ilgilenebilirken, her yeni bilişim sistemi diğerlerinden farklı bir sistemde çalışması nedeniyle forensic alanı birden fazla uzmanlık alanına (Mobile forensic, Network forensic gibi) ayrılmak zorunda kalınmıştır. Bu kadar fazla türde forensic alanının bulunması ve bunların birbirleriyle etkileşimleri nedeniyle, adli bilişim uzmanlığı, detaylı ve en zor çalışma alanlarından biri haline gelmiştir.

Adli bilişim uzmanı olarak çalışan kişilerin, gelişen teknolojideki yeniliklerin yanında bu alandaki yerel ve uluslararası (AİHM gibi) mahkeme kararlarını da takip etmesi gerekmektedir. Bir adli bilişim uzmanı, Cumhuriyet Savcılığı veya mahkeme

tarafından görevlendirildiğinde, görev bitimine kadar kamu görevlisi olarak kabul edildiğinden verdikleri raporlar soruşturma veya mahkeme sonuçlarına etki etmektedir. Mahkeme sürecinin sonunda iddia edilen konulara yönelik maddi gerçeğin ortaya çıkarılması amaçlanmaktadır. Bu nedenle, başlatılan soruşturma içerisinde teknik hususların bulunmasına rağmen soruşturmayı başlatan Cumhuriyet Savcılığı teknik hususlara yönelik bilirkişi görevlendirmesi yapmamış ise, mahkeme sırasında taraflardan herhangi birisi bu konuda bilirkişi görevlendirilmesi yapılmasını talep edebilecektir. Savunma tarafı mahkeme tarafından görevlendirilen bilirkişinin hazırladığı veya hazırlayacağı rapora karşı iddia edilen konulara karşı bu alandaki uzman kişilerden de Uzman Mütaala Raporu adı altında rapor talep edebilmektedir.

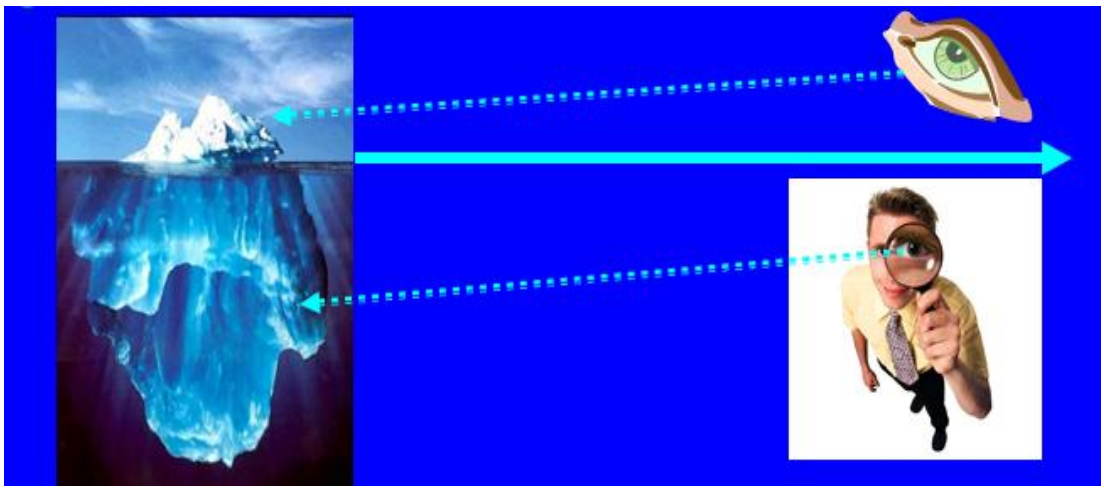
1.9. Bilirkişi

Teknolojinin baş döndürücü hızına yetişmek mümkün görülmemektedir. Bu nedenle bu kadar yenilik ve değişikliklerin her konusunda bilgili olmak imkânsız hale gelmektedir. Teknolojinin bu kadar ilerlemesi bu alandaki sistemlerde de güvenlik açıklarına sebep olmaktadır. Suç işleme düşüncesinde olan kişi/kişiler bilişim sistemlerinin güvenlik açıklarını inceleyerek bu alanda kendilerine uygun suç işleme ortamı oluşturmaya çalışmaktadırlar.

Mesleki bilgi ile çözülmeyen, ayrıntılı bilgi gerektiren hususlarda bilgisine başvurulanlara bilirkişi denir. Teknik hususlar içeren mahkemelerde bilirkişinin önemi daha iyi anlaşılabilmektedir. Bilişim suçları veya bilişim vasıtasıyla işlenen suçlarda, hiç ilgisi olmayan kişi veya kişiler adına suç işlenebildiği gibi işlenen suçlarda faillerin izleri yok edilebilmektedir. Bu nedenle, bilişim suçlarının incelenmesi ve gerçek anlamda iddia edilen hususların gerçekleşip gerçekleşmediği ile gerçek faillerin tespit edilebilmesi için soruşturma veya mahkeme aşamasında bu alanda görev yapan uzman kişilerin bilirkişi vasfı ile görevlendirilmesi gerekmektedir.

Hâkimin yönettiği ve içerisinde teknik hususlar veya deliller barından mahkemede, hiçbir şüpheye mahal bırakmadan adaletli bir karara varabilmesi için teknik uzmanın desteğine ihtiyaç bulunmaktadır. Genelde bu destek bilirkişi listelerinde kayıtlı ve görev almak için hazır bekleyen kişilerden sağlanmaktadır.

Bir mahkeme hakimi şüphenin tamamen ortadan kaldırılması için aynı konuda faklı zamanlarda farklı kişileri bilirkişi olarak görevlendirebileceği gibi, gerektiğinde birkaç uzmanı heyet olarak da görevlendirebilmektedirler. Teknik hususlar veya dijital deliller barından davalarda, bilirkişi görevlendirilmesi yapılmadan karar verilmesi, adalet dağıtımında yanlış kararların verilmesine veya suçlu insanlar yerine masum insanların cezalandırılmasına neden olunabilecektir(Şekil 1.4).



Şekil 1.4. Bilirkişi

Hukuk Muhakemeleri Kanunu madde 269'da, bilirkişinin görevinin genel sınırlarını düzenlenmiştir. Bilirkişi, öncellikle mahkeme tarafından yapılan davete yerinde ve zamanında icabet etmeli, tarafsız ve objektif olacağı taahhüdünü içeren

yemin etmeli ve bilirkişi kendisine verilen dosyaya uygun kararını mahkemeye sunmalıdır.

Bilirkişi olmak için başvuran ve başvurusu onaylanan uzman kişiler belirli bir yemin ettikten sonra bilirkişi listesinde yerlerini alırlar ve kendilerine verilecek görev için beklemeye başlarlar.

Görev verilecek alanlarda liste içerisinde bilirkişi tespit edilemez ise liste dışından da bilirkişi görevlendirilmesi yapılabilmektedir. Görev verilmesi öncesinde bu hususa resmi gerekçe Bilirkişilik Daire Başkanlığına bildirilmesi ve gelecek cevaba göre görevlendirilmenin yapılması gerekmektedir. Görevlendirilme sırasında yine bilirkişiye usulüne uygun yemin ettirilir.

Mahkeme asgari olarak;

- Nelerin incelenmesi istediği belirtilmeli,
- Ne istendiği, çözülemeyen hangi hususun açıklanması gerektiği yazılmalı,
- İncelenecek şeyleri mühürlü olarak dizi pusulasıyla bilirkişiye teslim edilmelidir.

Bilirkişinin raporunu hazırlaması için teslim edilen soruşturma dosyası veya dijital deliller neticesinde inceleme için verilecek süre sınırlıdır. Bu süre üç ayı geçemez. Daha az süre de belirlenebilir. Mahkeme, duruma göre değerlendirerek bir defaya mahsus üç aylık ek yeni bir süre verebilir.

Bilirkişiye sağlanan hak ve yetkiler ile birlikte bir takım yükümlülükleri vardır. Bu yükümlülükler bir kamu görevi ifa etmesinin sonucudur. Bu yükümlülükler HMK ve CMK da düzenlenmiştir. HMK 279 ve 280'de bilirkişi raporunun içeriği ve mahkemeye sunulması düzenlenmiştir. Bilirkişi mahkemenin isteğine göre hazırladığı raporu mahkemeye sözlü olarak da sunabilir. Takdir hakkı mahkemeye aittir. Bilirkişi, özel ve teknik bilgisi ile tespit yapmak ve elde ettiği sonuçları mahkemeye iletmekle görevlidir.

1.9.1. Bilirkişi Raporuna Karşı Başvuru Yolları

Bilirkişi raporunda çelişkilerin olması, açıklığa sahip olmaması veya kapsamına uygun olmaması durumunda rapora itiraz edilebilir. Bizzat mahkeme tarafından rapora itiraz edilebilir. Dava da taraflar da itiraz edebilir. Böyle bir durum ile karşılaşılması durumunda ek rapor hazırlanmasını mahkeme talep edebilir.

Taraflar veya mahkeme ek raporda bulunan belirsizlik ya da çelişkilerin giderilemeyeceğini anlarsa, ikinci bir bilirkişiye başvurulabilir. İlk alınan rapor ile ikinci alınan rapor arasında çelişki olursa bertaraf edilmesi için üçüncü bilirkişiye başvurulur. Verilen raporun hakime kanaat edindirmesi gerekmektedir. Bilirkişilerin bu alandaki yetkinliği çalışmaları, hakime kanaat edinmesi için karar vermede verecekleri rapor çok önemlidir. Çelişkiye mahal verilmemesi gerekmektedir.

1.9.2. Bilirkişi Raporunun Değerlendirilmesi

HMK madde 282'de bilirkişinin oy ve görüşünün nasıl değerlendirileceği düzenlenmiştir. Hakim, diğer delillerle birlikte bilirkişi raporunu serbestçe değerlendirmelidir. Rapor, eksik veya yetersiz ise hakim, raporun tersine karar verebilir. Hâkimin bilirkişinin görüşü tersine karar vermesi gerektiğinde yeni bir bilirkişi raporu almasına ihtiyaç yoktur. HMK. 281'de düzenlenmiştir.

1.9.3. Bilirkişinin Sorumluluğu

Bilirkişi, görevlendirildiği süre zarfında kamu görevlisi sıfatı taşımaktadır. Rapor teslimi̇nden sonrasında, hazırladığı rapor nedeniyle bilirkişiye yönelik herhangi bir saldırı yine kamu görevlisine yönelik saldırı olarak değerlendirilecektir.

Bu görevi yerine getirirken çeşitli sorumlulukları vardır. Bilirkişinin gerçeğe aykırı raporunu kasten veya ağır ihmal sureti ile düzenlemiş olması durumunda, mahkemece hükme esas alınmasıyla zarar görmüş olanlar, bu zarardan dolayı şikayetçi olabilirler. Tazminata konu olabilir ve raporu hazırlayan bilirkişiye yüklenir.

1.10. Bilirkişi Raporları

Başlatılan bir soruşturmada soruşturma konusu içerisinde herhangi bir teknik bilgi içeren delillerin bulunması (dijital delil veya veri gibi) neticesinde Cumhuriyet Savcılıkları hazırlayacakları iddianame öncesinde bu delillerin incelenmesi için bilirkişi görevlendirmesi yapmakta ve hazırlanan rapor içerisindeki lehe veya aleyhe olan hususlar ile iddianame şekillenmektedir.

Son dönemlerdeki adli süreçlerde, dijital delil veya verilerin incelenmesi biraz zaman aldığında Cumhuriyet Savcılıkları gelen dijital delil veya verileri incelettirmeden veya kriminal sonuçları beklemeden hazırladıkları bilirkişi raporu olmadan hazırladıkları iddianameleri mahkemelere göndermektedirler. Bu gibi durumlarda dijital delil veya verilerin incelettirilmesi işi mahkemelere kalmaktadır.

Devam eden mahkeme aşamasında, sanığın lehine veya aleyhine olabilecek bütün deliller tartışılmalı ve hiçbir şüphe kalmaması neticesinde bir karara varılması gerekmektedir. Bu nedenle, teknik bir husus olan dijital delil veya verilerin incelenmesi ve raporlanması (bilirkişi raporu) mahkemelerin verecekleri kararı doğrudan etkilemektedir.

Ancak son dönemde alanında nitelikli ve yetişmiş uzman personelin bulunmaması veya bu kişilerin bilirkişi olarak başvuruda bulunmaması neticesinde yeterli eğitimi almamış veya bu alanda fazla tecrübesi olmayan kişiler bilirkişi olarak görevlendirilmekte, bu durumda olan kişilerin hazırladıkları raporlar neticesinde taraflar tam olarak güven duymamaktadırlar.

Cumhuriyet Savcılığı veya mahkemeler tarafından resmi liste üzerinden veya gerekçesi ile belirtilmek üzere liste dışından görevlendirilen kişiler bilirkişi olarak isimlendirilmekte ve bunların hazırladıkları raporlar ise Bilirkişi Raporu olarak ifade edilmektedir. Savunma makamı, soruşturma konusu dijital delil veya verileri iddia edilen hususlara yönelik bu alandaki uzman kişi veya şirketlere incelettirebilmektedirler. İnceleme neticesinde hazırlanan rapor içerik olarak Bilirkişi Raporu ile aynı içeriğe sahip olsa da, Uzman Mütaala Raporu olarak isimlendirilmektedir.

Mahkemece aldırılan bilirkişi raporu ile savunma makamı tarafından alınan ve mahkemeye sunulan Uzman Mütaala Raporu arasında herhangi bir fark bulunursa, mahkeme tarafından üçüncü bir bilirkişi görevlendirmesi yapılması ve aradaki farkın giderilmesi neticesinde karar vermesi gerekmektedir.

Mahkemeye sunulan bilirkişi veya Uzman Mütaala Raporları, herkesin anlayabileceği sadelikte, kısa ve net bilgiler içermelidir. İnceleme ile ilgisi olmayan bilgiler ile hukuki konular rapora eklenmemelidir. Fazla miktarda sayfanın olması veya çok sayıda teknik/akademik bilgilerin olması raporun kalitesini artırmadığı gibi anlaşılmasını da zorlaştıracak ve yeni bir bilirkişi görevlendirilmesi neticesinde adaletin gecikmesine neden olunacaktır.

Bilirkişinin adli bilişim prosedürüne uygun olarak yaptığı/yapacağı inceleme neticesinde tespit edilen hususların, başka uzmanlar tarafından yapılabilecek incelemeler neticesinde de tespit edilebileceğinin bilinmesi gerekmektedir. Ülkemizde adli bilişim incelemeleri neticesinde hazırlanan raporlara yönelik herhangi bir resmi format bulunmamaktadır. Bu nedenle, her bilirkişi veya uzman

geçmiş tecrübelerinden elde ettiği kazanımlar neticesinde kendisini en iyi ifade edebileceği bir format geliştirmiş ve bu format ile raporlarını hazırlamaktadırlar.

İnceleme neticesinde hazırlanan ve taraflara sunulan bir raporun incelenmesi sırasında, inceleyen kişilerin ek bilgiye ihtiyaç duymaması gerekmektedir. Bu nedenle, raporun açıklamasına yönelik bütün ek bilgiler sade bir şekilde rapora ilave edilmelidir.

1.11. Bilirkişi Raporunun Hazırlanma Esası

Rapor bir başlık altında hazırlanmaya başlanmalı, eğer bilirkişi tarafından hazırlanmışsa "Bilirkişi Raporu", savunma tarafınca hazırlatılmışsa "Uzman Mütaala Raporu" olarak isimlendirilmelidir. Bu sayede, hazırlanan raporun kim tarafından talep edildiği ve hazırladığı daha rahat anlaşılabilecektir.

Rapor incelemesi neticesinde çok miktarda alt başlık olduğu/olabileceği dikkate alındığında, rapor içerisinde aranılan hususların bulunabilmesi için başlık altına "içerisindekiler" konulabilir.

Raporun girişinde talep makamının inceleme konusu ayrıntılı bir şekilde ifade edilmelidir. Devamında, raporu talep eden kurum/şirket/avukat/şahıs bilgileri, raporun tanzim tarihi ve raporu hazırlayan şirket/kurum/kişilere ait ayrıntılı bilgiler yazılmalıdır. Bu ayrıntılı bilgiler içerisinde, raporu hazırlayanlara yönelik iletişim bilgileri mutlaka bulunmalıdır. Talepte bulunan ve inceleme maksadıyla teslim

edilen deliller "İnceleme İçin Teslim Edilen Deliller/Materyaller" başlığı altında ayrıntısı ile belirtilmelidir.

Tarafların (Cumhuriyet Savcılığı ve savunma makamı) dava konusuna yönelik mahkemeye sundukları materyallerin ilgili kanun kapsamında delil olup olmadıklarına mahkeme karar verecektir. Bu nedenle, eğer inceleme neticesinde mahkeme tarafında sunulan materyaller delil, davanın taraflarınca sunulanlar ise henüz delil aşamasında olduklarından materyal olarak ifade edilmektedir.

İnceleme amacıyla teslim edilen delil/materyallerde herhangi bir arıza, kırık gibi herhangi bir zarar-ziyan tespit edilmişse veya delil/materyaller üzerindeki seri/IMEI numaralarında bir uyumsuzluk varsa mutlaka belirtilmelidir. İnceleme için dijital materyal/delil teslim edilmişse, öncelikle bunların adli imajları alınmalı, bunlara ait özellikler ve HASH değerleri ile birlikte liste hazırlanmalıdır. Eğer dijital delillerin kendileri yerine daha önceden alınan dijital delillerin imajları teslim edilmişse, bu imajlara ait log kayıtlarındaki ayrıntılı bilgiler ile yapılacak Hash kontrolleri neticesinde elde edilecek hash hesaplama değeri listeye eklenmelidir. Re-Hash işleminde, hash değerlerinde herhangi bir değişiklik veya tutarsızlık varsa, bu durum ekran görüntüsü ile kayıt altına alınarak incelemeden iade edilmelidir.

Bilirkişi veya uzmanların incelemede kullandıkları lisanslı donanım ve yazılım ile free-licence bütün yazılımlar belirtilmelidir. Raporun inceleme aşamasında geçilmeden önce, rapor içerisinde kullanılan teknik hususlar "Kullanılan Teknik Terimler" başlığı altında herkesin anlayabileceği şekilde açıklanmalıdır. İncelemede sadece talep edilen hususlar incelenmelidir. İnceleme ve raporlama aşamasında dava konusu ile ilgili olmayan veya kişisel verilere girilmemelidir. Raporun son aşaması Sonuç kısmı, raporun özeti mahiyetinde olup en önemli yeri olarak kabul

edilmektedir. Bu bölüm talep edilen hususlara yönelik yapılan incelemede tespit edilen veya tespit edilemeyenler gerekçesi ile birlikte kısaca açıklandığı yerdir. Bu nedenle, taraflar öncelikle sonuç kısmını incelemekte, gerektiği durumlara özete esas asıl maddeler de incelenebilmektedir.

1.12. Adli Bilişim İncelemeleri

Adli bilişim incelemesi, klasik delillerden farklılık arz eden bir sistemdir. Bu nedenle, dijital materyaller veya delillerin toplanması için bu alanda eğitim almış uzman kişilerin görevlendirilmesi gerekmektedir. Eğer dijital bir materyalin kendisi veya içerisindeki verinin doğrudan suç ile ilgisi varsa veya doğrudan suç ile ilgisi olmamasına rağmen olayın aydınlatılmasına katkı sağlayabilecek diğer materyallerin incelenmesi gerekmektedir. Adli bilişim incelemeleri her zaman suç neticesinde kullanılan bir sistem değildir. Bazı zamanlarda, kurum veya şirketlerin veri güvenliği, veri kaybı, veri trafiği gibi güvenliğe yönelik uygulamalarda da kullanılabilmektedirler.

Ülkemizde adli bilişim incelemeleri, kurumsal bilirkişiler, siber şubeler, üniversitelerin ilgili bölümleri, adli bilişim uzmanları ve bilirkişiler aracılığıyla yapılmaktadır. Kurumsal bilirkişilerin Emniyet, Jandarma ve Adli Tıp personellerinin belirli bir eğitim süreci vardır. Eğitimi ve belirlenen süre tamamlanmadan inceleme ve analiz yapılamamaktadır. Verdikleri inceleme raporlarının ulusal ve uluslararası geçerliliği vardır.

Çok geniş bir alan olduğundan ve delil elde etme süreci zor olduğundan dolayı bu alanda çok büyük bir boşluk bulunmakta ve giderek daha karmaşık bir süreç haline gelmektedir.

Ülkemizde bilişim suçu ve bilişim cihazları ile işlenen suçlar konusunda genel bir ayırım yapılmamakta, hepsi genel incelenmektedir. Bir suç içerisinde doğrudan veya dolaylı şekilde çok fazla bilişim cihazları kullanıldığından, suç sayısı ve çeşitliliği her geçen gün artmaktadır. Bir suç içerisinde bilişim cihazı kullanıldığının iddia edilebilmesi için o cihaz veya sistemin özelliklerinin de bilinmesi gerekir.

Bazı durumlarda, bilişim suçları birkaç ili kapsadığı gibi bazı durumlarda da uluslararası boyuta kadar varabilmektedir. Suça konu materyaller üzerinde inceleme yapılması ve delile dönüşebilmesi için uzman personele ve uygun ortama ihtiyaç vardır. Operasyonel durumlar için önceden hazırlıklı olunması ve gerekli tüm ekipmanların temin edilmesi gerekmektedir. İnceleme ve analiz için özel tasarlanmış programlar ve donanımlar çok kolaylık sağlamaktadır.

Ülkemizde adli bilişim inceleme süreçleri çeşitli çalışmalarla yorumlanmıştır (Şekil 1.5).

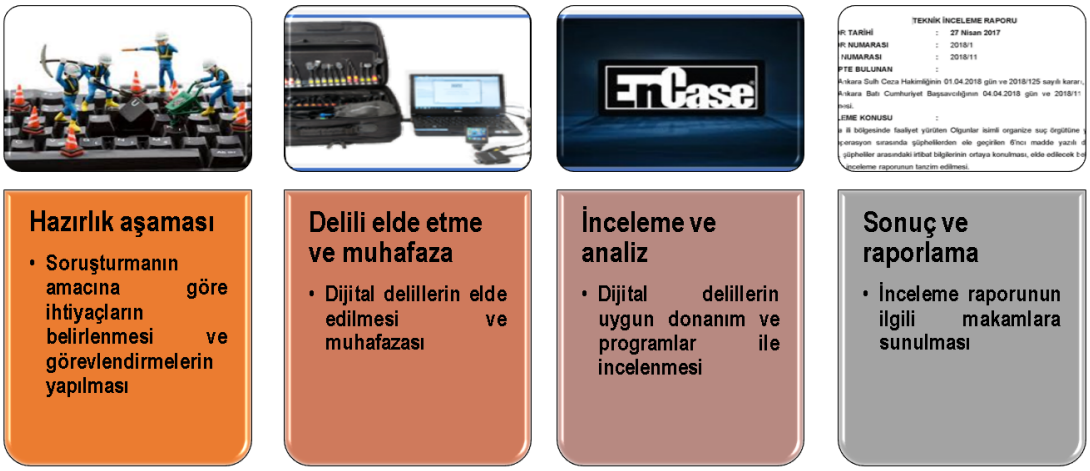
Bu aşamalar da ideal bir Adli Bilişim Süreci;

1- Hazırlık Aşaması

2- Delillerin Tespit Edilmesi, Toplanması, Muhafazası ve Laboratuvara Gönderilmesi Aşaması

3- Deliller Üzerinde Gerekli İnceleme ve Analiz Faaliyetleri Aşaması

4- İnceleme Sonucu Raporlama ve Delillerin İadesi Aşaması olarak tez çalışması olarak tanımlanmıştır (OĞUZ R. Yüksek Lisans Tezi).



Şekil 1.5. Adli Bilişim Süreci

1.13. Bilişim Suçlarına Müdahale

Bilişim suçlarında şüpheli tarafından doğrudan veya dolaylı şekilde kullanıldığı değerlendirilen dijital delillere yönelik işlemlerin nasıl ve ne şekilde yapılacağı CMK 134'de belirtilmiştir.

Bahse konu suçlarda bir soruşturmanın öncelikle başlatılmış olması gerekmektedir. Devam eden soruşturma veya mahkeme aşamasında başkaca delil elde etme imkanı yok ise son çare olarak şüpheli/sanığa ait dijital delil incelemesine geçilmesi gerekmektedir. Her ne kadar kanuni ve öğretide bu şekilde ifade edilmiş olsa da, pratik uygulamalarda daha soruşturmanın başlangıç aşamasında şüphelilerin kullandıkları bütün dijital delillerin toplanması ve incelemesi için mahkeme kararı alınmaktadır. CMK 134'ncü madde içeriği aşağıda gösterilmiştir(Şekil 1.6).

- ***Başka surette delil elde etme imkânının bulunmaması*** *halinde bir suç dolayısıyla yapılan soruşturmada somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ile Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilir.*

- *Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir.*

- *Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde,* ***elkonulan cihazlar gecikme olmaksızın iade*** *edilir. Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır. Alınan yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır.*

- *Ayrıca bilgisayar veya bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kâğıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır.*

Şekil 1.6. CMK 134

1.14. Sosyal Medya Suçları

Suç çeşitlerinin çoğaldığı gibi sosyal medya üzerinden işlenen suçlar da çoğalmıştır. Normal hayatta işlenen suçların çoğu sosyal medya üzerinden gizli kimlik bilgileri veya sahte kimlik bilgileri kullanarak işlenebilmektedir. Akıllı telefonların ve cihazların artması ile birlikte internetin yaygınlaşması, sosyal medya kullanımını da artırmıştır. Sosyal medyanın yaygın kullanılması suçluların rahat hareket ettiği bir ortam olmuştur. Sosyal medyada işlenebilen suçlar çeşitlilik arz etmektedir. Hakaret, tehdit, cinsel taciz, özel hayatın gizliliği, şantaj, dolandırıcılık, müstehcenlik, terör propagandası gibi çeşitli suçlar için kullanılabilmektedir. Sosyal medyada işlenebilecek olan klasik suçlar, TCK'da tanımlanmış olup bu suçlardan bazıları;

1.14.1. Cinsel Taciz-Madde 105

Bazı suçların soruşturulması veya kovuşturulması için şikayetçi olunması gerekmektedir. Bu suç için de geçerlidir. Şikayetçi olunmaz ise doğrudan kovuşturulmaz. Taciz içeren durum yazılı, sesli veya görsel herhangi bir araç kullanılması neticesinde tamamlanmış olur. Herhangi bir şekilde bir fiziksel temas olmadan işlenen ve cezalandırılan bir eylemdir. Suçu işleyene, üç aydan yirmidört aya kadar hapis cezası veya adlî para cezası verilmesine karar verilebilir. 18 yaşından küçüklere işlenmesi durumunda ceza artırılır. Cinsel içerikli ifade, işaret, fotoğraf ve vücudun çıplak teşhir edilmesi de cinsel taciz suçunu oluşturur. Bilişim sistemlerinden herhangi biriyle twitter üzerinden işlenmesi durumunda ceza artırılmaktadır.

1.14.2. Tehdit-Madde 106

Twitter'da en çok işlenen suçlardan birisidir. Kişiler twitter üzerinden gerçek kimlikleri ile veya sahte profil ile bu suçu işleyebilmektedirler. Suçun işlenmesi halinde altı aydan 24 aya kadar hapis cezası vardır. Tehdit suçu da şikayete tabii suçlardandır. Şikayet olmaz ise kovuşturulmaz. Tehdite maruz kalan kişinin bu durumu deliller kaybolmadan delillendirmesi şikayetçi olması gerekmektedir. Ağırlaştırıcı durumları bulunmaktadır.

1.14.3. Şantaj-Madde 107

Şantaj suçunu soruşturmak için mağdurun şikayetine gerek yoktur. Herhangi bir şekilde bir bildirim olması soruşturmaya başlanılması için yeterlidir. Twitter'da kendisine şantaj yapılan kimsenin şikayetçi olabileceği gibi tanık olan kişilerinde bildirimde bulunması ile soruşturma başlatılmalıdır. Şantaj suçu bu özelliğiyle de tehdit suçundan farklıdır. Delillerin kaybolmadan hızlı bir şekilde toplanması ve mağduriyetlerin giderilmesi adaletin tecellisi için önemlidir. Yapılan şantaj içerikli paylaşımın silinmeden delillendirilmesi gereklidir. Şantaj suçunu işleyenlere 12 aydan 36 aya kadar hapis cezası ve beş bin güne kadar adli para cezası verilebilir. Ağırlaştırıcı durumları vardır.

1.14.4. Nefret ve Ayrımcılık-Madde 122

Ayrımcılık ve nefret suçu takibi şikayete bağlı suçlardan değildir. Doğrudan kovuşturulan suç türleri arasındadır. Twitter üzerinden kişiler yakalanmayacakları düşüncesiyle de bu suçu işleyebilmektedirler. Kanun kapsamında ayrıntılı belirtilmiştir. Bu suçu işleyenlere 12 aydan 36 aya kadar hapis cezası verilebilir.

1.14.5. Kişilerin Huzur ve Sükununu Bozma-Madde 123

Bir kimsenin kanunda belirtilen suç kapsamında suç işlemesi halinde üç aydan 12 aya kadar hapis cezası verilir. Bu suç hakaret, tehdit, şantaj gibi diğer suçlar sonucunda da meydana gelebilir. Twitter aracılığıyla işlenen bir suçun devam ettirilerek sürdürülmesi durumunda bu suç unsurları oluşmaktadır

1.14.6. Haberleşmenin Engellenmesi-Madde 124

Haberleşmenin engellenmemesi gerekir engellendiğinde yasa kapsamında cezası altı aydan 24 aya kadar hapis veya adlî para cezasıdır. Kitle iletişim araçlarının engellenmesi ve resmi kurumlar arasındaki haberleşmeyi engelleyenlerin cezası 12 aydan 60 aya kadar hapis cezasıdır.

1.14.7. Hakaret-Madde 125

Cezası üç aydan 24 aya kadar hapis veya adli para cezasıdır. Kovuşturulması için şikayetçi olunması gerekmektedir. Twitter üzerinden hakaret suçuna maruz kalan kişinin şikayeti ile soruşturma işlemlerine başlanılmaktadır. Twitter üzerinden bu suçun işlenmesi ve şüphelinin tespiti durumunda üçte bir oranında ceza miktarı artırılır. Suç işlendiği farkedildiğinde durumu delillendirmek için kayıt almak gerekmektedir. Ekran görüntüsü olarak ve ekran görüntüsüne ait video kaydının alınması gerekmektedir. Aynı durum diğer işlenen suçlar için de gereklidir. En yaygın şikayet konularından bir tanesidir.

1.14.8. Haberleşmenin Gizliliğini İhlal-Madde 132

Cezası altı aydan 24 aya kadar hapis veya adli para cezasıdır. Bilişim sistemi ile bu suçun işlenmesi durumunda 12 aydan 36 aya kadar hapis cezası verilebilir. Twitter üzerinden bu suçu işleyenlerin cezası artırılmaktadır. Sahte hesaplar ve suç grupları tarafından genellikle bu suçlar işlenmektedir.

1.14.9. Kişilerin Dinlenmesi ve Kayda Alınması-Madde 133

Yasa özel hayatın gizliliğine önem vermiş ve koruma altına almıştır. Bu suçu işleyenlerin cezası iki aydan altı aya kadar hapis cezasıdır. Twitter üzerinden aldığı kaydı yayınların cezası altı aydan 24 aya kadar hapis cezası ve bin güne kadar adli para cezasıdır. Soruşturulması için suçun mağdurunun şikayetçi olması gerekmektedir.

1.14.10. Özel Hayatın Gizliliği-Madde 134

Twitter üzerinden bu suçu işleyenlerin cezası 24 aydan 60 aya kadar hapis cezasıdır. Suçun işlendiği tarihten sonra altı ay içerisinde şikayetçi olunması gerekmektedir.

1.14.11. Şahsi Verilerin Kaydı-Madde 135

Bu suçu işleyenlere altı aydan 36 aya kadar hapis cezası verilebilir. Doğrudan kovuşturulan bir suçtur. Kişisel verilerinin kaydedildiğini öğrenen kişinin şikayetini

beklenmeksizin suç öğrenildiğinde gerekli adli işlemlerin yapılması gerekmektedir. Kamu görevlilerinin kişisel verileri yasal olmayan şekilde kaydetmeleri durumunda verilecek ceza yarı oranında artırılmaktadır.

1.14.12. Kişisel Verileri Yayma-Madde 136

Twitter üzerinden başkasına ait bilgileri yayan kişi/kişilere 12 aydan 48 aya kadar hapis cezası verilebilir.

1.14.13. Nitelikli Hırsızlık-Madde 142

Twitter üzerinden hırsızlık suçu işlendiğinde nitelikli hırsızlık suçu işlendiği anlamına gelmektedir ve bilişim sistemi kullanmak suretiyle işlendiğinden dolayı ağırlaştırıcı nedenlerdendir. Bilişim suçları ile bazen karıştırılabilmektedir. Maddi bir değer para, altın gibi hırsızlık söz konusu olduğunda bu madde hükümlerine göre suçlular yargılanmaktadırlar.

1.14.14. Nitelikli Dolandırıcılık-Madde 158

Sosyal medya yaygın kullanıldığından dolandırıcılar sosyal medya ortamları üzerinde çeşitli tuzaklar kurup insanların parasını haksız olarak almaktadırlar. Twitter üzerinden de insanlar iş bulma, kolay yoldan zengin olma, yattığın yerden para kazanma gibi vaatlerle kandırılmaktadır. Dolandırıcılar koordineli olarak çalışıp insanların saf temiz duygularını da istismar edebilmektedirler. Twitter üzerinden dolandırıldığında nitelikli dolandırıcılık suçuna maruz kalmış bulunmaktadırlar. Cezası 24 aydan 84 aya kadar hapis ve beş bin güne kadar adli para cezasıdır. Parasal işlemler yapılırken daha dikkatli olunmalı ve vaatlere kapılmamak gerekmektedir.

1.14.15. Twitter'da Övme-Madde 215

Twitter üzerinden, suç işleyen kişiyi öven ve övmesi sonucunda asayiş yönünden tehlikeli bir durumun olmasına sebebiyet veren kişiye iki yıla kadar hapis cezası verilebilir.

1.14.16. Twitter'da Tahrik veya Aşağılama-Madde 216

Twitter üzerinden kişi/kişileri aşağılayanlar yakalanamayacakları düşüncesiyle rahat hareket etmekte ve bilgisayar başında tahrik edici paylaşımlar

yapabilmektedirler. Paylaşımı nedeniyle asayişe müessir herhangi tehlikenin olması nedeniyle paylaşım yapana 12 aydan 36 aya kadar hapis cezası verilebilir.

1.14.17. Twitter Üzerinden Hayasızca Hareket-Madde 225

Twitter üzerinden teşhircilik yapıldığında cezası altı aydan bir yıla kadar hapis cezasıdır. İhbar ile işlem yapılabilir şikayet olmasına gerek yoktur.

1.14.18. Twitter'da Müstehcenlik-Madde 226

Uluslararası alanda çocuk müstehcenliği ile ilgili kapsamlı çalışmalar yapılmaktadır. Twitter uygulamasına müstehcen çocuk resmi veya görüntüsü yüklendiği zaman yükleme yapan ip numarası anlaşmalı olunan ülkeye Twitter tarafından anında bildirilmektedir. Türkiye'de Emniyet Genel Müdürlüğü Siber Suçlar Daire Başkanlığı bu husus ile ilgili görevlendirilmiştir. Suç içeren resim veya dosyayı yükleyen ip numarası, dosyanın hash değeri ve yüklendiği tarih saat bilgisi bildirilmektedir. İlgili daire başkanlığı ip numaranın belirtilen tarih saatte kime tahsis edildiğinin tespitinden sonra şüphelinin bilişim delillerinde gerekli tespitin yapılması için ilgili Cumhuriyet Savcılığına yazmaktadır. Cumhuriyet Savcılıklarınca adli işlemlere başlanılarak gerekli adli işlemler yapılmaktadır. Cezası altı aydan 24 aya kadar hapis ve adli para cezasıdır.

1.14.19. Twitter Üzerinden İftira-Madde 267

Twitter üzerinden iftira atan ve iftira suçu unsurlarını tamamlayan kişiye 12 aydan 48 aya kadar hapis cezası verilebilir. Cezanın ağırlaştırıcı ve hafifletici etkenleri bulunmaktadır. İftira atılan kişinin mağduriyeti ve aldığı ceza durumuna göre değişmektedir.

Twitter üzerinden işlenen suçlar saydığımız suçlarla sınırlı değildir. Bilişim sistemi üzerinden twitter kullanarak TCK'da bulunan diğer suçlar da şartlar oluştuğunda işlenebilmektedir.

1.15. Twitter Üzerinden İşlenen Suçlarda Ülkemizdeki Kararlara Dair Haberler

Sosyal medya uygulamalarından twitter üzerinden işlenen suçlardan en çok karşılaşılanlar, Cumhurbaşkanı'na hakaret ve tehdit gibi suçlardır. Bu saydığımız suçlarla da sınırlı değildir. Başka suçlar da işlenebilmektedir.

Ülkemizdeki internet siteleri, kullanıcıların eriştiği tüm içeriklerden sorumludur ve suça konu olup olmadığı hususunda gerekli tedbirleri almak

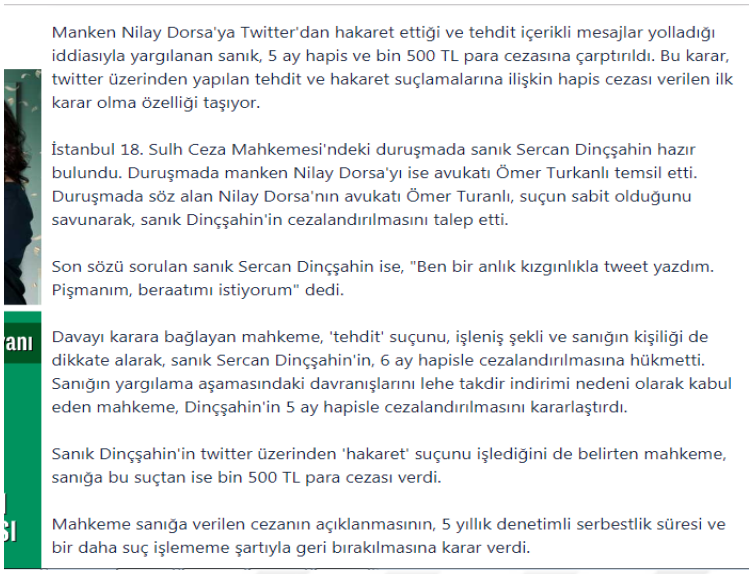
zorundadır. Twitter'da Türkiye'de içerik sağladığından dolayı bu sorumluluğa sahiptir. Herhangi bir suç işlendiğinde kullanıcıya ait bilgiler istenmektedir.

Şüpheli veya suç konusu twitter paylaşım yapanların tespiti için şirket ile iki ülke arasındaki uluslararası anlaşma metni de dayanak gösterilerek istenmektedir. Ancak ülkeler arasındaki hukuki farlılıklar nedeniyle çok başarılı olunamamaktadır. Bizde suç olarak görülen bir durum Amerika yasalarına göre suç olmadığı durumlarda işlemler hem uzun sürmekte hem de neticesiz kalmaktadır.

Türkiye'de Twitter hesabına ait IP'yi tespit edilemediği zaman suçluların kim olduğu bilinememektedir. Suçluların kimlik bilgilerine erişilemediği ve Twitter tarafından da erişim bilgilerinin silinmiş olması durumunda soruşturma dosyalarında boşluklar bulunmaktadır. Amerikan hukuk sistemine göre suç kapsamında görülmeyen durumlardan sonuç alınamamaktadır.

1.15.1. Twitter Paylaşımı Nedeniyle Ceza Verilenler

Twitter üzerinden suç işleyenler genellikle sahte hesaplar ve sahte bilgiler üzerinde işlem yapmaktadırlar. Suçlulara gereken cezanın verilebilmesi için önce kullanıcı bilgileri tespit edilmesi gerekmekte ve delil toplamaya nereden nasıl başlanacağının belirlenmesi gerekmektedir. Tespit edilen kişilerin suçu ikrar etmeleri durumunda adli yargılamalar yapılabilmektedir. Ülkemizde twitter aracılığıyla işlenen suçlara verilen cezalarla ilgili çeşitli örnekler bulunmaktadır.



Manken Nilay Dorsa'ya Twitter'dan hakaret ettiği ve tehdit içerikli mesajlar yolladığı iddiasıyla yargılanan sanık, 5 ay hapis ve bin 500 TL para cezasına çarptırıldı. Bu karar, twitter üzerinden yapılan tehdit ve hakaret suçlamalarına ilişkin hapis cezası verilen ilk karar olma özelliği taşıyor.

İstanbul 18. Sulh Ceza Mahkemesi'ndeki duruşmada sanık Sercan Dinçşahin hazır bulundu. Duruşmada manken Nilay Dorsa'yı ise avukatı Ömer Turkanlı temsil etti. Duruşmada söz alan Nilay Dorsa'nın avukatı Ömer Turanlı, suçun sabit olduğunu savunarak, sanık Dinçşahin'in cezalandırılmasını talep etti.

Son sözü sorulan sanık Sercan Dinçşahin ise, "Ben bir anlık kızgınlıkla tweet yazdım. Pişmanım, beraatımı istiyorum" dedi.

Davayı karara bağlayan mahkeme, 'tehdit' suçunu, işleniş şekli ve sanığın kişiliği de dikkate alarak, sanık Sercan Dinçşahin'in, 6 ay hapisle cezalandırılmasına hükmetti. Sanığın yargılama aşamasındaki davranışlarını lehe takdir indirimi nedeni olarak kabul eden mahkeme, Dinçşahin'in 5 ay hapisle cezalandırılmasını kararlaştırdı.

Sanık Dinçşahin'in twitter üzerinden 'hakaret' suçunu işlediğini de belirten mahkeme, sanığa bu suçtan ise bin 500 TL para cezası verdi.

Mahkeme sanığa verilen cezanın açıklanmasının, 5 yıllık denetimli serbestlik süresi ve bir daha suç işlememe şartıyla geri bırakılmasına karar verdi.

Şekil 1.7. Verilen İlk Ceza (İlk ceza 2013)

Bu verilen ceza, belirttiğimiz gibi şüphelinin ikrarı üzerine ceza takdir edilen ilk karar olma özelliğini taşımaktadır. Hakaret suçundan beş ay hapis cezası verilmiş ve denetimli serbestlik ile hükmün açıklanması geri bırakılmıştır (Şekil 1.7).

Ana sayfa » ... » Yargı ve Düzenleyici Kurum Kararları

Twitter'dan hakaret eden sanığa ceza

Milli Takımlar Teknik Direktörü Fatih Terim'in kızı Buse Terim'e Twitter üzerinden hakaret ettiği belirlenen sanığa para cezası verildi.

Haberi Kopyala

19 Aralık 2013 16:36

Yazdır

Şekil 1.8. (Buse Terim Hakaret 2013)

Fatih Terim'in kızı Buse Terim, şikayette bulunarak kendisine hakaret edildiğini bildirmiştir. Şüpheli H.S.E.'ye dava açılmış, 2 yıla kadar hapis istemiyle

yargılanan H.S.E, hâkim karşısına çıkmıştır. Hakaret suçundan ceza almış ve cezası ertelenmiştir(Şekil 1.8).


Haberler > Magazin > Twitter'dan hakarete hapis cezası

06 Nisan 2013 Cumartesi 15:44 | Son Güncelleme: 06 Nisan 2013 Cumartesi 15:44

Twitter'dan hakarete hapis cezası

Twitter'a 'Cihan Ünal sakallarına s..m. Grönland merkez cami imamı gibi herif' yazarak Cihan Ünal'a hakaret ettiği öne sürülen İsmail Ozan Saka, hapis cezasına çarptırıldı.

Şekil 1.9. (Cihan Ünal'a Hakaret 2013)

Oyuncu Cihan ÜNAL, kendisine hakaret edildiği gerekçesiyle şikayetçi olmuş şikayet ettiği şüpheli İ.Ö.S. 2 ay 27 gün hapis cezasına çarptırılmıştır. Verilen ceza için hükmün açıklanması geri bırakılmıştır (Şekil 1.9).

Şekil 1.10. (Başbakan'a Hakaret 2014)

Başbakan Recep Tayyip Erdoğan, Başbakan olduğu 2014 yılında kendisine hakaret edildiğini iddiasıyla şikayette bulunmuştur. L.P'nin suç işlediğine karar verilerek iki ay 15 gün hapis cezası verilmiştir. Verilen ceza için hükmün açıklanması geri bırakılmıştır (Şekil 1.10).

Şekil 1.11. (Hasan Şaş'a Hakaret**)**

Eski ünlü futbolcu Hasan Şaş, hakaret ettiği nedeniyle M.K. isimli şahıstan şikayetçi olmuştur. M.K. ifadesinde dava konusu tweeti attığını kabul etmiş ve verilen karar da; adli para cezası almıştır. Ayrıca aldığı ceza ertelenmiştir (Şekil 1.11).

Şekil 1.12. (Emre B. Hakaret 2018)

Emre Belözoğlu, küfür ettiği iddiasıyla C.İ.C. isimli şahıs hakkında şikayetçi olmuştur ve mahkeme C.İ.C.'ye hakaret suçu nedeniyle bin 500 TL para cezası vermiştir. Verilen ceza için hükmün açıklanması geri bırakılmıştır (Şekil 1.12).

Şekil 1.13. (Ayşe Hür Ceza 2018)

Yazar Ayşe HÜR, twitter'dan örgüt propagandası yaptığı gerekçesiyle hakkında açılan davada; bir yıl üç ay hapis cezası almıştır (Şekil 1.13).

Şekil 1.14. (Nazlı Ilıcak Ceza 2018)

Nazlı ILICAK, Anadolu 53. Asliye Ceza Mahkemesinde görülen bir dava da twitter'dan yaptığı paylaşım nedeniyle bir yıl iki ay hapis cezası almıştır (Şekil 1.14).

Şekil 1.15. (Önder Aytaç Ceza 2014)

Ankara 1'inci Sulh Ceza Mahkemesi'nde görülen duruşma da; Önder Aytaç, on ay hapis cezası almıştır (Şekil 1.15).

Şekil 1.16. (Aydın Doğan'a Hakaret 2015)

Twitter üzerinden Aydın Doğan'a hakaret ettiği gerekçesiyle Mihriban Merent isimli hesap sahibine 109 gün adli para cezası verilmiştir (Şekil 1.16).

Şekil 1.17. (Ö.F.Gergerlioğlu Twitter Ceza 2022)

Twitter'dan ceza alanların listesine HDP Milletvekili Ömer Faruk Gergerlioğlu'da katılmıştır. Twitter paylaşımı nedeniyle hakkında iki yıl altı ay hapis

cezası verilmiştir. Verilen ceza Yargıtay'ın ilgili Dairesi tarafından onanmıştır (Şekil 1.17). 17 Mart 20211'de milletvekilliği düşürülmüş 1 Temmuz 2021'de Anayasa Mahkemesi kararıyla 16 Temmuz 2021 tarihinde yeniden milletvekili olmuştur(Gergerlioğlu 2021).

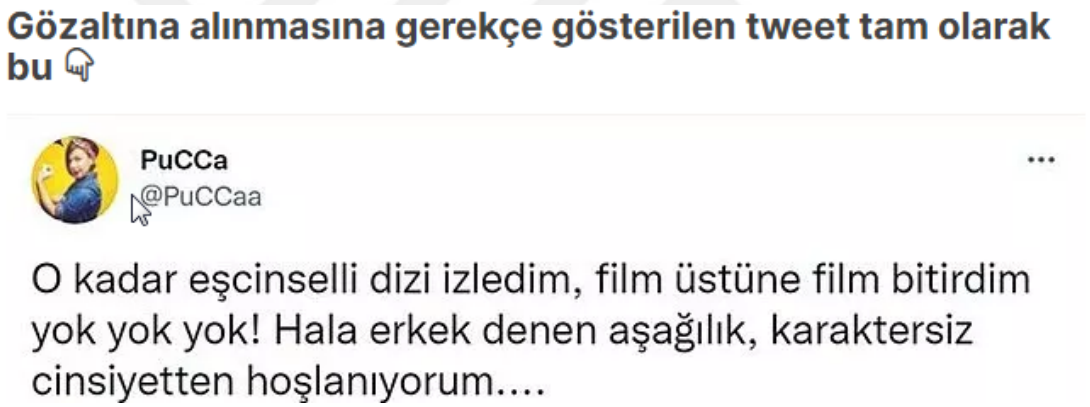
Şekil 1.18. **(**Metin Uca Ceza 2020)

Twitter'dan yaptığı paylaşımlar nedeniyle açtığı davada gerekçeli Karar'da; Metin Uca, bir yıl iki ay on yedi gün ceza almıştır (Şekil 1.18).

Şekil 1.19. **(**Uludağ Ceza 2021)

Gazeteci Alican Uludağ, dönemin Ankara Cumhuriyet Başsavcısı Yüksel Kocaman'ı hedef gösterdiği iddiasıyla yargılandığı davada 10 ay hapis cezası almıştır. (Şekil 1.19)

Twitter üzerinden ve diğer sosyal medya sitelerinden yapılan paylaşımlar ile ilgili yasal bir düzenleme yapılmalı suç çerçevesi içerisine oturtulan durumlar mutlaka cezalandırılmalıdır. Paylaşılan konunun suç olup olmadığı hususunda tereddüt olmamalıdır.



Şekil 1.20. (Pınar YILDIRIM Ceza 2020)

Pucca takma adını kullanan Pınar YILDIRIM, twitter paylaşımından beş ay hapis cezası almıştır (Şekil 1.20).

Şekil 1.21. (Kaftancıoğlu Twitter 2022)

Yargıtay, sosyal medya paylaşımlarına ilişkin emsal bir karar vermiştir. Twitter'da, bir tweeti retweetlemek kişiyi suçlu yapabilir. Retweet yaptıktan sonra sorumluluk kabul etmiyorum yazılsa bile bu tarz ibareler kurtarıcı olmamaktadır (Yargıtay 2021). Suç olan bir durumun twitter üzerinden retweetlenmesi suçlamalara konu olabilmektedir. Bu retweetleme çeşitli suç tasnifleri için de değerlendirilebilir. Karar hakaret suçu üzerinden verilmiştir ancak diğer suçlar ile ilgili paylaşımlar da bu durumdan değerlendirilmelidir.

1.15.2. Takipsizlik ile Sonuçlanan Twitter Kararları

ABD'de bulunan Twitter'dan IP bilgilerinin istenmesi ve verilmesi durumunda gelmesi çok uzun sürmektedir. Bazen sonuçlanamamaktadır. Şüphelinin kullandığı IP adresinin elde edilmesi sonrası suç konusu paylaşımı yapan kişiye ulaşılırsa adli makamlara başvurulması ile soruşturma işlemleri başlamaktadır. Kendisine karşı suç işlendiğini düşünen kişi ekran görüntüsü alsa da fotomontaj ihtimali nedeniyle Savcılık ekran görüntüsünü tek başına delil kabul etmeyebilmektedir.

Twitter aracılığıyla kendisine karşı suç işlendiğini düşünen kişinin ekran kayıtlarını alması gerekmektedir. Türkiye Noterler birliğinin E Tespit özelliği ile de kayıt alınabilir. En fazla 10 dakika ile bağlantı kurarak kayıt alınabilmektedir. Verilen özellik ile ilgili esaslar doğru kullanılarak suça konu paylaşım ile ilgili delillendirme yapılmalıdır(E-tespit 2020).

Hakkında suç işlendiği düşünen kişilerin durumu derhal kolluk makamlarına veya Cumhuriyet Savcılıklarına bildirmelidir. Bildirimden sonra adli prosedürler başlatılır ve gerekli adli işlemler yapılır. Deliller toplanır ve suç görülür ise iddianame düzenlenir. Yapılan çalışmalar neticesiz kalır delil tespit edilemez ise takipsizlik veya kovuşturmaya gerek olmadığı kararı verilmektedir. Ülkemizde takipsizlik ile sonuçlanan twitter paylaşımlarından bazıları aşağıda gösterilmiştir.

Şekil 1.22. (Şensayar Tehdit 2018)

Şanlıurfa, Suruç'da öldürülen Adil, Celal ve Hacı Esvet Şenyaşar'ın kardeşi Osman Şenyaşar şikayette bulunmuştur (Şekil 1.22). Şanlıurfa Cumhuriyet Başsavcılığınca soruşturma başlatılmış ve takipsizlik kararı verilmiştir. Karar aşağıda gösterilmiştir (Şekil 1.23).

Facebook, Twitter, gerekse Yahoo gibi yurtdışı kaynaklı hizmet sağlayıcıları üzerinden gönderilen e-mail header bilgilerini içeren çıktılarda IP numarasının bazen yazılı olduğu görülse de, hukuken bu bilgilerin hizmet sağlayıcı kuruluşça (Facebook, Twitter, Yahoo ve Google gibi) doğrulanmadıkça kesin delil sayılmayacağı, bu nedenle dosya içeriğinde yer alan ekran görüntülerinin ilgili site uhdesinde bulunan IP bilgileri ile doğrulanmadıkça delil niteliğine havi evraklar olamayacakları, yurt dışı merkezli bu işlemlerin yapıldığı ülkelerdeki yasal yapı ve 'Kişisel verilerin gizliliğine ilişkin hükümler' gereği söz konusu bilgilere ulaşılmasının mümkün bulunmadığı, istinabe yolu ile yapılacak taleplere açıklanan gerekçelerle olumlu cevap verilmediği, bilişim yolları kullanılarak işlenen suçlarda dijital delil araştırmasının güvenilir sertifika otoritesinin bulunmasına ve küresel ortak protokoller ile kanunlar ile düzenlemesine bağlı olduğu, ilgili sitenin bağlı olduğu elektronik servis hizmetlerinin yurtdışı kaynaklı olduğu, yabancı ülke, şirket ve serverlarının kullanılması nedeniyle dijital delil elde edilmesinin mümkün bulunmadığı, Şüpheli hakkında üzerine atılı suçtan dolayı delil yetersizliği nedeniyle kamu adına kovuşturma yapılmasına yer olmadığına Savcılık karar verilmiştir.

Şekil 1.23. Mahkeme Kararı (Şensayar Tehdit 2018)

Şekil 1.24. (Murat Boz Hakaret 2012)

Şarkıcı Murat BOZ' un hakaret ile ilgili başvurusu karşılıksız kalmıştır(Şekil1.24).

Suça maruz kalan insanlar tabii olarak suçluların cezalandırılmasını ve aynı suçun tekrar işlenmemesini talep etmek için adalete başvurmaktadırlar. Bazen neticelenmekte bazen de iddianame hazırlanacak delillerin elde edilememesi nedeniyle dosyalar kapatılmaktadır. Adli makamların karar vermeleri için delil çok önemlidir. Delillerin toplanması ve kıymetlendirilmesi çok önemlidir. Deliller olmadan herhangi bir karar verilemez. Bilişim suçlarında da bilişim ortamından delil elde etmek gerekmektedir.

Şekil 1.25. (Sedat Peker Takipsizlik 2015)

Eski savcı Zekeriya ÖZ'ün, Twitter üzerinden yaptığı paylaşımlarla kendisine hakaret ettiği iddiasıyla Sedat PEKER hakkında yaptığı suç duyurusu, takipsizlikle sonuçlanmıştır (Şekil 1.25).

Savcılık, gazeteci Enver Aysever'e Twitter'da **'geri zekâlı'** diye hakaret eden AKP'li Bülent Turan hakkında hakaret suçundan yapılan soruşturmada üç kez takipsizlik verdi. Gerekçe ise Twitter'dan onaylı hesabın Turan'a ait olup olmadığının **'tespit edilemeyecek'** olması.

Şekil 1.26. (Bülent Turan Takipsizlik 2017)

Twitter'dan kendisine hakaret edildiği gerekçesiyle şikayetçi olunan Bülent Turan hakkında takipsizlik kararı verilmiştir (Şekil 1.26).

1.16. Twitter Üzerinden İşlenen Suçlarda Uluslararası Ceza İstinabe İşlemleri

Mahkemenin başka bir mahkemeden kendi yargı işlemi için yerine getirme talebinde bulunmasına istinabe denir. Twitter, yer sağlayıcısı Amerika Birleşik Devletleri'nde bulunmaktadır. Dolayısıyla twitter üzerinden suç işlendiğinde gerekli bilgiler de Twitter genel merkezinden veya genel merkezin yetkilendirdiği birimlerinden elde edilmektedir.

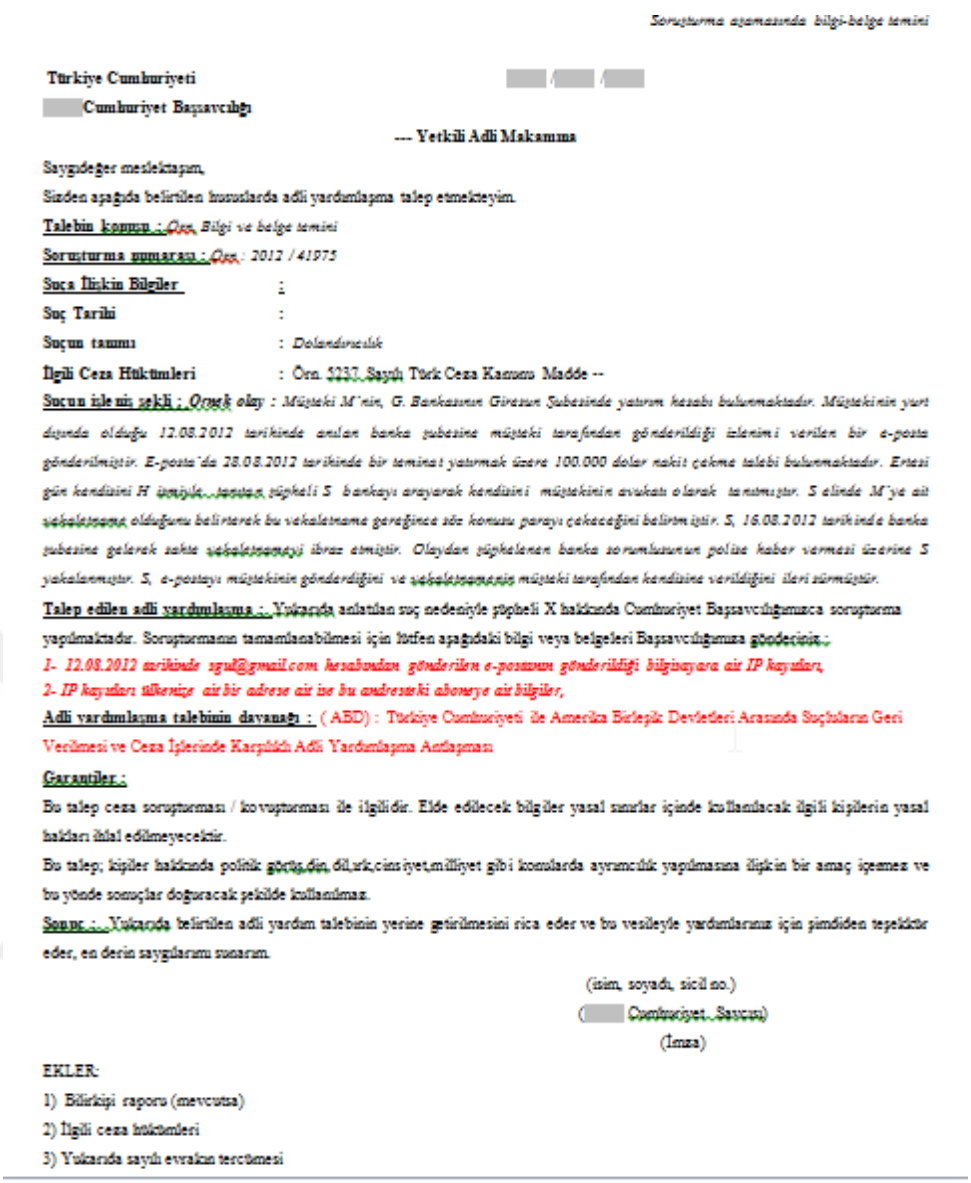
ABD hukuku ve yasalarına tabi olan Twitter için Türk hukuk sistemiyle etkili olunamamaktadır. Gerekli olduğunda IP bilgisini sadece site verebilmekte ancak hiçbir makama bazı istisnalar dışında vermemektedir (İstinabe 2021).

Twitter'a bir yazı yazılması gerektiğinde, Twitter'ın IP ve trafik bilgisi saklama süresi dikkate alınmalıdır. Twitter'ın genellikle diğer ülkelerde bulunan şubeleri ve bizim ülkemizde bulunan şubesi adli isteklere cevap vermemektedir.

Sakıncalı veya suç içeren durumlarda kullanıcılara yönelik bölümler bulunmaktadır. Kullanıcıların şikâyeti dikkate alınarak içerik kaldırılmaktadır. Bazı durumlarda ifade özgürlüğü şeklinde yorumlanmakta, mevzuatımıza göre suç sayılabilecek bazı söylemler içerik sağlayıcı twitter tarafından eleştiri sınırları içinde kabul edilerek içeriği kaldırmayabilmektedirler(İstinabe 2022). Türkiye ile Amerika arasındaki istinabe Antlaşması 1 Ocak 1981'de yürürlüğe girmiştir. Adli yardımlaşma hususlarını düzenlemektedir.

Ceza istinabe talebinde bulunmak için evraklar ABD yargı makamlarına yönelik düzenlenmeli ve gerekli prosedürler tamamlanmalıdır (Evraklar 2022). Soruşturma ve kovuşturma esnasında gerekli olan evraklar ve örnekleri https://diabgm.adalet.gov.tr/home/SayfaDetay/uluslararasi-ceza-istinabe-evrakinin-hazirlanmasi14022020013214 adresinden indirilerek doldurulmalıdır.

Talepname, detaylı hazırlanmalı, yalın bir dil kullanılmalı ve Sözleşmeye atıf yapılmalıdır. Talepnamede kısaltmalara yer verilmemeli ve süre belirtilmemelidir. Kimlik veya pasaport fotokopisi dosyaya eklenmelidir. Evrak, fiziki ortamda gönderilmelidir. Twitter için evraklar İngilizce diline tercüme ettirilmelidir. Örnek talepname evrakı aşağıda gösterilmiştir (Şekil 1.27).



Soruşturma aşamasında bilgi-belge temini

Türkiye Cumhuriyeti
[redacted] Cumhuriyet Başsavcılığı

--- Yetkili Adli Makamına

Saygıdeğer meslektaşım,

Sizden aşağıda belirtilen hususlarda adli yardımlaşma talep etmekteyim.

Talebin konusu : *Örn. Bilgi ve belge temini*

Soruşturma numarası : *Örn.: 2012 /41975*

Suça İlişkin Bilgiler :

Suç Tarihi :

Suçun tanımı : *Dolandırıcılık*

İlgili Ceza Hükümleri : Örn. 5237 Sayılı Türk Ceza Kanunu Madde --

Suçun işleniş şekli : ***Örnek olay :*** *Müştaki M'nin, G. Bankasının Giresun Şubesinde yatırım hesabı bulunmaktadır. Müştakinin yurt dışında olduğu 12.08.2012 tarihinde anılan banka şubesine müştaki tarafından gönderildiği izlenimi verilen bir e-posta gönderilmiştir. E-posta'da 28.08.2012 tarihinde bir teminat yatırmak üzere 100.000 dolar nakit çekme talebi bulunmaktadır. Ertesi gün kendisini H ismiyle tanıtan şüpheli S bankayı arayarak kendisini müştakinin avukatı olarak tanıtmıştır. S elinde M'ye ait vekâletname olduğunu belirterek bu vekâletname gereğince söz konusu parayı çekeceğini belirtmiştir. S, 16.08.2012 tarihinde banka şubesine gelerek sahte vekâletnameyi ibraz etmiştir. Olaydan şüphelenen banka sorumlusunun polise haber vermesi üzerine S yakalanmıştır. S, e-postayı müştekinin gönderdiğini ve vekâletnameyi müştaki tarafından kendisine verildiğini ileri sürmüştür.*

Talep edilen adli yardımlaşma : Yukarıda anlatılan suç nedeniyle şüpheli X hakkında Cumhuriyet Başsavcılığımızca soruşturma yapılmaktadır. Soruşturmanın tamamlanabilmesi için tarafen aşağıdaki bilgi veya belgeleri Başsavcılığımıza gönderiniz.:

1- 12.08.2012 tarihinde sgul@gmail.com hesabından gönderilen e-postanın gönderildiği bilgisayara ait IP kayıtları,
2- IP kayıtları ülkeniz ait bir adrese ait ise bu adresteki aboneye ait bilgiler,

Adli yardımlaşma talebinin dayanağı : (ABD) : Türkiye Cumhuriyeti ile Amerika Birleşik Devletleri Arasında Suçluların Geri Verilmesi ve Ceza İşlerinde Karşılıklı Adli Yardımlaşma Antlaşması

Garantiler :

Bu talep ceza soruşturması / kovuşturması ile ilgilidir. Elde edilecek bilgiler yasal sınırlar içinde kullanılacak ilgili kişilerin yasal hakları ihlal edilmeyecektir.

Bu talep; kişiler hakkında politik görüş,din,dil,ırk,cinsiyet,milliyet gibi konularda ayrımcılık yapılmasına ilişkin bir amaç içermez ve bu yönde sonuçlar doğuracak şekilde kullanılmaz.

Sonuç : Yukarıda belirtilen adli yardım talebinin yerine getirilmesini rica eder ve bu vesileyle yardımlarınız için şimdiden teşekkür eder, en derin saygılarımı sunarım.

(isim, soyadı, sicil no.)
([redacted] Cumhuriyet Savcısı)
(İmza)

EKLER:
1) Bilirkişi raporu (mevcutsa)
2) İlgili ceza hükümleri
3) Yukarıda sayılı evrakın tercümesi

Şekil 1.27. Talepname Evrakı Örneği

1.17. İnternet Ortamında İşlenen Suçlarda Twitter Üzerinden Talep İşlemleri

Twitter, herkese açık sohbetler sunmak amacıyla kullanılmaktadır. Twitter'a hukuki bir talep geldiğinde; incelemekte ve kendi yasal gereklilikleri ile değerlendirmektedir. Twitter, suç içeren hesap ile ilgili talep sahibinden ek bilgi

sunmasını isteyebilmektedir. Yasal bir engel yoksa suç konusu durumu hesap sahibine şeffaflık ve müşteri memnuniyeti gibi gerekçelerle bildirebilmektedir. Çok hassas durumlarda çocuk istismarı, terörizm ve öldürme gibi istisnalar bir karar ile bildirilmesi durumunda adli işlemlerden sonra bildirmektedir.

Amerika Birleşik Devletleri'nde veya Avrupa Birliği ya da Avrupa Ekonomik Alanı dışındaki ülkelerde yaşayan kişiler için kişisel verilerden sorumlu veri denetleyicisi, San Francisco, Kaliforniya merkezli Twitter Inc. şirketidir. Avrupa Birliği veya Avrupa Ekonomik Alanı dâhilinde yaşayan kişiler için ise kişisel verilerden sorumlu veri denetleyicisi, Dublin, İrlanda merkezli Twitter International Unlimited Company'dir. Hesap bilgisi talepleri de aynı merkezlerden istenmektedir(Talep Twitter 2022).

Geçerli yasalar uyarınca, kullanıcı hesabı bilgisi taleplerinde hangi bilgilerin istendiği eksiksiz yazılmalı ve soruşturma ile bağlantısına dair ayrıntılar bulunmalıdır(Twitttter kolluk 2022). Acil durum ifşa talebi gönderilebilir. Eklenmesi gereken belgeler; Kolluk kuvvetlerine ait antetli kağıt üzerinde acil durum ifşa talebine ilişkin gerekli tüm içerik bulunmalıdır. Kullanıcılar, kendi Twitter hesaplarına gönderilen Tweetler de dahil kendi hesap bilgilerinin indirilmiş kopyasını edinebilmektedirler.

1.18. Türkiye Twitter Ofisi

Dünyanın çeşitli yerlerinde twitter ofisi bulunmaktadır. Türkiye'de de şirketleşmiştir. Reklam geliri temini ve müşteri memnuniyeti gibi etkenler nedeniyle şirket açılmıştır (Şekil 1.28). Türkiye'de tüzel kişilik kazanmıştır (Şirket 2021).

T.C. İSTANBUL TİCARET SİCİLİ MÜDÜRLÜĞÜ'NDEN

İlan Sıra No: 78156
MERSİS No: 0859122063200001
Ticaret Sicil/Dosya No: 307267-5

Ticaret Unvanı:
TWİTTER İNTERNET İÇERİK HİZMETLERİ LİMİTED ŞİRKETİ

Adres : Esentepe Mah. Büyükdere Cad. Kanyon Blok No: 185 İç Kapı No: 271 Şişli / İstanbul
Yukarıda bilgileri verilen şirket ile ilgili olarak aşağıda belirtilen hususlar müdürlüğümüze ibraz edilen belgelere istinaden ve Türk Ticaret Kanunu'na uygun olarak 22.4.2021 tarihinde tescil edildiği ilan olunur.
Tescil Edilen Hususlar: Kuruluş

1. Kuruluş
Aşağıdaki adı, soyadı, unvanı, yerleşim yeri ve uyruğu yazılı kurucu tarafından bir Limited Şirket kurulmuş bulunmaktadır.

Sıra No	Kurucu	Adres	Uyruk	Kimlik No
1	T.I. REDWING LLC	CORPORATİON TRUST CENTER, 1209 ORANGE STREET, WİLMİNGTON, NEW CASTLE İDARİ BÖLGESİ, DELAWARE 19801, AMERİKA BİRLEŞİK DEVLETLERİ	AMERİKA BİRLEŞİK DEVLETLERİ	**********

Şekil 1.28. Twitter Türkiye Şirket (Twitter Şirket)

1.19. Twitter Üzerinden İşlenen Suçların İncelenmesi

Çalışmamızda twitter üzerinden hangi eylemlerin suç olabileceği, suç konusu durumların bilirkişi aracılığıyla incelenmesi, bilirkişi raporu hazırlanma esasları, bilişim suçlarının hukuki durumu, ülkemizde twitter üzerinden işlenen suçlarda verilen cezalar ve takipsizlik ile sonuçlananlar, işlenen suçlar ile ilgili istinabe işlemleri anlatılmıştır.

Twitter üzerinden işlenen suçlarda uluslararası standartta inceleme yapılabilmesi için hangi yazılımlarla adli kopya alınması ve hangi adli bilişim yazılımları ile inceleme yapılabileceği, adli bilişim uzmanlarının sahip olmaları gereken sertifikalar ve Google ve Firefox gibi arama motorları üzerinden tespit edilebilecek kayıtlar anlatılması hedeflenmektedir. Ayrıca twitter üzerinden en sık yapılan oturum açma, paylaşım yapma, mesaj gönderme gibi işlemlerin örnek olaylar üzerinden yapılacak işlemler ve delillerin tespiti amaçlanmaktadır.

2. GEREÇ VE YÖNTEM

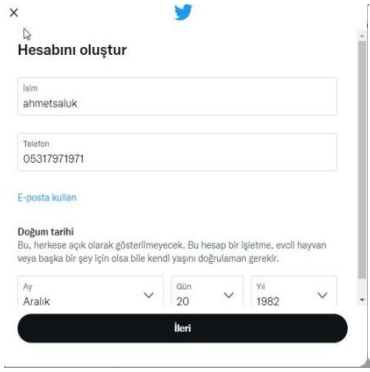
2.1. İncelemelerde Kullanılan İşletim Sistemleri, Uygulamalar ve Dosyalar

- Windows 7 Professional, 64 bit,
- Windows 10 N 64 bit,
- EnCase Law Enforcement(Versiyon 6.19.1)
- Recovery My Files (Versiyon 16.7)
- AccessData FTK Imager 3.1.0.1514
- Google Chrome 86.0.4240.111
- Firefox Browser 74.0
- (4) adet ".jpg" uzantılı dosya

2.2. İncelemelerin Yöntemi

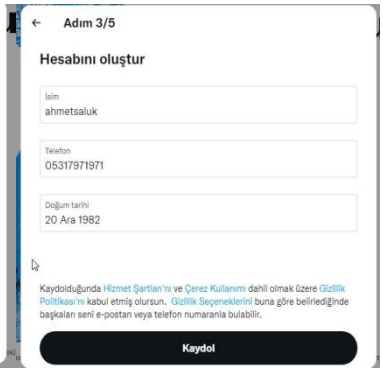
2.2.1. www.twitter.com İnternet Sitesinde Kullanıcı Hesabı Alma

Oturum alma işlemi Google hesabı üzerinden facebook hesabı üzerinden ve cep telefon numarası üzerinden alınabilmektedir. Ahmet Saluk ve Kamer Acar olmak üzere iki ayrı hesap alınmıştır. Ahmet SALUK kullanıcısının görünen ismi "ahmetsaluk"tur. Her kullanıcıya üye olunması sırasında bir adet User ID numarası atanmaktadır. Hesap alma işlemleri Şekil 2.1-2.12'de gösterilmiştir.



Şekil 2.1 İlk Hesap-1

Şekil 2.2. İlk Hesap-2



Şekil 2.3. İlk Hesap-3

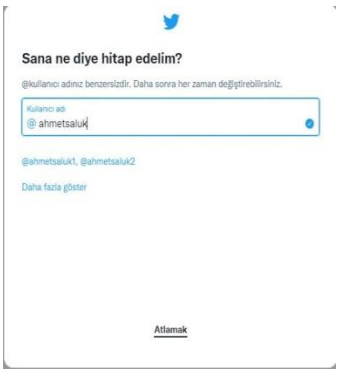
Şekil 2.4. İlk Hesap-4

Şekil 2.5. İlk Hesap-5

Şekil 2.6. İlk Hesap-6

Şekil 2.7. İlk Hesap-7

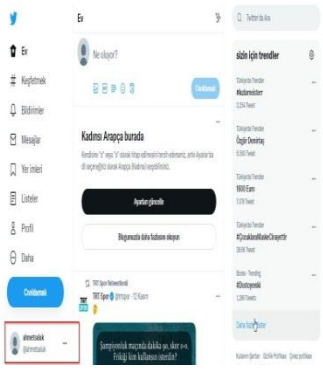
Şekil 2.8. İlk Hesap-8



Şekil 2.9. İlk Hesap-9

Şekil 2.10. İlk Hesap-10

Şekil 2.11. İlk Hesap-11

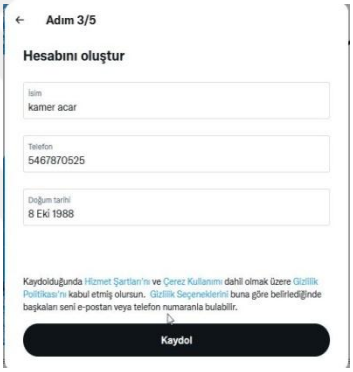


Şekil 2.12. İlk Hesap-12

Kamer Acar kullanıcısının görünen ismi "kameracar5"dir ve bu kullanıcıya hesap alma işlemleri Şekil 2.13-2.24'de gösterilmiştir.

Şekil 2.13. İkinci Hesap-1

Şekil 2.14. İkinci Hesap-2

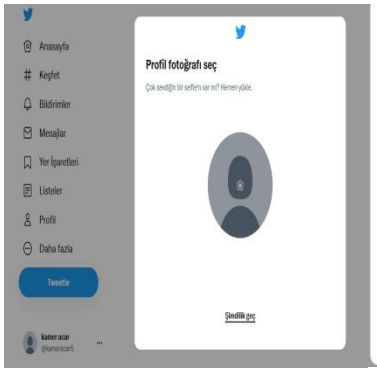


Şekil 2.15. İkinci Hesap-3

Şekil 2.16. İkinci Hesap-4

Şekil 2.17. İkinci Hesap-5

Şekil 2.18. İkinci Hesap-6

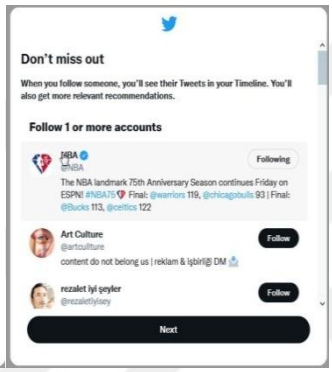


Şekil 2.19. İkinci Hesap-7

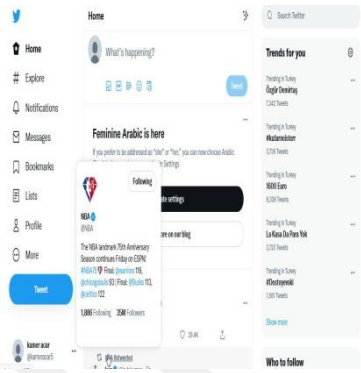
Şekil 2.20. İkinci Hesap-8

Şekil 2.21. İkinci Hesap-9

Şekil 2.22. İkinci Hesap-10



Şekil 2.23. İkinci Hesap-11



Şekil 2.24. İkinci Hesap-12

2.2.2. Twitter'da Oturum Açma Tespiti

Adli bilişim incelemeleri açısından oturum açma tespiti önemlidir. Çoğu işlem oturum açıldıktan sonra yapılmaktadır. Öncelikle oturum açıldığının tespiti daha sonra diğer işlemlerin tespiti yapılmalıdır.

Çalışmamız da "Ahmet saluk" ve "kamer acar" hesapları kullanılmıştır. Twitter'da chrome ve firefox tarayıcısında "**id_str**" en yeni oturum açma bilgisidir. Twitter güncellemeler ile bu verileri değiştirebilmektedir. "**data-user-id=**", "**data-user-screenname=**" eski oturum açma verileridir.

“ahmetsaluk” kullanıcı adına atanmış Twitter ID numarası olan “1459456753586868232 ” ve “kameracar” hesabına atanmış Twitter kullanıcı kimlik numarası olan “1459475185015443458” verileri aratılmış ve değerlendirilmiştir. Verileri arama ve analiz işlemi EnCase 6.19 adli bilişim yazılımı yardımıyla yapılmıştır.

2.2.3. Silinmiş Dosyaların Kurtarılması

Windows işletim sisteminde kullanılan yeni teknoloji dosyalama sisteminin kısaltması NTFS’dir. Yeni bir dosya oluşturulduğunda MFT(Master File Tablo) ve $LogFile dosyaları içerisinde kayıt tutulur ve $Bitmap ilgili dosyanın kullandığı alanları dolu olarak gösterir.

MFT kaydı içerisinde 22 ve 23’üncü baytlarındaki veri “00 00” ise bu dosyanın silinmiş, “01 00” ise mevcut, “02 00” ise silinmiş dizin (klasör) ve “03 00” ise mevcut dizin anlamına gelmektedir. Hard disk üzerindeki bir dosya silindiğinde dosya sadece silinmiş olarak işaretlenir ve Mft kaydında 22 ve 23’üncü baytlarına bu dosyaların silindiği yazılır.

Özel bir silme programı yerine işletim sistemi ile bir dosya silindiğinde, ilk etapta dosya içeriği tam olarak silinmeyecektir. Bu nedenle, veri kurtarma programı ile bu dosyaların içerikleri kurtarılabilmektedir. Dosyalama sisteminin olduğu sistem dosyaları bölümü bozulmuş veya silinmiş ise farklı kurtarma metotları kullanılmaktadır.

Çalışmamızda “ahmetsaluk” ve “kameracar” kullanıcısına bir adet profil resmi yüklenmiştir. Birer adet resim profilde paylaşılmıştır. Daha sonra internet sayfası kapatılmıştır. Yüklenen dosyaların kurtarılması için Recovery My Files yazılımı kullanılarak kurtarma işlemi yapılmış ve değerlendirilmiştir. İnceleme işlemleri için EnCase yazılımı kullanılmıştır. Anahtar kelime arama yöntemiyle sonuçlar değerlendirilmiştir.

2.2.4. Hash Hesaplanması

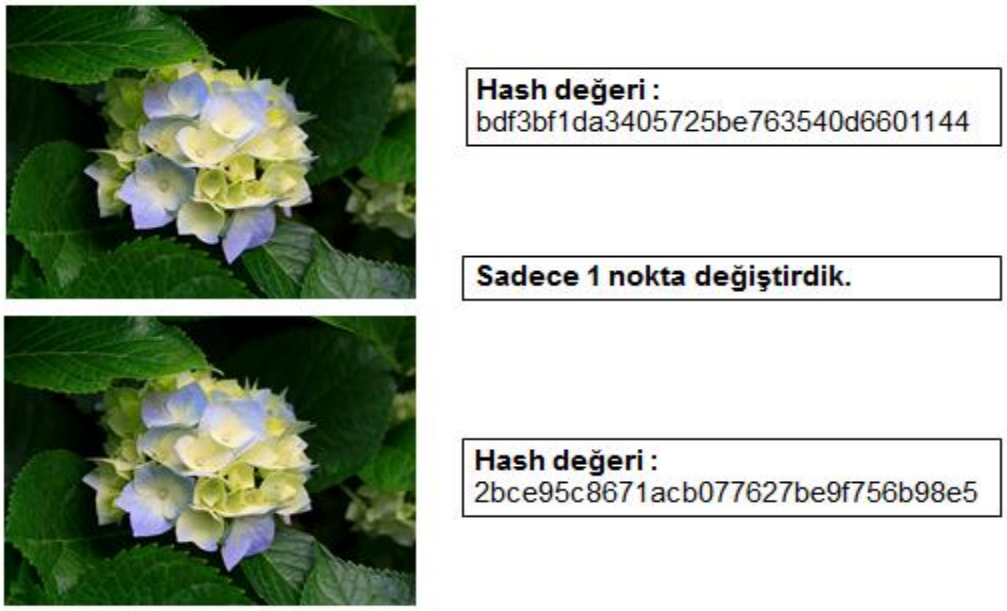
HASH hesaplaması, bir dosya veya veriyi matematiksel işlemlere tabi tutarak özet bir bilgi çıkarma işlemidir (Şekil 2.25). Bir dosyanın değişmez sayısal imzası veya parmak izi denilebilir. Tek yönlü yapılan bir işlemdir. Ürettiği özet bilgiden dosyaya ulaşamayız. Verinin veya dosyanın güvenliği için kullanılmaktadır.

Şekil 2.25. Hash Hesaplanması Yöntemi

Girdinin boyutu fark etmeksizin tüm dosyalar için hexadecimal (onaltılık) karakterde özetler üretir. Girdi düz yazı veya hexadecimal karakterlerde olabilmektedir. En yaygın kullanılan MD-5’dir. 32 hex karakterden oluşur. Dosyadan bir değer üretir ancak üretilen değerden dosyaya ulaşılamaz(MD-5 2015). Aşağıda kelime içindeki bir harf değiştiğinde hash değerinin de değiştiği örnekte gösterilmiştir.

DOSYA ADI	HASH DEĞERİ
Ahmet	cc8c47a835d66e943d85083693042717
a**H**met	b5f44b086480d8e1ef19c57e28fece97
ah**M**et	25fab0a03df5bb1c6f19b920aa330b82
ahm**E**t	df0b303082a6638031053044ff5d109d
ahme**T**	14aabc8101b880f7efd1fcaee91d0003

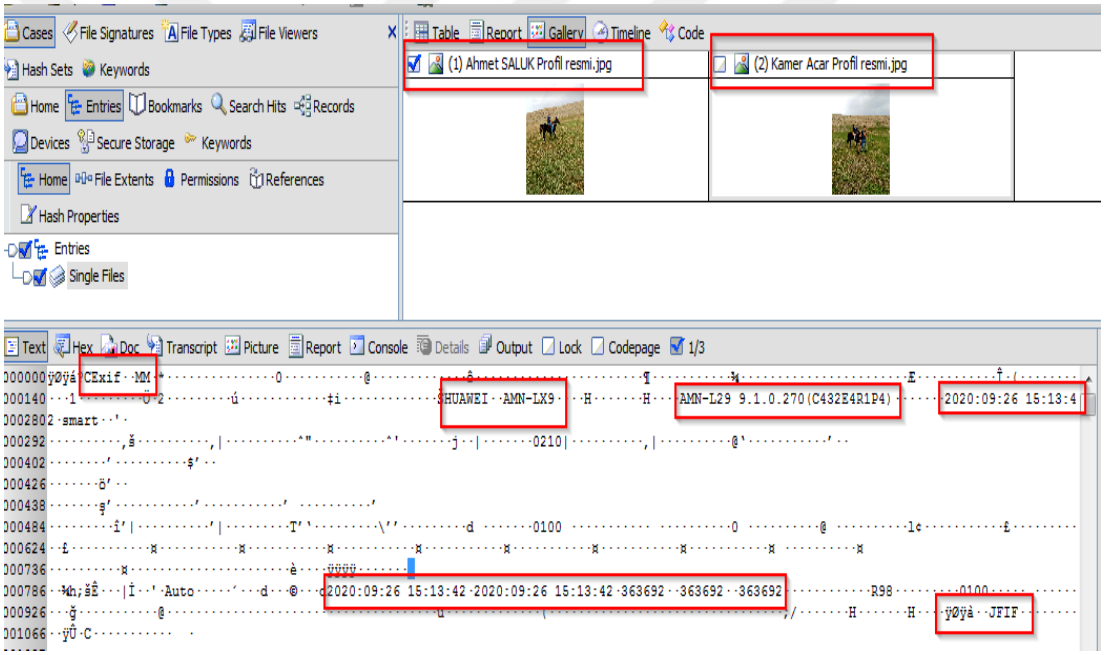
Hash değerleri sayesinde ileride meydana gelebilecek itirazlar ortadan kaldırılır ve delil bütünlüğü korunmaktadır. Resim dosyası içerisindeki bir noktanın değişmesi sonrasında hash hesaplandığında değerinin değiştiği Şekil 2.26'da gösterilmiştir.



Şekil 2.26. Hash Değişikliği

2.2.5. Exif Bilgileri

Bilgiler, çekilen cihaza göre farklılık göstermektedir. Kullanıcı çektiği cihaz ayarlarıyla da hangi bilgilerin yazılıp yazılmayacağını belirleyebilir. Genellikle çekim ayarları, fotoğrafın tarihi, konumu, boyutu gibi bilgileri barındırır. Fotoğraf makinelerinin coğrafi konum bilgisi açık olduğunda koordinat olarak bilgi bulunmaktadır. Örnek'te oturum hesabı almak için kullanıcıların profil resmi exif bilgileri Şekil 2.27'de gösterilmiştir.



Şekil 2.27. Exif Bilgileri

3. BULGULAR

3.1. Özel Adli Bilişim Ekipmanı Kullanmanın Önemi

Adli bilişimde kullanılan malzemelerin bazı standartlar taşıması ve bazı testlerden geçirilmesi gerekmektedir. Türkiye de bu şekilde bir standart bulunmamaktadır. Başka ülkelerde mesela ABD örnek olarak göstermemiz gerekirse Standartlar ve Teknoloji Enstitüsü (NIST- National Standarts and Tecnology) altında Adli Bilişim Testi yapılmaktadır. Sonuçları internet üzerinden yayınlanmaktadır. Test süreci aşağıdaki gibidir.

1. Test edilecek yazılım temin edilir.
2. Dokümanları incelenir.
3. Desteklediği özelliklere göre testler seçilir.
4. Test yöntemi geliştirilir.
5. Test yapılır.
6. Raporlanır.
7. Komite raporu inceler.
8. Yazılımı üreten, raporu inceler.
9. NIST yazılıma destek mesajını sitede yayımlar.
10. NIJ (National Institute of Justice-Amerikan Ulusal Adalet Enstitüsü) test raporunu internette yayımlar (CFTT Methodology Overview, www.cftt.nist.gov/Methodology_Overview.htm).

Suçla mücadele açısından olay yeri inceleme ve delillere el koymakla görevli personelin son derece bilgili ve eğitimli olması gerekmektedir. Neyin delil olup olmayacağı, delile el koyma şekli, delilin muhafazası ve sevk edilmesi ile incelenmesi suçu ve suçluları tespit etmede son derece önem arz etmektedir. Zira

delilin eksik tespit edilmesi, sevk esnasında zarar görmesi, uzman olmayan personelce incelenmesi halinde; suçun ortaya çıkartılması ve suçluların yakalanmasında çok büyük sorunlara neden olmaktadır.

Ülkemizde kullanılan adli bilişim donanım ve yazılımlarından yaygın olarak kullanılanlar anlatılacaktır. Tamamı bunlar değildir, bunlarla sınırlı da değildir. Olayın durumu, bilirkişinin kullandığı donanım ve yazılımların kabiliyeti, ücretli olup olmama durumuna göre kullanılan yazılım ve donanım değişiklik gösterebilir.

3.1.1. İmaj Almada Kullanılan Ekipmanlar

Adli bilişimin ilk ve en önemli aşamalarından biri imaj alma (birebir kopya) işlemidir. İmaj alma işleminde uluslararası geçerliliği olan firmalar ve cihazlar bulunmaktadır. Adli bilişim uygulamalarında kaynak sürücü olarak isimlendirilen sürücüler, imajı alınacak sürücüler, hedef sürücüler ise içerisine imaj alınacak sürücüler olarak isimlendirilmektedir. İnceleme sırasında herhangi bir sıkıntı yaşanmaması ve imaja ait verilerin güvenliği için imaj alma işlemlerinde yeni (sıfır) hard diskler tercih edilmelidir.

Birebir kopya alma cihazları delil içeriğini bozmadan herhangi bir sektörüne değişiklik yapmadan cihazın ilk bit'inden son bit'ine kadar verilerin hedef sürücüye alınmasını sağlamaktadır. Kopya işlemi tam olarak sorunsuz şekilde tamamlandığında, kopyalanan verilere yönelik olarak sayısal parmak izi olarak da adlandılan HASH değerleri üretilmektedir. Delilin kopyasını alan kişi ile delili inceleyen kişi aynı olmadığı zaman delil inceleyen, alınan imajın öncelikle HASH değerlerini doğrulamasını yapmaktadır. HASH değerlerinin tutması çok önemlidir. HASH değeri tutmadığı zaman delil üzerine değişiklik yapıldığı veya bozuk

sektörlerin bulunduğu değerlendirilmektedir. Delil bütünlüğünün sağlanması için HASH değerlerinin tutması çok önemlidir.

Bir sürücünün imaj alma işlemi hem yazılımsal (programlar kullanılarak) ve hem de donanımsal (özel cihazlar kullanılarak) alınabilmektedir. Yazılımsal imaj almada mutlaka bir işletim sistemi kullanılması gerekmektedir. Eğer Windows işletim sistemi kullanılacaksa imaj alma işleminde FTK İmager, Encase İmager gibi ücretsiz (free-licence) gibi programların kullanılması gerekmektedir.

Yine Windows işletim sistemi ve ücretsiz yazılımlar ile alınacak imajlarda, kaynak sürücünün bilgisayara takılması sırasında bilgisayardan herhangi bir dosyanın kaynak sürücüye bulaşarak delil bütünlüğünün bozulmaması için tedbir alınması gerekmektedir. Bu tedbirin başında özel olarak üretilen yazma koruma cihazları veya Windows bilgisayarın USB kapılarının çıkışlar için kapatılmasıdır (Şekil 3.1).

Şekil 3.1. İmaj Alma İşlemi

Adli bilişim uygulamalarında, hız ve veri güvenliği için genelde donanımsal imaj alma sistemleri kullanılmaktadır. Ancak imaj alınacak çok sayıda delil bulunması, sürenin kısıtlı olması nedeniyle de zaman zaman yazılımsal imaj metodu da kullanılmaktadır.

Adli imaj alabilen cihazların hepsi imaj alma, imaj doğrulama, HASH değeri üretme, formatlama ve wipe yapma (üzerine yazarak silme) gibi özellikleri desteklemektedir. Ücretli veya ücretsiz çok farklı imaj alma yazılımları geliştirilmiştir. Adli bilişim uygulamalarının hepsinin imaj alma yazılımı vardır. İmaj alma formatlarından en yaygın olanları raw (dd) ve e01'dir. Raw (dd), herhangi bir sıkıştırma uygulamaz. İmaj alınan medya ile imaj boyutu aynıdır. İçerisinde meta data bulunmaz sadece ham veri bulunur. Üzerinde çalışırken hızlı işlem yapılır. İmajları canlandırma işlemi için de kullanılmaktadır. E01, Expert Witness Format olarak da bilinir. Medyaların, bölümlerin ve dosyaların kopyasının alınmasını sağlamaktadır. E01 uzantısını kullanır. EnCase yazılı tarafından geliştirilmiş bir formattır. İmaj alma işlemini sıkıştırarak yapmaktadır. İmaj alırken girilen meta dataları bulundurur. Bazı adli bilişim yazılımlarının kendine has imaj formatı bulunmaktadır. İmaj alma donanım ve yazılımlarının hepsi genel imaj formatlarını desteklemektedir

Uluslararası geçerliliği olan imaj alma ekipmanları anlatılacaktır. İmaj alma donanımları anlattıklarımızla sınırlı değildir. Farklı ülkelere ait farklı firmalar ve aynı firmaya ait farklı özelliklerde çok çeşitli cihazlar bulunmaktadır. Özelliklerinin hepsi değil genel ve yaygın kullanılan özellikler anlatılacaktır.

3.1.1.1. Forensic Falcon Neo

Amerika'da kurulu bulunan Logicube firması tarafından geliştirilen bir birebir kopya alma cihazıdır. Dakika da 50 GB'ı aşan hız ile PCI kaynaktan PCI sürücüye kopya alabilmektedir. Dosya Tarayıcısı ve yazma engellenmiş sürücü ön izleme özelliği vardır. Bağlı sürücülere ve ağ havuzlarına mantıksal erişim sağlar. dd, e01, ex01 ve dmg görüntü dosyalarının içeriğini görüntüleyebilir. NIST tarafından önerilen XTS-AES-256 şifreleme modunu kullanarak sürücü şifrelemesi yapmaktadır. Şifrelenmiş diskleri ve sürücüleri algılama özelliği vardır. Özel

filtreler kullanarak, anahtar kelime araması ve dosya imza dosyaları oluşturarak mantıksal bir kopya alabilmektedir. Önyükleme istemcisi kullanılarak sabit diski çıkarmadan MAC bilgisayardan kopya alabilmektedir. Beş adet kaynaktan dokuz adet sürücüye aynı anda kopya alabilmekte ve doğrulama yapmaktadır. İsteğe bağlı abonelik ile OneDrive, GoogleDrive ve Dropbox dosyalarının uygun şekilde yakalanmasını ve Apple iPhone'lar, iPad'ler, Android telefonlar ve tabletler dahil olmak üzere mobil cihazlardan potansiyel kanıt verilerini almayı sağlamaktadır(Falcon 2022). Güncel bağlantıları şekillerini desteklemektedir. Cihaz paket halinde satılmakta ve imaj alınabilecek medyalara uygun kabloları bulunmaktadır (Şekil 3.2). Belirtilen özellikler yanında Adli Bilişim incelemelerine yönelik başka özellikleri de bulunmaktadır.

Şekil 3.2. Forensic Falcon Neo (User Manuel)

3.1.1.2. Tableau Tx1

Amerika'da kurulu bulunan OpenText firması tarafından geliştirilen birebir kopya alma cihazıdır. Dokunmatik ekran üzerinden kullanılmaktadır(TX1 2022). Tüm dosya sistemlerini görüntüleme, belirli klasörleri ve dosyaları manuel olarak seçme veya önceden tanımlanmış ve özel kriterler kullanarak hedeflenen bir arama özellikleri vardır. Şifrelenmiş diskleri ve sürücüleri algılama özelliği vardır. Kit olarak satılmakta olup kopya almak için uygun ekipmanlar bulunmaktadır (Şekil 3.3).

Şekil 3.3. Tableau Tx1(User Manuel)

3.1.1.3. Tableau TD2u

OpenText firması tarafından geliştirilen tuş takımı üzerinden kontrol edilen imaj alma cihazıdır. Sabit diskler ve diğer veri tutan materyallerden, imaj alınmasını saglamaktadır. Basit bir kullanımı vardır. Bilişim incelemeleri için kullanılan imaj formunda kopya alabilmektedir. Hızlı bir şekilde imaj alma özelliği vardır. Kit halinde bulunmaktadır. Çok çeşitli kablo desteği bulunmaktadır. Kablolar ve dönüştürücüler bağlantı yapılarak farklı bağlantı tiplerindeki cihazlardan kopya alabilmektedir. Çoğu saha birimlerinde TABLEAU cihazına ait kopya alma donanımı bulunmaktadır (Şekil 3.4).

Şekil 3.4. Tableau Td2u

3.1.1.4. Image MASSter Solo 5

Amerika'da kurulu bulunan ICS firması tarafından geliştirilen birebir kopya alma cihazıdır. ICS tarafından geliştirilen adli bilişim ürünleri, ABD'deki ve dünyanın diğer bölgelerindeki çeşitli kolluk kuvvetleriyle yakın istişare ve işbirliğinin sonucudur(ics 2022). Dakika da 69 GB'a kadar hız ile PCI kaynaktan PCI sürücüye kopya alabilmektedir. Toplam 17 giriş çıkış bağlantı noktasıyla Solo 5 Enterprise, 16 adede kadar depolama cihazının eşzamanlı olarak çoğaltılmasını destekleme yeteneğine sahiptir. LinkMASSter Seçeneği, adli araştırmacının ethernet arabirimini kullanarak açılmamış bilgisayarlardan veri almasına olanak tanır. Verileri kopyalamadan önce Word, Excel, PDF, metin veya multimedya (resim, video ve ses) dosyalarının ön izlemesine olanak tanır. 3. Parti Cep Telefonu Edinme Yazılım ve Donanım çözümlerini kullanarak Cep Telefonu verilerini almak için kullanılabilir (Şekil 3.5). Üniteler, Micro Systemation XRY ve Paraben'in Cihaz Ele Geçirme Cep Telefonu Toplama Çözümlerini destekler (Solo 2022).

Şekil 3.5. Image MASSter Solo 5

3.1.1.5. Data Copy King II

Çin'de bulunan Salvation Data firması tarafından geliştirilen birebir kopya alma cihazıdır (Data Copy 2022). Çok işlevli yazma koruma özelliği bulunan depolama sürücüleri ile donatılmış hem saha hem de laboratuvar uygulamaları için tasarlanmış taşınabilir bir imaj alma cihazıdır (Şekil 3.6). Yaygın depolama aygıtlarına çözüm sağlar. Birebir kopya alma ve wipe yapma işlemlerini yapmaktadır. Sağlam disklerin kopyalanabilmesiyle birlikte bozuk sektöre (bad sektör) sahip disklerden kopya alabilmektedir.

Şekil 3.6. Data Copy King II

3.1.1.6. Wiebe Tech Ditto DX A

Amerika'da bulunan CRU Data Security firması tarafından geliştirilen birebir kopya alma cihazıdır kopya alma istasyonu olarak isimlendirilmektedir(ditto 2022). Çeşitli ortam biçimleri için optimize edilmiştir. Delil içerisindeki dosyaları mantıksal görüntüleme zaman ve yer tasarrufu açısından önem kazanmıştır. Mantıksal görüntülemede önceden seçilmiş arama özelliklerine sahiptir. Ağ kablosu ile uzaktan kopya alma özellikleri de bulunmaktadır. Bilinen yaygın materyaller üzerinden kopya alabilmektedir. İmaj türlerini desteklemektedir. Kit halinde bulunmakta ve gerekli araçlar kit içerisinde bulunmaktadır (Şekil 3.7).

Şekil 3.7. Wiebe Tech Ditto DX A (difose.com.tr)

3.1.1.7. BeeCube

Almanya'da bulunan mh Service GmbH firması tarafından geliştirilen birebir kopya alma cihazıdır. Serisinin en küçük adli çözümüdür. Özellikle çok az alana sahip operasyonlar için tasarlanmıştır. Dijital kanıtları kaydetmek için tüm özellikleri içerir (BeeCube 2022). Adli görüntüler oluşturma işlemi kolaylaştırılmıştır. OxyCube: Önceden yüklenmiş Oxygen Forensics yazılımıyla, CellCube: önceden yüklenmiş Cellebrite yazılımı ile MOBILedit Forensic Express yazılımı önceden yüklenmiş olan MOBILedit Cube, Belkasoft Kanıt Merkezi önceden yüklenmiş Belkasoft yazılımıyla kullanılabilecek konfigürasyonları vardır. Standart özelliklerin yanında firmanın cihazları ayrı ayrı yapılandırma seçeneği de sunmaktadır (Şekil 3.8).

Şekil 3.8. BeeCube (User Manuel)

3.1.2. Yazma Koruma Cihazları

Deliller üzerinde ön inceleme yapmak için veya delillerin imajını almak için veya imajı alınan disk içerisindeki kopyaları inceleme bilgisayarına kopyalamak için bilgisayara bağlanması gerekir. İnceleme bilgisayarına bağlandığında iletişime geçeği delil üzerine veri yazması durumunda hash değeri değişmekte ve delil bütünlüğü bozulmaktadır. İnceleme bilgisayarlarına dahili veya harici bağlanan yazma koruma ekipmanları sayesinde bunun önüne geçilmektedir. Yazma koruma ekipmanları bağlanan cihaza veri gitmesini engellemekte sadece veri okuması yapmaktadır. Delil güvenliğinin sağlaması için mutlaka yazma koruma (write blocker) kullanılmalıdır. OpenText firmasının Tableau markası ile, CRU firmasının WiebeTech markası ile ve Logicube firmasının Bay-mount markası ile ve çeşitli firmaların farklı farklı yazma koruma ekipmanı bulunmaktadır. Delillerin incelendiği profesyonel oluşturulmuş laboratuvarlarda inceleme bilgisayarlarında bulunmakta ve delillere bir bit bile veri gitmeden inceleme yapılmakta ve veri bütünlüğü korunmaktadır.

3.1.2.1. Difose wb1

Türkiye'de Ankara Çankaya'da kurulu bulunan DIFOSE firması tarafından geliştirilen yazma koruma cihazıdır (Şekil 3.9). Olay inceleme ve kanıt toplama uzmanı deneyim ve görüşleri ile tasarlanıp üretilmiştir(Difose 2022). Şüpheli sürücülerin adli kopyalarını, sabit disk ve bellek kartlarından bir bilgisayar yardımıyla alan yazma koruma donanımıdır. Canlı araştırmalar için de kullanılabilmektedir. Sistem açıldığında tüm veri yollarının salt okunur olması nedeniyle, veri depolama cihazında yanlışlıkla değişiklik yapılması bile mümkün olmamaktadır. DIFOSE WB1, inceleme bilgisayarının USB 3.0 portuna takılarak çalışabilmektedir. USB 3.0 veri yolunu kullanan SATA ve PATA HDD'lerin, USB depolama aygıtlarının ve tüm hafıza kartlarının adli kopyası (imaj) alınabilmektedir.

Şekil 3.9. Difose Wb1 (User Manuel)

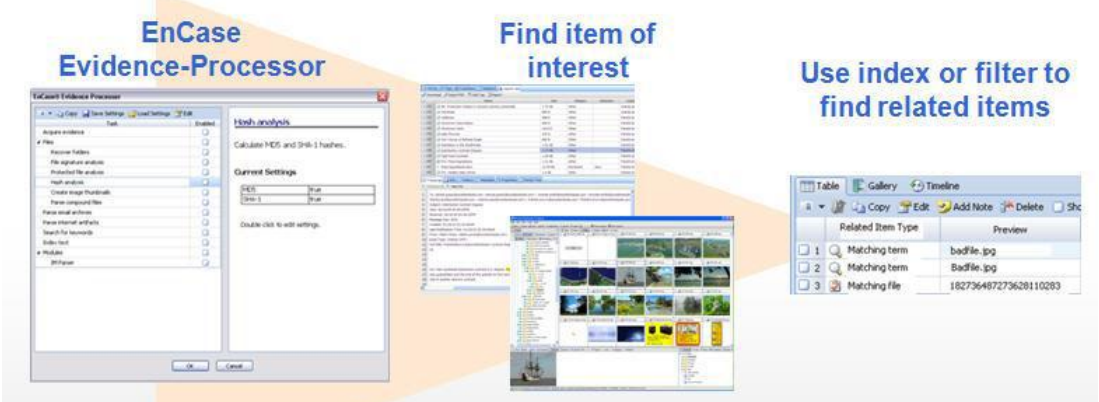
3.1.3. Adli İncelemelerde Kullanılan Çok Fonksiyonlu Yazılımlar

Dosya ve disk boyutlarının artması adli bilişim uzmanları açısından zorluk oluşturmaktadır. 2 terabayt kapasiteli bir disk içerisinden ufak bir resim, ses, video

dosyası veya ufak bir yazı istenebilmektedir. Çok fonksiyonlu yazılımlar adli incelemeleri kolaylaştırmakta ve hata payını azaltmaktadır. Yazılımların çeşitli sürümleri ve eklentileri olabilmektedir. Bazı özelliklere üçüncü parti yazılımlar sayesinde sahip elde edebilmektedirler. Yazılımların tamamı çok kapsamlı inceleme özelliklerine sahiptir. Yazılımların tamamı veya bir yazılımın tüm özellikleri anlatılmayacak yazılımların genel özellikleri anlatılacaktır. Yazılımlar anlatılan özelliklerle sınırlı değildir.

3.1.3.1. Encase Forensic

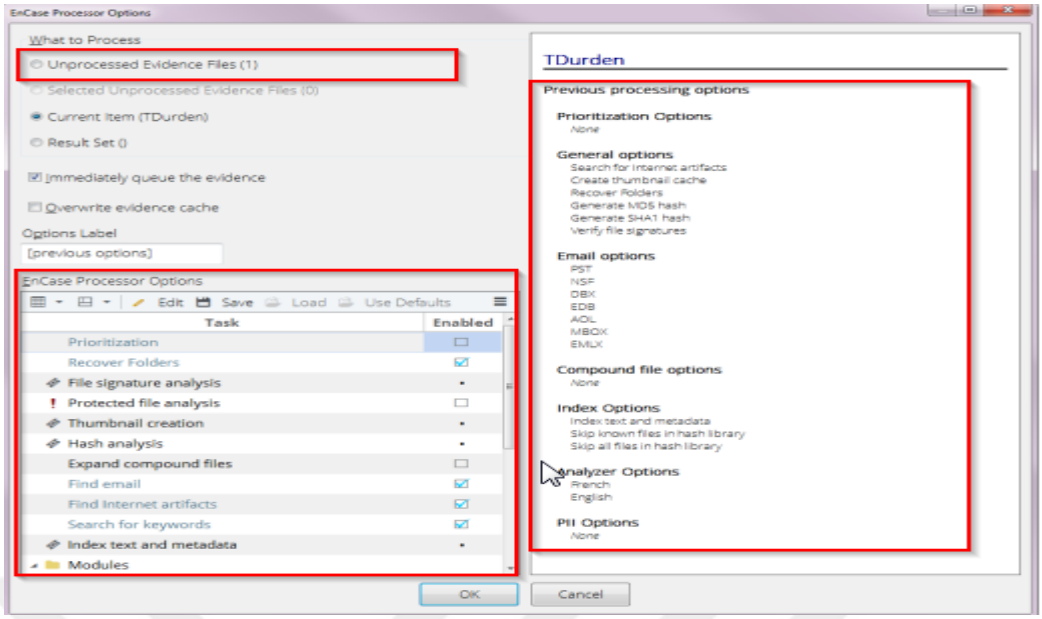
Amerika'da kurulu bulunan OpenText (Guidance) firması tarafından geliştirilmektedir. En yaygın kullanılan adli bilişim programlarından biridir. Kapsamlı bir adli bilişim inceleme yazılımdır. Akıllı cihazlar üzerinde de inceleme yapabilmektedir. Delillerin incelenmesi sonucu ayrıntılı raporlama yapabilmektedir (EnCase 2022). Kullanıcının işlemlerini kolaylaştırmak için 8.07 versiyonunun 780 sayfalık kullanım kılavuzu bulunmaktadır. Etkin bir inceleme ara yüzü vardır. Sürekli yenilenmekte ve yeni gelişen durumlara göre güncellemeler yapılmaktadır. Çeşitli dosya sistemi ve dosya türlerini destekleme özellikleri ile çok fonksiyonlu bir yazılımdır (Şekil 3.10).



Şekil 3.10. Encase Forensic (User Manuel)

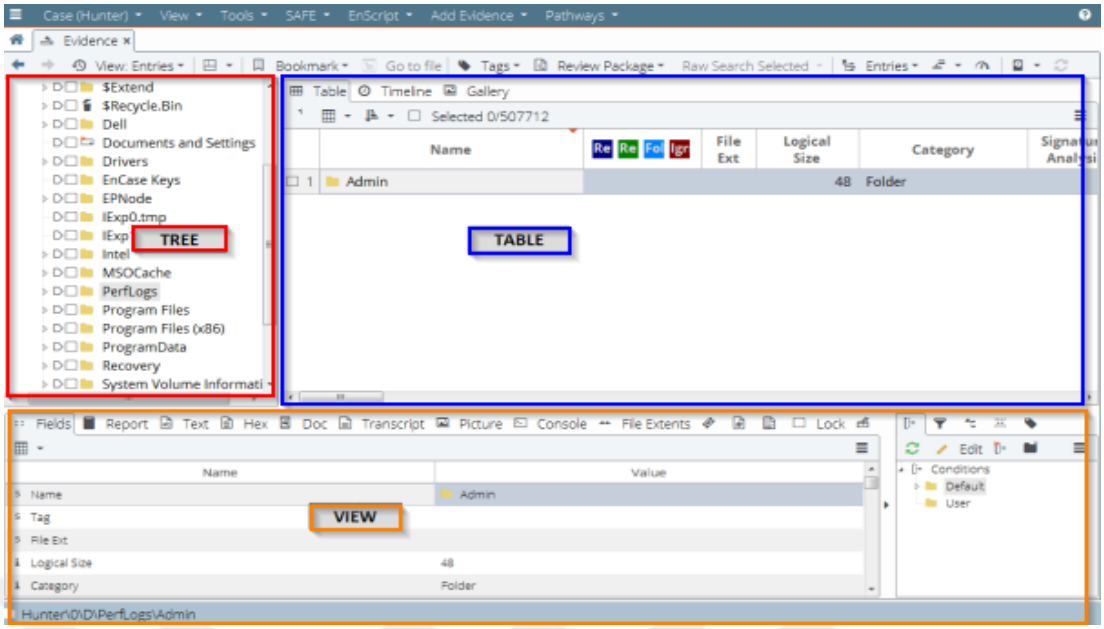
Çeşitli medya veya kopya ekleme yöntemleri vardır. Desteklenen cep telefonları kopyaları alınabilir ve incelenebilir. Telefon kopyası alma ve bulut'tan Kimlik doğrulama belirteçleri olması koşuluyla Facebook, Google veya Twitter'dan kullanıcının hesap kimlik bilgilerini alabilmektedir. Sosyal medya yapı desteği ile daha fazla kanıt ortaya çıkarma ve doğrudan şüphelinin tarayıcı geçmişinden ayrıştırılan çevrimiçi içeriği inceleme yeteneği de dahildir. Sosyal medya yapı desteği, Twitter, Instagram, LinkedIn ve Facebook'u içerir (open text 2022).

Normal kullanıcıları göremedikleri HPA ve DCO alanlarına ATA-6 disklerde erişebilmekte ve üzerinde inceleme yapılabilmektedir. Yaygın dosyalama türlerinin hepsini desteklemektedir. RAID ve Linux sistemler üzerinde inceleme yapabilmektedir. Raw imajları sürükle bırak yöntemiyle ekleyerek varsayılan ayarları kullanarak üzerine çalışma seçeneği vardır. İş akışını kolaylaştırmak için procesler kaldırılabilir, eklenebilir çeşitli şekillerde düzenlenebilir. Düzenleme delilin durumu, boyutu, içeriği, dosyanın konusuna göre değişiklik gösterebilir. Bir iş akışı yapıldığı zaman bize tasarruf sağlamaktadır. Klasörleri kurtarma (Recovery Folders), Dosya imza analizi (File signature analysis) ve şifreli dosyaların tespit edilmesi (Protected file analysis) özelliği bulunmaktadır. Arşiv dosyalarını açma özelliği bulunmaktadır. Email arama, internet kayıtları arama, anahtar kelime arama, sistem bilgilerini ayrıştırma, anlık mesajlaşma, dosya kurtarma ve daha fazla işlemi process olarak çalıştırabiliriz. Şekil 3.11'de process seçenekleri gösterilmiştir.



Şekil 3.11. EnCase Process (User Manuel)

EnCase'in, Tree (Ağaç) bölmesi, Table (Tablo) bölmesi ve View (Görünüm) bölmesi olmak üzere üç bölümü vardır. Şekil 3.12'de gösterilmiştir. Ağaç bölmesindeki seçimler Tablo bölmesini etkiler. Tablo bölmesindeki seçimler Görünümü etkiler. Bölme modu düğmesi ile ekran bölmelerinin yapılandırılma şekli değiştirilebilir. Ağaç görünümü, imajı standart bir hiyerarşik klasör yapısında sunar. Sadece dosyalar ve içerdikleri klasörler bu görünümde görüntülenir. Ağaç ve Tablo bölmesi birleştirilip TRAEBLE ismiyle kullanılabilir.



Şekil 3.12. EnCase Bölümleri

Tablo bölmesinde baktığımız dosya ile ilgili çok kapsamlı bilgiler bulunmaktadır. Bilgiler sütun şeklinde bulunur. Bu bilgiler;

-**Name**, dosya / klasör / birim vb. kanıt dosyasında ismi

-**Tag**, kullanıcı tarafından bir girişe yerleştirilen etiket (ler) i görüntüler.

-**File Ext**, dosyanın uzantısıdır.

-**Logical size**, işletim sistemindeki dosya boyutunu belirtir.

-**Item Type**, Girdi (dosya veya klasör), E-posta, Kayıt veya Belge. Bu sütun varsayılan olarak gizlidir.

-**Category**, dosya türü tablosundan dosyanın kategorisini gösterir.

-**Signature Analysis**, bir dosya imza analizinin sonuçlarını görüntüler.

-**Signature**, bir eşleşmenin veya bir takma adın (yeniden adlandırılmış uzantı) imzasını imza analizinden görüntüler.

-**Protected**, kanıt işleme sırasında dosyanın şifrelenmiş veya parola korumalı olarak tanımlanıp tanımlanmadığını gösterir.

-**Protection Complexity**, dosyanın korunması hakkında ayrıntılı bilgi sağlar.

-**Last Accessed**, dosyaya erişildiği son tarihi / saati görüntüler. İşletim sistemi veya uyumlu herhangi bir uygulama dosyaya en son erişildiğinde (görüntüleme, sürükleme veya sağ tıklatma gibi). FAT birimlerindeki girdilerin son erişim zamanı yoktur.

-**File Created**, dosya / klasörün o konumda oluşturulduğu tarihi / saati yansıtır.

-**Last Written**, dosyanın en son açıldığı, düzenlendiği ve kaydedildiği tarih / saati yansıtır.

-**Is Picture**, dosyanın resim olup olmadığını gösterir.

-**Is Indexed,** öğenin işleme sırasında dizine eklenip eklenmediğini gösterir.

-**Code Page,** dosyanın dayandığı karakter kodlama tablosunu görüntüler.

-**MD5**, karma analiz işlemi tarafından oluşturulan bir dosya girişi için 128 bitlik bir değer görüntüler.

-**SHA1**, karma çözümleme işlemi tarafından oluşturulan bir dosya girişi için SHA1 karma değerini görüntüler.

-**Entropy**, entropi analizi işlemi tarafından oluşturulan bir dosya girişi için entropi değerini görüntüler.

-**From,** gönderen e-posta mesajını görüntüler. Bu sütun varsayılan olarak gizlidir.

-**Recipient,** alıcı, e-posta iletisinin alıcısını görüntüler. Bu sütun varsayılan olarak gizlidir.

-**Primary Device**, kullanılan birincil aygıtı görüntüler. Bu sütun varsayılan olarak gizlidir.

Item Path, imaj da dahil olmak üzere imaj dosyası içindeki dosyanın dosya adı ve birim tanımlayıcısı konumunu tanımlar

-**Description,** girdinin durumunu açıklar: bir dosya veya klasör olup olmadığı, silindiği veya silindi / üzerine yazıldı.

- **Is Deleted,** girdinin silinip silinmediğini gösterir.

-**Entry Modified**, dosyanın yönetim verilerinin NTFS ve Linux' da en son ne zaman değiştirildiğini gösterir.

-**File Deleted,** dosya Geri Dönüşüm Kutusu'nun Info2 dosyasındaysa silinen tarih / saati görüntüler.

-**File Acquired,** bu girdinin bulunduğu imaj dosyasının alındığı tarih ve saattir.

-**Initialized Size,** açıldığında dosyanın boyutunu gösterir. Yalnızca NTFS ve exFAT dosya sistemleri için geçerlidir

-**Physical Size,** dosyaya ayrılan depolama alanlarının boyutunu belirtir.

-**Starting Extent**, girdinin başlangıç kümesini tanımlar.

-File Extents, dosyaya ayrılan küme parçalarını görüntüler. Önce sütuna tıklanır sonra sonra küme parçalarını görmek için Görünüm bölmesindeki Dosya Kapsamları sekmesini tıklanır.

-Permissions, Görünüm bölmesinde bir dosya veya klasörün güvenlik ayarlarını gösterir.

-Physical Location, bir girdinin verilerinin başladığı aygıta bayt sayısını görüntüler.

-**Physical Sektör,** girdi verilerinin başladığı aygıta sektör numarasını listeler.

-Evidence File, girdinin bulunduğu yeri gösterir.

-File Identifier, bir Ana Dosya Tablosu (NTFS) veya bir İnode Tablosu için dizin numarası görüntüler(Linux / UNİX).

-GUID, inceleme boyunca izlemeyi etkinleştirmek için girişin Genel Benzersiz Tanımlayıcısını belirtir.

-Hash SetNames, bir dosya bir veya daha fazla karma kümeye aitse, Boole değerini true olarak görüntüler. Bu sütun varsayılan olarak gizlidir.

-Short Name, DOS 8.3 adlandırma kuralını kullanarak Windows'un girdiye verdiği adı görüntüler.

-VFS Name Windows Gezgini'nde EnCase Sanal Dosya Sistemi (VFS) modülüyle birleştirilmiş dosyaların adını görüntüler. Bu, Encase'in önceki sürümlerindeki Benzersiz Ad sütununun yerini alır.

-Original Path, verilerden elde edilen bilgileri Geri Dönüşüm Kutusu'nda görüntüler. Bu sütun, Geri Dönüşüm Kutusu'ndaki dosyaların silindiklerinde nereden kaynaklandığını gösterir. Silinen / üzerine yazılan dosyalar için bu sütun orijinalin üzerine yazılan dosyayı gösterir.

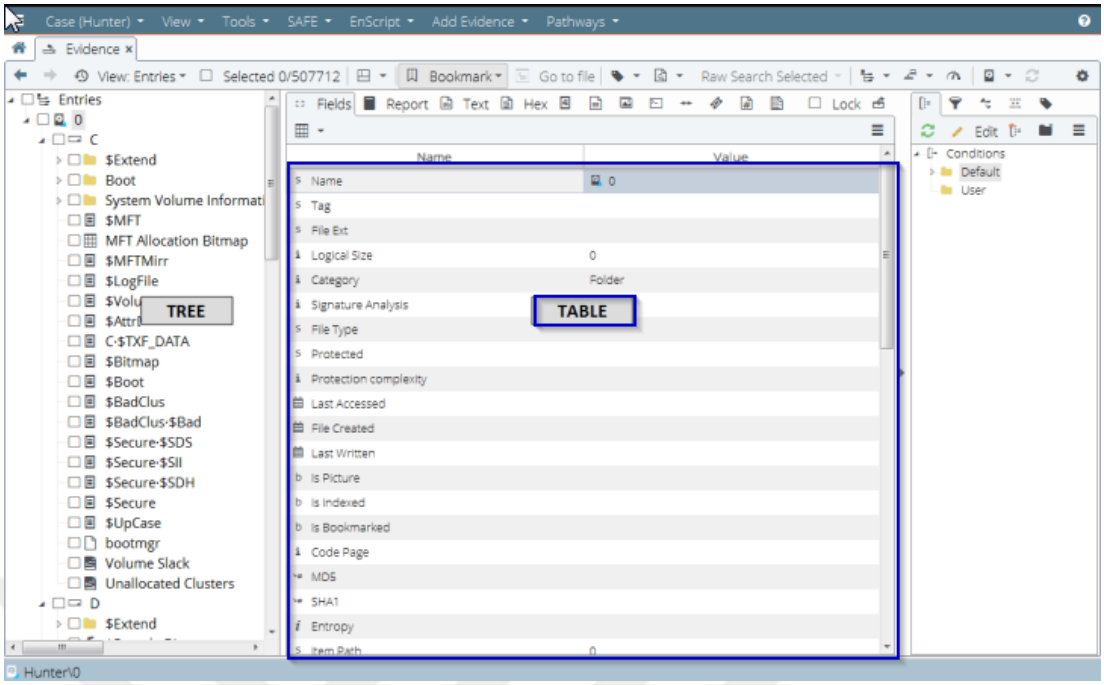
-Sembolik Link, Linux ve Unix'te bir Windows Kısayoluna eşdeğer verileri görüntüler.

-Is Duplicate, dosya diğerinin bir kopyasıysa True (Evet) değerini görüntüler.

-Is Internal, dosyanın NTFS birimindeki $MFT gibi dahili bir sistem dosyası olup olmadığını gösterir.

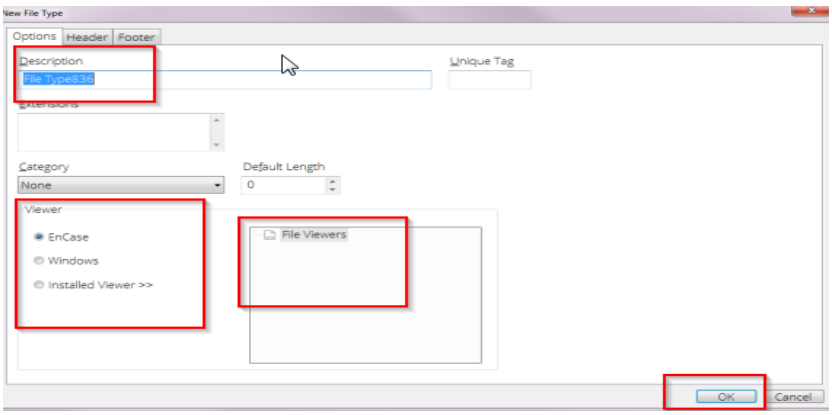
-Is Overwritten, bir girdinin ilk veya daha fazla kümesinin sonraki bir nesne tarafından üzerine yazılıp yazılmadığını gösterir.

Tablo penceresinde bulunan verileri süzülebilir bazıları gizlenebilir kullanıma göre ayarlanabilir (Şekil 3.13).



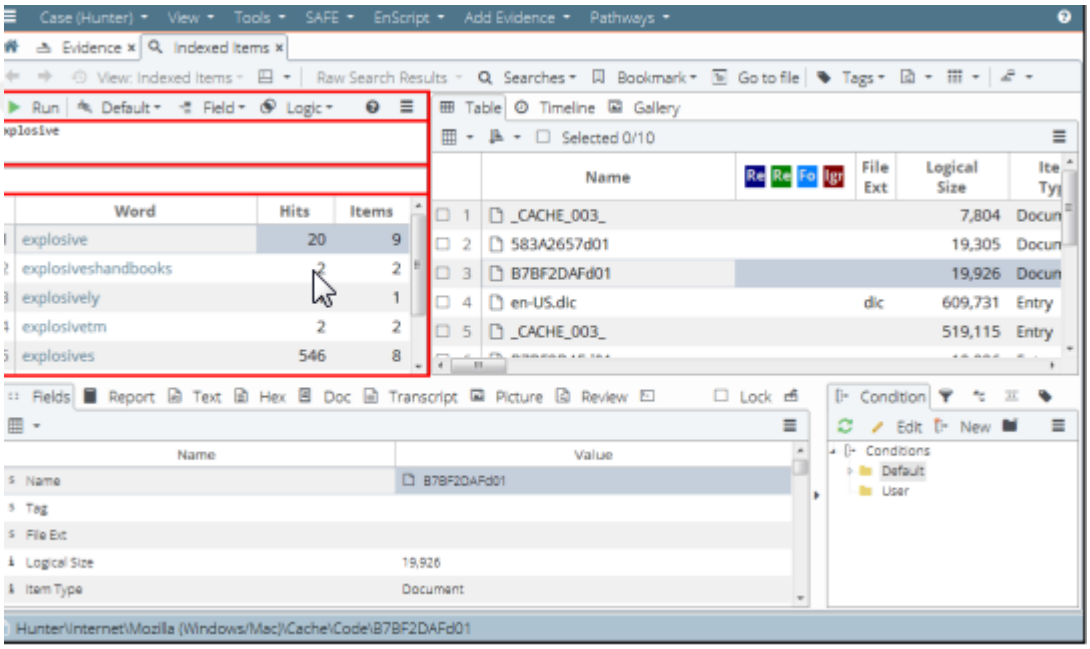
Şekil 3.13. EnCase Tablo Bölümü

Görünüm bölmesinde durum çubuğu dosya hakkında fiziksel adres, mantıksal adres, küme numarası, boyutu gibi ek bilgileri göstermektedir. Görünüm bölmesinde üzerinde çalışılan dosyalar ön izlemek için açılmakta bazıları açılmamaktadır. Açılmayan dosyaları ön izlemek için viewer (görüntületici) ayarlarının yapılması ve görüntüleyici programların yüklenmesi gerekmektedir. Görünüm menüsünden Dosya Türleri seçilir, dosya türleri sekmesi görüntülenir. Yeni tıklanır ve yeni dosya türü iletişim kutusu görüntülenir (Şekil 3.14). Bilgiler girilerek yeni görüntüleyici eklenir.



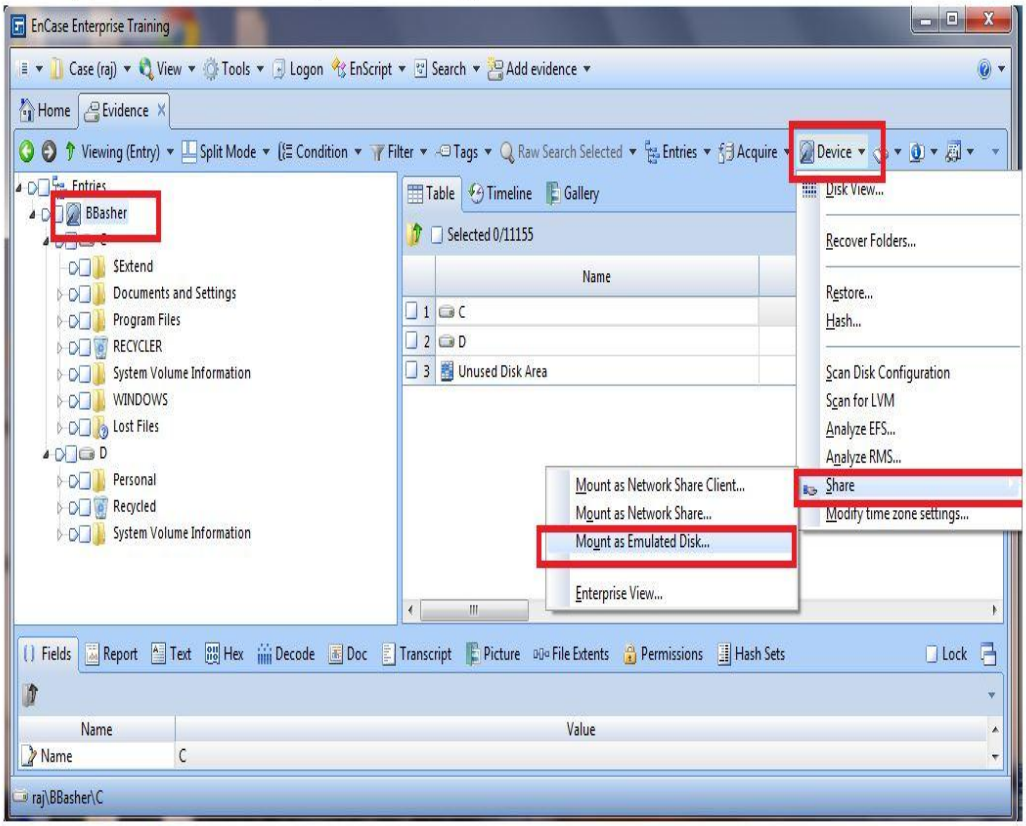
Şekil 3.14. EnCase Yeni Görüntüleyici Ekleme

İndeksleme özelliği sayesinde diskin tamamı indekslenerek indeks search yapılabilir. İndeksleme bakılarak süzülebilir. İndeks search arama sonuçlarından orijinal dosya tespit edilebilir. İndekslenmiş veriler arasında istediğimiz kelime, dosya metni veya meta veri aranabilir (Şekil 3.15). Sorgu bölümünden verilere bakılabilir. Sorgu dili değiştirilebilir. Kelime araması yapılabilir veya daha karmaşık sorgular yapılabilir. Sorgu sonucu isabet sayısı ve öge sayısı birlikte görüntülenir. Process işlemi haricinde ayrıca Raw Search yapılabilir.



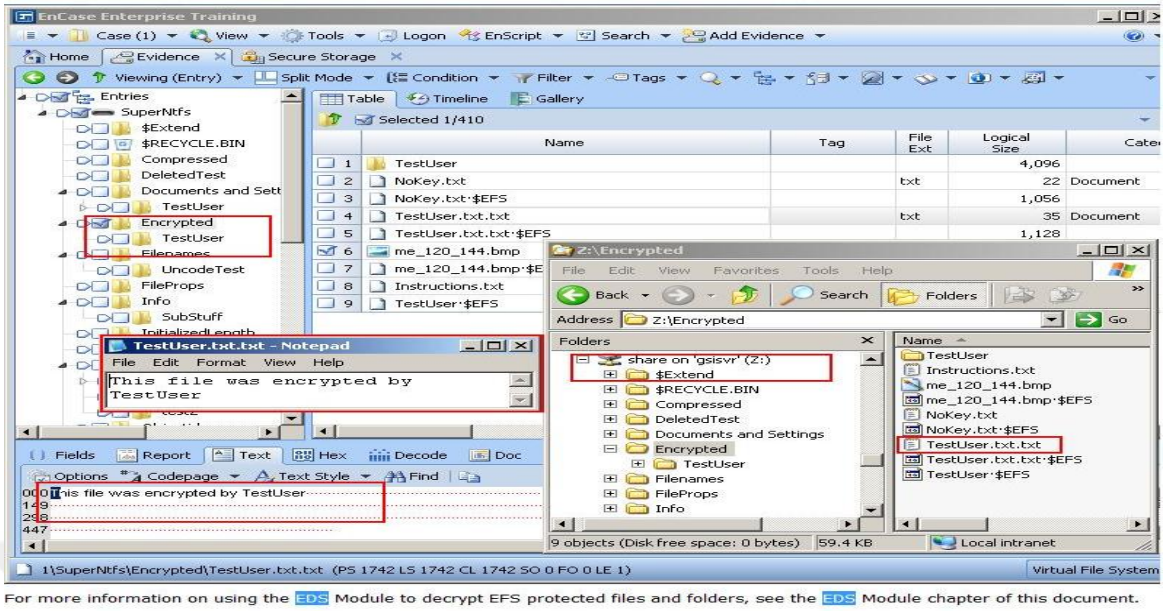
Şekil 3.15. EnCase indeks Search (User Manuel)

Fiziksel diskler, sabit disk bölümleri, E01, EX01, VMDK, L01, LX01 ve VHD uzantılı imaj dosyaları inceleme yapılabilir. PDE (fiziksel disk emule etme) özelliği bulunmaktadır. Fiziksel disk emule edilerek virus, malware vb. incelemeler yapılabilir (Şekil 3.16).



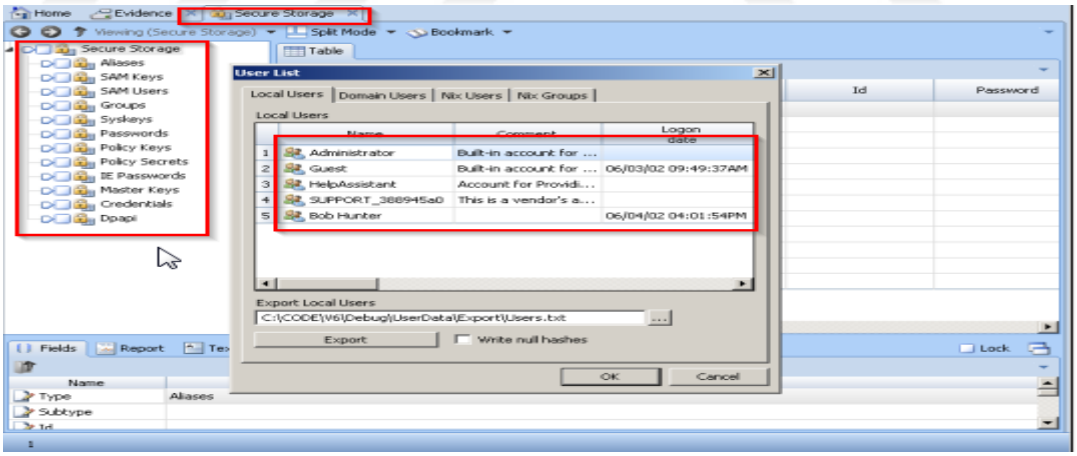
Şekil 3.16. EnCase PDE (User Manuel)

VFS-Virtual File System (sanal dosya sistemi) inceleme özelliği bulunmaktadır. VfS'yi EnCase ile birlikte kullandığınızda şifresi çözülmüş dosyaları Windows'ta görüntüleyebilirsiniz. Şifre Çözme Paketi (EDS) ile şifresi çözülmüş dosya ve klasörleri içeren kanıtları monte edebilirsiniz. Şifresi çözülmüş verileri Windows Gezgini'nde veya üçüncü taraf araçlarıyla görüntülemek için VFS ile EDS (şifre kırma) özelliği ile desteklediği şifreleme algoritmaları şifresini bulmaktadır. VFS ve EDS ile birlikte kullanıldığında şifrelenmiş bir delil dosyası çözümü Şekil 3.17'de gösterilmiştir.



Şekil 3.17. EnCase VFS-PDE (User Manuel)

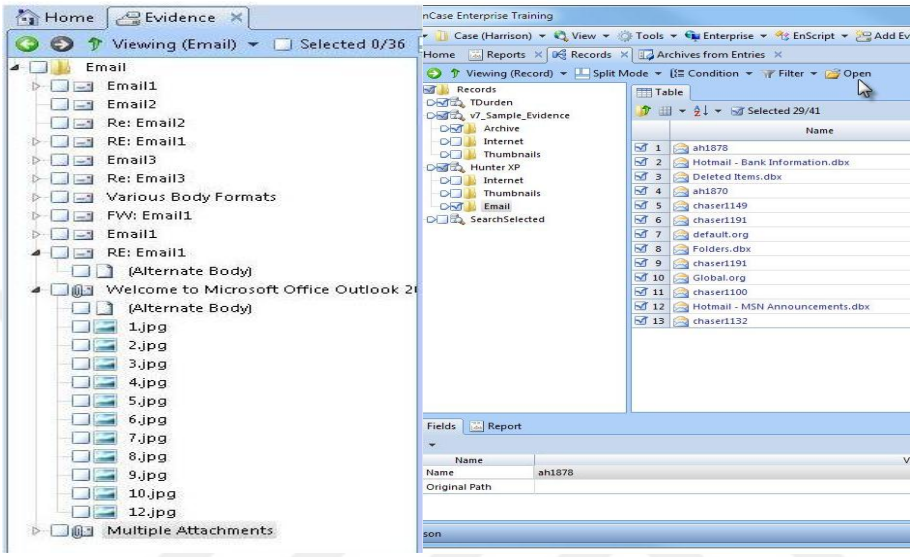
Windows şifresinin tutulduğu dosyayı dışarı aktararak şifre kırma hususunda kullanılmaktadır (Şekil 3.18).



Şekil 3.18. EnCase Secure Stroage (User Manuel)

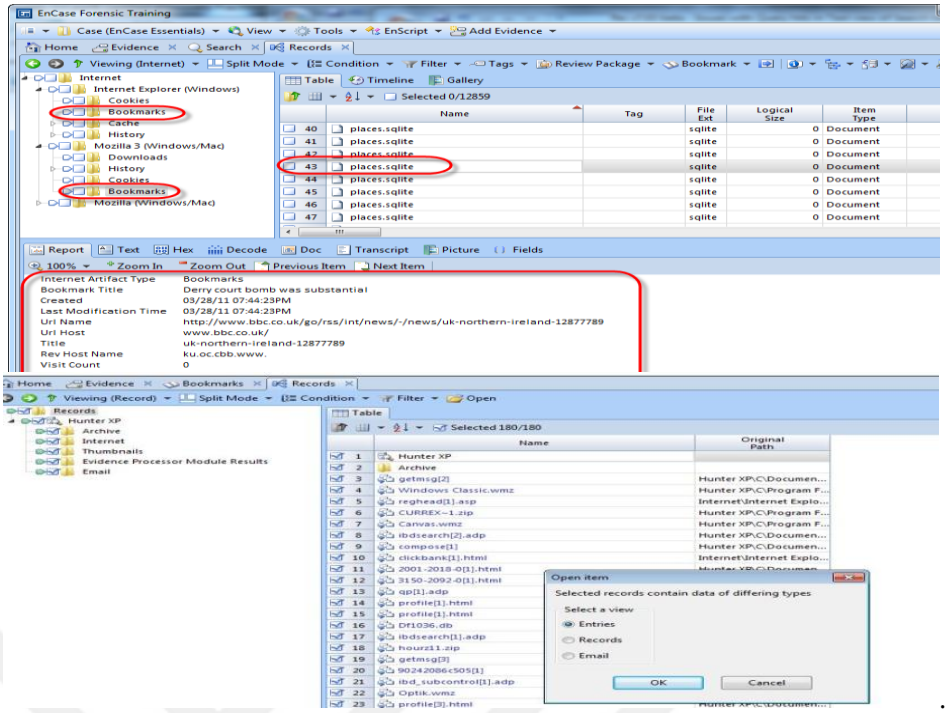
View sekmesinden Record özelliğinden arşiv dosyalarına bakılabilir. Sayısal dosya imzası analizi (Hash analysis) özelliği sayesinde hash kütüphanesinde bulunan dosyalar ile incelen dosyalar mukayese edilebilir. Yeni hashsetler eklenebilir ve

incelemeler esnasında faydalanılabilir. Hashset işlemi binlerce dosya arasından aradığımız hashsetine sahip dosya varsa bulmamıza yardımcı olmaktadır. E-posta bulma (Find email) özelliği kullanılarak desteklediği e-postalar tespit edilerek incelenebilir (Şekil 3.19).



Şekil 3.19. EnCase E-Posta

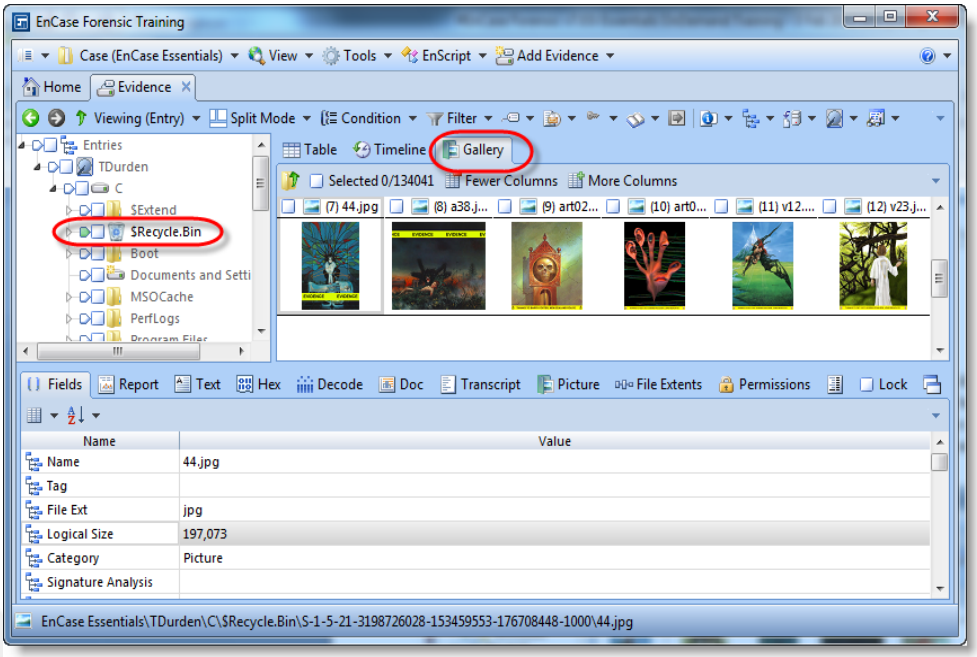
İnternet geçmişi tespiti (find internet artifacts), Internet Explorer, Macintosh Internet Explorer, Safari, Firefox, Opera Google Chrome web tarayıcıları üzerinden yapılan internet erişim kayıtları incelenebilir. View sekmesinden Record özelliğinden internet dosyalarına bakılabilir. İnternet Sonuçlarını analiz edebiliriz (Şekil 3.20).



Şekil 3.20. EnCase İnternet Geçmişi

Anahtar kelime arama (Search for keywords) özelliği sayesinde istediğimiz kelimeyi veya ifadeyi arayabiliriz. Anahtar kelime aramayı etkinleştirmek gerekir. Standart kayıtlı kelimeler yanında istediğimiz yeni anahtar kelimeler eklenebilir ve arama yapılabilir.

İstediğimiz kelime ve ibareyi ekleyerek aratabiliriz. Çoklu anahtar kelime ekleme özelliği bulunmaktadır. Eklenen anahtar kelimeler aranması için tik konarak aktif hale getirilmelidir. Etkinleştirilen anahtar kelimeler process işlemi esnasında aratılarak sonuçlara bakılabilir. Anahtar kelime arama sonucu search menüsünden bakılarak incelenebilir. Gallery görünümü ile resim dosyaları incelemesi daha kolay yapılmaktadır (Şekil 3.21).

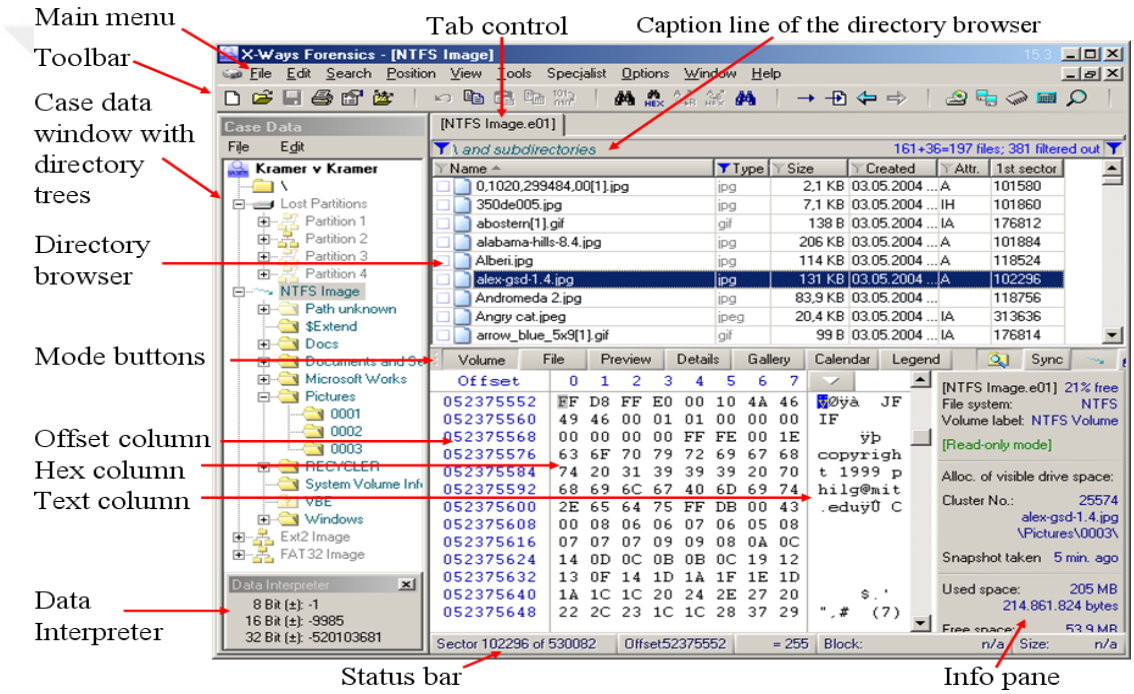


Şekil 3.21. EnCase Galeri Görünümü (User Manuel)

Bookmark özelliği ile tespit edilen dosyalar işaretlenerek raporlama esnasında kolaylıkla kullanılabilir. Dil kodlaması değiştirilerek değişik dil kodlarında veriler incelenebilir. İnceleme esnasında işletim sistemi yüklü sabit disklerin tarih saat grubuna göre inceleme yapılan programın ayarlanması gerekir. Windows kayıt defteri açılabilmekte ve analiz edilebilmektedir. Optik karakter tanıma (OCR) özelliğini bulunmaktadır. TEXT, RTF, HTML, XML, PDF olarak raporlama özelliği vardır. Teknik işlemlerin ile birlikte bazı eklentiler ile birlikte kopyalar alınabilmektedir. Kendi özellikleri ile birlikte üçüncü parti yazımlarla entegre de çalışabilmektedir. Encase'in genel özelliklerinin yanında daha kapsamlı incelemeye yönelik özellikleri vardır. En önemli özelliklerinden enscript (betik) özelliği sayesinde küçük programlar yapılarak incelemeler daha pratik hale getirilebilir.

3.1.3.2. X-Ways Forensics

Merkezi Almanya'dadır. X-Ways Software Technology firması tarafından geliştirilmiştir. Adli bilişim yazılımları ile benzer özellikler taşımaktadır. Sabit diskler, sürücüler ve medyaların mevcut ve silinmiş tüm alanları incelenebilmektedir. İndeksleme, arama yapma, internet geçmişi çıkartma, e-posta analizi, şifreli dosya tespiti gibi genel işlemlerin yanında bir sürü özelliği bulunmaktadır. Bu sistemin hızlı ve pratik kullanımı Şekil 3.22'de gösterilmiştir.



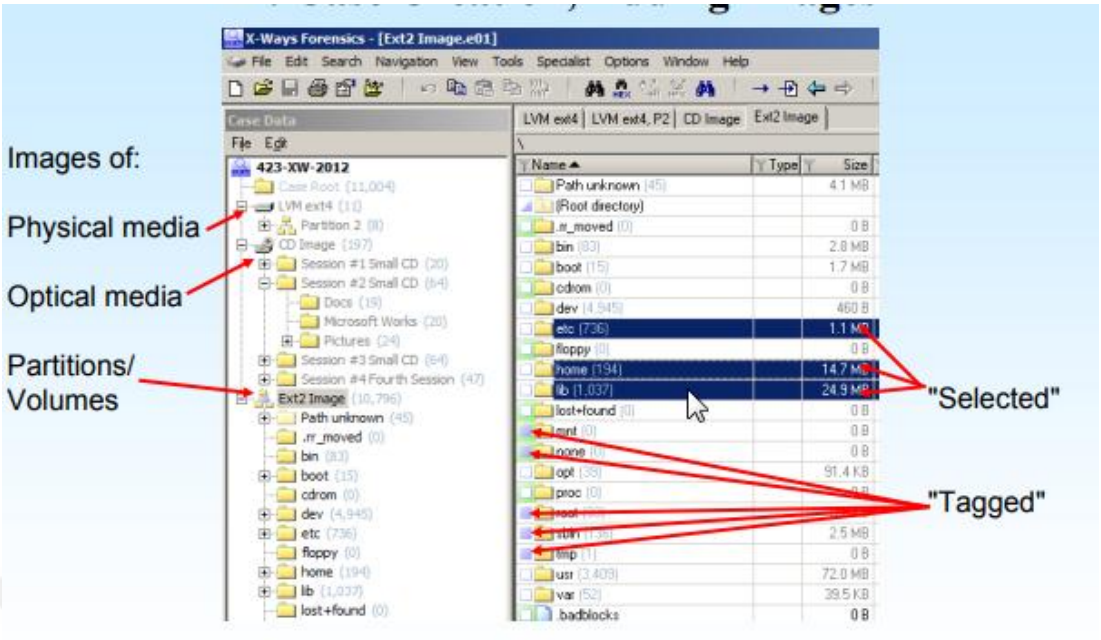
Şekil 3.22. X-Ways Kullanımı (User Manuel)

Veri kurtarma işleminde de çok başarılıdır. X-Ways Forensics tamamen taşınabilirdir ve herhangi bir Windows sisteminde kurulum yapmadan bir USB bellek ile çalışır. Saniyeler içinde indirilir ve kurulur (X-ways 2022).

Çok kapsamlı özellikleri vardır. Disk klonlama ve görüntüleme, dosya sistemi yapılarını okuyabilme, kayıp/silinmiş bölümlerin otomatik olarak tanımlanması,

orijinal diski veya görüntüyü değiştirmeden, veri bozulmasına rağmen dosya sistemlerini tamamen ayrıştırmak için düzeltilmiş bölüm tabloları veya dosya sistemi veri yapıları gibi sektörlerin üst üste getirilmesi, çalışan işlemlerin mantıksal belleğine erişim, çeşitli veri kurtarma teknikleri, dosya kurtarma, GREP notasyonuna dayalı, dosya başlığı imza veri tabanı, veri yorumlayıcısı, şablonları kullanarak ikili veri yapılarını görüntüleme ve düzenleme, adli olarak steril ortam üretmek için sabit disk temizleme, sürücülerden ve imajlardan boş alan, bölümler arası alan veri toplama, tüm bilgisayar ortamları için dosya ve dizin kataloğu oluşturma, NTFS alternatif veri akışlarının (ADS) kolay algılanması ve bunlara erişim, dosyalar için toplu hash hesaplaması aynı anda birçok arama terimi için fiziksel ve mantıksal arama yetenekleri, tüm alt dizinlerdeki tüm mevcut ve silinmiş dosyaların özyinelemeli görünümü, NTFS'deki dosya kayıtlarının yapısı için otomatik renklendirme, yer imleri/açıklamalar tespiti özelliklerine sahiptir.

F-Response ile birlikte uzak bilgisayarları analiz etme yeteneği vardır. Yaygın dosya sistemlerini desteklemektedir. Akıllı sıkıştırma seçenekleriyle üstün, hızlı disk görüntüleme, dosyaları etiketleme ve vaka raporuna dikkate değer dosyalar ekleme yeteneği vardır. Windows hesaplarına göre farklı kullanıcılar arasında ayrım yaptığı durumlarda birden fazla denetçi için destek sağlamaktadır. Kullanıcılar aynı vaka üzerinde farklı zamanlarda veya aynı anda çalışabilir ve sonuçlarını (arama isabetleri, yorumlar, rapor tablosu ilişkilendirmeleri, etiket işaretleri, görüntülenen dosyalar, hariç tutulan dosyalar, ekli dosyalar) ayrı tutabilir veya istenirse paylaşılabilir. Dosyalar için filtreleme, anlık görüntü özelliklerini bulma, dosya sistemi veri yapılarının analiz edilerek dosya izi bulmaktadır. Dizin ağacı, tüm alt dizinleri de dahil olmak üzere dizinleri keşfetme ve etiketleme yeteneği vardır (Şekil 3.23).



Şekil 3.23. X-Ways Dizin (User Manuel)

Dosya kaydı, dizin kaydı, $LogFile, birim gölge kopyası, FAT dizin girişi, Ext düğümü, gömülüyse dosya içeren vb. tanımlandığı dosya sistemi veri yapısına kolayca erişebilmektedir. Dosya sahiplerini, NTFS dosya izinlerini, nesne kimliklerini/GUID'lerini, özel nitelikleri gösterir. Tüm dahili dosya sistemi zaman damgalarını gösterebilmektedir. Dosyaların diğer dosyalar içinde de kurtarılmasını yapılabilmektedir. FuzZyDoc, farklı bir dosya formatında saklansa, yeniden formatlanmış, düzenlenmiş, olsa bile tanıma özelliğine sahiptir. PhotoDNA özelliği ile farklı bir dosya biçiminde saklansa, yeniden boyutlandırılsa, renk ayarlı, kontrast ayarlı, bulanık, keskinleştirilmiş, kısmen pikselli, düzenlenmiş dosyalar olsa bile bilinen fotoğrafları (örneğin çocuk pornografisi) tespit edilebilmektedir. Hash setlerini içe aktarabilmekte ve veri süzme yapabilmektedir. Resimlerin, videoların, belgelerin ve diğer birçok resim olmayan dosya türünün küçük resimlerini galeri görünümünde gösterebilmektedir. Tüm meta verilerle aynı dosya türlerini doğrudan program içinden yazdırabilmektedir. Windows Kayıt dosyaları için dahili görüntüleyebilme özelliğine de sahiptir. Firefox geçmişi, Firefox indirmeleri, Firefox form geçmişi, Firefox oturumları, Chrome çerezleri, Chrome arşivlenmiş geçmişi, Chrome geçmişi, Chrome oturum açma verileri, Chrome web verileri, Safari

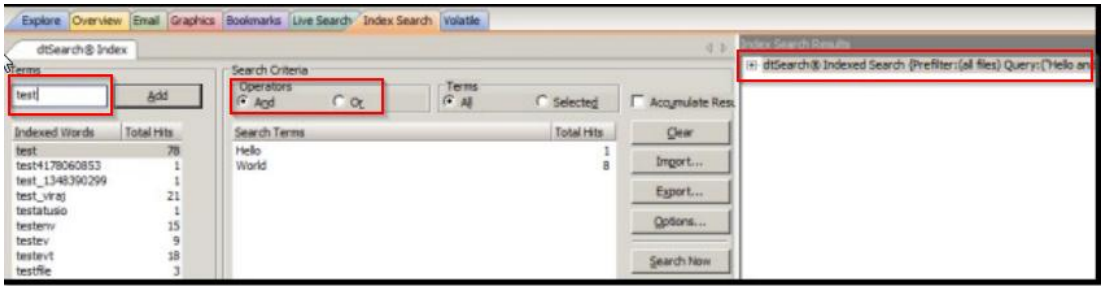
önbelleği incelenebilmektedir. Boş alanda veya boş alanda bulunan Internet Explorer geçmişini ve tarayıcı önbelleği index.dat kayıtlarını sanal tek bir dosyada toplama yeteneği vardır. Çeşitli dosya türlerinden meta verileri ve dahili oluşturma zaman damgalarını çıkarabilmekte ve bu bilgiler filtrelenebilmektedir. Yaygın e-postaları inceleyebilmektedir. Olay zaman damgaları, olayların zaman çizelgesini almak için kronolojik olarak sıralanabilir. Şifreli MS Office ve PDF belgeleri otomatik olarak tanımlanmaktadır. Ten rengi algılama (ten rengi yüzdesine göre sıralanmış bir galeri görünümü, çocuk pornografisi izlerini aramayı büyük ölçüde hızlandırır) özelliği varır. Belgelerde veya dijital olarak saklanan fakslarda taranabilecek siyah beyaz veya gri tonlamalı resimleri algılama yeteneğine sahiptir. Optik karakter tanıma OCR'lenmesi gereken PDF belgelerinin tespitini yapmaktadır. Belirtilen özelliklerin yanında daha kapsamlı özellikleri de bulunmaktadır.

3.1.3.3. AccessData Ftk

Amerika'da bulunan AccessData firması tarafından geliştirilen hız, kararlılık ve kullanım kolaylığı için üretilen adli bilişim yazılımıdır. İmajlar içerisinden aranan izleri bulmakta ve analiz etmektedir. Birden fazla imaj bir arada incelenebilmektedir. FTK, mahkemeler tarafından atıf yapılmış ödüllü bir programdır (Ftk 2022). Bilinen adli bilişim uygulamalarına ait özelliklerin çoğu bulunmaktadır. Yüz ve nesne algılama özelliği ile bir kişinin veya nesnenin tüm görüntülerini hızlı bir şekilde bulmaktadır. UFED ve XRY vaka dosyaları incelenebilmektedir. İnternet verilerini kapsamlı inceleme özelliği vardır.

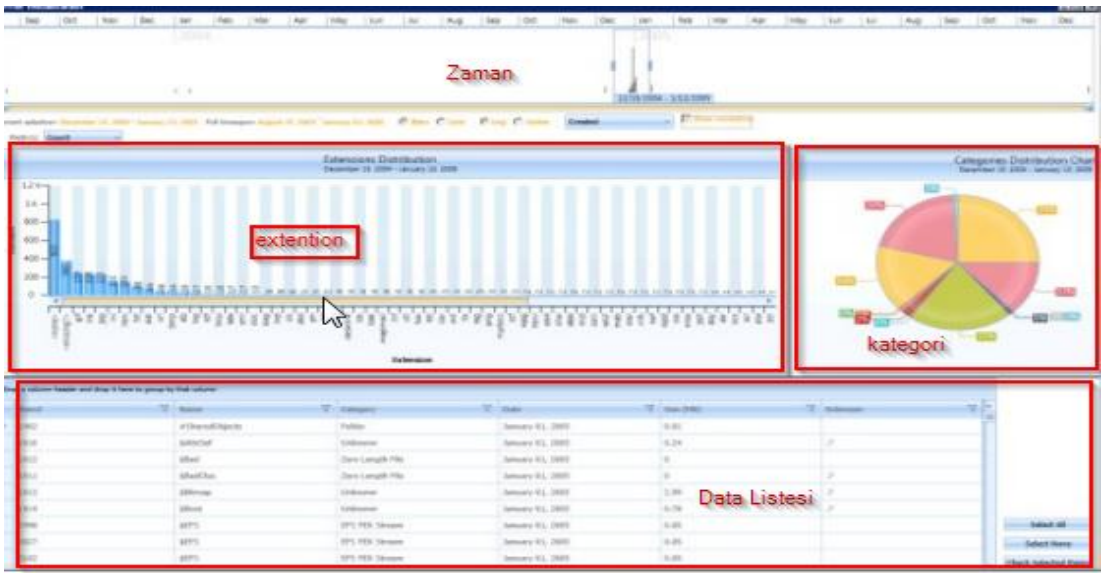
Ftk'nın en güçlü yanlarından bir tanesi de indeks arama özelliğidir. Dizin araması anlık sonuçlar verir ve metin arama ve onaltılık arama gibi modları destekler. Arama sonuçları, Arama sekmesindeki Dosya Listesinden ve Dosya İçeriği görünümlerinden görüntülenir (Şekil 3.24). İndeks süzme seçenekleri vardır.

İndekslenen dosyalar içerisinden tespit edilen veriler ve dosyalar imaj dışına export edilir (aktarılabilir).



Şekil 3.24. Ftk İndeks Search (User Manuel)

İnceleme esnasında veriler, bir kaynaktan elde edileceği gibi bir veya daha fazla kaynaktan elde edilebilmektedir. Dosya, e-posta, sosyal görselleştirme de zaman çizelgeleri, küme grafikleri dahil olmak üzere birden çok görüntüleme biçimi, pasta grafikler, coğrafi konumlar gibi özellikler vardır. Dosyaları görselleştirilerek gönderebilir. Belirli ayarlar yapılarak görsel hale getirilebilir (Şekil 3.25). Görselleştirmeyi doğru kullanmak için, verileri görüntülemek istenen temel zaman çizelgesinin belirtilmesi gerekir.

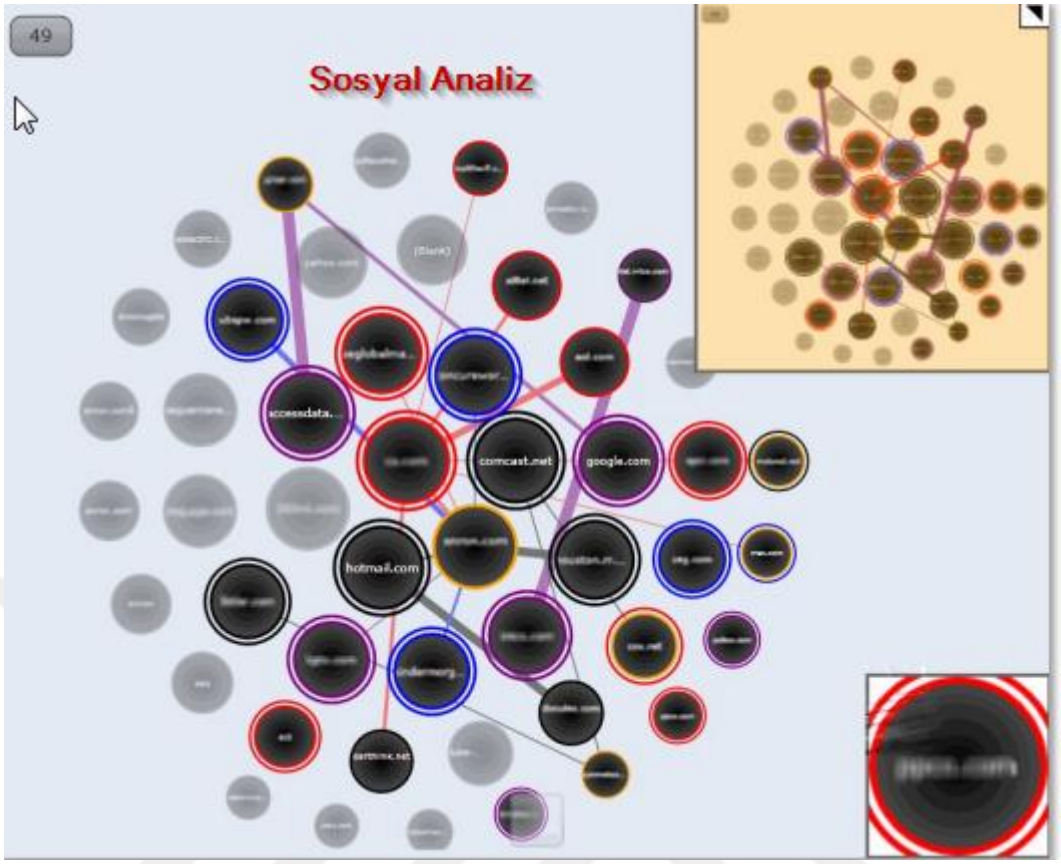


Şekil 3.25. Ftk Dosya Görselleştirme

E-posta dosyalarının görselleştirilmesi incelemeyi kolaylaştırmaktadır. Zaman çizelgesi, veri kümesinde gönderilen ve alınan e-posta öğelerinin toplu görünümünü sağlamaktadır. Ölçeklendirilebilmektedir. Kapsam ve ölçek değiştirilebilmektedir (Şekil 3.26).

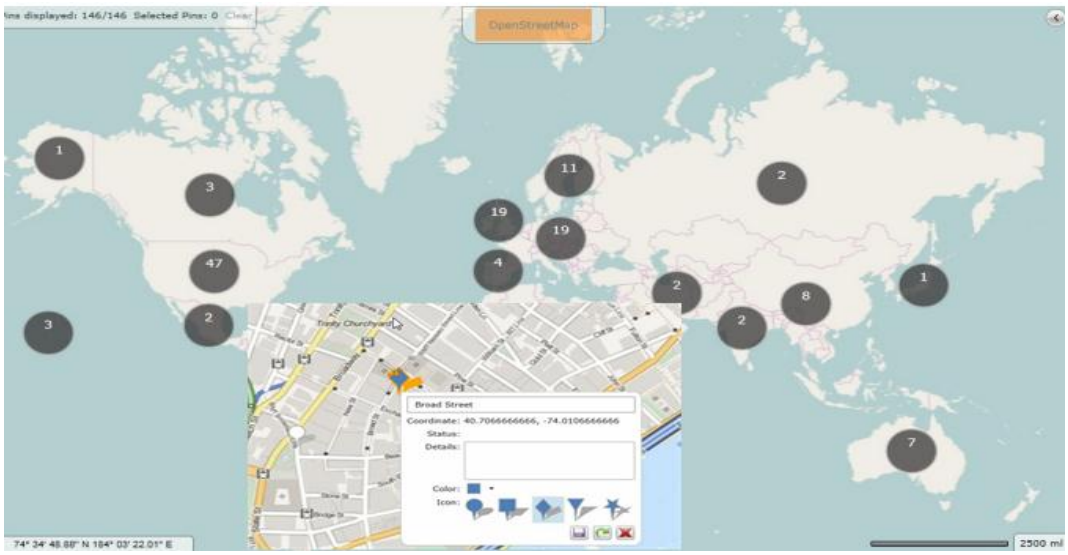
Şekil 3.26. Ftk E-Posta Görselleştirme

Sosyal Analizör, veri kümesinde bulunan e-posta hacminin görsel bir temsilini gösterir. Bir projedeki tüm e-posta etki alanlarının yanı sıra projedeki tek tek e-posta adreslerini de görüntüleyebilir. Social Analyzer haritası, veri kümesi grubundaki e-postaları etki alanı adına göre görüntüler. Bu alan adları haritada "kabarcıklar" adı verilen daireler görünür (Şekil 3.27). Küredeki merkez balonu, bu alandan gönderilen en çok e-postaya sahiptir. Merkezden saat yönünde yayılan etki alanları etki alanlarında daha az e-postaya sahiptir.



Şekil 3.27. Ftk Sosyal Analiz (User Manuel)

Coğrafi Konum, bunlarla ilişkili coğrafi konum bilgilerine sahip kanıt öğelerinin gerçek dünyadaki coğrafi konumlarına sahip bir haritayı görüntülemenizi sağlar. Bu, belirli etkinliklerin / eylemlerin nerede gerçekleştiğini anlamanızı sağlar. GPS bilgisi olan fotoğraflar ve imajlarda exif'de GPS verisi olan fotoğrafların nerede çekildiği görülebilmektedir (Şekil 3.28).

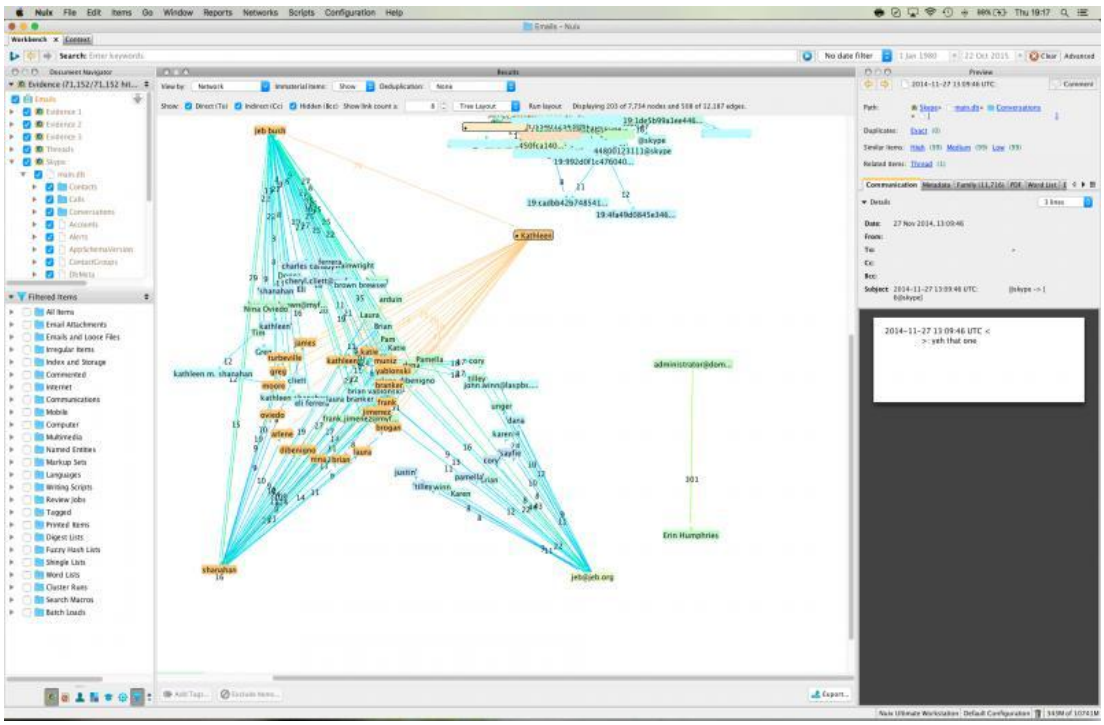


Şekil 3.28. Ftk Coğrafi Konum (User Manuel)

FTK içinde kendi Python betiği çalıştırılıp veri incelemesi yapılabilir. Ayrıntılı raporlama özelliği vardır. Desteklediği dosyalama sistemleri ve işletim sistemlerinden ayrıntılı veri kurtarma özelliği vardır. FTK, paylaşılan bir vaka veri tabanını kullanmaktadır. Veri tabanının kullanımı aynı zamanda istikrar ve tasarruf sağlar. E-posta analizi için sezgisel bir ara yüz sağlar. Belirli kelimeler için e-postaları ayrıştırma, kaynak IP adresi için başlık analizi bilgileri analiz eder. FTK'nın merkezi bir özelliği de şifre çözmedir. FTK'nın 100'den fazla uygulama için şifre çözme özelliği varır. Veri kurtarma motoru çok sağlamdır. Dosyaları boyuta, veri türüne ve hatta piksel boyutuna göre arama seçeneğine sahiptir. KFF(Bilinen Dosyaları Süzme) özelliği inceleme süresinin daha a kısaltılmasını sağlamaktadır. Cerberus eklentisi ile güçlü bir otomatik kötü amaçlı yazılım algılama özelliği vardır. Kötü amaçlı yazılımları tespit etmek için makine zekasını kullanır ve bulunursa onunla başa çıkmak için eylemler önerir. Optik Karakter Tanıma motoru, görüntülerin okunabilir metne hızlı bir şekilde dönüştürülmesine olanak tanır. Çoklu dil desteğine sahiptir.

3.1.3.4. Nuix Investigater Workstation

Avusturalya'da bulunan Nuix firması tarafından geliştirilmiştir. Nuix, adli bilişim için kullanılan tüm dosya türlerini desteklemektedir. Çok büyük boyutlarda dosyalarda inceleme yapabilir. Gelişmiş analiz özellikleri bulunmaktadır. Birden fazla delil analiz için değerlendirilmekte ve deliller ile kişilerin arasındaki bağlantılar yorumlanabilmektedir (Nuix 2022). Birden fazla kaynaktan analiz yapabilir ve tespit edilen veriler ile bağlantıları ortaya çıkarmaktadır. Araştırmacı hipotezlerini test etme ve delillerden yola çıkarak şüpheliler arasındaki bağlantıların tespitini yapmaktadır. Bağlantı analizi Şekil 3.29'da gösterilmiştir.



Şekil 3.29. Nuix Bağlanyı Analizi (User Manuel)

Adli kopya formatlarını desteklemektedir. Microsoft SQL Server veri tabanlarında inceleme yapabilmektedir. Yaygın dosya formatlarını desteklemektedir. OCR desteği bulunmaktadır. Yaygın dosya sistemlerini derinlemesine analiz

edebilmektedir. Desteklediği bulut sistemlerde analiz yapabilmektedir. Mikrosoft sistem dosyaları üzerinde derinlemesine analiz yapmaktadır.

3.1.3.5. FEX (Forensic Explorer)

Avustralya'da kurulu bulunan GetData firması tarafından geliştirilen Türkçe desteği olan adli bilişim yazılımıdır(Fex 2022). Veri kurtarma konusunda çok başarılıdır. Kolay kullanım ara yüzü vardır. Yazılım ile ilgili teknik tavsiyeler Türkiye bağlantısı olan Difose firması ile de yapılabilmekte ve geliştirilmesini istediğiniz konularda çözüm üretilebilmektedir. Shadow kopyaların incelenmesini kolaylaştırmaktadır. Windows sistem dosyalarını incelemekte ve analiz etmektedir.

Delphi betik dili ile analiz yapılabilmektedir. Otomatik delil işleme, birden çok dosya veya adli kopya ekleme, gelişmiş seviye klasör kurtarma, hash değerinin hesaplanması ve karşılaştırılması, çoklu ekran düzenleri, indeksleme ve anahtar kelime araması, detaylı metadata analizi, artifacts analizi, kayıt defteri analizi, detaylı e-posta analizi, Itunes yedeği analizi, video analizi, Shadow (gölge) kopya dosyalarını ekleme ve tarama ve Live boot sanallaştırma özellikleri bulunmaktadır(Şekil 3.30).

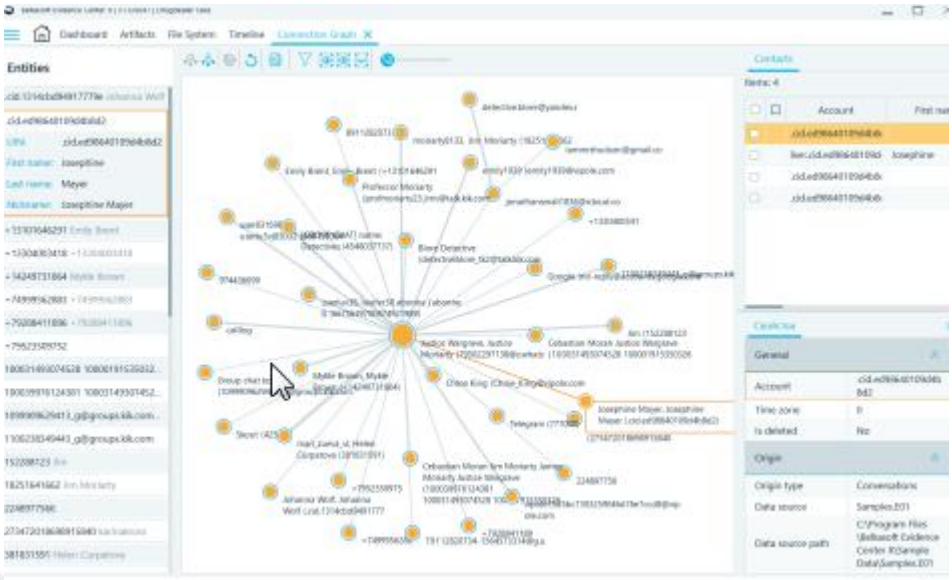
Şekil 3.30. Fex (www.difose.com.tr)

300'den fazla dosya desteği, gelişmiş filtreler ve kategorizasyon, DTSearch indeksleme ve anahtar kelime araması, veri kazıma, Türkçe destekli ve özelleştirilebilir raporlama özelliği ve video ön izleme özellikleri vardır. Yaygın işletim sistemi ve dosyalama sistemlerini desteklemektedir. Kapsamlı bir adli bilişim yazılımıdır (Şekil 3.31).

Şekil 3.31. Fex Dosyalar (User Manuel)

3.1.3.6. Belkasoft Evidence Center

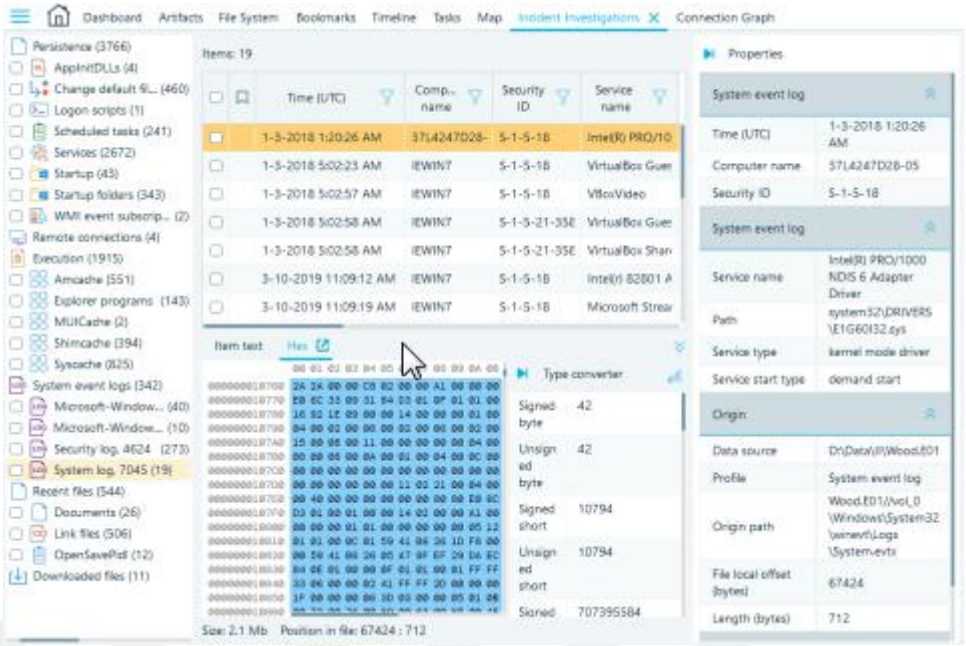
Rusya'da bulunan Belkasoft firması tarafından geliştirilmiştir. Diskler, mobil cihazlar ve alınan kopyalar üzerinde inceleme yapılabilmektedir. İncelediği medyaların erişebildiği tüm alanlarında inceleme yapabilmektedir. Bölümleri, sürücüleri, birimleri, klasörleri, dosyaları, varsa gölge kopyaları analiz edebilmektedir. Kötü amaçlı yazılımları tespit etmek için RAM dökümleri bellek işlemlerini analiz etme, hashset çalıştırma özellikleri vardır. Bağlantı Grafiği sekmesinde Belkasoft, kişiler arasındaki etkileşimlerin görselleştirmektedir. Birbirine bağlanan noktalar kişilerin bağlantılarını göstermektedir. Kişilerin, aramalar, SMS, anlık mesajlaşma sohbetleri, dosya aktarım oturumları, e-postalar ve diğer yollarla birbirleriyle etkileşime girdiği (iletişim kurduğu) anlamına gelmektedir. Şekil 3.32'de gösterilmiştir.



Şekil 3.32. Belkasoft Bağlantı Grafiği (User Manuel)

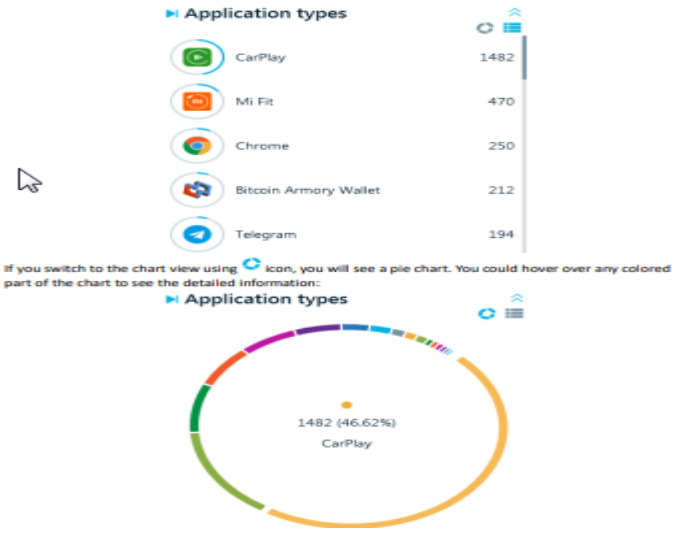
Olay inceleme modülü, kullanıcıların Windows tabanlı bilgisayarların bilgisayar korsanlığı girişimlerini araştırmasına yardımcı olmayı amaçlamaktadır. Kayıt defteri, olay günlükleri ve bellek dökümleri gibi çok sayıda kaynağı analiz ederek, bilgisayar korsanları tarafından sistemin altyapısına sızmak için kullanılan çeşitli hilelere özgü izler bulmaya çalışmaktadır.

Belkasoft, Amcache, Shimcache, Syscache, BAM / DAM, AppİnIt dll'leri, Varsayılan dosya ilişkilendirmesi değişikliği, zamanlanmış görevler, uzak bağlantılar (RDP, Uzak Bağlantı, TeamViewer ve diğerleri), başlangıç görevleri, tarayıcı uzantıları vb. içinde bulunan çeşitli eserlere bakar; şüpheli bağlantıları ve komut dosyalarını algılar(Belkasoft 2022) Analiz sonuçları daha sonra ayrı bir Olay inceleme penceresinde sunulur ve şüpheli faaliyetleri normal kayıtlardan ayırmayı kolaylaştırır. Bağlantı analizi Şekil 3.33'de gösterilmiştir.



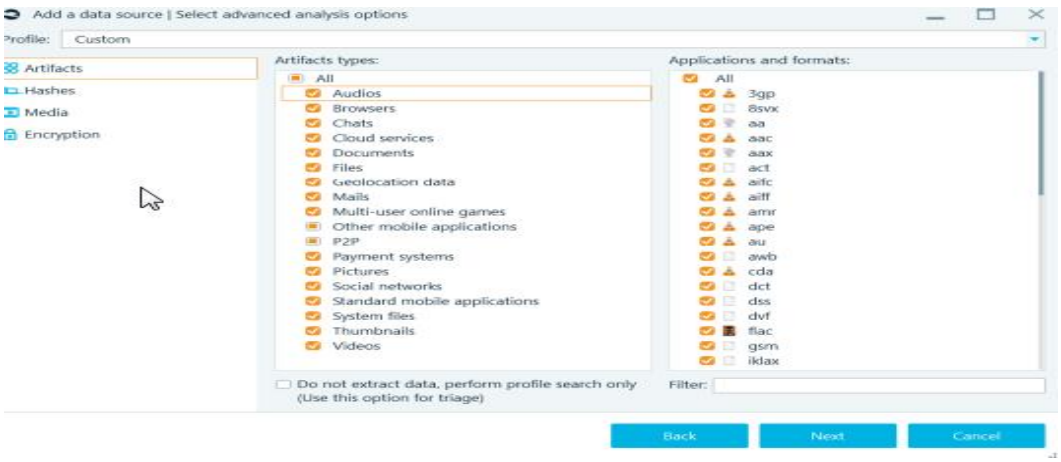
Şekil 3.33. Belkasoft Bağlantı Analiz (User Manuel)

Yaygın imaj dosyalarını eklendiğinde analiz edebilmektedir. Silinen veya gizlenen kanıtları kurtarılmasını yapmaktadır. Yaygın dosya türleri için inceleme ve analiz yapabilmektedir. İnternet izlerini tespit edebilmektedir. Popüler bulut uygulamalarını desteklemektedir. Belkasoft popüler bulut uygulamalarını destekler. Kripto para birimlerinin analizini yapabilmektedir. Belkasoft, Bitlocker gibi 280'den fazla şifreleme türünü destekler. Anlık mesaj uygulamalarını desteklemektedir. Coğrafi konum verilerini EXIF ve GPS etiketleriyle tespit edip Google Haritalar üzerinde gösterebilmektedir. Desteklediği oyun programlarına ait verileri çıkartabilmektedir. Silahları, pornografik görüntüleri, cilt tonu ve yüzleri tarayabilmektedir. Desteklediği mobil uygulamaları analiz edebilmektedir. Uygulama türleri altında, uygulama türüne göre eserler dökümünü diyagram şeklinde göstermektedir. Şekil 3.34'de gösterilmiştir. E-postalar, sohbetler veya tarayıcı verileri de görselleştirilebilmektedir.



Şekil 3.34. Belkasoft Uygulama Diyagramı (User Manuel)

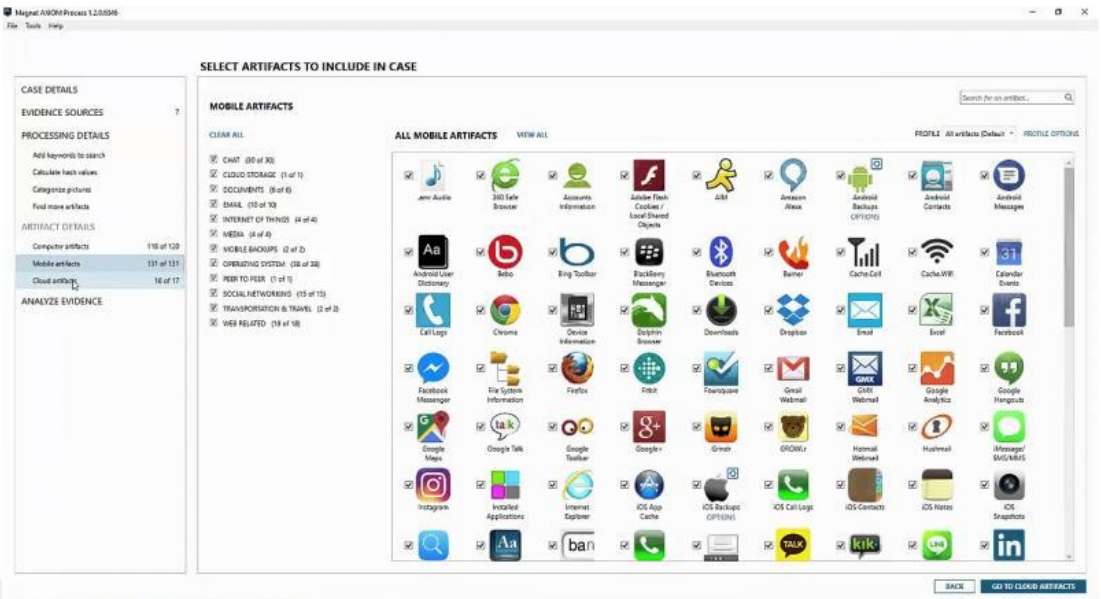
Ayrıntılı veri inceleme için analiz türü ve Carving (kazıma) yöntemlerini kullanmaktadır. Analiz işleminde; dosya sistemi bilgilerine dayanan tüm işlemleri birleştirir, mevcut dosyaların içindeki izleri arar, delile göre birim gölge kopyası anlık görüntülerini analiz eder ve geri dönüşüm kutusuna gönderilen ve silinen dosyaların dosya adlarıyla ilgili bilgileri analiz etmektedir. Carving işleminde diskin tamamında ve adreslenmemiş alanlarında dosya özelliklerine göre kurtarma yapmaktadır. Analiz edilen için dosya türleri Şekil 3.35'de gösterilmiştir.



Şekil 3.35. Belkasoft Dosya Analiz (User Manuel)

3.1.3.7. Magnet Axiom

Magnet Forensics Inc. firması tarafından Kanada'da geliştirilen bir yazılımdır. Fiziksel diskler, veri depolama cihazları ve desteklediği mobil cihazlardan kopya alabilmektedir. 50'den fazla sosyal ağ, bulut ve e-posta hizmetinden veri alabilmektedir. Passware ile tamamen entegredir (Axiom 2022). Desteklenen imaj dosyalarını inceleme ve analiz etme desteği vardır. Whats app mesajları orijinal şekli ile görüntüleyebilmektedir. Rebuilt Webpages özelliği sayesinde ziyaret edilen internet siteleri yeniden oluşturularak görüntülenebilir. World Map View özelliği ile tespit edilen koordinat bilgileri ve exif bilgileri harita üzerinde görüntülenebilir. Anahtar kelime ekleyerek kapsamlı arama yapma özelliği bulunmaktadır. Hash ekleyerek dosyalarını hash değerine göre süzme özellikleri vardır. Verileri özelliklerine göre süzme özelliği vardır. Cilt tonu tanıma özelliği vardır. Bağlantılar özelliğiyle dosyalar, yapılar, kişiler ve cihazlar arasındaki ilişkiyi otomatik olarak görselleştirmektedir. Kolay kullanılan bir ara yüzü vardır. Analiz edilen veriler arasında seçilen veriler raporlanabilmektedir. Mevcut ve silinmiş alanlar dahil diskin tüm alanlarında desteklediği uygulamaları ve internet verilerini tespit etmektedir. İnternet verilerini desteklediği medyalar üzerinde tespit edebilmekte ve analiz etmektedir. Uygulamaları destekleme konusunda çok kapsamlıdır (Şekil 3.36).

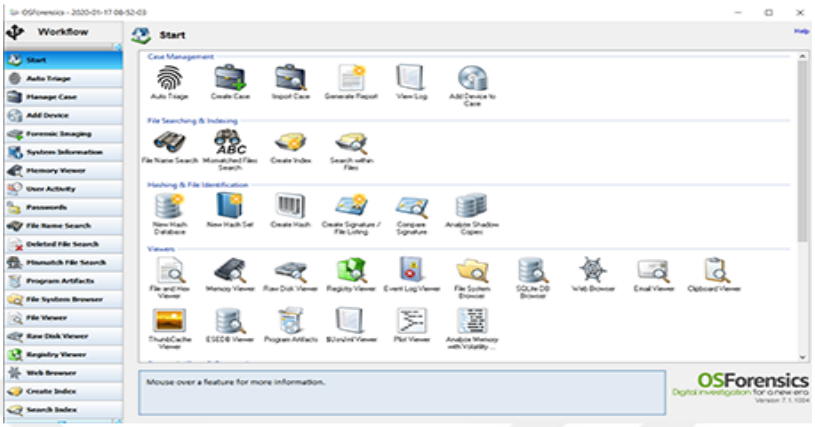


Şekil 3.36. Magnet Axiom (User Manuel)

3.1.3.8. OS Forensic

Avusturalya'da kurulu bulunan PassMark Software firmasının üretmiş olduğu bir yazılımdır. PassMark firması Sidney, Avustralya'da bir merkez ofisi ve Kaliforniya, Amerika Birleşik Devletleri'nde bir şube ofisi bulunan özel bir yazılım geliştirme grubudur(Os Forensic 2022). Yazılım, fiziksel diskler, sabit disk bölümleri, USB bellekler, hafıza kartları ve desteklediği imaj dosyaları üzerinde inceleme yapılabilir. Dosyaları süzme, dosya arama, elektronik posta bulma, silinmiş dosya arama kurtarma, Volume Shadow kopyalarnı önceki versiyonlarına yönelik incelemeler diğer incelemeler yapılabilir. Indeks search, disk mount etme, son yapılan işlemlerin belirlenmesi, sabit disk üzerinde gizlenen alanların incelenmesi yapılabilir. Kullanıcı aktiviteleri, uygulamaların incelenmesi, Windows kayıt defteri ve loğlarının incelenmesi yapılabilmektedir. Dosyalama sistemleri analiz edilebilmekte hash değerlerine ve özelliklerine dosyalar süzülebilmektedir. Grafiksel kolay kullanım ara yüzü vardır. Üzerine çalıştığı kopyaları emule edip incelemek için sanal makine haline getirebilmektedir. Resim ön izleme özelliği ile analiz

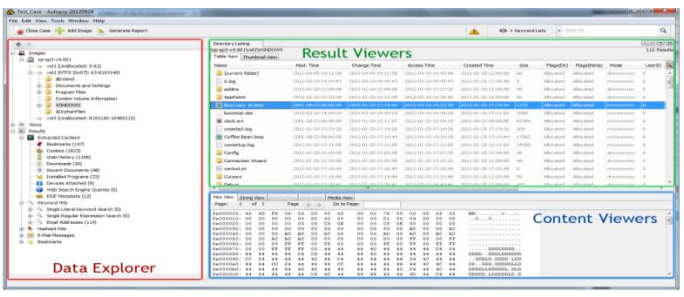
yapılabilmektedir. Desteklediği şifreleri tespit edebilmektedir. Daha farklı kapsamlı özellikleri bulunmaktadır (Şekil 3.37).



Şekil 3.37. OS Forensic (User Manuel)

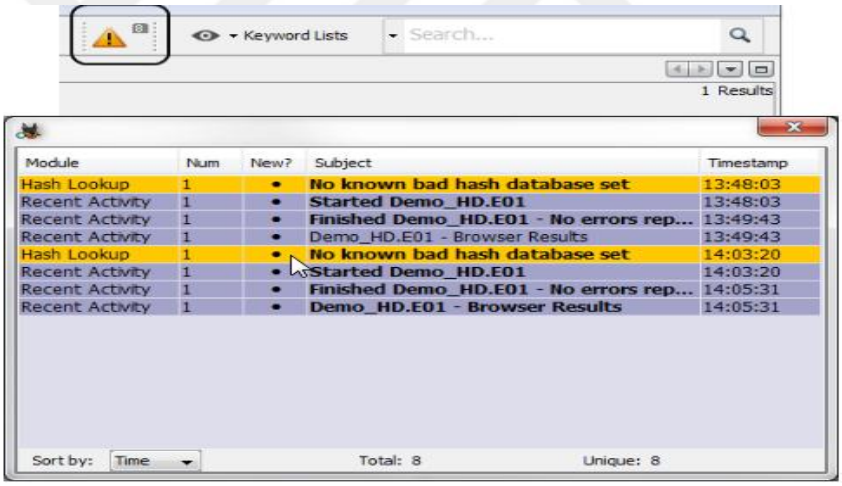
3.1.3.9. Autopsy

Ücretsiz bir yazılımdır. The Slueth kit tarafından oluşturulmuş Brian Carrier tarafından geliştirilen Basis Technology tarafından desteklenen ücretsiz bir yazılımdır (Autopsy 2022). İnternet verilerini, Firefox, Chrome ve Internet Explorer geçmişi, yer imlerini ve çerezleri tespit edebilmektedir. Silinen dosyaları kurtarabilmektedir. Anahtar kelime arama, gelişmiş olay görüntüleme, hash filtreleme özellikleri bulunmaktadır. Gelişmiş Kolay kullanılabilir grafiksel ara yüzü vardır (Şekil 3.38).



Şekil 3.38. Autopsy Ara Yüz

Java veya Python'da eklenti modülleri bulunmakta veya özel modüller geliştirilmeyi sağlayan bir eklenti mimarisine sahiptir. Multimedya dosyalarından exif bilgilerini çıkartabilmektedir. Android kopyaları üzerinde çalışılabilmekte ve kayıtlar çıkartabilmektedir. Bilinen dosya türlerini kategorize etmektedir. Arşivinde bulunan dosya türü bilgileri eklenerek incelenebilmektedir. Dosyalar için zaman çizelgesi görünümü vardır. Desteklediği cihazlar ve kopyalar üzerine işlemler yapılabilmektedir. Son etkinlik tespit etme özelliği bulunmaktadır. Uzantı uyuşmazlığı dedektörü ile uzantısı değiştirilen dosyalar tespit edilebilmektedir. Raporlama yapılabilmektedir. Otomatik tanımlı modül bulunmaktadır. Modüllerden istenilen etkinleştirilip, istenilen devre dışı bırakılabilmektedir. Modüllerin analiz sonuçları Şekil 3.39.'da gösterilmiştir.



Şekil 3.39. Autopsy Modül Analiz Sonuçları (User Manuel)

Ücretsiz yazılım olmasına rağmen çok başarılı bir yazılımdır. Çok kapsamlı ve ayrıntılı inceleme yapılabilmektedir. Sürekli geliştirilmekte ve yeni sürümleri ücretsiz yayınlanmaktadır.

3.1.4. Yazılımsal Ekipmanların Önemi

Çok fonksiyonlu yazılımlar özellikli yazılımlarla birlikte daha etkin kullanılabilmektedir. Şifre kırma yazılımları çok fonksiyonlu yazılımlara entegre çalışabilmektedir. AccessData Group firması tarafından geliştirilen PRTK (pasword Recovery Toolkit) şifre kırma için FTK ile entegre olabilmekte ve şifre kırma işleminde kullanılabilmektedir. Tespit ettiğimiz şifreli dosyaları fare ile tutarak program üzerine bıraktığımızda bazı dosya türlerini otomatik olarak analiz ederek şifre kırma işlemine başlamaktadır. Aynı şekilde Pasware Pasword Recovery programı desteklediği dosya türlerinin şifrelerini tespit edebilmektedir. EnCase ile entegre çalışabilmektedir. Aynı ana birden çok dosyanın şifresini kırabilmektedir. Recover My Files, Easy Recovery ve R-Studio gibi dosya kurtarma yazılımları fiziksel diskler, sabit disk bölümleri, USB bellekler, hafıza kartları ve desteklenen imaj dosyaları üzerinde veri kurtarma işlemi yapmakta, bilinen dosya türlerini başarı bir şekilde kurtarmaktadır. AOPR (Advanced Office Pasword Recovery) Windows Microsoft Office dosyalarının şifrelerini tespit edebilmektedir. CD/DVD Inspector, optik medya inceleme yazılımıdır. Blacklight, Macintosh ve IOS işletim sistemlerinin incelenmesine yönelik geliştirilmiş yazılımdır. Anahtar kelime arama ile MAC adresi, IP adresi, e-posta adresi, URL, telefon numarası ve posta kodu gibi düzenli ifadeleri arama, hash kütüphanesinde bulunan dosyalar ile incelen dosyalar analiz ve mukayese etme, dosya süzme, iOS ve OS X mesajlaşma uygulamaları da dahil olmak üzere iChat, SMS, MMS, Skype, iMessage mesaj uygulamalarını destekleme, video Frame Analysis, GPS verisi bulunan dosyaların harita üzerinde görüntüleme ve Web tarayıcılarına ait internet geçmişi verileri tespit edilebilme özellikleri vardır. WMvare WorkStation, sanal işletim sistemi yazılımıdır. Bütün işletim sistemleri sanal makine üzerine kurulabilir. WFC (Virtual Forensic Computing) sanallaştırma yazılımıdır. Internet Evidence Finder (IEF), internet trafiğini tespit etmek için de kullanılmaktadır, IEF çok kapsamlı ve ayrıntılı izler bulmakta ve analiz edip raporlamaktadır. WetStone Technologies tarafından geliştirilmiş bir Garygoyle Investigator yazılımı, Botnets, Truva atları, Steganografi, Şifreleme, Keylogger, trojan, toolkit ve daha birçok casus ve kötü niyetli yazılımlara

yönelik inceleme yapılabilmektedir. Arşiv dosyaları içerisinde de tarama yeteneği vardır.

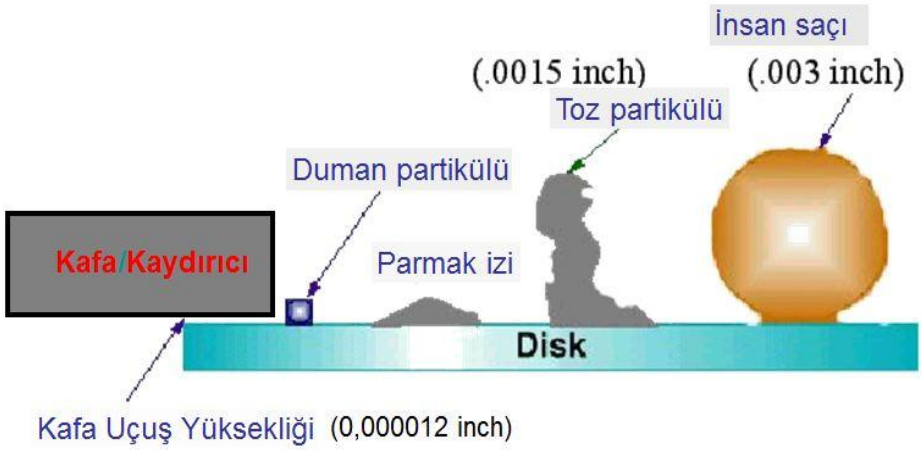
Adli bilişim incelemelerinin çeşitli alt dalları vardır. Canlı incelemeler de bunlardan bir tanesidir. Ölü inceleme olarak adlandırılan durumlarda imaj alma yazılım ve donanımları ile kopyalar alınmakta ve incelenmektedir. Canlı incelemelerde durum biraz farklıdır. İncelenecek sistem kapatıldığında sistem içindeki verilere erişilememesi durumunda canlı incelenmelidir. Sistem şifrelenmiş veya kriptolanmış işe canlı incelenmesi gerekir. Bazen RAM' de çalışan bir zararlı yazılımın tespiti için de canlı analiz yapılması gerekmektedir. Veri tabanı sistemlerinin analizi canlı analiz ile yapılmalıdır. Sistemden kapatıldığında sistem izleri temizleniyorsa canlı incelenmelidir. Canlı incelemeler operasyonel durumlarda da kullanılmaktadır. Canlı incelemek için adli bilişim şirketlerinin bu alanda da ürettiği ürünler bulunmaktadır. Belkasoft firması tarafından Belkasoft Live RAM Capturer, EnCase'in Encase Portable, AccessDate firması tarafından Live Response, Topala Software firması tarafından geliştirilen SIW (System Information For Windows) ve PassMark firması ve çok çeşitli firmalar tarafından geliştirilen yazılımlar bulunmaktadır. FBI Uzman Ajan Eric R. Zimmerman tarafından yazılıp geliştirilen OS Triaj yazılı da başarılıdır. Canlı inceleme yazılımları, RAM'in kopyasını almakta, bilgisayarda açık olan dosyalar, çalışılan programlar ve süreçler hakkında veri toplamaktadır. Verileri raporlayabilmektedir. F-Response yazılımı, bir araştırmacının gerekli ayarları yaparak IP ağı üzerinden canlı inceleme veri kurtarma ve inceleme yapmasını sağlayan yardımcı programdır.

Çok farklı fonksiyonel yazılım ve donanım vardır. Adli bilişim uzmanının tecrübesine göre kullandığı yazılım ve donanım değişebilmektedir. Fonksiyonel yazılımlar adli bilişim incelemeleri açısından çok önemli yazılımlardır. Çok fonksiyonlu yazılımlarla birlikte ve tek başına da kullanılabilmektedirler.

3.1.5. Hasarlı Medya Onarım ve Veri Kurtarma

Şüpheliler bazen suç işledikten sonra bilgisayar içerisinde bulunan disklere zarar vererek diski temizlemek istemektedirler. Diskler veya dijital materyaller bilgisayar tarafından görülmeyecek hale geldiğinde içerisindeki verilere erişilemeyeceğini düşünebilirler ancak verilerin tutulduğu alan tamamen zarar görmedikçe içerisindeki veriler çeşitli yöntemlerle kurtarılabilmektedir. Özellikle sabit disk tahribatları çok zor ve zahmetlidir. Çok ayrıntılı teknik bilgi, birikim ve donanım gerektirmektedir.

Sabit diskler dönen manyetik disklerden oluşan cihazlardır. Disklerin yüzeyi manyetiktir ve plakaları son derece hassastır. Okuma/Yazma kafası ve disk plakaları yüzeyi arasında gözle görülemeyecek kadar küçük bir boşluk bulunmaması gerekmektedir. Sabit disk yüzeyi şekil 3.40'da gösterilmiştir. Bu boşluğa hiçbir yabancı cismin girmemesi gerekir. Disk plakaları üzerinde kirlenmeye neden olan herhangi bir şey okuma/yazma kafasının işlevinin yerine getirmesine engel olabilir. Bilgi kümesi okunamayabilir. Okuma/yazma kafasının herhangi bir nedenden dolayı disk yüzeyine çarpması sonucunda ilgili bölge hasar görürse BAD SECTOR diye adlandırılan ölü bölgeler oluşur. Bu bad sektörler hash doğrulaması sırasında sorun olmaktadır.



Şekil 3.40. Sabit Disk Yüzeyi

Fiziksel veri kurtarma işlemi sırasında clean bench/room (temiz hava kabini/odası) olması ve bu işlemler yapılırken eldiven ve koruyucu elbise giyilmesi gerekir. Arızalı sabit disklerin arızası giderilmesi işlemi esnasında sabit diskin üst kapağının açılması gerekiyorsa Clean bench/room olarak bilinen cihazlar içerisinde incelenmesi gerekir. Clean bench lerin hava dışarıya iten motorunun havayı dışarıya itmeden önce hepa veya ultra filtre ile temizlenerek gönderilmesi gerekir. Kabinin paslanmaz çelikten antistatik malzeme ile kaplanmış olması gerekir. Mikron büyüklüğünde ve daha büyük partikülleri temizlemesi gerekir. Temiz hava kabini sisteminin aynı şekilde clean room (temiz oda) kullanım şekli vardır. Koruyucu kıyafetler ve malzemeler ile girilmesi gerekir.

Hasarlı sabit disklerin arıza tespiti, onarımı ve derinlemesine teşhis edilmesi için Rusya'da bulunan ACE LAB firması tarafından geliştirilen PC3000, Çin'de bulunan Salvation Data firması tarafından geliştirilen ve Çin' de bulunan Dolphin firması tarafından geliştirilen donanım ve yazılımlar bulunmaktadır. Donanım ve yazılımlar ile elektrik kesintisi, fiziksel/mekanik hasar veya denetleyicisi veya sistem alanında (bakım parça) üzerindeki firmware modülleri hataları gibi işlemleri sabit diskin durumuna göre düzeltmektedirler. Hızlı tarama yaparak, tekrar

kalibrasyon, otomatik tarama, sürücü kimlik okuma, sabit disk plakasını durdurma/hareket ettirme, yüzey doğrulama ve okuma, yazma yapabilmektedirler. Karmaşık testler ile PLIST (Fabrika çıkışı Bad sektörlerin kayıtların tutulduğu yer) ve GLIST (Kullanıma bağlı Bad sektörlerin kayıtların tutulduğu yer) kusur tabloları okuma ve izleme, kusurların gizlenmesi (göz ardı ederek yeniden yapılandırma), Low Level Format (Düşük seviyeli format) veya (Düşük düzeyde biçimlendirme), Hasarlı Firmware modülleri (RAM veya Sabit diske) yükleme/sabitleme, disk yüzeyinde bad sektörlerin (kusurlu alanların) atlanması ve çalışmayan disk kafalarını kapatarak sabit diski yeniden yapılandırma, hasarlı SA (Servis Area: sabit diskin doğru çalışması için ilgili kritik bilgilerin depolandığı diskin ayrılmış alandan bir bölümü) modüller için kurtarma, sabit disk performansını test ile gerçekleştirme ve şemalar şeklinde sonuç verme, veri kurtarma, veri aktarımı ve sabit disk ile ilgili birçok işlemleri yapmaktadırlar.

3.1.6. Mobil Cihazlar İçin Kullanılan Donanımlar ve Yazılımların Önemi

Mobil cihaz verilerinin boyutları da çok artmıştır. Boyutlarının artması ile birlikte mobil cihazların özellikleri de çok artmıştır. Akıllı telefonlar, küçük bir bilgisayar niteliği kazanmıştır. İnceleme yeteneğine de sahip olmak gün geçtikçe daha fazla gerekli hale gelmektedir. Çok çeşitli mobil cihaz bulunmaktadır. Cep telefonu incelemede kullanılacak uygun ekipman seçimi için piramit şeklinde seviyelendirme yapılmıştır. Şekil 3.41.'de gösterilmiştir. Piramitte yukarı çıkıldıkça ekipman daha pahalı olmakta, metot daha teknik olmakta, inceleme zamanı uzamakta, daha çok eğitim gerektirmekte ve cihaza fiziksel müdahale artmaktadır (Mobil İnceleme 2013)

Şekil 3.41. Mobil İnceleme Piramiti

1. **Manüel İnceleme:** Cihazın fiziksel olarak elle incelenerek mevcut içerisindeki mesajlar, rehber, resimler, videolar gibi ekranda görülebilen mevcut verilerin fotoğraflanarak ya da kamera kaydına alınması şeklinde yapılan incelemedir.
2. **Mantıksal İmaj Alma:** Cihazın kullanılan ekipman türüne göre kablolu veya kablosuz olarak bağlanılması, mantıksal veya dosya sistemi olarak imajının alınması ve sadece mevcut verilerin analizi şeklinde yapılan incelemedir.
3. **Fiziksel İmaj Alma**: Cihazın kullanılan ekipman türüne göre kablolu veya kablosuz olarak bağlanılması ve fiziksel imajının alınarak mevcut ve silinmiş verilerin analizi şeklinde yapılan incelemedir.
4. **Çip Sökme:** Cihazın içerisinde, hafızanın bulunduğu çipin sökülerek başka bir telefonda veya EEprom okuyucuda incelenmesiyle tüm verilerin analizi şeklinde yapılan incelemedir.
5. **Mikro İnceleme:** Cihazdaki elektronik devrelerin mikroskobik olarak incelenmesi ve verilere ulaşılması şeklinde yapılan incelemedir.

Mobil incelemeler konusunda, XRY, UFED, Oxygen Software, Paraben, EnCase, Magnet Forensics, AccessData, Salvation Data ve çeşitli firmaların ürettiği donanım ve yazılımları vardır. Ülkemizde en çok kullanılanlar XRY ve UFED

firmalarına ait ürünlerdir. XRY ve UFED yazılımlarının aldığı kopyalar çoğu adli bilişim yazılımı tarafından incelenebilmektedir.

XRY, 2003 yılından İsveç'de MSAB firması tarafından geliştirilen bir üründür. Cep telefonu inceleme konusunda çok başarılıdır (Xry 2022). Çok çeşitli alt ürünleri vardır.

Cellebrite, dijital verileri toplamak, incelemek, analiz etmek ve yönetmek için federal, eyalet ve yerel kolluk kuvvetlerinin yanı sıra kurumsal şirketler ve servis sağlayıcılar için araçlar sağlayan bir İsrail dijital istihbarat şirketidir (Ufed 2022). UFED, Cellebrite firmasının mobil cihaz incelemelerine yönelik olarak, UFED (Universal Forensic Extraction Device) markasıyla geliştirdiği yazılım ve donanımlardır. Çok çeşitli alt ürünleri vardır.

İşlev olarak çoğu benzer işlevleri yapmakla birlikte inceleme yazılımları, SIM kart okuma ve SIM ID klonlama, mobil cihazların mantıksal ve fizksel olarak incelemesi, GPS cihazlarının fiziksel incelemesi, hex görüntüleme, bütünlük doğrulaması yapabilme, dosya imzası analizi, seçime bağlı veri kopyalama, tüm verilerde arama yapabilme, rapor alabilme, bluetooth veya kızılötesi bağlanarak kopya alabilme fonksiyonları mevcuttur. Bulut hesaplarda bulunan verilere erişerek verileri derleyebilmektedir. Aradığınız verilere hızlı bir şekilde ulaşmanız için arama çemberini daraltarak çeşitli filtreler sunmaktadır. Raporlama istenilen bilgilere göre ve farklı formatlarda (Excel, word, xml vb.) yapılmaktadır. Ağ bilgileri, kişiler, notlar, SMS veya MMS, resim, görüntü, ses, e-posta, belgeler, dosyalar, cihaz bilgileri, log kayıtları ve desteklediği uygulama verilerinin çekilmesi gibi verileri analiz edebilmektedir.

3.1.7. Adli Bilişim Sertifikasyonları

İşi ehline vermek gerekir. Adli bilişim işlemlerinin ilk aşaması hazırlık aşamasından son aşaması raporlanması aşamasına kadar titiz çalışılmalıdır. Yapılan yanlış işlemler masum birinin ceza almasını veya suçluların suç işlemeye devam etmesini sağlayabilir. Her bilgisayardan anlayanın bilirkişi olarak görevlendirilmemesi gerekir. Kurs katılım belgeleri bir kişiyi konunun uzmanı yapmaz. Bu alanda yeterliliğin değerlendirilmesi için sertifikasının olması gerekmektedir. Uzman kişilerin bu alanda alabilecekleri çok çeşitli eğitimler ve sertifikalar vardır. Sertifika bilgili odluğumuz konularda uzmanlaşılması gereken alanda alınmalıdır. Bu alanda ulusal ve uluslararası çok fazla sertifika programı bulunmaktadır. Bunlardan en geçerli ve yaygın olanlar;

Certified Computer Examiner (CCE), adli bilişim alanındaki yetkinliği gösterir. CCE, dünya çapında bilgisayar denetçileri için yüksek standartlar oluşturmayı ve sürdürmeyi uman bir kuruluş olan Uluslararası Bilgisayar Denetçileri Derneği (ISFCE) tarafından sunulmaktadır. CCE adaylarının sabıka kaydı bulunmamalı ve ISFCE etik kurallarına bağlı kalmalıdır. En az 18 aylık mesleki deneyime veya belgelenmiş eğitime sahip olmalı ve çevrimiçi bir sınavı geçmelidirler. Adaylar, çevrimiçi sınavın yanı sıra en az üç "test ortamı" üzerinde adli inceleme yapmalıdır. Adaylar, ISFCE gerekliliklerini başarıyla tamamladıktan sonra, Sertifikalı Bilgisayar Denetçileri ve ISFCE üyeleri olarak kabul edilirler. Sertifikayı korumak için, her iki yılda bir elli saatlik eğitim veya öğretim tamamlanmalıdır. Ayrıca adayların bu süre içinde en az üç medya üzerinde çalışması gerekmektedir. Yeniden sertifikalandırma için her iki yılda bir çevrimiçi sınav da gereklidir (CCE 2022). Adil bir sertifikadır. Komiteler sertifika verme konusunda yetkilidir.

Certified Forensic Computer Examiner (CFCE), Windows tabanlı bilgisayarlarla ilgili olarak bilgisayar adli tıp alanında yetkinlik gösteren ilk

sertifikadır. CFCE eğitimi ve sertifikasyonu, dijital adli tıp uzmanlarının gönüllü bir kuruluşu olan Uluslararası Bilgisayar Araştırma Uzmanları Birliği (IACIS) tarafından yürütülmektedir. Sertifika dahili ve harici olarak alınabilmektedir. Bir dahili sertifika adayı, IACIS tarafından verilen iki haftalık bir eğitim kursuna katılır. Yılda iki kurs düzenlenmektedir. ABD merkezli kurs takvim yılının ilk yarısında, Avrupa merkezli kurs ise yılın ikinci yarısında yapılır. Kursu başarıyla tamamlayan üyeye (gönüllü) bir koç atanır. Koç, öğrenciye, öğrencinin zorluk yaşayabileceği konuları tam olarak anlamasına yardımcı olmayı amaçlayan, genellikle öğrenciye okuma materyalleri veya deneyler önererek, Akran Değerlendirmesi aşaması boyunca öğrenciye rehberlik eder. Akran Değerlendirmesi aşamasını başarıyla tamamlayan aday, sabit disk sınavına dayalı bir uygulama sınavı ve bir final sınavından oluşan Sertifikasyon aşamasına girmeye hak kazanır. Harici bir sertifika adayı eğitime katılmaz, ancak IACIS eğitimine eşdeğer 72 saatlik eğitime sahip olmaları gerekir(CFCE 2022). Sertifikasyonun güncel kalabilmesi için, bir üyenin sertifikasyondan sonraki üç yıllık dönemde bir kez yeterlilik testi yaptırması ve bilgisayar adli bilişim veya ilgili bir alanda 40 saatlik sürekli eğitimi tamamlaması gerekir. Ayrıca üye, üç yıllık süre içinde en az üç inceleme için yılda en az ortalama bir adli inceleme yapmalıdır.

GIAC, Global Information Assurance Certification, bilgi güvenliği uzmanlarının becerilerini doğrulamak amacıyla 1999 yılında kurulmuştur. Giac'ın amacı, sertifikalı bir bireyin bilgisayar, bilgi ve yazılım güvenliğinin kilit alanlarında bir uygulayıcı için gerekli bilgi ve becerilere sahip olduğuna dair güvence sağlamaktır. GIAC sertifikaları dünya çapında binlerce şirket ve devlet kurumu tarafından güvenilmektedir. GIAC sertifikaları dört yıl geçerlidir. Öğrenciler yeni ders bilgilerini gözden geçirmeli ve sınavlara tekrar girmeli veya sertifikalı kalmak için her dört yılda bir yapılan sınavda başarılı olmalıdır(Giac 2022). Certified Forensic Examiner (GCFE) Adli İncelemeci, adayların resmi olay araştırmaları yürütme ve dahili ve harici veri ihlali izinsiz girişleri, gelişmiş kalıcı tehditler, saldırganlar tarafından kullanılan adli tıp önleme teknikleri ve karmaşık dijital adli vakalar dahil olmak üzere gelişmiş olay işleme senaryolarını ele alma bilgisine ve

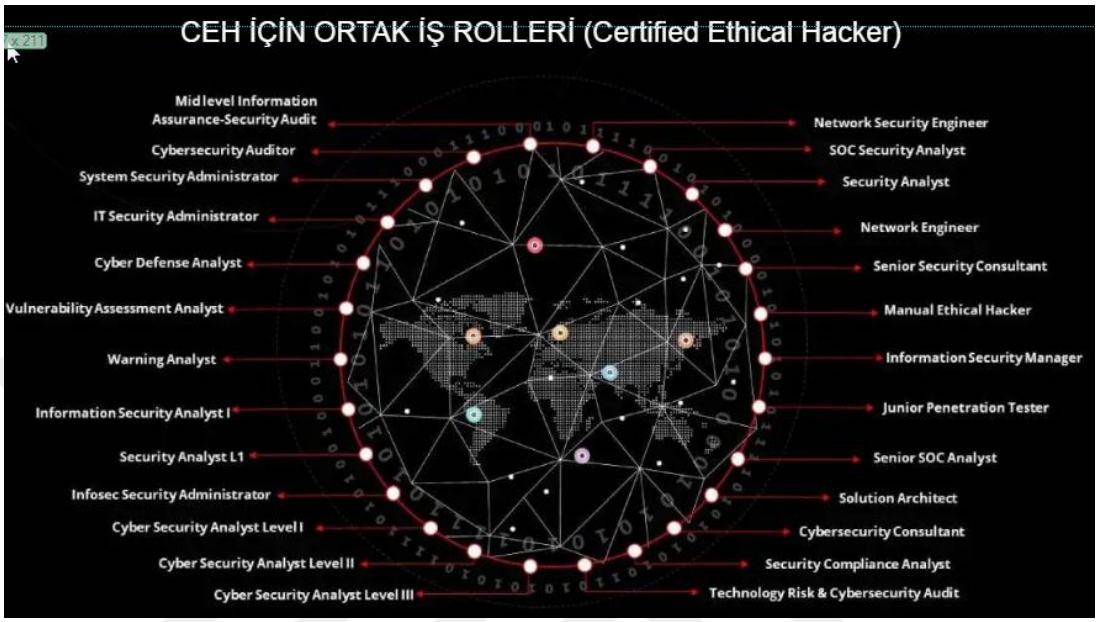
becerisine sahip olduğunu onaylar. Certified Forensic Analyst (GCFA) Adli Analist sertifikası, veri bilgisayar sistemlerini toplamak ve analiz etmek için gereken temel becerilere odaklanır. Windows bilgisayar sistemlerinden veri toplamak ve analiz etmek için gereken temel becerilere vurgu yaparak, bir uygulayıcının adli bilgisayar analizi bilgisini doğrulamaktadır.

ENCE-EnCase Certified Examiner, sertifikası alabilmek için altı aşama vardır. İki aşaması yazılı ve pratik sınavdır. Sertifika üç yıl geçerlidir(EnCase Kurs 2022).

AccessData Certified Examiner (ACE), 25 soruluk üç saat içinde bitirilmesi gereken vaka inceleme sınavı yapılmaktadır. Sertifika iki yıl geçerlidir. Uygulamanın lisanslı bir şekilde olması gerekmektedir. Önceden hazırlanmış belirli işlemlerin yapıldığı imaj dosyası üzerine çalışılmaktadır(Ftk Kurs 2022).

EC-Council (International Council of Electronic Commerce Consultant-Uluslararası E-Ticaret Danışmanları Konseyi), 11 Eylül saldırısından sonra ABD'de kurulmuştur. Kurucu Jay Bavisi, saldırıların ortaya çıkışını izledikten sonra, "Siber alanında benzer bir saldırı yapılacaksa ne olur?" sorusunu sormuş ve EC-Council, yıkıcı bir siber saldırıdan kurtarmak ve güveneceği topluma yardımcı olmak için bilgi güvenliği eğitimi ve sertifikasyon programları oluşturmuştur. EC-Council, dünyanın dört bir yanındaki önde gelen araştırmacıların ve konu uzmanlarının desteğini almış ve ilk bilgi güvenliği programı olan Sertifikalı Etik Hacker'ı başlatmıştır. 145 ülkeden 200.000'den fazla uzmanı sertifikalandırmıştır (EC-Council 2022) . Certified Ethical Hacker (CEH), bir kuruluşu yasal olarak heklemek için bilgisayar korsanlığı araçları, tekniklerini ve yöntemlerini öğretmektedir. Sürekli yenilenmekte ve güncellenmektedir. Kendi içine sürümleri vardır. Eğitimini vermek için yetkilendirilmiş akredite kuruluşlar bulunmaktadır. 150 soruluk bir sınavı vardır. Başarı yüzdesi 70'dir. 105 sorunun doğru cevaplanması gerekir. CEH sertifika

sahipleri çeşitli iş alanlarında çalışabilmektedir. Kişinin bilgi, beceri ve seviyesine göre değişiklik göstermekle birlikte çalışabilecekleri iş alanları Şekil 3.42.'de gösterilmiştir.



Şekil 3.42. Certified Ethical Hacker (CEH) İş Rolleri (eccouncil.org)

EC-Council, Computer Hacking Forensic Investigator (CHFI), Adli Bilişim alanında uzmanları tasdik eden sertifikasyondur. Program, bilgi sistemi güvenliği, bilgisayar incelemesi ve olay müdahalesi için bilişim uzmanları için tasarlanmıştır. Adli analistler, siber suç araştırmacıları, siber savunma adli analistleri, bilgi teknolojisi denetçileri, kötü amaçlı yazılım analistleri ve güvenlik danışmanları için adli bilişim alanındaki uygulama bilgisini güçlendirmek için tasarlanmıştır. Sertifika sınavına girebilmek için iki seçenek vardır. Birincisi akredite bir kuruluştan CHFI eğitimi almaktır. İkincisi adli bilişim alanında çalışmak ve en az iki yıl tecrübe sahibi olmak ve uygunluk için başvuru onayı almak gereklidir.

Certified Computer Crime Investigator (CCCI- Sertifikalı Bilgisayar Suçları Araştırmacısı), Amerikan Yüksek Teknoloji Suçları Network'u Organizasyonunun sertifika programıdır. İki aşamalıdır. Sertifika, adli bilişim çalışanlarına, kolluk

birimlerine ve kanun uygulayıcılara yöneliktir. Başlangıç seviye veya ileri düzeyden oluşan sertifikasyonlara sahip olabilmek için bazı gereksinimler ve yeterlilikler vardır (CCCI 2022).

(ISC)², 1989 yılında International Information System Security Certification Consortium, Inc olarak kurulan kurum, siber güvenlik endüstrisinde standardizasyon ve sertifikasyon ihtiyacını karşılamaktadır (ISC 2022). Bilgi güvenliği mesleğini şekillendirmiştir. Belirli etik kuralları bulunmaktadır. Sertifikaları, dünyanın önde gelen otoritelerinden profesyonel sertifikalar için en yüksek küresel standartlara bağlılığı akredite edilmiştir ve tanınmaktadır. Çeşitli adli bilişim sertifikaları vardır. Belirli gereksinimleri ve ön şartları vardır.

3.2. Arama Motorları Üzerinden Tespit Edilebilecek Veriler

Arama motorları, internet'te bulunan içerikleri aramak için kullanılmaktadır. İnternet kullanıcılarının siteler arasında istediği en alakalı bilgiye ulaşmasını sağlamaktır. Kütüphane görevlisi gibi çalışmakta ve daha hızlı çalışarak saniyeler içerisinde sonuçları göstermektedir. En yaygın kullanılan arama motoru Google'dır. NetMarketShare tarafından sağlanan veriler ile masaüstü bilgisayarlarda, Google Chrome'un %67 ile birinci sırada olduğunu göstermektedir. İkinci sırada Mozilla Firefox'un kullanım oranı da %9'lardadır. Google Chrome ile Firefox'un arasında %56''lık fark bulunmaktadır (Şekil 3.43) (Google Kullanım 2019).

Browser	Share
Chrome	67.39%
Firefox	8.63%
Internet Explorer	6.37%
Edge	6.09%
Safari	4.81%
Sogou Explorer	1.84%
QQ	1.69%
Opera	1.33%
Yandex	0.85%
UC Browser	0.31%

Şekil 3.43. Tarayıcı Kullanım Oranları

Bu kullanım oranlarından (2019) en yaygın kullanılan internet tarayıcılarının Google chrome ve mozilla firefox olduğu anlaşılmaktadır.

3.2.1. Google

Arama motorları içerisinde en çok tercih edilen ve en çok özelliği olan Google'dır. Dünyanın en büyük birinci arama motorudur. Dünyada bulunan çoğu arama motorunun da sahibidir. Çok fazla ziyaretçisi olan 18 internet sitesinin de sahibidir (Google 2019).

Chrome, Google tarafından geliştirilmiştir. Açık kaynak kodlu bir ağ tarayıcısıdır. Chrome adli bilişim incelemeleri açısından çok önemlidir. Chrome kullanılarak erişilen dosyalar, adresler işletim sistemine göre farklılık göstermektedir. Bazı tarih zaman verilerini kendi formatına göre saklamaktadır. Kurulum esnasında kullanıcı tarafından başka yol belirlenmemiş veya farklı ayarlar yapılmamış ise standart olarak kullanıcının yaptığı işlemler aşağıda belirtilen yolda saklanır.

- Windows Vista/Win 7-8-10-11

C:\Users\[USERNAME]\AppData\Local\Google\Chrome\

- Windows XP

C:\Documents and Settings\[USERNAME]\Local Settings\Application Data\Google\Chrome\

- OS X: <userdir>/Library/Application Support/Google/Chrome/Default
- Linux: /home/$USER/.config/google-chrome/
- Linux: /home/$USER/.config/chromium/

Google Chrome sabit diskte tuttuğu dosyaları veri tabanı dosyası şeklinde tutar. Kendine has tuttuğu dosyalar da herhangi bir uzantı bulunmaz. Kullanıcıya kolaylık olsun diye çabuk erişsin diye bazı dosyaları cache'de saklar. Cache incelenerek chrome üzerinden erişilen internet izleri analiz edilebilir. Chrome'un önbellek dizininin dosya yolu yerel disk üzerinde "C:\Users\%KULLANICIADI%\AppData\Local\Google\Chrome\UserData\Default\Cache" klasöründedir.

Göz atma geçmişini bulunan veri tabanı dosyası "Geçmiş" olarak belirtilen dosya yolunda saklanır. Herhangi bir SQLlite programı kullanılarak incelenebilir. Çeşitli tablolardan oluşur. İnternet erişim kayıtlar, indirilenler, kayıtlı sayfalar, aranan sayfalar, adres çubuğuna yazılarak girilen sayfalar hepsi tablolar halinde tutulmaktadır. Google chrome'da sistemde gerçekleştirilen kalıntılar ve izler kötü niyetli trafiğin ve saldırının kaynağını belirlemeye yardımcı olur. Chrome, bu yapıları işletim sistemindeki belirli klasörlerde saklar. Navigasyon Geçmişi, Otomatik Tamamlama Verileri, Yer İmleri (JSON Formatında Saklanır), Sık Kullanılanlar, Eklentiler, Uzantılar ve Eklentiler, Form Verileri, Favicons, Oturum Verileri, Küçük Resimler ve Favoriler'de Chrome tarafından depolanan yaygın yapılardır. Chrome üzerinden tespit edilebilecek veriler ücretsiz adli bilişim

yazılımları veya internet trafiği kaydı çıkaran adli bilişim yazılımları ile de çıkartılabilmektedir. Bu işlemler sonucu internet erişim kaydı bilgisayarın kullanılma, silinme, formatlanma durumlarına dayalı olarak değişkenlik göstermektedir.

3.2.2. Mozilla Firefox

Çoğu internet kullanıcısı arama motolarını kullanmakta arka planda nasıl çalıştığına bakmamaktadır. Arama motorları internet trafiğinin belirli kısımlarını kullanıcının işlemlerini daha kolay ve hızlı olması için sabit diske kaydeder. Firefox bu verileri veri tabanı şeklinde kaydeder. Adli bilişim incelemeleri açısından internet trafiği bilgileri çok önemlidir.

Firefox, Kasım 2004'te piyasaya çıkmıştır ve 9 ay içinde 60 milyon kişi indirerek kullanmıştır (Firefox 2022). Microsoft'un internet tarayıcısından daha hızlı olduğu için daha popüler hale gelmiştir.

Firefox uygulaması verilerini Sqlite formatında saklar. Mozilla Firefox Sqlite dosyalarında çeşitli tablolar bulunmaktadır. Adli incelemeler için bu tablolar önemlidir. Sqlite dosyalarının yolu işletim sistemlerinde değişiklik göstermektedir. Mozilla Firefox, Sqlite dosyalarının varsayılan konumu aşağıda gösterildiği gibidir.

- Windows Vista/Win 7-8-10-11
  C:\Users\admin\AppData\Roaming\Mozilla\Firefox\Profiles_.
- Windows XP
  C:\Documents and Settings\%kullanıcı%\Application Data\Mozilla\Firefox\
- Linux
  ~/.config/mozillafirefox/Default/databases

- Mac OS X
  ~/Library/Application Support/Mozilla/Firefox/Profiles/ şeklinde ayrıdır.

Tablolar içeriğinde adli incelemeler açısından önemli dosyalar bulunmaktadır. İçerik-prefs, sqlite içerisinde gruplar, tercihler ve ayarlar isimli tablolar bulunur. Bir kullanıcı, tarayıcı geçmişi ile birlikte tüm tarama oturumu boyunca kalıcı kalan tarayıcı ve içerik ayarları için belirli tercihleri ayarlayabilir.

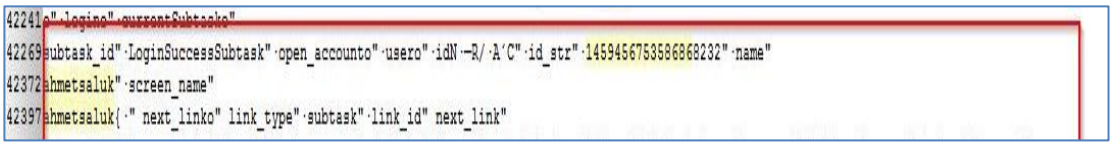
Adli incelemeler için önemli sqlite uzantılı dosyaları vardır. Site ziyaretleri sırasında kullanıcı tarafından kaydedilen kullanıcı adı ve şifre gibi kullanıcı kimlik bilgileri hakkındaki bilgiler Signons sqlite dosyasında bulunur. Bu bilgiler "şifreli kullanıcı adı" ve "şifreli şifre" sütunlarında şifreli olarak saklanır. Zaman damgası bilgileri, oluşturulma zamanını, en son kullanım tarihini ve şifrenin en son değiştirildiği zamandan da oluşur. Bir sitenin ziyaret edilme sayısı da "timeUsed" sütununa kaydedilir. Addons sqlite, Bu tablo, eklenti adı, sürüm numarası, açıklama, geliştirici notları, destek URL'si, içerik oluşturucu ve içerik oluşturucu URL'si, ana sayfa URL'si ve toplam indirme sayısı gibi her eklentiyle ilgili tüm gerekli bilgileri saklamaktadır. Cookies.sqlite, Çerezler iki şekilde üretilir. Kullanıcı profilleri oluşturmak ve reklam amaçlıdır. Çerezin bulunması kullanıcının bu siteyi ziyaret ettiği anlamına gelmeyebilir. Reklam amaçlı da bulunabilir. Firefox, çerezleri "moz_cookies" tablosunda saklanır. BaseDomain, host, lastAccessed ve creationTime, veri tabanındaki sütunlar'dır. Downloads.sqlite, indirilen tüm geçmişler, kullanıcı tarafından silinene kadar aynı kalan "downloads" tablosunda saklanır. Extensions.sqlite, farklı tablolarda bulunan uzantılarla ilgili veriler vardır. Bu tablolardan addon tablosunda "tanımlayıcı", "installDate" ve "sourceURL" sütunlarında bulunabilecek önemli bilgileri içerir. Formhistory.sqlite, online form doldurmak için kullanılan tüm verileri tutan bir dosyadır. Potansiyel veriler "değer" sütununda bulunur; diğer sütunlar "firstUsed" ve "lastUsed" ise ilgili zaman damgası bilgileri saklanır. Permissions.sqlite, Pop-up'lara izin verilip verilmeyeceği birden çok siteye atanan izin ayrıntılarını barındırır. Siteler "host"

sütununda, veriler ise "moz_hosts" tablosunda saklanır. Webappstore.sqlite, web tarayıcısında ve web depolama türlerinde kullanılan yazılım yöntemlerini ve protokollerini saklamak için bir tablo vardır. Bu dosyalar adli incelemeler için kullanılmaktadır. Normal kullanıcıların bu dosyalara ulaşmak ile pek fazla işi olmayabilir, adli bir durum veya yanlışlıkla silinen ve tekrar ulaşılmak istenen bir kayıt olduğunda kullanıcı tarafından erişilmek istenildiği zaman bu dosyalar kullanılır.

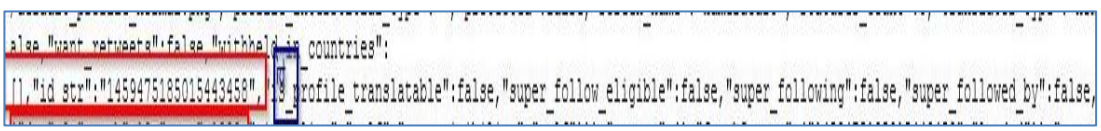
3.3. Örnek Olaylar Üzerinden Tespit Edilen Veriler

3.3.1. Twitter'da Oturum Açma Tespiti

Twitter her kullanıcıya kimlik numarası gibi herkese ayrı bir ID numarası tahsis etmektedir. "ahmetsaluk" kullanıcısına tahsis edilen id numarası "1459456753586868232" dir. "kameracar"a tahsis edilen id numarası "1459475185015443458"dir. "id_str" oturum açma bilgisinden oturum açan kullanıcı ID numarası tespit edilebilmektedir. Şekil 3.44. ve 3.45'de gösterilmiştir**.** Kullanıcı adı ve ID numarasını anahtar kelime olarak aratarak dosyaya ulaşabilir.



Şekil 3.44. Ahmet Saluk Oturum Açma Bilgisi



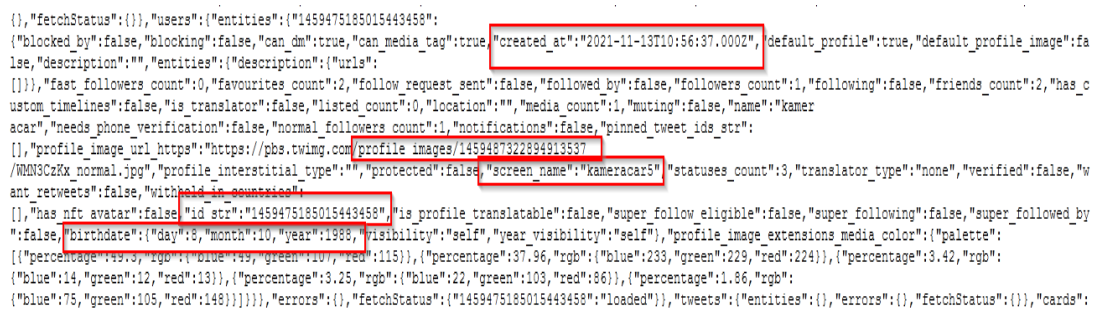
Şekil 3.45. Kamer Acar Oturum Açma Bilgisi

3.3.2. Hesap Oluşturulma ve Doğum Tarihi ile Profil ID Bilgisi

Twitter da her kullanıcının profil resmine ayrı bir id numarası verilmektedir. 1459456753586868232 id numaralı "ahmetsaluk" kullanıcısı oturumu alınma tarihi "created_at" ile belirtilen tarihte alınmıştır. Kullanıcıya ait profil id numarası "1459486989422632961" dir. Kullanıcının hesap alırken girdiği doğum tarihi bilgisi "birthdate" olarak belirtilmiştir (Şekil 3.46).

Şekil 3.46. Ahmet Saluk Profil id

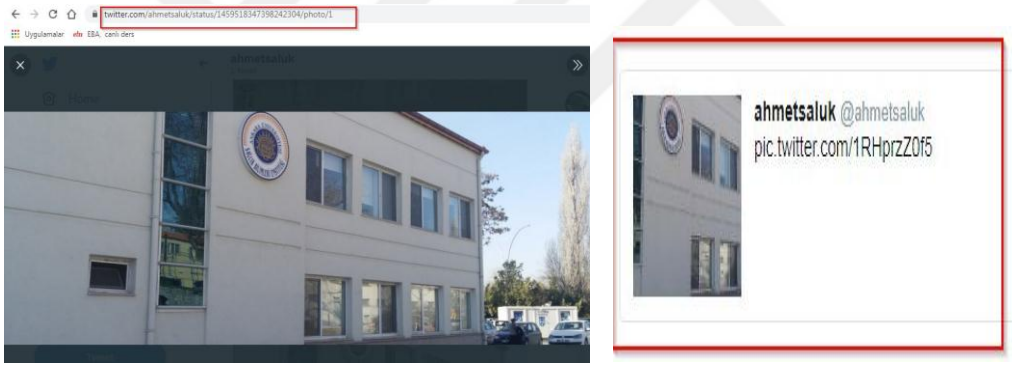
1459475185015443458 id numaralı "kameracar" kullanıcısı oturumu alınma tarihi "created_at" ile belirtilen tarihte alınmıştır. Kullanıcıya ait profil id numarası "1459487322894913537"dir. Kullanıcının hesap alırken girdiği doğum tarihi bilgisi "birthdate" olarak belirtilmiştir (Şekil 3.47).



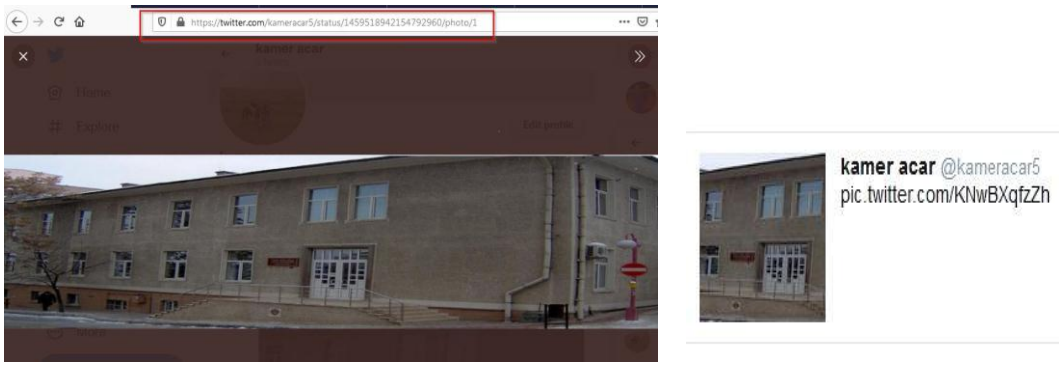
Şekil 3.47. Kamer Acar Profil id

3.3.3. Paylaşılan Resmin ID Bilgisi

Twitter üzerinden paylaşılan her resim dosyanın bir ID numarası bulunmaktadır. Kullanıcıların yaptığı bazı işlemler (beğenme, paylaşım vs) dosyaya özgü bir numara tarafından işlem görmektedir. Paylaşılan her resim dosyasının bir ID numarası ve farklı bir numarası bulunmaktadır. Ahmetsaluk tarafından yüklenen resim ID'si ve numarası Şekil 3.48'de gösterilmiştir. Kameracar tarafından yüklenen resim ID'si ve numarası Şekil 3.49'de gösterilmiştir. Dosyayı veya numarasını anahtar kelime olarak aratarak dosyaya ulaşabilir.



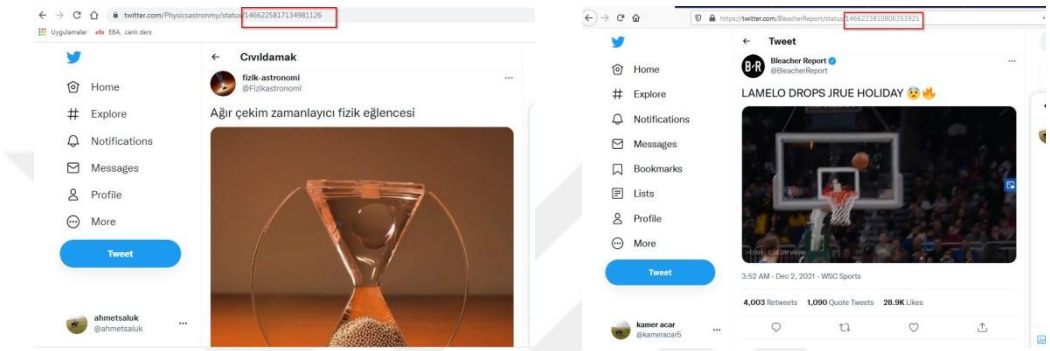
Şekil 3.48. Ahmet Saluk Paylaşılan Resim ID ve Numarası



Şekil 3.49. Kamer Acar Paylaşılan Resim ID ve Numarası

3.3.4. Mesaj Gönderilen Video Dosyasının ID Numarası

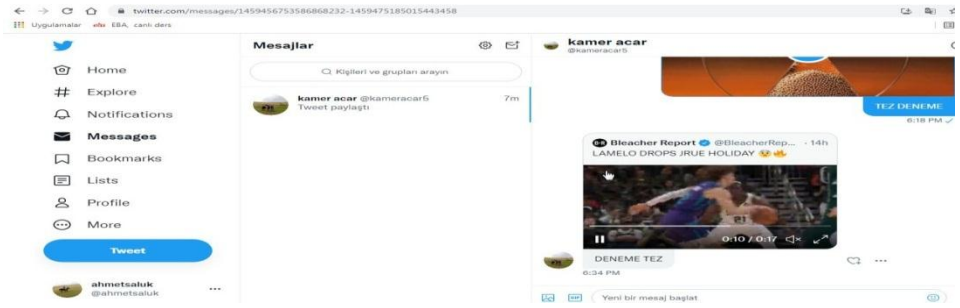
Twitter üzerinden paylaşılan her video dosyanın bir ID numarası bulunmaktadır. Videolar Şekil 3.50.‘de gösterilmiştir.



Şekil 3.50. Paylaşılan Video Dosyaları

3.3.5. Mesaj ile Gönderilen Video Bilgisi

Twitter üzerinden mesaj gönderilen video dosyasının hangi ID numaralı kullanıcıdan hangi ID numaralı kullanıcıya gönderildiği tespit edilebilmektedir. “1459456753586868232” id numaralı kullanıcı Ahmet SALUK’tan “1459475185015443458” id numaralı kullanıcı Kamer ACAR’a gönderilmiştir. Dosyaya ait bilgiler ve kullanıcıya ait bilgiler anahtar kelime olarak aratıldığında bulunabilmektedir (Şekil 3.51-52).



Şekil 3.51. Gönderilen Video Dosyası

Şekil 3.52. Gönderilen Mesaj Bilgisi

3.3.6. Profil Resmi ve Paylaşılan Dosyaların Kurtarılması

Twitter kullanıcılarında bazıları sahte profil oluşturmakta ve kendilerine ait olmayan resimler ile hesap almaktadırlar. Alınan bu hesaplarda kullanılan profil resmi ve yüklenen resimlerin tespiti önem arz etmektedir. Profil resmi ve paylaşılan resimler silinmiş alanlardan tespit edilmiştir. Ahmet saluk profil resmi Şekil 3.53.'de paylaştığı resim dosyası Şekil 3.54.'de gösterilmiştir.

Şekil 3.53. Ahmetsaluk Profil Resmi

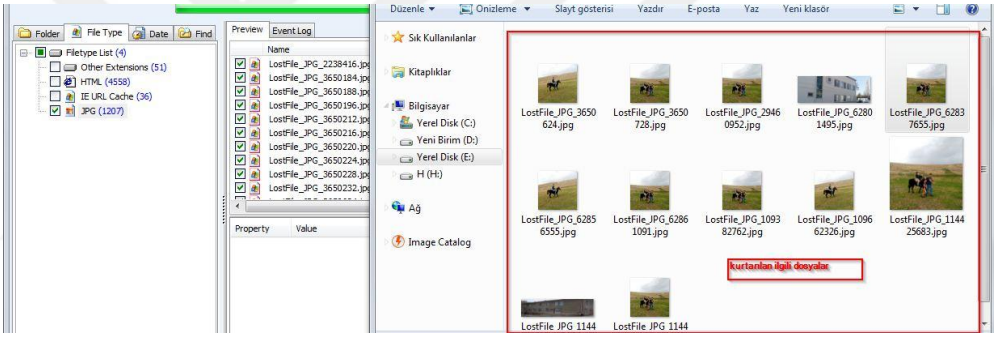
Şekil 3.54. Ahmetsaluk Paylaştığı Resim

Kameracar profil resmi Şekil 3.55.'de, paylaşılan resim Şekil 3.56.'da gösterilmiştir.

Şekil 3.55. Kameracar Profil Resmi

Şekil 3.56. Kameracar Paylaştığı Resim

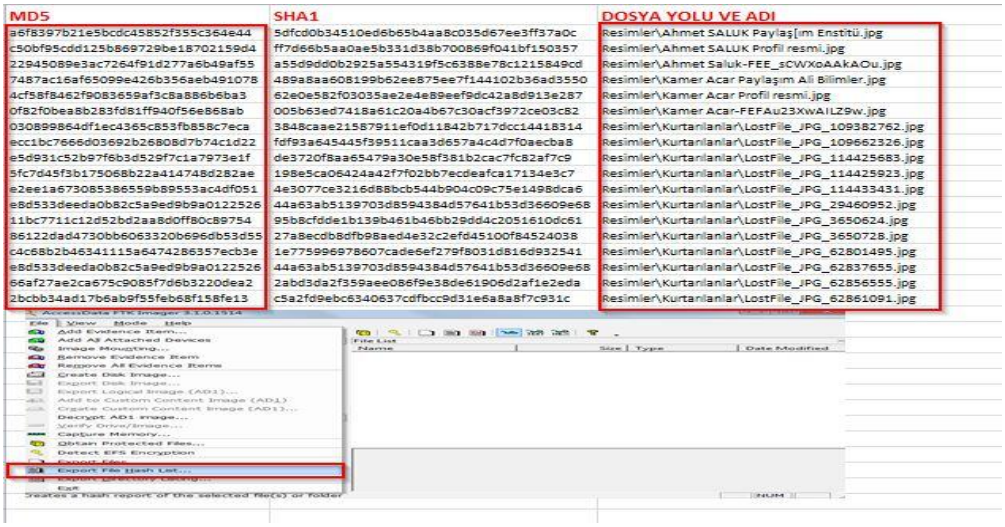
Ahmetsaluk ve kameracar kullanıcıları hesaplarının profil resmi ve paylaşılan resimler veri kurtarma yazılımı ile kurtarılmıştır. Şekil 3.57.'de gösterilmiştir



Şekil 3.57. Kurtarılan Resimler

3.3.7. Dosyaların Hash ve Exif Verileri Bilgisi

Twitter'a fotoğraf yüklendiğinde ve aynı fotoğrafı twitter üzerinden indirildiğinde exif bilgileri ve hash değerleri de değişmektedir. Bu işlem için yüklediğimiz profil resmi ve dosyaların hash değerlerini hesaplatarak baktığımızda değişmiş olduğu görülmektedir (Şekil 3.57). Exif bilgileri için dosyalar, EnCase yazılımı ile incelenmiştir. Twitter'a yüklenen resim dosyalarına ait exif bilgilerinin tekrar indirildiğinde bulunmadığı tespit edilmiştir.



Şekil 3.58. Dosyaların Hash Değerleri

Sosyal medya uygulamalarından twitter üzerinden tespit edilebilecek veriler çok çeşitlidir çalışmamızda en fazla istenen konular üzerinde durulmuştur. Şüpheli kullanıcı ismiyle oturum açan veya kullanıcının tespiti çok önemlidir. Adli incelemeler de istek konusu üzerinde örneklemeler yapılmalıdır. İstek konusu üzerinde denemeler yapılmalı ve bıraktığı izler tersine mühendislik yöntemi ile değerlendirilerek incelenmeli ve raporlanmalıdır.

4. TARTIŞMA

- Bu çalışma içinde, twitter üzerinden oturum açma, paylaşım yapma, resim veya video paylaşma gibi işlemlerin adli olarak tespiti ele alınmıştır.

- Yaygın adli bilişim uygulamalarının kabiliyetleri ve tespit ettikleri veriler ve kullanım alanları anlatılmıştır.

- Uluslararası geçerliliği olan ve yaygın kullanılan imaj alma cihazları hakkında bilgi verilmiştir.

- Web tarayıcılarından Google ve firefox üzerinden tespit edilebilecek adli izler anlatılmıştır.

- Adli bilişim uzmanlarının sahip olmaları gereken sertifikasyon programları anlatılmıştır.

- Twitter üzerinden veya adalet birimleri üzerinden başvuruların nasıl yapılacağı hangi evrakların eklenmesi gerektiği anlatılmıştır.

- Twitter kullanıcılara kimlik numarası gibi herkese ayrı bir ID numarası tahsis ettiği ve güncel oturum açma verisinin "id_str" olduğu tespit edilmiştir.

- Twitter' da her kullanıcının profil resmine ayrı bir id numarası verildiği ve kullanıcı ile eşleştirilebildiği tespit edilmiştir.

- Twitter üzerinden paylaşılan her resim dosyanın bir ID numarası bulunduğu ve kullanıcının yaptığı işlemler(beğenme, paylaşım) dosyaya özgü ID numarası ile işlem gördüğü tespit edilmiştir.

- Twitter üzerinden paylaşılan her video dosyanın bir ID numarası bulunduğu tespit edilmiştir.

- Twitter üzerinden mesaj gönderilen video dosyasının hangi ID numaralı kullanıcıdan hangi ID numaralı kullanıcıya gönderildiği tespit edilmiştir.

- Twitter'da kullanıcının yüklediği profil resmi ve paylaştığı resim dosyalarının normal yollarla silindiği durumlarda kurtarılabildiği tespit edilmiştir.

5. SONUÇ VE ÖNERİLER

- Suçluların tespiti ve adli işlemler için Twitter üzerinden veya adli makamlar aracılığıyla evraklar eksiksiz ve hızlıca gönderilmelidir.

- Suç konusu içerik ile karşılaşıldığında delillendirilmelidir. Ekran görüntüsü ile birlikte video kaydı alınmalı ve zaman damgası mutlaka delillendirilmelidir. Ekran görüntülerinin delillendirilmesi için noterler birliğinin sunduğu E-TESPİT uygulaması da kullanılabilir.

- İnceleme yapılan kişi ile ilgili bilgiler suçlayıcı olsa bile masumiyet karinesi dikkate alınarak tarafsız inceleme yapılmalıdır. İddia edilen husus doğru da olabilir yanlış da olabilir veya iftira da olabilir. Deliller içerisinden ne tespit edildi ve hangi yöntemler kullanıldı ise belirtilmeli ve bu doğrultuda rapor yazılmalıdır. Yazılan rapor kişilerin suçluluğunun veya suçsuzluğunun ispatı için çok önemlidir. Kesin bir veri tespit edilmemiş ise tespit yapılamadığı belirtilmelidir.

- Adli bilişim incelemelerinde şüpheli veya mağdura işlemler CMK 75-82'de düzenlendiği gibi gizlilik içerisinde KOD verilerek yapılmalıdır.

- İstek konusu üzerinde denemeler yapılmalı ve bıraktığı izler tersine mühendislik yöntemi ile değerlendirilerek incelenmeli ve raporlanmalıdır.

- İncelemenin her aşamasında, plan yapılmalı veya tespitler kaydedilmelidir. Gelen delillerin birebir kopyası alınmalı ve birebir kopya üzerinde çalışılmalıdır. Aksi halde delillerin zarar görme ihtimali vardır. Yapılan yanlış işlemler masum birini ceza almasını veya suçluların suç işlemeye devam etmesini sağlayabilir.
- Ülkemizde 16,1 milyon Twitter kullanıcısı vardır. Sosyal medya paylaşımları ile ilgili kapsamlı, ayrıntılı ve açıklayıcı kanun çıkartılmalıdır.

- CMK 134. maddesi 4 kere güncellenmiştir. CMK 134. maddesi daha ayrıntılandırılarak güncellenmelidir. Bilgisayar kütükleri ibaresine akıllı cihazlar, akıllı telefonlar, IoT (nesnelerin interneti) gibi türlü bilişim sistemini kapsayacak şekilde ekleme yapılmalıdır. Suç işlemeye devam edilebilecek durumlarda çalınmış kredi kartı bilgileri, çocuk pornografisi gibi özellikli dosyalarda delil ve delilin kopyası verilmeyerek alınan kopyalara ait hash değerlerini içeren tutanak verilmelidir. Bu gibi durumlar için düzenleme yapılmalıdır.

- Suçlularla daha etkin bir mücadele için ulusal birimler arasında daha etkin bir koordinasyon ve bilgi havuzu ve Ulusal hash set veri tabanı oluşturulmalıdır.

- Suçluların suç işlemede, kullanılan cihaz (bilgisayar, tablet veya telefon), işletim sistemi (Windows veya Android), dosyalama sistemi, üzerinde çalışılan arama motoru, telefon uygulaması ve bunlara ait sürümler değişken olmakla birlikte bütün bu etkenler değerlendirilmelidir. Yapılan işlemlerin yanlış olması durumunda suçsuz bir insanın suçlanması sonucunu doğurmaktadır ve telafisi mümkün değildir. Varsayımsal değil net bilgilere göre rapor yazılmalıdır. Ya suç kaydı vardır ya da yoktur. İhtimaller ile bilirkişi raporu verilmemelidir.

- Her bilgisayardan anlayan bilirkişi yapılmamalıdır. Bilirkişiler, belirli eğitimden geçtikten ve yeterlilik sınavlarında başarılı olduktan sonra yetkilendirilmelidir.

ÖZET

Sosyal Medya Üzerinden İşlenen Suçlarda Twitter Örnek Olaylarının Adli Olarak İncelemesi

İnsanlar her zaman duygularını ve düşüncelerini başkalarına aktarma ihtiyacı duymuşlardır. İfade özgürlüğü insanların en temel haklarından biridir. Bazen bu ifade özgürlüğü sınırı aşıp suç konulu bir içerik olabilir ve adli bir olaya konu olabilir. Sosyal medya, çift taraflı ve eşzamanlı bilgi paylaşımı ve tartışma sağlayan medya sistemidir. İfade özgürlüğü ile bilinen twitter üzerinden suç konusu paylaşımlar yapılırsa adliyeye intikal ettiğinde ve inceleme sürecinde nelerin yapılması gerektiği hususunda çalışmalar yapılmıştır. Bu çalışmada, bu alanda var olan kaynak eksikliğini gidermek amacı ile Twitter yazılımının özellikleri ve adli bilişim uygulamalarında erişilebilecek sonuçlarla ilgili çeşitli bilgiler verilmeye çalışılmıştır. Bu çalışma içinde, twitter üzerinden oturum açma, paylaşım yapma, resim veya video paylaşma gibi işlemlerin tespit edilmesi için yapılabilecek uygulamalar ve bu uygulamaların sonuçları ele alınmıştır. Yapılan uygulamalarda, twitter üzerinden (suç konusu) paylaşım yapanların veya resim, video paylaşanların adli olarak incelenmesi yapılmış ve verilerin tespit edildiği görülmüştür. Twitter' a fotoğraf yüklendiğinde ve aynı fotoğrafı twitter üzerinden indirildiğinde exif bilgileri ve hash değerlerinin değiştiği tespit edilmiştir. Adli incelemeler de istek konusu üzerinde örneklemeler yapılmalıdır. İstek konusu üzerinde denemeler yapılmalı ve bıraktığı izler tersine mühendislik yöntemi ile değerlendirilerek incelenmeli ve raporlanmalıdır.

Anahtar Sözcükler: Adli Bilişim, Dosya Kurtarma, Oturum Açma, Paylaşım ve Twitter

SUMMARY

Forensic Investigation Of Twitter Cases For Committed Through Social Media Crimes

People have always needed to convey their emotions, thoughts to other. Freedom of expression is one of the most fundamental rights of people. Sometimes this freedom of expression can cross the border, be criminal content, and be the subject of a judicial incident. Social media is a media system that provides bilateral and simultaneous information sharing and discussion. Studies have been conducted on what should be done when the subject of a crime is shared via twitter, which is known for its freedom of expression, when it is transferred to the judicial authorities and during the review process. In this study, it has been tried to be given various information about the features of twitter and the results that can be accessed in computer forensic examinations in order to make up for existing resource shortages. Within this workout, applications that can be performed to detect transactions such as logging in to twitter, sharing, sharing images or videos, and the results of these applications are discussed. Within the tests, In the applications made, it was seen that those who shared on Twitter (the subject of crime) or shared pictures and videos were forensicly examined and the data were determined. It has been found that exif information and hash values change when a photo is uploaded to twitter and the same photo is downloaded via twitter. Forensic examinations should also be carried out on the subject of the request. Experiments should be carried out on the subject of the request, and the traces left by it should be evaluated by reverse engineering and examined and reported.

Keywords: Computer forensics, File Recovery, Login, Share and Twitter

KAYNAKLAR

5237 Sayılı Türk Ceza Kanunu

5271 Sayılı Ceza Muhakemesi Kanunu

AccessData FTK Imager (Versiyon 3.1.0.1514), ABD'de bulunan AccessData Firmasının ücretsiz imaj alma yazılımıdır [https://accessdata.com/].

Axiom 2022, Erişim: [https://www.magnetforensics.com/docs/axiom/html/Content/Resources/PDFs/Magnet%20AXIOM%20User%20Guide.pdf] Erişim Tarihi: 29.04.2022

Axiom 2022, Erişim: [https://www.emt.com.tr/wiys/plugins/ckfinder/userfiles/files/AXIOM_WhyUpgrade_Turkish_EMT.pdf] Erişim Tarihi: 16.05.2022

Aydın Doğan'a Hakaret 2015, Erişim: [http://www.hurriyet.com.tr/gundem/twitterdan-hakarete-ceza-40025497] Erişim Tarihi:22.06.2019

Ayşe Hür Ceza 2018, Erişim: [http://www.cumhuriyet.com.tr/haber/turkiye/959835/Yazar_Ayse_Hur_e_Twitter_paylasimindan_hapis__Sanatci_Suavi_ye_Erdogan_a_hakaretten_para_cezasi.html] Erişim Tarihi: 21.06.2019

Autopsy 2022, Erişim: [https://www.sleuthkit.org/about.php] Erişim Tarihi: 29.04.2022

Başbakan'a Hakaret 2014, Erişim: [https://www.yenisafak.com/gundem/erdogana-twitterda-hakarete-hapis-cezasi-650136] Erişim Tarihi: 21.06.2019

Belkasoft 2022, Erişim: [https://belkasoft.com/downloads/info/Evidence%20Center%20Help.pdf] Erişim Tarihi: 27.04.2022

BeeCube 2022, Erişim: [https://www.mh-service.de/en/products/beecube] Erişim Tarihi: 12.05.2022

Bilişim Suçu, Erişim: [https://profhukuk.com.tr/bilisim-sucu-nedir-cezalari-nelerdir/] Erişim Tarihi: 18.05.2022

Buse Terim Hakaret 2013, Erişim: [https://www.memurlar.net/haber/440497/twitter-dan-hakaret-eden-saniga-ceza.html] Erişim Tarihi: 21.06.2019

Bülent Turan Takipsizlik 2017, Erişim: [http://www.diken.com.tr/savcilik-dokunmadi-aysevere-twitterdan-geri-zekali-diyen-akpli-turana-takipsizlik/] Erişim Tarihi: 22.06.2019

CCCI 2022, Erişim: [https://www.ekizer.net/adli-bilisim-sertifikasyonlari/] Erişim Tarihi: 14.08.2021

CCE 2022, Erişim: [https://en.wikipedia.org/wiki/Certified_Computer_Examiner] Erişim Tarihi: 15.05.2022

CFCE 2022, Erişim: [https://en.wikipedia.org/wiki/Certified_Forensic_Computer_ Examiner] Erişim Tarihi: 16.05.2022

Cihan Ünal'a Hakaret 2013, Erişim: [https://www.aksam.com.tr/magazin/twitterdan-hakarete-hapis-cezasi/haber-184306] Erişim Tarihi:21.06.2019

DALKIRAN D. 2017, *GELECEĞİ KEŞFEDENLER* Dijital Çağın Biyografisi WALTER ISAACSON ÇEVİRİ: DUYGU DALKIRAN SAYFA: **438** DOMİNGO YAYINEVİ BASKI: ŞUBAT 2017

Data Copy 2022, Erişim: [https://blog.salvationdata.com/2018/06/15/products-launch-boost-your-imaging-speed-with-salvationdata-new-generation-forensic-hardware-dck-2-and-write-blocker/] Erişim Tarihi: 08.04.2022

Difose 2022, Erişim: [https://www.difose.com.tr/wp-content/uploads/2021/01/BR.D.015_ DIFOSE-WB1-TURKCE.pdf] Erişim Tarihi: 18.05.2022

Ditto 2022, Erişim: [https://www.difose.com.tr/portfolio/a02-ditto-dx-adli-kopya-alma-cihazi/] Erişim Tarihi: 11.05.2022

Emre B. Hakaret 2018, Erişim: [https://www.posta.com.tr/emre-belozogluna-twitterdan-kufure-1500-tl-ceza-330161] Erişim Tarihi: 21.06.2019

EnCase Law Enforcement (Versiyon 6.19.1) ABD'de bulunan Open Text firmasının geliştirdiği Adli Bilişim yazılımıdır [https://www.opentext.com/].

Encase 2022, Erişim: [https://www.emt.com.tr/tr/markalar/opentext-45#encase-forensic-software] Erişim Tarihi: 16.04.2022

EnCase User Manuıel) Erişim: [http://encase-docs.opentext.com/documentation/encase/forensic/8.07/Content/Resources/External%20Files/EnCase%20Forensic%20v8.07%20User%20Guide.pdf] Erişim Tarihi: 11.04.2022

EnCase Kurs 2022, Erişim: [https://www.opentext.com/TrainingRegistry/course/details/2687] Erişim Tarihi: 25.04.2022

Ec-council 2022) Erişim: [https://www.eccouncil.org/#] Erişim Tarihi: 18.05.2022

E TESPİT 2022, Erişim: [https://e-hizmet.tnb.org.tr/tespit/public/uyariKisit.xhtml?faces-redirect=true] Erişim Tarihi: 01.05.2022

Evraklar 2022, Erişim: [https://diabgm.adalet.gov.tr/home/SayfaDetay/uluslararasi-ceza-istinabe-evrakinin-hazirlanmasi14022020013214] Erişim Tarihi: 08.05.2022

Falcon 2022, Erişim: [https://www.logicube.com/shop/forensic-falcon-neo/] Erişim Tarihi: 11.04.2022

Fex 2022, Erişim: [https://www.difose.com.tr/wp-content/uploads/2021/03/BR.Y.001_ForensicExplorer_TR.pdf] Erişim Tarihi: 30.04.2022

Firefox 2022, Erişim: [https://tr.wikipedia.org/wiki/Mozilla_Firefox] Erişim Tarihi: 08.02.2022

Ftk 2022, Erişim: [https://www.exterro.com/forensic-toolkit] Erişim Tarihi: 09.05.2022

Ftk 2022, Erişim: [https://www.exterro.com/resources/forensic-toolkit-ftk-brochure] Erişim Tarihi: 16.05.2022

Ftk kurs 2022, Erişim: [https://training.accessdata.com/exam/accessdata-certified-examiner] Erişim Tarihi: 27.04.2022

Gergerlioğlu-2021, Erişim: [https://web.archive.org/web/20210716124838/https://www.internethaber.com/hdpli-omer-faruk-gergerlioglu-4-ay-sonra-yeniden-meclise-dondu-aym-hak-ihlali-karari-verdi-2196620h.htm] Erişim Tarihi: 01.05.2022

Giac 2022, Erişim: https://www.giac.org/about/company-info/?msc=main-nav Erişim Tarihi: 17.05.2022

Google 2019, Erişim: [https://bertanuzun.com/arama-motorlari/] Erişim Tarihi: 11.10.2019

Google Kullanım 2019, Erişim: [https://www.webtekno.com/google-chrome-tarayici-pazarindaki-ezici-ustunlugunu-gosteren-tablo-h78947.html] Erişim Tarihi: 22.12.2019

Hasan Saş'a Hakaret, Erişim: [https://skor.sozcu.com.tr/2019/03/07/hasan-sasa-twitterdan-hakarete-ceza-1038127/] Erişim Tarihi: 21.06.2019

Ics 2022, Erişim: [https://ics-iq.com/about-us/] Erişim Tarihi: 16.05.2022

ISC 2022, Erişim: [https://www.isc2.org/about] Erişim Tarihi: 19.05.2022

İlk ceza 2013, Erişim: [https://www.sabah.com.tr/aktuel/2013/02/15/twitterdan-tehdit-ve-hakarete-ilk-ceza] Erişim Tarihi: 21.06.2019

İnternet 2019, Erişim: [http://www.internetarsivi.metu.edu.tr/tarihce.php] Erişim Tarihi: 30.06.2019

İstatistik Twitter 2022, Erişim: [https://www.websiterating.com/tr/research/twitter-statistics/] Erişim Tarihi: 01.04.2022

İstinabe 2021, Erişim: [https://diabgm.adalet.gov.tr/Home/SayfaDetay/internet-ortaminda-islenen-suclarda-uluslararasi-ceza-istinabe-islemleri14022020041756] Erişim Tarihi: 21.03.2022

İstinabe 2022, Erişim: [https://diabgm.adalet.gov.tr/arsiv/sozlesmeler/ikitaraflisoz/ceza/abd.pdf] Erişim Tarihi: 19.04.2022

Kaftancıoğlu Twitter-2022, Erişim: [https://www.haberler.com/haberler/canan-kaftancioglu-ne-dedi-neden-tutuklandi-14937203-haberi] Erişim Tarihi: 08.05.2022

Konsey 2022, Erişim: [https://www.mbkaya.com/hukuk/avrupa-konseyi-siber-suc-sozlesmesi.pdf] Erişim Tarihi: 21.12.2021

MD-5 2015, Erişim: [http://tr.wikipedia.org/wiki/MD5] Erişim Tarihi: 04.01 2022.

Medya 2019, Erişim: [https://www.makaleler.com/medya-nedir] Erişim Tarihi: 18.11.2019

Metin Uca Ceza-2020, Erişim: [https://tr.euronews.com/2020/06/05/gazeteci-metin-uca-ya-twitter-paylas-m-nedeniyle-14-ay-hapis-cezas] Erişim Tarihi: 03.01.2022

Mobil İnceleme 2013, *Developing Process for Mobile Device Forensics, Det. Cynthia A. Murphy*, Erişim: [http://www.mobileforensicscentral.com/mfc/documents /Mobile%20 Device%20Forensic%20Process%20v3.0.pdf] Erişim Tarihi: 03.01.2022

Murat Boz Hakaret-2012, Erişim: [https://t24.com.tr/haber/twitterdan-hakaret-serbestmi,198627] Erişim Tarihi: 23.06.2019

Nazlı Ilıcak Ceza-2018, Erişim: [https://www.trthaber.com/haber/turkiye/nazli-ilicaka-cumhurbaskanina-hakaret-sucundan-hapis-399007.html] Erişim Tarihi: 22.06.2019

Nuix 2022, Erişim: [https://www.emt.com.tr/tr/markalar/nuix-43#nuix-workstation] Erişim Tarihi: 20.05.2022

OĞUZ R. Adli Bilişimde İnceleme Süreçleri Ankara Üniversitesi Sağlık Bilimleri Enstitüsü Yüksek lisans Tezi S: **63**

Ö.F. Gergerlioğlu Twitter Ceza-2022, Erişim: [https://www.cumhuriyet.com.tr/haber /hdpli-omer-faruk-gergerlioglunun-vekilligi-dustu-1821298] Erişim Tarihi: 18.04.2022

Open text 2022, Erişim: [https://blogs.opentext.com/announcing-opentext-security-and-protection-cloud-ce-21-2/] Erişim Tarihi: 21.05.2022

Os Forensic 2022, Erişim: [https://www.passmark.com/about/index.php] Erişim Tarihi: 21.04.2022

Önder Aytaç Ceza-2014, Erişim: [https://www.mynet.com/erdogana-twitterdan-hakarete-10-ay-hapis-110101206140] Erişim Tarihi: 22.06.2019

Pınar YILDIRIM Ceza-2020, Erişim: [https://onedio.com/haber/sosyal-medya-fenomeni-pucca-nin-hapis-cezasi-almasina-sebep-olan-tweet-bircok-kisiyi-sasirtti-1011303**]** Erişim Tarihi: 02.04.2022

Recovery My Files (Versiyon 16.7) Avusturalya'da bulunan GetData firmasının geliştirdiği veri kurtarma yazılımıdır [https://getdata.com/recovermyfiles/]

Sedat Peker Takipsizlik-2015, Erişim: [https://www.timeturk.com/zekeriya-oz-un-suc-duyurusuna-takipsizlik/haber-106465] Erişim Tarihi: 23.06.2019

Şensayar Tehdit-2018, Erişim: [https://www.demokrathaber.org/senyasara-yonelik-olum-tehdidinde-takipsizlik-facebook-twitter-yahoo-ve-google-delil-sayilamaz] Erişim Tarihi: 08.05.2022

Social-2022, Erişim: [https://wearesocial.com/uk/blog/2022/01/digital-2022-another-year-of-bumper-growth-2/] Erişim Tarihi: 26.01.2022

Social-1 2022, Erişim: [https://wearesocial.com/wp-content/uploads/sites /2/2022/01/02-Global-headlines-DataReportal-20220124-Digital-2022-Global-Overview-Report-v01-Slide-9-1024x576-1-1.png] Erişim Tarihi: 26.01.2022

Social-2 2022, Erişim: [https://wearesocial.com/wp-content/uploads/sites/2/2022/01/03-Global-growth-DataReportal-20220124-Digital-2022-Global-Overview-Report-v01-Slide-10-1024x576-1-1.png] Erişim Tarihi: 26.01.2022

Social-3 2022, Erişim: [https://wearesocial.com/wp-content/uploads/sites/2/2022/01/06-Social-media-growth-10-year-chart-DataReportal-20220124-Digital-2022-Global-Overview-Report-v01-Slide-88-1-1024x576-1-1.png] Erişim Tarihi: 26.01.2022

Solo 2022, Erişim: [https://ics-iq.com/solo-5-enterprise-m-2-kit-i7-forensic/] Erişim Tarihi: 11.05.2022

Şirket 2021, Erişim: [https://www.haberturk.com/twitter-turkiye-temsilcisi-belli-oldu-iste-detaylar-haberler-3049649-teknoloji] Erişim Tarihi: 17.02.2022

Talep Twitter 2022, Erişim: [https://help.twitter.com/tr/rules-and-policies/twitter-legal-faqs] Erişim Tarihi: 28.03.2022

Teknoloji 2022, Erişim: [https://www.teknolojioku.com/guncel/iste-twitteri-en-cok-kullanan-ulkeler-turkiye-kacinci-sirada-6269730d5cb7817f0a535426?p=2] Erişim Tarihi: 28.04.2022

Twitter kolluk 2022, Erişim: [https://help.twitter.com/tr/rules-and-policies/twitter-law-enforcement-support] Erişim Tarihi: 21.04.2022

TX1 2022, Erişim: [https://www.emt.com.tr/tr/markalar/tableau-63] Erişim Tarihi: 12.04.2022

Twitter social, Erişim: [https://wearesocial.com/uk/blog/2022/01/digital-2022-another-year-of-bumper-growth-2/] Erişim Tarihi: 27.04.2022

Ufed 2022, Erişim: [https://www.sec.gov/Archives/edgar/data/0001854587/000121390021026630/ff42021_cellebritedi.htm#T16] Erişim Tarihi: 14.05.2022

Uludağ Ceza-2021, Erişim: [https://www.gazeteruzgarli.com/gazeteci-alican-uludaga-twitter-paylasimi-nedeniyle-10-ay-hapis-cezasi-verildi/] Erişim Tarihi: 03.04.2022

Xry 2022, Erişim: [https://www.emt.com.tr/tr/markalar/msab-39#xec-director] Erişim Tarihi: 13.05.2022

x-ways 2022, Erişim: [http://www.x-ways.net/forensics/index-m.html] Erişim Tarihi: 09.04.2022

x-ways user, Erişim: [http://www.x-ways.net/winhex/manual.pdf] Erişim Tarihi: 10.04.2022

Yargıtay 2021, Erişim: [https://www.trthaber.com/haber/gundem/yargitaydan-retweet-karari-603641.html] Erişim Tarihi: 01.05.2022