



T.C

FIRAT ÜNİVERSİTESİ

TEKNOLOJİ FAKÜLTESİ

ADLİ BİLİŞİM MÜHENDİSLİĞİ

ADLİ BİLİŞİMDE OLAY YERİ İNCELEMESİ

VE İNCELEME SÜREÇLERİ

NİDA CANPOLAT

İçindekiler

ADLİ BİLİŞİM NEDİR	4
OLAY YERİ VE ADLİ BİLİŞİM UZMANI	4
DELİLİN ÖZELLİKLERİ	7
ADLİ BİLİŞİM SUÇLARI VE DELİLLERİ	8
OLAYA İLK MÜDAHALE VE TESPİT	9
İNCELEME VE ANALİZ	10
İMAJ ALMA ARAÇLARI	11
FTK İMAGER.....	11
ENCASE IMAGER.....	12
WINHEX.....	12
FEX İMAGER	13
PRODISCOVER STANDART	14
TABLEAU TD2	14
CRU DİTTO	15
HARDCOPY	15
FORENSİC DOSSİER	16
RAM İMAJİ ALMA ARAÇLARI.....	17
BELKASOFT	17
DUMPIT.....	17
X-WAYS CAPTURE	18
AĞ TRAFİĞİ İNCELEME ARAÇLARI.....	19
SAVVİUS INSİGHT	19
NETFLOW ANALYZER	19
WIRESHARK.....	20
PİNK.....	21
VERİ KURTARMA ARAÇLARI	21
PC3000.....	21
DFL-PCIE 4X DATA RECOVERY EXPRESS.....	22
İNCELEME YAZILIMLARI	23
FTK	23
FEX	24
UFED	25
ENCASE.....	26
AUTOPSY	27
OXYGEN FORENSİC	28

RAPORLAMA	29
OLABİLECEK SORUNLAR	30
İNCELEME SÜRECİNDE KARŞILAŞILAN FARKLILIKLAR	32
ARIZALI USB BELLEK VE SSD KART	32
HAZIR UYGULAMA KULLANILAMADIĞI DURUMLAR	34
THE SLEUTH KIT	34
HEXADECİMAL KODLAR.....	35
MFT ANALİZİ.....	37
REGİSTERY KAYITLARININ İNCELENMESİ	38
SANAL MAKİNE İNCELENMESİ	39
VİRÜSLÜ DOSYALAR.....	42
NET OLMAYAN FOTOĞRAF VE VİDEOLAR	42
NET OLMAYAN SES DOSYALARI	44
ÖRNEK VAKALAR SENARYOLAR	45
VAKA 1	45
ÇÖZÜM 1	45
VAKA 2	46
ÇÖZÜM 2	46
VAKA 3.....	48
ÇÖZÜM 3.....	48
Kaynakça	51

ADLİ BİLİŞİM NEDİR

Adli bilişim kavramı, elektronik cihazların da dâhil olduğu siber suçların tespit edilmesine ve incelenmesine yarayan bilim dalıdır. Adli bilişim, elektronik ortamda var olan görüntüler, sesler ve ya herhangi bir verilerin delil niteliği taşıyacak bir biçimde tespit edilmesi, incelenmesi ve işlenmesi çalışmalarını kapsayan alandır. Tespit ve inceleme işlemlerini yaparken sabit disk, harici disk, bilgisayar, tablet ve telefon gibi elektronik cihazlardan veri kurtarma ve kazıma işlemlerini yapar. Kazıma işlemi için kullanıcının aktif olarak kullandığı alanlardan, tahsis edilmemiş alanlardan, artık alanlardan ve silinmiş verilerin bulunduğu alanlardan yararlanılır. Ardından elde edilen bilgileri hukuki süreçlere uygun bir şekilde, delil bütünlüğü ve doğruluğu korunarak mahkemeye sunulmak üzere belgeleme işlemi yapar. Belgeleme işlemi mahkemenin kabul edeceği bir şekilde yapılmalıdır ve bu belgede kişiyi aklayacak ya da suçlayacak bir yorum olmamalıdır. Araştırmalar tamamen bilimsel olup tarafsız bir rapor sunulmalıdır. Bunu için farklı maddeler ve kurallar bulunmaktadır. Adli bilişim alanı aynı zamanda; bilişim ile ilgili suçlarda, siber güvenlikte, adli analizlerin yapılmasında ve bilgi güvenliğinin korunması alanlarında kullanılan bilim dalıdır.

Olay yeri incelemeleri sırasında Adli bilişim kavramlarından sıkça faydalanılır. Bu yazıda hangi adli bilişim süreçlerden geçildiğini ve bu süreçlerin nasıl işlendiğine değinilecektir. Olay yeri incelemelerinde uygulanan genel adımlar; ilk müdahale aşaması, inceleme aşaması, çözümleme aşaması ve raporlama aşamasıdır. Bu adımlar kendi içinde de bazı ana dallara ayrılır. Bilişim suçlarının var olduğu bir olayda, delillerin bulunmasından mahkemeye sunulduğu süreçteki aşamalar adli bilişim süreçlerini ifade eder. Suçun aydınlatılması, kişi veya kişilere gerekli hükmün giydirilmesi için kuralına uygun bir biçimde delil elde edilmesi, delinin doğruluğunun ve bütünlüğünün korunması, delinin usulüne uygun işlenmesi, aydınlatılması ve belgelenmesi gibi aşamaların hepsi adli bilişim kavramını oluşturan bir bütündür.

OLAY YERİ VE ADLİ BİLİŞİM UZMANI

İlk olarak olay yeri; herhangi bir suçun işlenmesi durumunda, olayın gerçekleştiği yerlerde suçun ortaya çıkarılmasına ilişkin yapılan işlemlere ve delilin tespit edilip,

korunup, incelenme aşamalarının gerçekleştirilmesine olanak sağlayan işlemler olay yeri incelemesi olarak bilinir.

Adli bilişim uzmanı ise, elektronik delillerin usulüne uygun tespit edilmesini, korunmasını, incelenmesini ve raporlanması sağlayan kişidir. Bu işlemler titizlik ve uzmanlık gerektirir. Aşamaların usulüne uygun bir biçimde gerçekleştirilmediği takdirde delil bütünlüğü ve doğruluğu bozulabilir. Bu durumda bir adli bilişim mühendisi veriyi eksiksiz ve doğru bir şekilde tespit edip, inceleyen kişidir.

Bahsedilen özelliklerden dolayı adli bilişim uzmanı, adli olaylarda bilirkişi olarak atanabilir. Bunun ile ilgili yasa CMK 63. Madde 'de belirtilmiştir. Kanuna göre;

“ (1) Çözümü uzmanlığı, özel veya teknik bilgiyi gerektiren hâllerde bilirkişinin oy ve görüşünün alınmasına re'sen, Cumhuriyet savcısının, katılanın, vekilinin, şüphelinin veya sanığın, müdafinin veya kanunî temsilcinin istemi üzerine karar verilebilir. (Değişik cümle: 3/11/2016-6754/42 md.) Ancak, genel bilgi veya tecrübeyle ya da hâkimlik mesleğinin gerektirdiği hukukî bilgiyle çözümlenmesi mümkün olan konularda bilirkişiye başvurulamaz. (Ek cümle: 3/11/2016-6754/42 md.) Hukuk öğrenimi görmüş kişiler, hukuk alanı dışında ayrı bir uzmanlığa sahip olduğunu belgelendirmedikçe, bilirkişi olarak görevlendirilemez.

(2) Bilirkişi atanması ve gerekçe gösterilerek sayısının birden çok olarak saptanması, hâkim veya mahkemeye aittir. Birden çok bilirkişi atanmasına ilişkin istemler reddedildiğinde de aynı biçimde karar verilir.

(3) Soruşturma evresinde Cumhuriyet savcısı da bu maddede gösterilen yetkileri kullanabilir.”

Adli bilişim uzmanında olması gereken bazı özellikler vardır. Bunların ilki deneyime sahip olmasıdır. Çünkü delillerin tespit edilmesinde raporlamasında kadar geçen sürede yapılan küçük bir yanlış bile delili karartabilir. Bunun sonucunda kişi veya kurumlar zarar görebilir. Diğer bir özellik ise delilin tespitinden raporlanmasına kadar geçen zamanın planlı bir şekilde yapılmasıdır. Delil türüne göre nasıl elde edileceğini ve incelenmesi gerektiğini önceden planlamalıdır. Plansız yapılan aşamalar delil ile ilgili olumsuzluklara yol açabilir. Aynı zamanda delili bir bütün olarak alabilmeli ve asıl hallerini koruyabilmelidir. Delil elde etme aşamasında zamanını iyi ayarlayarak olabildiğince çabuk olunmalıdır. Özellikle elektronik deliller yapısı gereği değişmeden,

olaydan kısa süre içinde delillerin elde edilmesi gerekmektedir. Elde edilen verilerin incelenmesi için, yazılım ve donanım bilgileri gerekmektedir. İyi bir adli bilişim uzmanı gerekli olan yazılımları ve donanımları etkili bir biçimde kullanabilmelidir. İnceleme yaptığı esnada verinin güvenliğini sağlamalı ve gizliliğe önem vermelidir.

Olay yeri inceleme sırasında bir adli bilişim uzmanının dikkat etmesi gereken durumlar olduğuna daha önce değinilmişti. Örneğin adli bilişim uzmanı orijinal delil üzerinde inceleme yapamaz. Çünkü delil bütünlüğünün ve doğruluğunun değişme riski vardır. Bunun için orijinal delilin bir kopyası alınır ve bunun üzerinde incelemeler yapılır. Bu konu ile ilgili düzenlemeyi CMK'nın 134. Maddesi düzenler. CMK 134'e göre;

“(1) Bir suç dolayısıyla yapılan soruşturmada, somut delillere dayanan kuvvetli şüphe sebeplerinin varlığı ve başka surette delil elde etme imkânının bulunmaması halinde, hâkim veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısı tarafından şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine (...) (2) karar verilir. (Ek üç cümle: 25/7/2018-7145/16 md.) Cumhuriyet savcısı tarafından verilen kararlar yirmi dört saat içinde hâkim onayına sunulur. Hâkim kararını en geç yirmi dört saat içinde verir. Sürenin dolması veya hâkim tarafından aksine karar verilmesi hâlinde çıkarılan kopyalar ve çözümü yapılan metinler derhâl imha edilir.

(2) Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması ya da işlemin uzun sürecektir olması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere el konulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, el konulan cihazlar gecikme olmaksızın iade edilir.

(3) Bilgisayar veya bilgisayar kütüklerine el koyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır.

(4) Üçüncü fıkraya göre alınan yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır.

(5) Bilgisayar veya bilgisayar kütüklerine el koymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kâğıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır. “

Bir adli bilişim uzmanının bu maddelere uymayıp, yedekleme işlemi yapmadan delil üzerinde inceleme yapması; delilin bütünlüğünün bozulması, değiştirilmesi ve doğruluğunu kaybetmesi gibi gerekçelerle mahkeme tarafından kabul edilmeyecektir. Sonuç olarak sistemin işleyişi bozulduğundan dolayı TCK bu konuyla ilgili yaptırımlar içerir. TCK'nın 244. Maddesinde;

“ (1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.

(3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır.

(4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beş bin güne kadar adlî para cezasına hükmolunur. “

DELİLİN ÖZELLİKLERİ

Sunulan delillerin mahkeme tarafından kabul edilebilmesi için bazı genel özellikleri içermesi gerekmektedir. Bunlardan biri delilin kanıtlanabilir olmasıdır. Bu konu ile ilgili yasa CMK'nın 217. Maddesinde düzenlenmiştir. Bu maddeye göre;

“ (1) Hâkim, kararını ancak duruşmaya getirilmiş ve huzurunda tartışılmış delillere dayandırabilir. Bu deliller hâkimin vicdanî kanaatiyle serbestçe takdir edilir.

(2) Yüklenen suç, hukuka uygun bir şekilde elde edilmiş her türlü delille ispat edilebilir.”

Diğer yandan delil gerçekçi ve akla uygun olmalıdır. Bu bağlamda deliller objektif olup ispat eder yapıda olmalıdır. Delillerin bir diğer özelliği ise kanuna uygun bir biçimde elde edilmiş olup, olayı aydınlatacak yapıda olmalıdır. Mahkemeye sunulamayan soyut deliller delilden sayılmaz. Kabul edilebilmesi için somut olmalıdır.

Ayrıca delilin kabul edilebilmesi için delil yasağı kapsamında ve delil değerlendirme yasağı kapsamında bulunmaması gerekmektedir. Bu konu ile ilgili 1982 Anayasası 38. Maddesinde bu konuya değinilmiştir. Maddeye göre;

“ (1) Kanuna aykırı olarak elde edilmiş bulgular, delil olarak kabul edilemez. “

Delil yasakları, delil elde etme konusuna bazı kısıtlamalar getirmiştir. Örneğin bir delil elde edilirken soruşturmacılar gizli soruşturmacı olarak çalışmak zorundadır. Bu konuyla ilgili CMK'nın 139. Maddesi 6. Fıkrası gereği kişisel bilgiler soruşturma dışında kullanılamayacaktır.

“ (6) Soruşturmacı görevlendirilmesi suretiyle elde edilen kişisel bilgiler, görevlendirildiği ceza soruşturması ve kovuşturması dışında kullanılamaz. (Ek: 21/2/2014–6526/13 md.) Suçla bağlantılı olmayan kişisel bilgiler derhâl yok edilir. “

Yani deliller sadece olay lehine kullanılabilir nitelikte olmalıdır, bunun dışındaki delille delilden sayılmamaktadır.

Delilin elde edilme yöntemi de delil yasağı kapsamına girebilir. Örneğin orijinal bir delil üzerinde çalışmak delilin kabul edilebilirliğine zarar verebilir. Bunun için delinin imajı üzerinde çalışılmalıdır.

ADLİ BİLİŞİM SUÇLARI VE DELİLLERİ

Adli bilişim çerçevesinde suç sayılabilecek birden fazla konu mevcuttur. Bunlar sahtecilik, kaçakçılık, bilgisayar ile hırsızlık, para tuzakları, yasa dışı ticaret, kişisel bilgilerin internet ortamına sızdırılması, internet casusluğu, dolandırıcılık ve hackleme olayları gibi genel başlıklar adli bilişim suçları arasındadır.

Bu gibi suçlar bilgisayarlarda, tabletlerde, USB belleklerde, DVD/CD gibi disklerde, sabit disklerde, yazıcı gibi elektronik aletlerde, cep telefonlarında ve hafıza kartlarında bulunabilir. Bahsedilen bu yapılarda delil olarak nitelendirebilecek birçok veri mevcuttur. Bu veriler genel olarak; fotoğraflar dosyaları, video dosyaları, tarayıcı geçmişi, çerezleri ve kaydedilen kullanıcı bilgileri, indirilmiş olan dosyalar, zararlı yazılımlar, gizlenmiş ya da uzantısı değiştirilmiş dosyalar, sistem dosyaları, çöp

kutusu, tahsis edilmemiş alan, log dosyaları, registry dosyaları, işletim sistemi gibi yapılardır.

OLAYA İLK MÜDAHALE VE TESPİT

Olay yerine ilk müdahale için ilk olarak gerekli izinlerin çıkması gerekmektedir. Delillerin elde edilebilmesi için hukuki olarak izin verilmelidir. Bu konu ile ilgili CMK'nın 119. Maddesi şu şekildedir;

“(1)(Değişik : 25/5/2005 – 5353/15 md.) Hâkim kararı üzerine veya gecikmesinde sakınca bulunan hâllerde Cumhuriyet savcısının, Cumhuriyet savcısına ulaşılamadığı hallerde ise kolluk amirinin yazılı emri ile kolluk görevlileri arama yapabilirler.

Ancak, konutta, işyerinde ve kamuya açık olmayan kapalı alanlarda arama, hâkim kararı veya gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısının yazılı emri ile yapılabilir. Kolluk amirinin yazılı emri ile yapılan arama sonuçları Cumhuriyet Başsavcılığına derhal bildirilir.

(2) Arama karar veya emrinde;

a) Aramanın nedenini oluşturan fiil,

b) Aranılacak kişi, aramanın yapılacağı konut veya diğer yerin adresi ya da eşya,

c) Karar veya emrin geçerli olacağı zaman süresi, Açıkça gösterilir.

(3) Arama tutanağına işlemi yapanların açık kimlikleri yazılır. (Mülga ikinci cümle: 25/5/2005 – 5353/15 md.)

(4) Cumhuriyet savcısı hazır olmaksızın konut, işyeri veya diğer kapalı yerlerde arama yapabilmek için o yer ihtiyar heyetinden veya komşulardan iki kişi bulundurulur.

(5) (Değişik: 25/7/2018-7145/14 md.) Askerî mahallerde yapılacak arama, Cumhuriyet savcısının nezaretinde askerî makamların katılımıyla adlî kolluk görevlileri tarafından yerine getirilir. Gecikmesinde sakınca bulunan hâllerde

Cumhuriyet savcısının yazılı emriyle de askerî makamların katılımıyla adlî kolluk görevlileri tarafından arama yapılabilir. “

Gerekli izinlerden sonra, incelenmeye başlanmadan önce olay yeri korunma altına alınmalıdır. Bu eylemin amacı, delillerin zarar görmemesi, değiştirilmemesi ve kaybolmamasıdır. Olay yerinde sadece inceleme yapacak olan ekip olmalıdır. İnceleme ekibinden olmayan herkes çıkarılmalıdır. İnceleme yapan ekibin, delillere çıplak elle dokunmaması ve delil bütünlüğüne zarar vermeyecek bir şekilde giyinmesi gerekmektedir. Delil elde edilirken delil elde etme yasakları ve delil inceleme yasakları göz önünde bulundurularak hareket edilmelidir. İncelenmeye başlamadan önce olay yerinde olanları kayıt altına alabilmesi için kamera gerekmektedir. Açık olan bir bilgisayar varsa ya da canlı analiz yapılmak zorunda kalırsa bu durum kesinlikle kayıt altına alınmalıdır. Olay yerinde bulunan tüm cihazlar incelenmeden önce etiketlenmelidir. Etiket delil ve olay ile ilgili gerekli bilgileri içermelidir. Etiketlenen cihazlar delil listesine eklenmelidir. Elde edilen elektronik delillerin kopyası yani imajı alınmalıdır. İmaj alınırken writeblocker kullanılmalıdır. Bu cihazın kullanılmasının sebebi tek yönlü veri akışını sağlamak ve cihazın değişmesini engellemektir. İmajı alınan verinin hash değeri hesaplatılmalıdır. Bu değer verinin değiştirilmediğini kanıtlamak için kullanılır. İmaj alınmadan önce imajı alınacak cihazla ilgili mümkün olduğu kadar bilgi elde edilmelidir. Örneğin imajı alınacak bilgisayarın işletim sistemi ve sürümü hakkında bilgi edinilirse daha rahat ve güvenli bir şekilde imaj alınabilir. Bu süreçte yapılan her eylem bir dosyaya kaydedilmelidir. RAM gibi geçici bellekler bilgisayarın kapanması ile kapanır. Bunu göz önünde bulundurarak gerekli müdahaleler yapılmalıdır. Ayrıca elde edilen deliller bir sonraki aşamaya kadar güvende tutulmalıdır.

İNCELEME VE ANALİZ

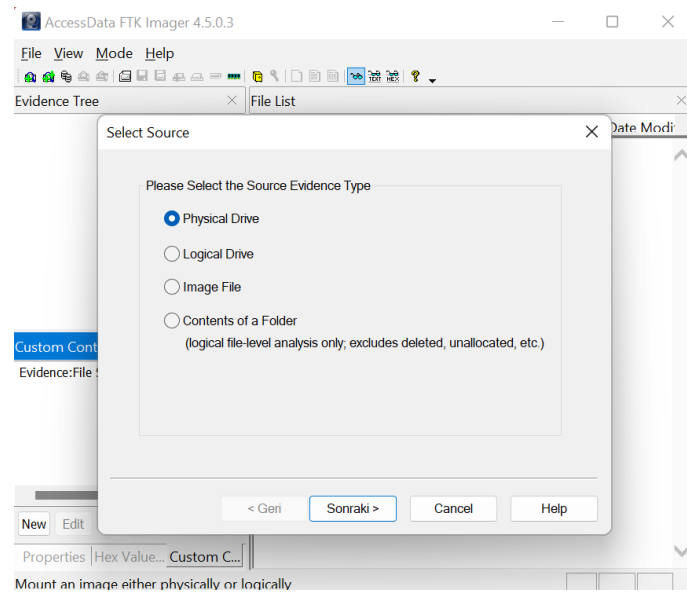
Bu aşama delil olduğuna karar verilen cihaz ya da cihazlardan bulguların elde edildiği aşamadır. Bu aşamada deliller incelenir ve bazı teknik analizler uygulanır. Ancak delil bütünlüğünün ve doğruluğunun korunabilmesi için inceleme ve analiz işleminde kopyalanmış veriler kullanılmalıdır. Analiz sırasında kullanılan yazılımlar doğru bir şekilde ve yerinde kullanılmalıdır.

İncelenme yapılabilmesi çeşitli yazılımlar ve donanımlar mevcuttur. Bu yapılar delil türüne göre kullanılmalıdır. Bir adli bilişim uzmanı delilin en doğru şekilde nasıl incelenebileceğini belirledikten sonra incelemelidir. Deliller en detaylı biçimde incelenir ve gerçekleşen suç ile ilgili bağlantılı olabilecek kanıtlar elde edilir. Bu işlem sırasında inceleyicinin amacı kişiyi suçlu ya da masum olarak göstermek olmayıp, sadece objektif bir şekilde delillerin aydınlatılması olduğu unutulmamalıdır. Bu aşamanın son işlemi elde edilen kanıtları mahkemeye sunmak üzere raporlanmasıdır.

İMAJ ALMA ARAÇLARI

FTK IMAGER

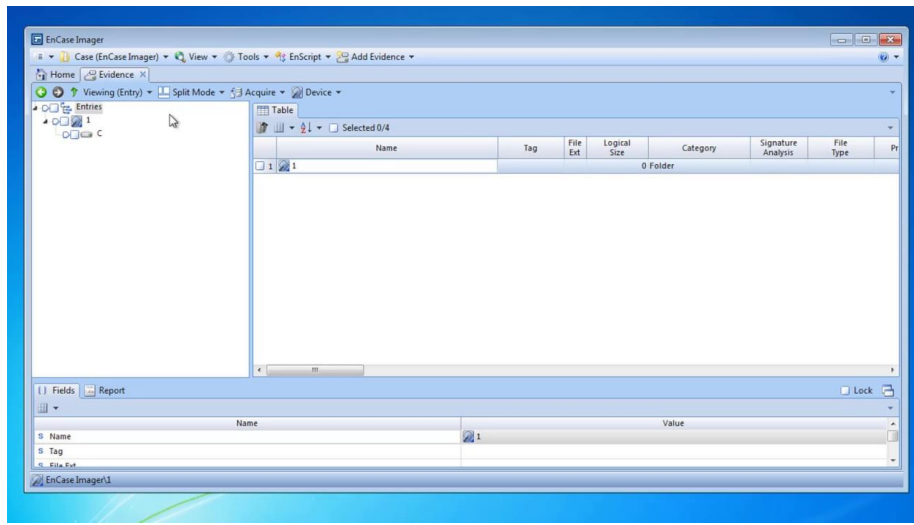
FTK IMAGER, Windows tabanlı bir yazılım olup cihazların imajını almaya yarar. Tamamen ücretsiz bir yazılımdır. Kopyası alınacak olan cihazın fiziksel, mantıksal ya da sadece bir kısmının imajını alabilir. İmaj alma işlemini yaparken farklı türlerde imaj almaya imkân sağlar. Bu türler genel olarak dd, e01, SMART ve AFF formatındadır. dd türü ile ham imaj alınır. Herhangi bir sıkıştırma yapmaz. İmajı alınan yapı ile aynı boyuttadır. İçerisinde metadata verisi bulunmaz. SMART türü, Linux işletim sistemi için geliştirilmiş bir formattır ve hem metadata verisi içerir hem de doğrulama kodlarını hesaplar. E01, EnCase imaj türüdür. Veriyi istenilen boyutta sıkıştırarak imajını alır. İmaj alma işlemi sıkıştırma yüzünden biraz daha uzun sürebilir. Hem metadata verisini hem de doğrulama kodlarını içerir. Son olarak AFF formatı ise gelişmiş dosya formatını ifade eder. Veriyi ve metadata verisini birleştirir.



Şekil 1. FTK Imager ara yüzü

ENCASE IMAGER

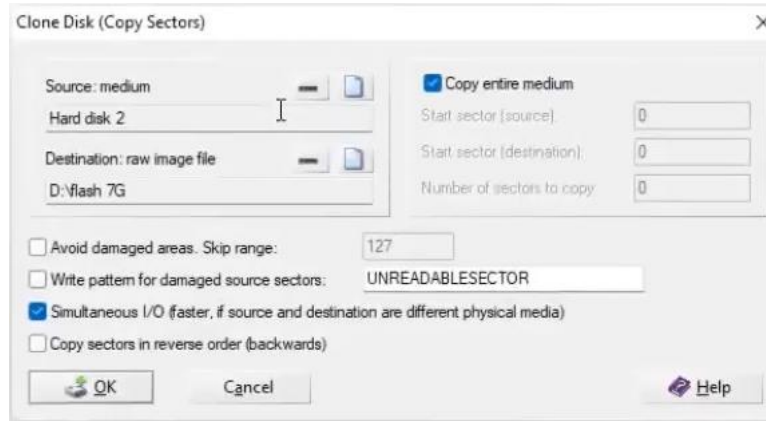
Encase yazılımının imaj almaya yarayan türüdür. Bu yazılım Encase yazılımının aksine sadece imaj almaya izin verir. Aldığı imajları E01 formatında alır. E01 formatı veriyi bloklara bölerek kopyalarını çıkarır. Yani sıkıştırma yapar. Sıkıştırma oranını kullanıcı seçer. Aldığı imajda metadata verisi ve doğrulama kodunu barındırır.



Şekil 2. Encase Imager ara yüzü

WINHEX

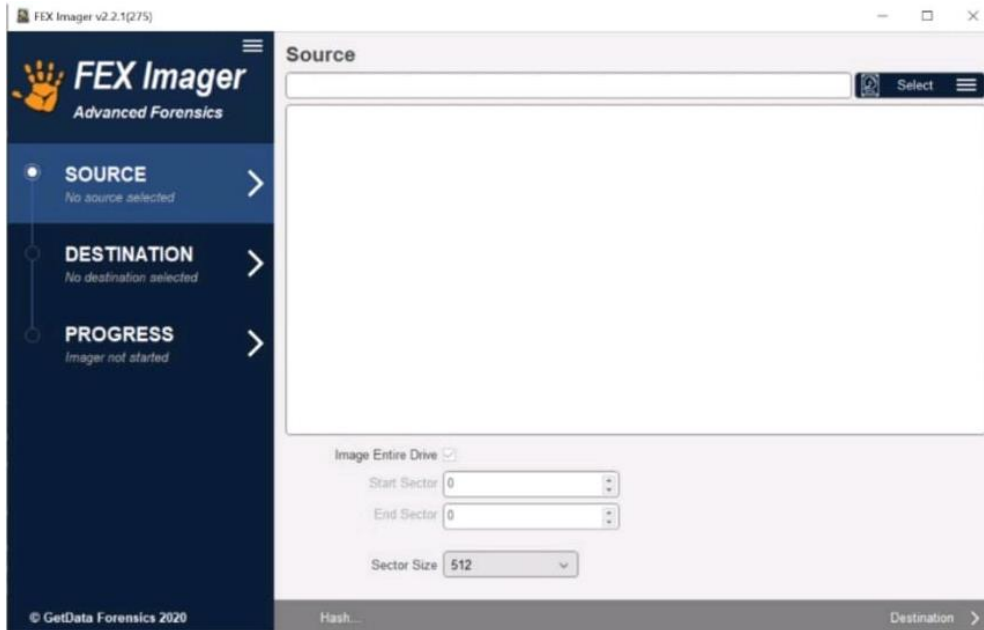
Ücretsiz imaj alma yazılımları arasındadır. Hem fiziksel hem mantıksal imaj almaya yarar. Özellikle DVD ve CD gibi cihazların imajını almada en sık kullanılan programlar arasındadır. Programın amacı sadece verinin imajını almak değildir. Bu program sayesinde disk formatları düzenlenebilir, yedekleme, kurtarma ve kalıcı silme gibi işlemleri de gerçekleştirir.



Şekil 3. Winhex ara yüzü

FEX İMAGER

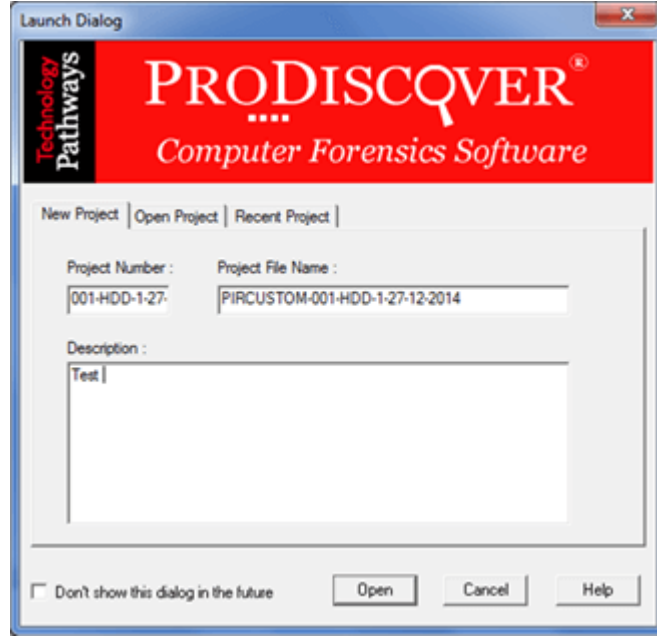
GetData Forensic tarafından geliştirilmiş bir yazılımdır. E01 ve dd formatında imaj almaya olanak sağlar. FEX programının imaj almak için kullanılan sürümüdür. Programın aynı zamanda writeblocker özelliği de vardır. Yani yazma korumalı bir şekilde çalışır. Bu da verinin güvenliğini arttıran bir durumdur.



Şekil 4. FEX Imager ara yüzü

PRODISCOVER STANDART

TechPathways şirketi tarafından kurulan ücretsiz bir imaj alma yazılımıdır. İmaj alma ve daha önceden var olan imaj türlerini farklı bir türe dönüştürme işlemlerinde kullanılır.



Şekil 5. ProDiscover Standart ara yüzü

TABLEAU TD2

İmaj alma işlemlerinde çok sık kullanılan bir donanımdır. Hem SATA hem IDE bağlantıları içermesi kullanım alanını arttırmaktadır. Elde edilen dijital verilerin kopyalarını oluşturmada kullanılır. Kopyalama işlemleri sırasında writeblocker özelliğini kullanır. Bu özellik sayesinde kaynak diske olabilecek herhangi bir erişim engellenerek, disk güvence altına alınır. Aynı zamanda imaj alma işleminden sonra bir de hash imajını alır. Bu cihaz imaj alma işlemi dışında diskin kopasını alabilir ve diski güvenli bir şekilde silebilir.



Şekil 6. Tableau TD2

CRU DİTTO

Özellikle Adli Bilişim alanında sıkça kullanılan adli kopya alma yazılımıdır. Ditto ile imaj alma, veri çıkarma ve veri analizi yapılır. CRU Ditto; Kaynak diski klonlanması, hash değerlerinin hesaplanması, diskin fiziksel ve mantıksal imajının çıkarılması, hedef diskin tamamen silinmesi, kayıt defterinin görüntülenmesi ve varsa cihazın bağlı olduğu ara yüzün görüntülenmesi gibi çeşitli özellikler mevcuttur.



Şekil 7. CRU Ditto

HARDCOPY

İmaj alma donanımları arasında yer alan bir diğer donanım ise HardCopy donanımdır. Hedef diskin imajını alma, klonunu oluşturma ve güvenli silme gibi özellikleri mevcuttur. Diğer donanımlar gibi HardCopy de hash değeri hesaplaması yapabilir. Aynı zamanda

dakikada 6 GB'a varan veri transferi yapabilir. HPA ve DCO alanlarını geçerek verileri okuyabilir.



Şekil 8. HardCopy

FORENSIC DOSSIER

Adli kopya alma işlemlerinde kullanılan Forensic Dossier; SAS, SATA, USB, IDE, PATA ve FIREWIRE girişlerini barındırdığı için kullanım alanı oldukça geniştir. Kaynak diskin aynı anda iki kopyasını oluşturabilir. HPA ve DCO alanlarından etkilenmez. Bu alandaki verileri de okuyabilir. Kopyalama işleminden sonra hash değeri hesaplayabilir. Dakikada 7 GB'a varan veri okuması yapabilir. Diğer birçok donanımdan farklı olan bir özelliği mevcuttur. Bu cihaz kaynak üzerinde kelime araması da gerçekleştirebiliyor. Elde ettiği bilgileri Ethernet kablosu yardımı ile paylaşımına açabilmektedir.



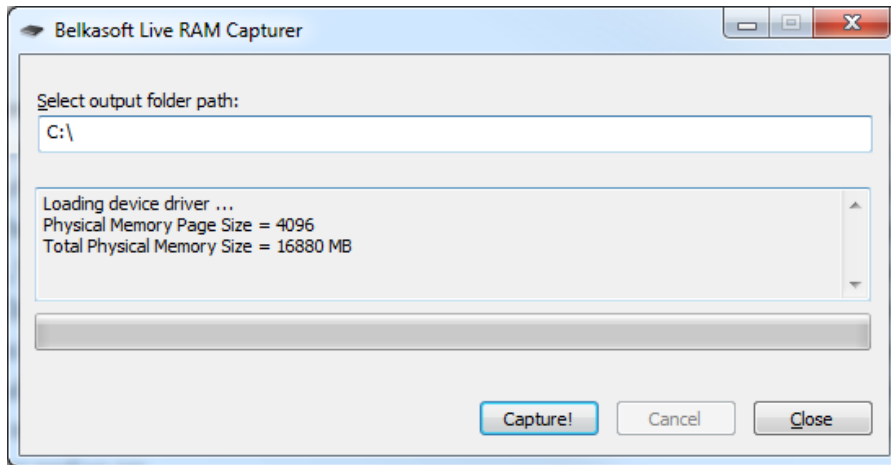
Şekil 9. Forensic Dossier

RAM İMAJİ ALMA ARAÇLARI

RAM imajı almak delil bütünlüğü bakımından çok önemlidir. RAM geçici bir depolama birimi olduğu için bilgisayarın kapanmasıyla birlikte içindeki veriler silinir. Silinen verilen içinde delil olabilecek öğelerin olabileceği unutulmamalıdır. Örneğin bir RAM içerisinde sistemde var olan prosesler, prosesin ait olduğu kullanıcı, şifreler, geçici dokümanlar, sohbet geçmişleri, zararlı yazılımlar, ağ bağlantı bilgileri ve internet hareketleri ile ilgili bilgiler çıkarılabilir.

BELKASOFT

Bunun için bilgisayar henüz açıkken RAM imajı alınmalıdır. Belkasoft'a ait olan Belkasoft Live Ram Capture programı ile RAM imajı alınabilir. Bu işlem yapılırken RAM miktarı çok az kullanıldığı için bilgisayar zorlanmadan **Belkasoft** kolay bir şekilde RAM imajı alınmış olur. İmaj alma işlemi gerçekleştirilirken RAM içeriğinin tamamını çıkarır. Bu aracın aynı anda hata ayıklama koruması işlevi de mevcuttur ve kurulum işlemi gerektirmeden çalışır.

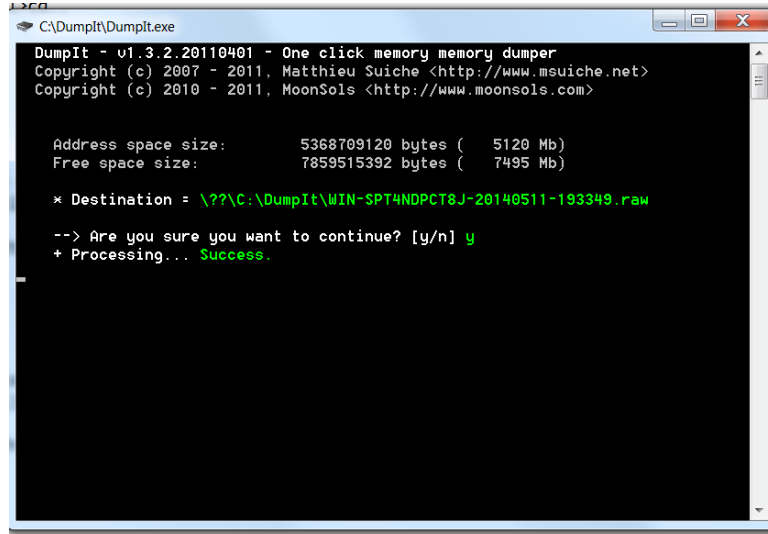


Şekil 10. Belkasoft Live RAM Capturer

DUMPIT

Ram imajı almaya yarayan bir diğer yazılım ise Dumpit yazılımıdır. Oldukça küçük bir boyuta sahiptir ve özel bir kurulumla ihtiyaç yoktur. RAM imajı alınacak olan bilgisayar

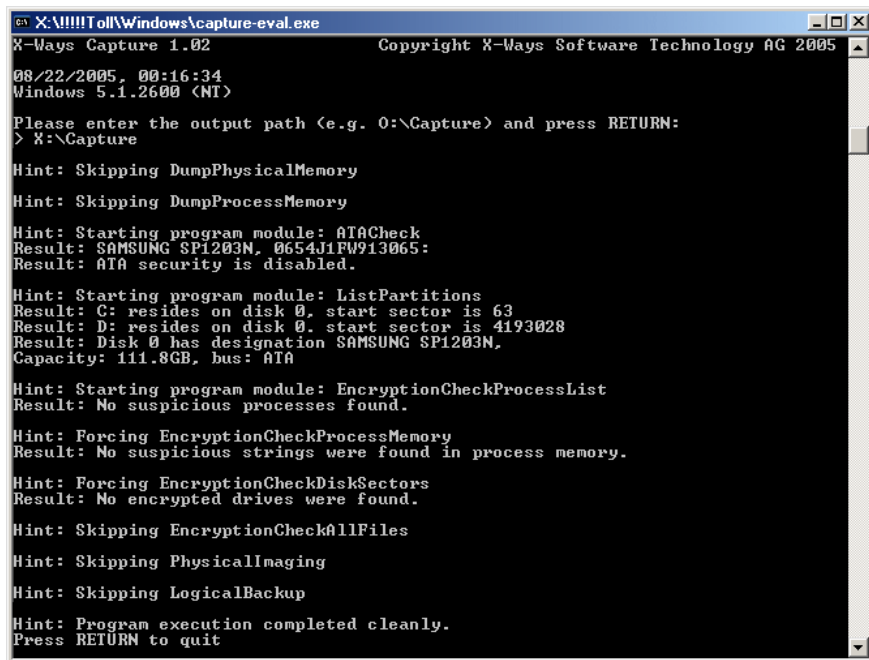
üzerinde bir USB bellek yardımıyla çalıştırılabilir. Kendine özgü bir komut ekranı kullanır.



Şekil 11. DumpIt

X-WAYS CAPTURE

Canlı RAM imajı almak için kullanılan bir diğer yazılım ise X-Ways Capture'dir. X-Ways uygulamasının canlı analiz işlemlerinde kullanılan bir sürümüdür. Bu yazılım hem Windows hem de Linux işletim sistemi üzerinde çalışır. Aynı zamanda yaptığı eylemleri ve elde ettiği sonuçların kapsamlı bir raporunu oluşturur.



Şekil 12. X-Ways Capture

AĞ TRAFİĞİ İNCELEME ARAÇLARI

SAVVİUS INSİGHT

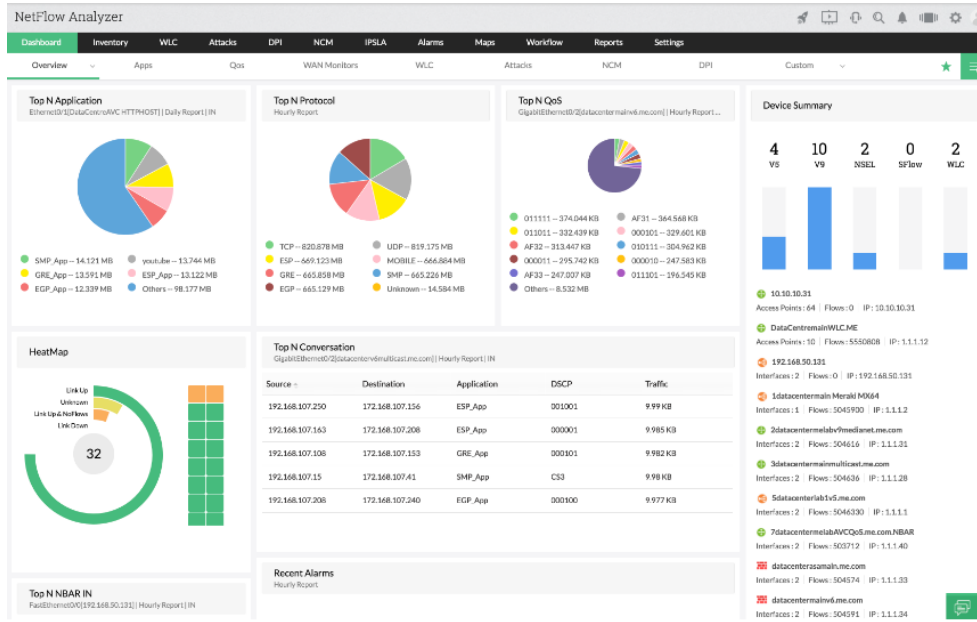
Bu cihaz ağ üzerinde bulunan trafiği kopyalar, monitör eder, inceler ve rapor oluşturur. Span portundan yönlendirilmiş olan trafik ile kablo üzerinde olan trafiğe girer ve izler. Sonrasında kopyalama, inceleme ve analiz ve rapor aşamalarını gerçekleştirir. Trafiği pasif olarak inceler ve kaydeder. Analiz işlemleri ayrıntılıdır ve kendisi otomatik olarak raporlar. Bu cihaz sayesinde ağ performansı ölçülür, paket kayıpları tespit edilir, zararlı yazılım analizi yapılır, ağ cihazlarının bazı sorunlarını tespit eder.



Şekil 13. Savvius

NETFLOW ANALYZER

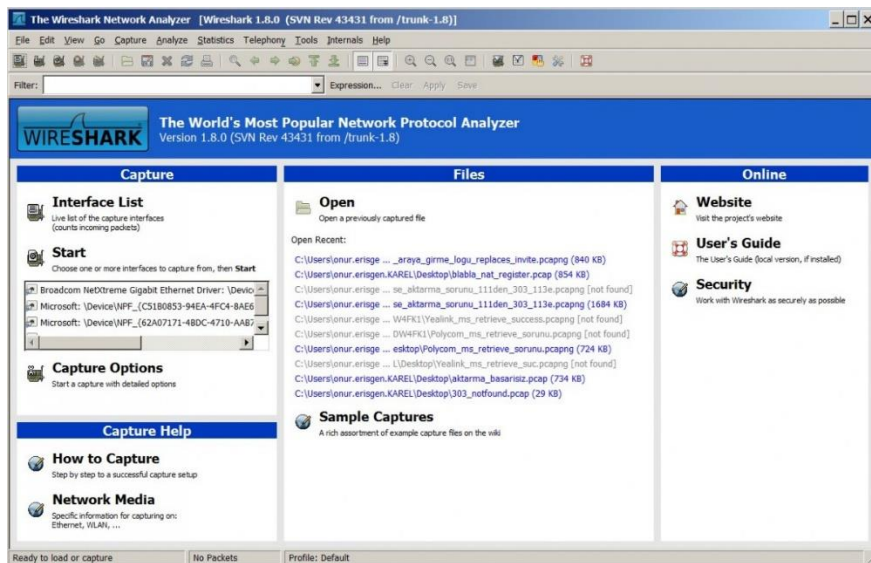
Gerçek zamanlı ağ trafiği analizi yapan bir yazılımdır. NetFlow Analyzer trafik yoğunluğu, trafik hızı, var olan paketler, kullanılan bant ile ilgili çeşitli bilgiler sunan web tabanlı ağ trafiği izleme aracıdır. Asıl ortaya çıkma amacı bant genişliği izleme işlemini sağlamaktır. Aynı zamanda bandın kimler tarafından hangi sebeple kullanıldığı hakkında bilgi elde edip raporlayan bir yapıdır ve bunu yaparken bant ve ağ kullanımını optimize edip güvenliğini artırır.



Şekil 14. NetFlow Analyzer

WIRESHARK

Dünyada sıkça kullanılan bir diğer ağ analiz yazılımı da Wireshark yazılımıdır. Hem daha önce kaydedilen dosyanın analizini hem de anlık olan ağ analizini yapabilir. Elde ettiği verileri bir ara grafik ara yüzü ile kullanıcıya sunar. Bu uygulama aynı zamanda ağ trafiğinin loglanması işlemini de gerçekleştirir. Wireshark programı aynı zamanda ağda olan zararlı yazılım tespiti gibi analizlerini de gerçekleştirir.



Şekil 15. Wireshark

PİNK

Komut ekranında çalışan Ping yazılımı çok eskiye dayanmaktadır. Ağ aracı olan Ping, hedef ağa paketler gönderir. Bu paket hedef ağa ulaştıktan sonra geri gelir. Sunucu ve istemci arasındaki uzaklıkla orantılı bir şekilde bekleme süresi değişir. Bu yazılımın amacı, hedef ağdaki makinenin çalışıp çalışmadığını tespit etmektir. Bununla beraber ağda olan paket kayıp oranı ve ağın yoğunluğu hakkında bilgi verir.

```
kousekip@ako-kaede-mirai ~ $ ping -6 -c 12 anilist.co
PING anilist.co(2606:4700:20::681a:e47 (2606:4700:20::681a:e47)) 56 data bytes
64 bytes from 2606:4700:20::681a:e47 (2606:4700:20::681a:e47): icmp_seq=1 ttl=64 time=26.7 ms
64 bytes from 2606:4700:20::681a:e47 (2606:4700:20::681a:e47): icmp_seq=2 ttl=64 time=22.8 ms
64 bytes from 2606:4700:20::681a:e47 (2606:4700:20::681a:e47): icmp_seq=3 ttl=64 time=24.6 ms
64 bytes from 2606:4700:20::681a:e47 (2606:4700:20::681a:e47): icmp_seq=4 ttl=64 time=23.0 ms
64 bytes from 2606:4700:20::681a:e47 (2606:4700:20::681a:e47): icmp_seq=5 ttl=64 time=27.4 ms
64 bytes from 2606:4700:20::681a:e47 (2606:4700:20::681a:e47): icmp_seq=6 ttl=64 time=22.0 ms
64 bytes from 2606:4700:20::681a:e47 (2606:4700:20::681a:e47): icmp_seq=7 ttl=64 time=23.0 ms
64 bytes from 2606:4700:20::681a:e47 (2606:4700:20::681a:e47): icmp_seq=8 ttl=64 time=23.5 ms
64 bytes from 2606:4700:20::681a:e47 (2606:4700:20::681a:e47): icmp_seq=9 ttl=64 time=23.4 ms
64 bytes from 2606:4700:20::681a:e47 (2606:4700:20::681a:e47): icmp_seq=10 ttl=64 time=22.0 ms
64 bytes from 2606:4700:20::681a:e47 (2606:4700:20::681a:e47): icmp_seq=11 ttl=64 time=24.3 ms
64 bytes from 2606:4700:20::681a:e47 (2606:4700:20::681a:e47): icmp_seq=12 ttl=64 time=25.2 ms

--- anilist.co ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 11016ms
rtt min/avg/max/mdev = 22.017/23.992/27.432/1.654 ms
kousekip@ako-kaede-mirai ~ $ ping -v
ping from iputils 20211215
```

Şekil 16. Pink

VERİ KURTARMA ARAÇLARI

PC3000

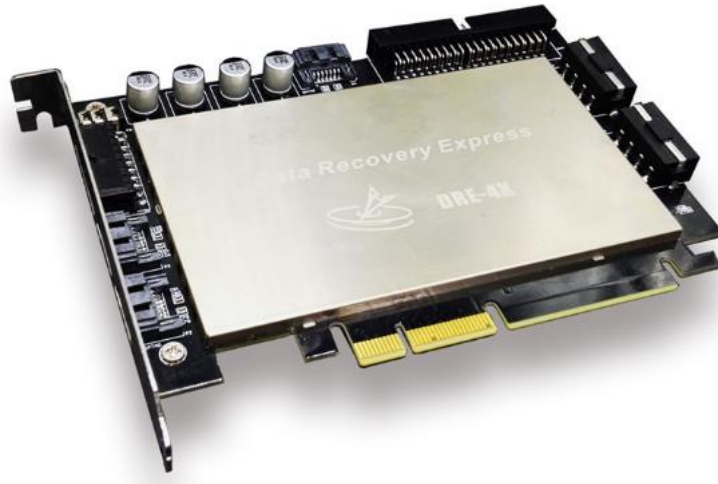
Bozuk olan disklerdeki ulaşılmayan verileri kurtarmaya yarayan hem yazılımsal hem de donanımsal bir araçtır. SATA ve PATA bağlantılarına sahiptir. Bir diskin kafası ya da farklı bir fiziksel parçası zarar görmüşse ve diske normal yollarla erişilemiyorsa, PC3000 aracı kullanılabilir. PC3000 öyle durumlarda sürücüyü çekirdek moduna geçirir ve özel komutlar kullanarak sürücü ile iletişime geçer. Böylece kullanıcının ulaşamadığı verilere ulaşmasını sağlar. Bu araç mikrokod yerleşimlerini, yapılandırma tablolarını, güvenlik alt yapısını ve denetleyici kart gibi bilgilere erişebilir.



Şekil 17. PC3000

DFL-PCIE 4X DATA RECOVERY EXPRESS

Dolphin Data Lab'a ait olan cihaz yüksek bir hız oranıyla arızalı diskten veri kurtarmaya olanak sağlar. 3 SATA ve 1 IDE girişi vardır. Yani aynı anda dört adet arızalı diskten veri kurtarmaya yarar. Veri kurtarma işlemi yaparken onarım işlemini de gerçekleştirmeyi sağlar. Bu ürünün çeşitli özellikleri vardır. Bu özellikler; bad sektör taraması, kafa okuma testleri, diskin kopyasını oluşturma, MBR dosya ve dizin okuma, imaj alma, kayıp bölüm taraması ve firmware onarmadır.



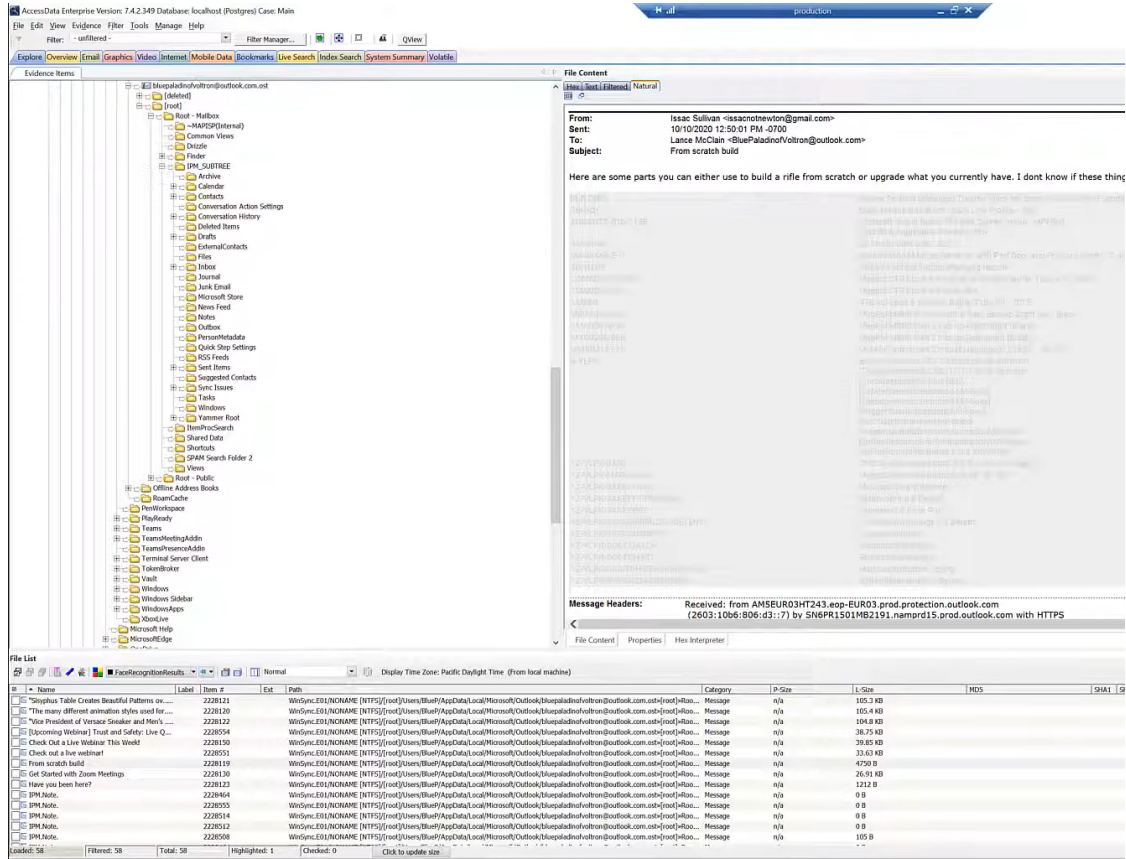
Şekil 18. DFL-PCle 4X Data Recovery Express

İNCELEME YAZILIMLARI

FTK

Accessdata firmasına ait olan Forensic Tool Kit, adli bilişim alanında kullanılan lisanslı bir inceleme yazılımıdır. FTK'nın sahip olduğu özelliklerden bazıları; şifreli olan dosyaların şifresini kırmak, kayıt defterleri dosyasını incelemek, veri kümelerini toplama, analiz etme, RAM gibi geçici bellek analizleri yapmaktır. Delil inceleme ve raporlama konusunda önde gelen programlardan bir tanesidir. Başta adli bilişim ve güvenlik güçleri tarafından sıkça tercih edilmektedir. FTK tarafından oluşturulan raporun mahkemelerce kabul edilir nitelikte olması kullanım sıklığını arttırmaktadır.

Ftk içerisinde farklı türde alanlar barındırır. Bu alanlardan her biri farklı görevlerde kullanılır. Örneğin Explore kısmında analizi yapılacak olan disk menü biçiminde gösterilir. Overview kısmında uzantısına göre normal dosyalar ve silinmiş dosyalar bulunur. E-mail kısmında, diskte bulunan e-mailler yer alır. Graphics kısmında diskte bulunan tüm görseller yer alır. Burası da kategoriler halinde gösterilir. Bookmark kısmı adli bilişim uzmanının önemli kabul ettiği verileri ayırdığı yerdir. Live Serach kısmında yapılan aramalar özelleştirilir. Iban numarası, telefon numarası gibi farklı türlerdeki aramaları içerir. Index search kısmında ise kelime ya da kelimeler aranır. Bu işlemi yaparken tüm imajı inceler.

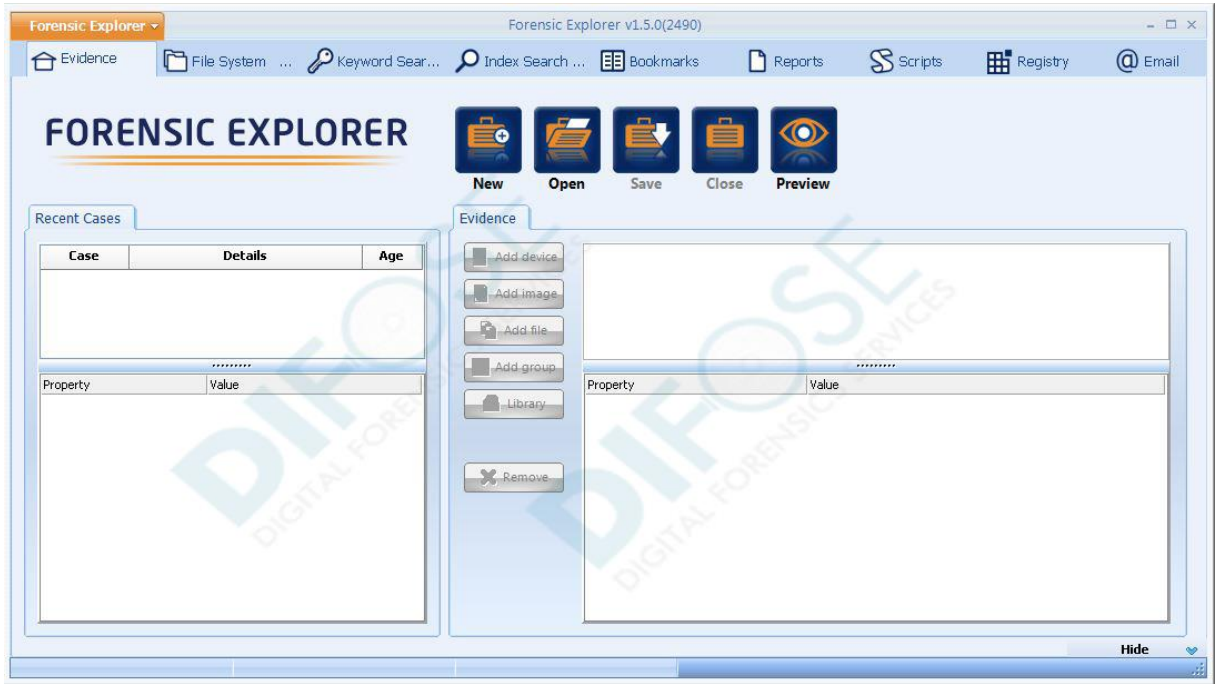


Şekil 19. FTK ara yüzü

FEX

Getdata firmasının ürettiği Forensic Explorer, lisanslı bir adli bilişim yazılımıdır. Fiziksel ve mantıksal imaj alıp aldığı imajlar üzerinde inceleme işlemleri gerçekleştirebilir. Forensic Explorer birçok özelliğe sahiptir. Bu özellikler arasında, hash değeri hesaplama, anahtar aramaları yapma, indeksleme ve sınıflandırma işlemleri, bookmark gibi etiketlemeler yapma, registry kayıtlarının incelenmesi, e-posta analizlerinin yapılması, diskten shadow Copy çıkarılması ve incelenmesi, veri kurtarması yapmak ve imza analizi yapmak yer alır.

Ancak FEX'i diğer birçok yazılımdan ayıran özelliği ise farklı imaj dosyalarını mounth etme ve inceleme işlemidir. Yani imaj dosyalarını birleştirir, karşılaştırır ve inceler. İki imajın aynı anda incelenmesini sağlaması olay ile ilgili kanıtlara daha erken ulaşılmasını sağlamaktadır.

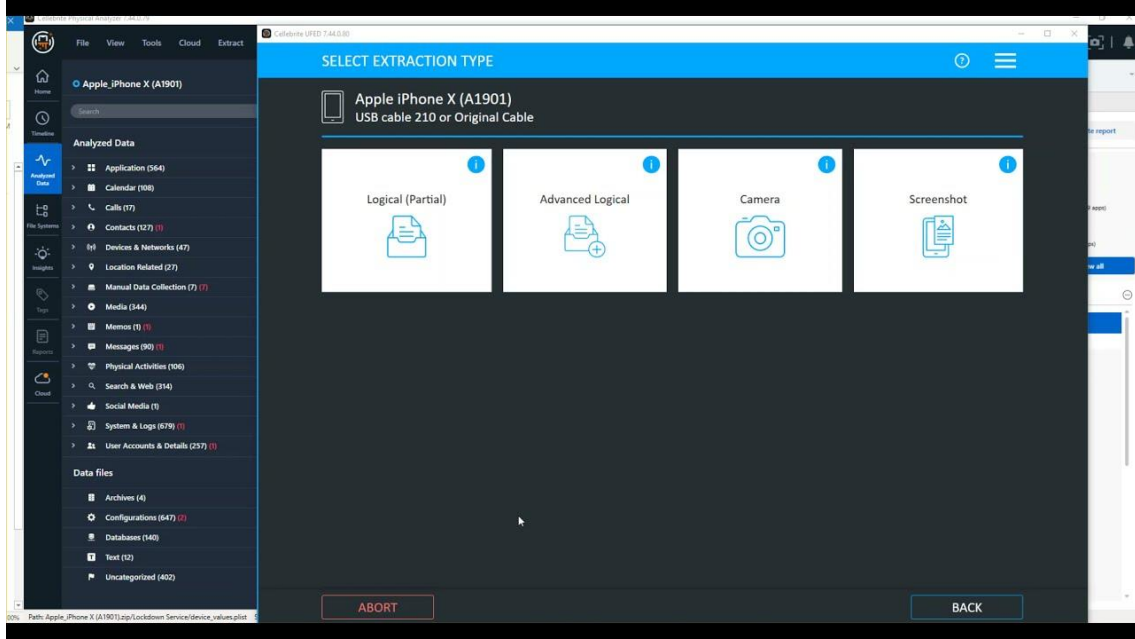


Şekil 20. FEX arayüzü

UFED

Cellebrite firması tarafından üretilen UFED mobil cihazların incelenmesini ve raporlanmasını sağlar. Şifreli olan telefonları içerisinde barındırdığı birden fazla yöntemi deneyerek kırabilir veya atlayabilir. Birçok telefon modelini inceleme özelliğine sahiptir ve bunlardan fiziksel çıkarım yapar. İçinde Android, IOS ve Windows mobile gibi işletim sistemlerinin de bulunduğu birçok işletim sistemindeki mobil cihazı incelemeye olanak sağlar. Telefonların dosya sistem analizlerini, SIM kartı analizleri, silinen verileri, yüklenen uygulamaları, telefonun kendine ait olan uygulamaları, kamera ve galeri incelemelerini, gelen ve giden aramaları, SMS bilgilerini, sohbet geçmişini, konum ve GPS bilgileri ve cihaza ait marka, model ve IMEI numarasını bulma gibi önemli sayıda özelliğe sahiptir. Silinmiş olan verileri, ilgili uygulamanın veri tabanını çözümleyerek bulmaya çalışır. Sadece telefon içindeki arama kayıtlarını değil aynı zamanda SIM üzerinden yapılan arama kayıtlarına da ulaşabilir. Mobil cihazda bulunan malware, trojan gibi zararlı yazılımların bulunmasına olanak sağlar. Verilerin, üzerinde indeksleme işlemi yaparak tarih sırasına göre sıralanmasını sağlayabilir. Ayrılmamış alan incelemeleri yapar. Bu da gizlenmiş olan verilerin de ortaya çıkmasını

sağlar. Aynı zamanda içinde bulunan Python Shell alanı ile Python dilinde eklentiler yazılabilir.

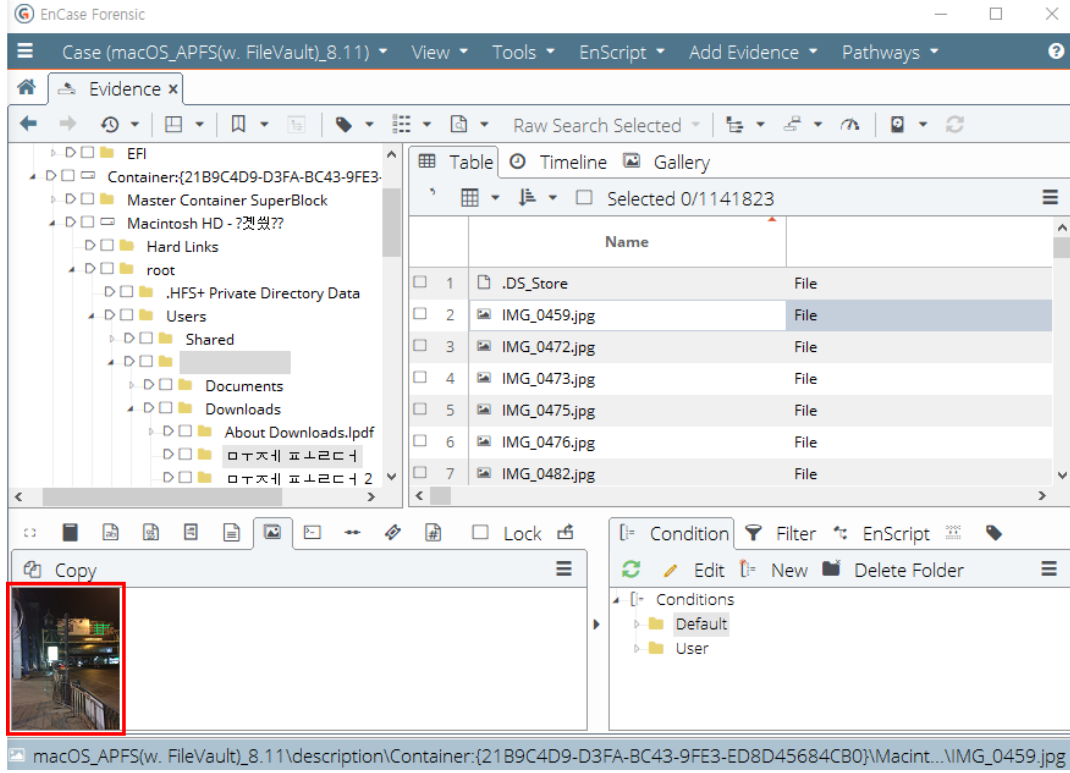


Şekil 21. UFED ara yüzü

ENCASE

Tıpkı diğer yazılımlar gibi Encase de bir inceleme yazılımıdır. Olay yerinde alınmış olan imajları incelemede kullanılabilecek olan kullanışlı bir adli bilişim yazılımıdır. Ancak Encase her imaj formatında inceleme yapamaz. Programın imaj dosyasını okuyup inceleyebilmesi için E01, Ex01, L01 ve Lx01 formatlarında olmalıdır. Aksi halde Encase dosyayı okumayacaktır. Bu formatlardan E01 Encase Forensic imajını ifade eder. Ex01, Encase yazılımının V7 ile birlikte gelen bir imaj türüdür. L01, Encase logic imaj türüdür ve son olarak Lx01 ise Encase V7 ile gelen bir imaj türüdür. Bu imaj türlerinin hepsi sıkıştırılmıştır.

Encase yazılımının, imaj dosyasını incelemek için çeşitli özelliklere sahiptir. Mobil cihazlarda dâhil olmak üzere birçok işletim sistemi ve dosya türü üzerinde inceleme yapabilir. Güçlü bir şifre kırma yapısı vardır. Şifre ile korunan dosyaları tespit edebilir ve şifreleri etkisiz hale getirebilir. İndeksleme motoru sayesinde kanıtlara ulaşma yolunda uzmanlara kolaylık sağlar. Kendine ait raporlama sistemi ile elde edilen kanıtları detaylı bir şekilde raporlar ve paylaşmaya olanak sağlar.

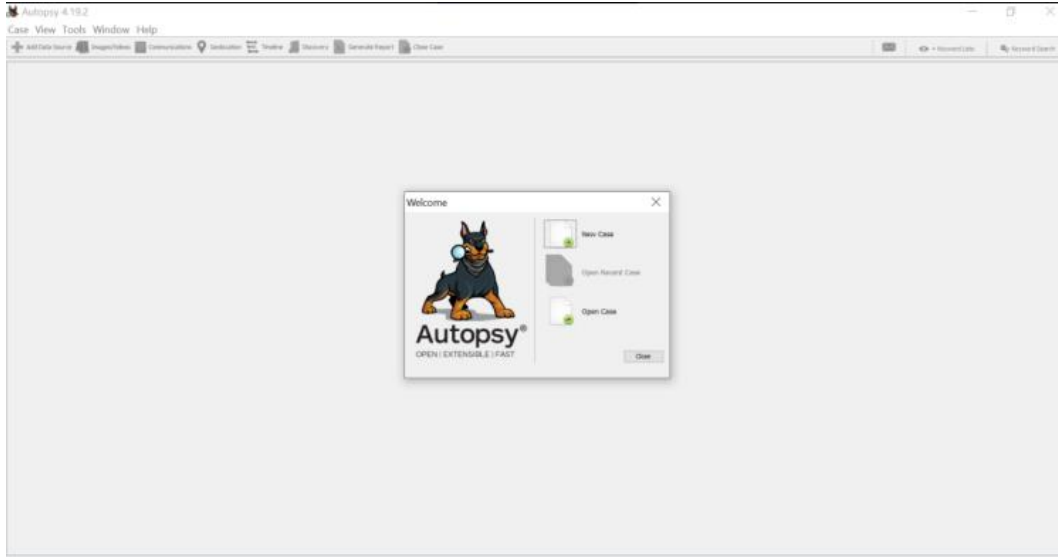


Şekil 22. Encase ara yüzü

AUTOPSY

Adli bilişimde inceleme yazılımı olarak kullanılan bir diğer yazılım ise Autopsy'dir. Bu yazılımın diğerlerinden en büyük farkı ücretsiz olarak kullanılmasıdır. Lisans gerektirmeyen bu yazılımda birçok özellik mevcuttur. Öncelikle Autopsy, birçok işletim sistemi üzerinde sorunsuz çalışmaktadır. Bu işletim sistemleri; Windows, Linux, Mac OSX ve BSD'dir. Bu uygulama ile DD, E01 ve AFF uzantısında imaj alınabilir. Ve alınan imajlar üzerinde incelemeler yapılabilir. Ardından hash değeri hesaplanıp hash tablosu incelenebilir. İçinde FAT ve NTFS dosya sisteminin de bulunduğu birçok dosya türü üzerinde çalışma yapılmasına olanak sağlar. Elde edilen imaj üzerinde stegonografi tespiti yapabilir. Silinmiş dosyaları carve işlemi uygulayabilir. MFT dosyalarına ulaşım tüm dosya ve izin yapısı hakkında bilgi çıkarımı yapar. Dosyaların metadata verilerini çıkarabilir. Kayıt defteri analizi yapmaya olanak sağlar. Kelime araması yaparak istenilen veriye daha çabuk ulaşılmasını sağlar. İmaj dosyasının içinde konum ile ilgili

bir bilgi bulunması halinde bu bilgileri ayrı bir alanda inceleyiciye sunar. Web tarayıcı verileri çıkarıp silinmiş olan verilere erişebilir. İmaj dosyasının içinde var olan tüm fotoğraf ve videoları farklı bir alanda toplar ve incelenmesini sağlar. Verilere timeline işlemi uygulayarak zamansal olarak sıralanmasını sağlar. Bu da inceleme yapan uzmanların analiz işlemlerini kolaylaştırır. Tek kullanıcı ve ya çok kullanıcı bir biçimde çalışabilmesi inceleme sürecini hızlandırır. Adli bilişim uzmanları analiz yaparken delil niteliğindeki verilere etiketleme işlemi yapabilirler. Bu özelliği sayesinde uzmanlar verileri incelemek adına sınıflandırabilir.



Şekil 23. Autopsy ara yüzü

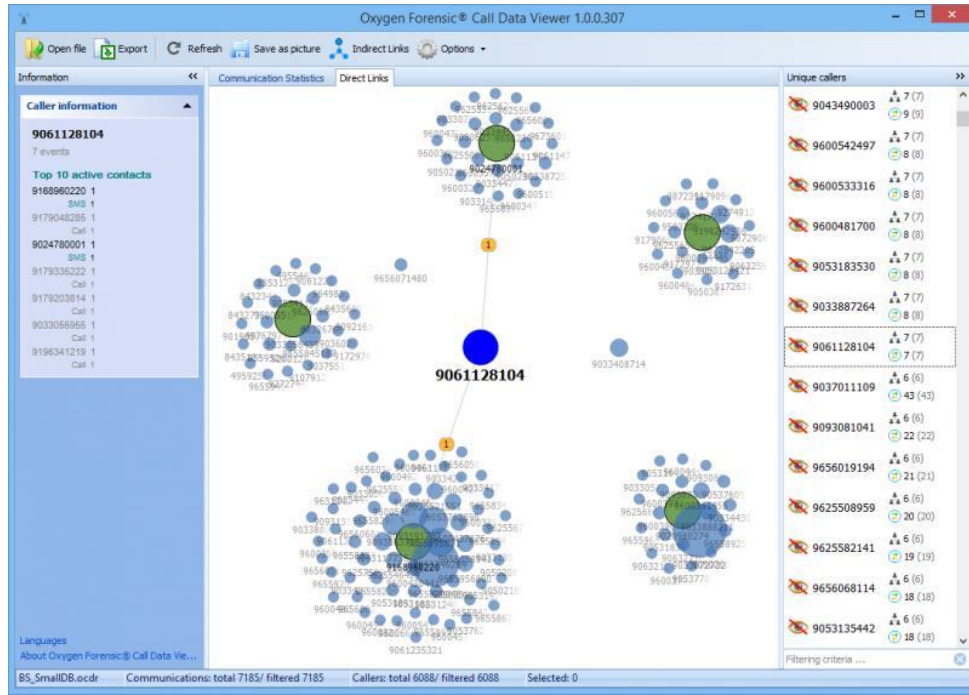
OXYGEN FORENSİC

Hem mantıksal hem de fiziksel olarak imaj almayı destekleyen ve birçok sayıda mobil cihazın kullanımına olanak sağlan oldukça yaygın bir adli bilişim analiz yazılımıdır. İçerisinde birçok sayıda uygulama barındıran Oxygen mobil cihaz ve drone cihazları gibi yapılardan veri analizi yapabilir.

Mobil inceleme yaparken, cihazda var olan e-mail hesapları, telefona ait cloud hesapları, tüm sosyal medya hesapları(Instagram, Twitter, Whatsapp, Telegram vs.), arama kayıtlar ve SMS, navigasyon gibi yapıların analizini yapıp sonuçlarını çıkarır. IOS ve Android marka cihazlara yüklenen zararlı yazılımların tespitini yapar. İçindeki uygulamaların veri tabanlarının şifrelerini çözer. Hesapların iletişim bilgilerini, sohbet geçmişini, paylaşılmış olan medya ve konumları tespit eder. Sonuç çıkarırken zaman

çizelgesi oluşturup verileri kronolojik bir şekilde sıralayabilir. Diğer uygulamaların aksine sosyal medya gibi uygulamaların analizini yaparken sosyal grafik oluşturması adli bilişim uzmanlarına kolaylık sağlar.

Diğer birçok uygulamadan farklı olarak drone analizi yapması Oxygen'in önemli özelliklerindendir. Drone ile ilgili uçuş kayıtlarını, varsa içindeki uygulamaları, drone cihazının kendine ait bulut hizmetlerini inceler ve analizini yapar. Drone'nin imajını alır ve cihazın yönü, hızı, yüksekliği gibi bilgilerini ayrıştırır.



Şekil 24. Oxygen Forensic ara yüzü

RAPORLAMA

Raporlama aşaması, delilin mahkemeye sunulmadan önceki son aşamasıdır. Bu aşamada yer alan deliller hukuki olarak kurallara uygun bir şekilde elde edilmiş olması ve işlenmiş olması gerekmektedir. Aksi halde hazırlanmış olan rapor mahkeme tarafından kabul edilmez. Toplanan delillere inceleme yapıldıktan sonraki sonuçlar detaylı bir şekilde raporda yer almalıdır. Ayrıca raporda sadece inceleme sonuçları değil en başından itibaren gerçekleşen süreçler de yer almalıdır. Rapor hazırlanırken verilerden elde edilen deliller anlaşılır ve net bir biçimde sunuma hazırlanır. Rapor

hazırlanırken yorum cümlelerinden ve terimsel ifadelerden kesinlikle kaçınılmalıdır. Yargı görevlilerinin anlayacağı sadelikte olmalıdır.

Sunulan raporlar genel olarak yazı formatında da olsa gerektiği durumlarda video, fotoğraf ve ses belgelerini de içerebilir.

Raporda bulunması gereken bazı başlıklar vardır. Bu başlıklar genel olarak; mahkemenin talep ettiği analizler, incelenmiş olan deliller, kullanılan araçlar, yöntem, inceleme sonuçları, delillere ait genel bilgiler, yapılmış olan analizler(zararlı yazılım analizi vs.) ve en son olarak da sonuçlar yer almalıdır. Örneğin delillere ait genel bilgiler kısmında bir disk hakkında bilgi verildiğini varsayalım. Diskin markası, modeli, sürümü, HPA ve DCO alanlarına sahip olup olmadığı, şifre bilgileri, hash değerleri, içinde gizli ya da değiştirilmiş dosyaların olup olmadığı ile ilgili bilgiler yer almalıdır. Böylece hazırlanan rapor, raporu inceleyen kişi tarafından daha net bir biçimde anlaşılabilir.

OLABİLECEK SORUNLAR

Bir suçun meydana gelmesi durumunda; arama izninin çıkarılmasından olay yerine bilirkşi atanmasına kadar her süreçte hukuki izinler gereklidir. Hukuksal olarak elde edilmeyen hiçbir delil ya da rapor kabul edilmez. Elde edilen delillerin incelenmesi aşamasında da çeşitli kanunlar ve kuralları mevcuttur. Bu kurallara uyulmadığı takdirde cezai işlem uygulanabilir.

Olay yerinde incelenmenin başlatılması için arama izninin çıkarılması gerektiği hususuna daha önceden değinilmiştir. Bu durumda çıkabilecek bir sorun ise arama izninin zamanında çıkarılmamasıdır. Olması gereken zamanından sonra delillerin tespit edilmesi, delil doğruluğunu etkileyebilir. Bu durumda iznin farklı kişiler tarafından çıkarılabilir. Normal şartlarda arama izni hâkim tarafından çıkarılır. Ancak bazı sakıncalı durumda cumhuriyet savcısı da bu kararı çıkarabilir. Eğer cumhuriyet savcısına ulaşım sağlanamıyorsa kolluk amiri de arama izni çıkarabilir. Bu duruma CMK 127’de detaylı bir şekilde yer verilmiştir.

CMK 134. Madde, orijinal bir delil üzerinde incelenme yapılamayacağı ve verilerin yedeklenmesi gerektiği hakkında kuralları içerir. Adli bilişim uzmanları bu kurallara uymak zorundadır ancak bazı istisnai durumlarda kurallara uymak mümkün

olmayabilir. Örneğin olay yeri incelemesine giden bir ekip açık bir bilgisayar ile karşılaştığı zaman ilk müdahaleyi canlı yapmak zorunda kalabilir. RAM gibi geçici bellekler bilgisayarın kapanması ile içindeki bilgileri silerler. Bu yüzden açık bir bilgisayarın RAM analizi olay yerinde yapılabilir. Ancak bu işlemler gerçekleştirilirken kesinlikle yapılan aşamalar kayıt altına alınmalıdır ve raporda bu kısımdan bahsedilmelidir. Ayrıca imajı alınan delillerin hash değerleri de alınmalıdır. Hash değerlerinin her biri benzersiz olduğundan dolayı şüpheliye ait verilerinin değiştirilmediği ya da oynanmadığının garantisini verir.

Önem teşkil eden bir diğer konu ise; elde edilen delillerin kopyaları alındıktan sonra bir kopyasının da sanığa ya da vekiline verilmesidir. Ancak bu işlem bir tutanak dâhilinde yapılır ve kişilerin imzası alınır. Bu işlemin önceki dönemlerde resmi bir hükmü yoktu ancak yapılmış olan bazı değişikliklerle zorunlu kılınmıştır. Ayrıca deliller üzerinde inceleme yapılmadan önce kopyalanma işlemi yapılırken ve hash değerleri hesaplatılırken, şüpheli taraftan yetkili bir kişinin de bulunması tavsiye edilir. Bu durum kayıt altına alınmalıdır ve değerler teslim edilirken mutlaka imzaları alınmalıdır.

Elde edilen verilerden delil çıkarılması için incelemeyi yapan kişi çok önemlidir. Yeterli bilgiye sahip olması gerekmektedir. Örneğin inceleme yaparken zaman damgalarının kullanılmaması ve incelenmemesi sorun teşkil edebilir. İnceleme yapılırken verinin oluşturulma, değiştirilme, varsa silinme gibi zaman damgalarına dikkat edilmelidir. Ayrıca inceleme yapan adli bilişim uzmanının, delile göre inceleme yapması çok önemlidir. Örneğin bir telefon incelenirken, analiz programı olarak UFED kullanılabilir ancak bilgisayar incelenirken kullanılması pek sağlıklı olmaz. Bunun için de bilgisayar incelemelerinden kullanılan bir program kullanılmalıdır. Tüm bu incelemeler için gerekli programlar temin edilmeli ve uygun laboratuvarın sağlanmış olması lazımdır. Aksi halde sağlıklı bir inceleme olamayabilir.

Diğer bir konu ise bazı durumlarda, atanmış olan bilirkişinin yardıma ihtiyacı olabilir. Yeterince bilgi sahibi olmadığı bir durumda mahkemeden ikinci bir bilirkişi atanmasını talep edebilir. Bu durum daha önce de bahsedilen CMK'nın 63. Maddesinin 2. Fıkrasında yer almaktadır. Fıkraya göre;

“ (2) Bilirkişi atanması ve gerekçe gösterilerek sayısının birden çok olarak saptanması, hâkim veya mahkemeye aittir. Birden çok bilirkişi atanmasına ilişkin istemler reddedildiğinde de aynı biçimde karar verilir. “

Diğer bir durum ise elde edilen verilerin detaylı bir şekilde incelenmesine rağmen, kişinin masumiyetine ya da suçluluğuna dair herhangi bir delile rastlanmayışıdır. Bu gibi durumlarda bir olay yeri inceleme uzmanı, kayda değer bir delil olsun ya da olmasın yapılan tüm işlemleri adım adım raporda yazmalıdır.

Deliller elde edildikten sonra incelenmesi için bir süre vardır ve olay yeri inceleme uzmanları bu süre içinde çalışmaları gerekmektedir. Ancak bazı olaylarda yeri deliller elde edilebilir ya da zaten var olan delilin incelenmesi planlandığı zamanda bitmeyebilir. Bu gibi durumlarda, ek süre istemek için mahkemeye bir dilekçe gönderilir. Dilekçe incelendikten sonra kabul edilirse ek süre verilir. Ancak gerekçeler mahkeme tarafından uygun bulunmaz ise bu istek reddedilebilir.

İNCELEME SÜRECİNDE KARŞILAŞILAN FARKLILIKLAR

Hemen hemen her olay yeri incelemesinde farklı türde deliller elde edilir. Dolayısıyla inceleme yolu ve yöntemleri de değişiklik gösterir. Bu kısımda en doğru ve etkili yolu bulmak adli bilişim uzmanlarının işidir. Bu bölümde, olay yeri incelemeleri sırasında karşılaşılan farklı durumlar ve çözüm önerilerine yer verilecektir.

ARIZALI USB BELLEK VE SSD KART

Bir diskin bozulmasında ya da arızalanmasında birden fazla neden vardır. Arızalanma türüne göre çözüm yolları değişiklik gösterir. Genel olarak bu arızalar yazılımsal ve donanımsal olarak ikiye ayrılır. İlk olarak yazılımsal arızalardan bahsedelim.

Örneğin dosya sistemi bozulmuş olan bir diskten mevcut hali ile veri okunması yapılamaz. Dosya sistemi, içindeki dosyaların isimlerini, oluşturulma, silinme ve değiştirilme gibi zamansal bilgilerini ve dosya konumu gibi bilgileri barındırır. Her dosya sisteminin yapısı farklıdır ve bilgileri farklı yerlerde tutarlar. Dolayısıyla incelenecek her diske aynı dosya sistemine sahipmiş gibi incelenme yapılamaz. Günümüz disklerinde genel olarak NTFS dosya sistemi kullanılır ancak bunun haricinde FAT16, FAT32, UFS, EXT gibi dosya sistemleri de kullanılmaya devam edilmektedir. Aynı zamanda bölümlendirme yapısı bozulmuş olan bir diskten de okuma ve yazma işlemleri yapılamayabilir. Örneğin normal bir sabit diskin bölümlendirme yapısı örneği Şekil

25’de gösterilmiştir. Bu yapının bozulması durumunda yeni birim ekleme seçenekleri ile disk yeniden bölümlendirilebilir ve veriler okunur hale getirilebilir.

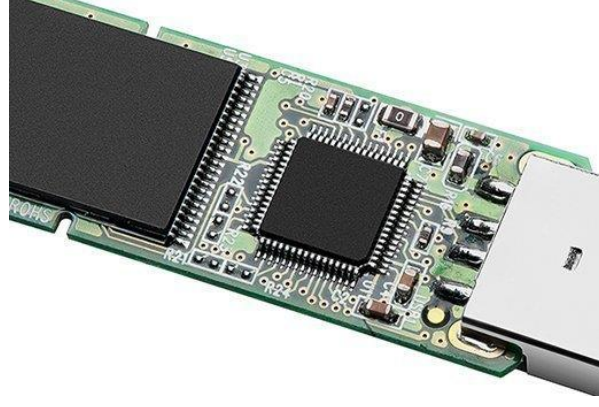
Birim	Düzen	Tür	Dosya Sistemi	Durum
(C:)	Basit	Temel	NTFS	Sağlam (Önyükleme, Disk Belleği Dosyası, Kilitlenme)
(Disk 0 Bölüm 1)	Basit	Temel		Sağlam (EFI Sistem Bölümü)
(Disk 0 Bölüm 4)	Basit	Temel		Sağlam (Kurtarma Bölümü)

Disk 0 Temel 238,46 GB Çevrimiçi	100 MB Sağlam (EFI Si	(C:) 237,78 GB NTFS Sağlam (Önyükleme, Disk Belleği Dosyası, k	594 MB Sağlam (Kurtarma Bö
--	--------------------------	--	-------------------------------

Şekil 25. Sabit disk bölümlendirme yapısı örneği

Fiziksel hasarlar sonucunda bozulan diskler de oldukça yaygındır. Fazla elektrik yüklenmesi ve diskin düşmesi gibi sorunlar diskin donanımsal yapısını bozabilir. Fiziksel hasarlar sonucunda diskin okuma yazma kafası, disk plakaları, veri kabloları ve disk konektörü gibi donanımsal yapıları zarar görmüş olabilir. Arızanın çeşidi ve nedeni bulunduğundan sonra türüne göre veri kurtarma işlemleri uygulanır. Hasarlı disklerden veri kurtarmak için çeşitli donanımlar vardır. Örneğin Dfl-Pcie 4x Data Recovery Express donanımı sayesinde (Şekil 18) aynı anda dört adet arızalı disk onarılabilir.

Fiziksel olarak USB belleklerde genel olarak Flash Memory yani hafıza çipi ya da Flash Controller yani denetleyici çip hasar görür. Hafıza çipi, verilerin tutulduğu yerdir. Denetleyici çip ise verinin hangi adrese yazılacağını ve nasıl yazılacağını denetler. Dolayısıyla önemli olan tek çip hafıza çipi değildir. Denetleyici çipin de zarar görmesi sonucunda veriler yazılamaz ya da okunamaz. Çiplerin çizilmesi ya da kırılması durumunda veriler kurtarılamaz ancak temassızlık gibi nedenlerden dolayı okunamayan veriler kurtarılabilir. PCB kartı, yani baskılı devre kartına verilen hasarlar daha kurtarılabilir durumdadır. EaseUS Data Recovery Wizard gibi programlar sayesinde bu tarz disklerden veri kurtarılabilir.



Şekil 26. Flash Memory Chip

Bir USB bellek çeşitli sebeplerden dolayı arızalanır. Fazla güç aktarımından, dosya sisteminin değiştirilmesinden ve ya fiziksel darbelerden dolayı arızalanabilir. Arızanın türlerine göre veriler kurtarılabilir ya da kurtarılamaz. Eğer arıza sebebi fiziksel ise, ilk olarak kolluk kuvvetlerine bağlı olan ekipler tarafından tamir edilmeye çalışılır. Eğer USB belleğin Flash Memory entegresi dışındaki donanımları zarar görmüşse, USB belleğin Flash Memory entegresi çıkarılır ve sağlam olan bir donanım ile birleştirilir. Bu durumda veriler zarar görmeden USB bellek kullanılır hale gelir. Ancak genellikle bu iş Adli Bilişim uzmanları tarafından yapılmaz.

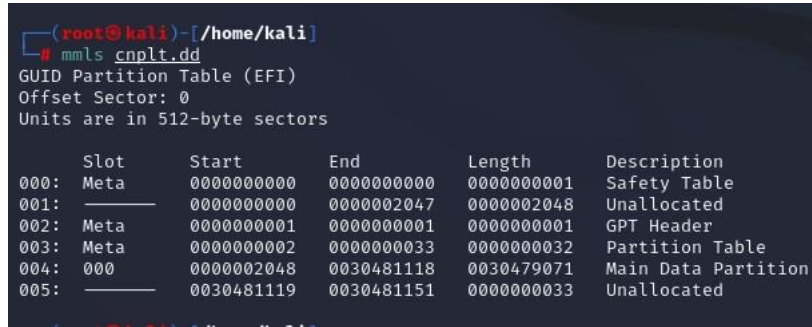
Eğer USB bellek donanımsal olarak tamir edilemiyorsa, Adli Bilişim uzmanları tarafından USB belleğin Flash Memory entegresi bilgisayar ortamına aktarılır. Bunun için tekrardan gerekli donanımlar sayesinde Flash Memory entegresi yerinden çıkarılır ve ara okuyucu üniteye bağlanır. İlk yol daha güvenlidir çünkü ikinci yolda Flash Memory entegresi zarar görebilir ve içindeki veriler okunamaz duruma gelebilir. Ardından imaj alma işlemi için Flash Memory entegre üretim numarasının bilinmesi gerekmektedir. Bu bilgi üretici firma sayesinde de öğrenilebilir. Bu kod ile imaj alma işlemine geçilebilir. Bu yöntem ile imaj alma işlemi için Flash Extractor yazılımı kullanılabilir.

HAZIR UYGULAMA KULLANILAMADIĞI DURUMLAR

THE SLEUTH KIT

Analiz programları, genel olarak kullanılan işletim sistemlerini, dosya yapılarını ve bölümlendirme yapıları gibi farklı formatlardaki delilleri inceler ve kanıt elde etmek üzere analiz yapar. Ancak bazı durumlarda, delil eski bir işletim sistemine ve ya bölümlendirme yapısına sahipse hazır programlar ile analiz yapılamayabilir. Bu gibi durumlarda manuel analizler yapılmalıdır. Dolayısıyla bir adli bilişim uzmanı gerektiği

durumlarda manuel analiz yapabilmelidir. Örneğin bir diskin manuel analizinin yapılması, disk bölümlendirme yapısını ve dosya sistemi ile ilgili bilgileri elde etmek için The Sleuth Kit (TSK) kullanılabilir. Şekil 27’de görüldüğü gibi bir diskin verisinin yazıldığı kısımlar, başlık bilgileri ve tahsis edilmemiş alanları ile ilgili başlangıç ve bitiş adreslerini verir. Bu adreslerden yararlanarak diskin içinde olan verilere ulaşılabilir ve silinmiş veriler kurtarılabilir.



```
(root@kali)-[/home/kali]
# mmls cnplt.dd
GUID Partition Table (EFI)
Offset Sector: 0
Units are in 512-byte sectors
```

	Slot	Start	End	Length	Description
000:	Meta	0000000000	0000000000	0000000001	Safety Table
001:	---	0000000000	0000002047	0000002048	Unallocated
002:	Meta	0000000001	0000000001	0000000001	GPT Header
003:	Meta	0000000002	0000000033	0000000032	Partition Table
004:	000	0000002048	0030481118	0030479071	Main Data Partition
005:	---	0030481119	0030481151	0000000033	Unallocated

Şekil 27. The Sleuth Kit

HEXADECİMAL KODLAR

Diğer bir manuel bilgi elde etme ve veri kurtarma yöntemi ise hexadecimal kodlardır. Hexadecimal kodlar verileri temsil etmek için 16 farklı sembol kullanan bir sayı sistemidir. Ve bu kodlar bir uzman tarafından okunabildiği takdirde birçok bilgi verir. Örneğin silinmiş bir dosyayı kurtarmak için ve ya uzantısı değiştirilmiş olan bir dosyayı tespit etmek için hexadecimal kodlardan yararlanabiliriz. Bu işlemi hazır uygulamalar da yapabileceği daha önceden belirtildiği ancak bazı sistem ve dosyaların hazır uygulamalar ile okunamadığı durumlarda uzmanlar hexadecimal kodlar gibi yöntemlerden faydalanarak manuel analiz yapmalıdırlar.

Örneğin uzantısı değiştirilmiş olan bir dosya bulunduğunda, bu dosyanın orijinal uzantısının bulunması hexadecimal kodlar ile gerçekleştirilebilir. Her bir dosyanın bir imza değeri vardır. Kullanıcı dosyanın uzantısını değiştirse bile bu değer hexadecimal kodlarda değişmez. Dolayısıyla uzantısı değişmiş olan dosya herhangi bir hex editör ile açıldığında, hexadecimal karakterlerin ilk birkaç baytı dosyanın uzantısı ile ilgili bir imza değeridir. Şekil 28’de mevcut uzantısı EXE olan bir dosya bulunmaktadır. Ancak dosya kullanılabilir bir formatta değildir. Bu durumda dosya, herhangi bir hex editör ile açılması sonucu hexadecimal değerleri Şekil 28’de olduğu gibi ortaya çıkar ve dosyanın aslında bir JPG yani fotoğraf dosyası olduğu anlaşılır.

ff	d8	ff	e0	00	10	4a	46	49	46	00	01	01	00	00	01
00	01	00	00	ff	db	00	84	00	06	06	06	06	07	06	07
08	08	07	0a	0b	0a	0b	0a	0f	0e	0c	0c	0e	0f	16	10
11	10	11	10	16	22	15	19	15	15	19	15	22	1e	24	1e
1c	1e	24	1e	36	2a	26	26	2a	36	3e	34	32	34	3e	4c
44	44	4c	5f	5a	5f	7c	7c	a7	01	06	06	06	06	07	06
07	08	08	07	0a	0b	0a	0b	0a	0f	0e	0c	0c	0e	0f	16
10	11	10	11	10	16	22	15	19	15	15	19	15	22	1e	24
1e	1c	1e	24	1e	36	2a	26	26	2a	36	3e	34	32	34	3e
4c	44	44	4c	5f	5a	5f	7c	7c	a7	ff	c2	00	11	08	06
40	06	0f	03	01	22	00	02	11	01	03	11	01	ff	c4	00
31	00	01	00	03	01	01	01	00	00	00	00	00	00	00	00
00	00	00	01	02	03	04	05	06	01	01	01	01	01	01	01

Şekil 28. Uzantısı değiştirilmiş dosya

Hexadecimal kodlar ile sadece uzantı analizi değil, birçok analiz yapılabilir. Bir örnekle açıklanacak olursa; PDF dosyasının içinde stegonografi ile bir JPG dosyası yerleştirilmiştir. Dışardan bakılınca PDF dosyasında gözle görülür bir fark olmaz ancak hexadecimal kodlar ile açıldığında Şekil 29’da görüldüğü gibi JPG dosyasının başladığı yer bulunur ve dosya tespit yine hexadecimal kodlar ve hex editörü ile kurtarılır.

Sonuç olarak manuel analizlerin yapılması durumunda genellikle hexadecimal kodlardan yararlanılır. Hexadecimal kodlardan yararlanarak Ram analizi, MFT analizi, dosya kurtarma, kazıma ve dosya yapısı gibi birçok alanda analiz yapılabilir.

000023f4	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f	
000022f0	5e	0e	f5	b4	dd	15	02	bc	df	5d	63	95	5b	1a	0d	86	^..ö'ı..%ß]c•[. .†
00002300	40	7d	c6	f6	b0	f5	d9	59	e5	60	1f	ae	65	c8	4b	e5	@}Äö'öÜYÄ'.°eEKÁ
00002310	8e	75	72	64	dd	ae	45	d2	c2	3f	d9	1f	8a	a2	f3	df	.urdI°EOA?Ü.Şöß
00002320	65	da	85	83	5d	9c	0f	02	e5	2a	a9	f0	1e	d7	9d	35	eÜ..f]œ..â*öğ.x.5
00002330	82	24	67	b5	9b	0e	80	c9	a1	b7	30	af	bc	7f	ba	02	,Şgu>.€E; .0°%.°.
00002340	cc	da	dd	4b	77	dd	bd	18	2f	ee	5e	9c	e7	ec	f1	86	IUIKwI%./ı^œıñ†
00002350	00	43	bb	f6	8e	45	aa	f1	c1	ce	b1	56	83	da	55	5b	.C>ö.E°ñAf±vfUU[
00002360	8b	bb	21	aa	68	36	3a	ea	52	41	84	6c	55	24	ab	47	<»!°h6:êRA,,ıU\$«G
00002370	1e	2b	9a	c6	f3	2a	63	d7	23	26	32	99	4d	59	92	ac	.+ŞÄö*c×#&2°MY'¬
00002380	5d	c1	bb	d7	5b	d5	73	49	f7	54	a1	de	b8	5b	dd	53]A»x[ÖsI÷T;Ş,[İS
00002390	15	00	6e	14	92	86	ae	de	0d	99	81	29	b6	0f	3c	50	..n.'†°Ş..°.)¶.<P
000023a0	a8	8d	a5	3b	08	83	1b	42	55	a4	87	e5	bd	e1	b4	b1	°.¥;.f.BU±#â%á'±
000023b0	1f	e5	40	f7	a3	7c	ff	d6	fb	75	dc	25	52	89	d0	8e	.â@÷f ÿÖÜuÜ%R%G.
000023c0	77	02	31	b2	b3	4a	c3	6f	81	0c	18	a1	39	9e	c7	ef	w.1²³JÄo...j9.Çİ
000023d0	61	97	40	7a	b8	24	33	19	72	05	e4	2a	56	14	c7	08	a-@z.\$3.r.â°V.Ç.
000023e0	ec	06	c8	e4	b2	99	ee	7f	cc	37	0e	36	f4	1c	b9	ff	ı.Eä²°ı.I7.66.'ÿ
000023f0	d1	f7	8d	5d	ff	d8	bc	61	23	29	57	e9	05	33	3e	0e	N±..]ÿ0%a#)wé.3>.
00002400	e6	99	fd	12	e0	11	70	ef	ff	f6	47	2e	67	d1	99	1d	æ°ı.â.pİÿöG.gN°.
00002410	2c	c5	af	e9	f2	47	62	99	4f	7c	b7	23	d8	f0	9d	5f	,A°éögb°ol.#öğ..
00002420	fe	88	e2	82	50	68	90	ee	c3	d3	88	d4	6c	e7	62	63	Ş°â,Ph.ıÄÖ'Ölçbc
00002430	74	33	31	a3	19	3c	1f	e0	33	dd	30	73	2b	de	ac	84	t3İf.<.â3İos+Ş¬..
00002440	ec	f5	bc	ab	5b	71	f8	e0	8b	0f	bb	b1	18	5b	2c	19	ıö%«[qea<..»±.[,. .
00002450	e7	b8	de	fb	e0	db	1d	3b	11	26	1d	b0	0e	bd	cb	71	ç.ŞÜâÜ.;.&.'°½Éq
00002460	ab	03	72	0b	32	c9	08	22	da	85	6c	b9	f7	85	14	fe	«.r.2E."Ü..ı'÷...Ş
00002470	54	62	86	0b	69	fc	ac	dc	ea	35	dc	97	97	05	ca	82	Tb†.ıü-Üâ5Ü—..É.
00002480	cd	6e	f3	eb	1a	b9	05	17	d5	0e	64	46	5f	58	41	84	Inöé.'..ö.dF_XA,,
00002490	4f	1f	d3	19	6d	f4	85	8d	0e	e5	20	d5	7c	67	b4	f1	O.O.mö...â Ö g'ñ
000024a0	96	45	08	41	ee	0c	f6	0e	af	6c	24	96	fb	a4	92	c3	-E.Aİ.ö..ı°Ş-ü±'A
000024b0	df	ba	33	9a	02	09	b0	33	da	78	47	74	27	ee	75	81	ß°Ş3...°3ÜxGt'ıü.
000024c0	dc	f7	43	ff	38	14	c4	1b	23	dc	c7	dd	06	97	56	44	Ü÷Cÿ8.Ä.°ÜÇİ.-VD
000024d0	1a	43	74	4e	8d	54	cd	6d	7d	43	62	60	cd	46	3b	4b	.CtN.Tİm}Cb İF;K
000024e0	08	4f	49	b0	39	6c	6d	52	a4	de	b6	dc	79	fd	9d	17	.OI°9İmR±Ş¶Üÿı..
000024f0	23	ba	05	fa	bc	e8	63	eb	5c	0d	c1	4a	17	52	20	7b	#°..ú%äcè\..ÄJ.R {
00002500	e5	ef	8e	6b	e1	d6	7a	de	0d	4e	10	65	05	38	49	b4	âı.kâÖzŞ.N.e.8İı

Şekil 29. Manuel stenografi tespiti

MFT ANALİZİ

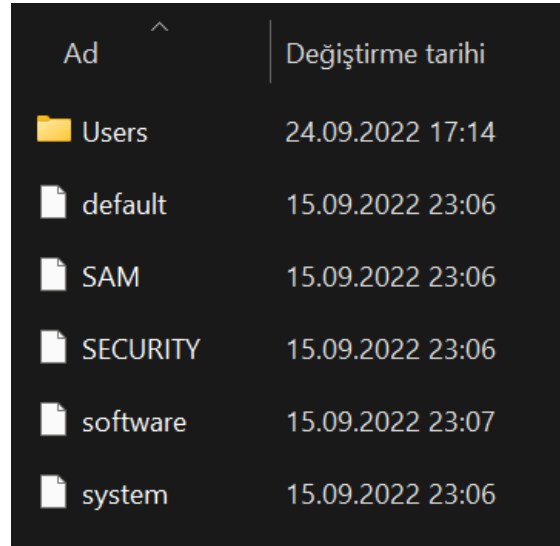
Adli bilişim uzmanları analiz yaparken, dosya sistemi ve yapısıyla ilgili bilgiler edinmeye çalışır. Bazı durumlarda analiz programları dışında da inceleme yapmak zorunda kalabilirler. Örneğin NTFS dosya sistemi kullanan bilgisayarlarda, oluşturulan dosyalar ile ilgili bilgi elde etmek için MFT (Master File Table) analizi yapılır. Çünkü MFT, bilgisayarda var olan dosyalar ile ilgili birçok önemli bilgi barındırır. Dosya ile ilgili dosyanın nerede bulunduğu, dosya metadata verileri ve dosyadaki veriler gibi bilgilere yer verir. Bir MFT tablosunun genel yapısı Şekil 30'da gösterilmiştir. Her MFT tablosu kendi içinde belirli kısımlara ayrılır. Bu kısımların her biri dosya ile ilgili farklı bilgiler bulundurur. Sırasıyla açıklanacak olursa; sarı kısım dosya uzantısı ve bayrak yapısını, mavi kısım dosyalarla ilgili standart bilgileri, yeşil kısım dosya isimleri, turuncu kısım güvenlik tanımlayıcılarını, mor kısım asıl verinin bulunduğu yeri ve kırmızı kısım ise dosyaların bittiği yerdir. Bir adli bilişim uzmanı gerektiği durumlarda bu kısımlardan elde etmek istediği verileri manuel olarak çıkarır ve rapora ekler. Böylelikle dosya yapısı ve dosya ile ilgili bilgileri hazır uygulamaların kullanılmadığı durumlarda manuel olarak tespit edilebilir ve delil elde edilebilir.

0000000000	46 49 4C 45 30 00 03 00-FA C5 19 83 04 00 00 00
0000000016	01 00 01 00 38 00 01 00-D0 01 00 00 00 04 00 00
0000000032	00 00 00 00 00 00 00 00-07 00 00 00 00 00 00 00
0000000048	6F 04 00 00 00 00 00 00-10 00 00 00 60 00 00 00
0000000064	00 00 18 00 00 00 00 00-48 00 00 00 18 00 00 00
0000000080	97 8E 90 F8 42 35 D8 01-97 8E 90 F8 42 35 D8 01
0000000096	97 8E 90 F8 42 35 D8 01-97 8E 90 F8 42 35 D8 01
0000000112	06 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00
0000000128	00 00 00 00 00 01 00 00-00 00 00 00 00 00 00 00
0000000144	00 00 00 00 00 00 00 00-30 00 00 00 68 00 00 00
0000000160	00 00 18 00 00 00 03 00-4A 00 00 00 18 00 01 00
0000000176	05 00 00 00 00 00 05 00-97 8E 90 F8 42 35 D8 01
0000000192	97 8E 90 F8 42 35 D8 01-97 8E 90 F8 42 35 D8 01
0000000208	97 8E 90 F8 42 35 D8 01-00 40 00 00 00 00 00 00
0000000224	00 40 00 00 00 00 00 00-06 00 00 00 00 00 00 00
0000000240	04 03 24 00 4D 00 46 00-54 00 00 00 00 00 00 00
0000000256	80 00 00 00 80 00 00 00-01 00 40 00 00 00 06 00
0000000272	00 00 00 00 00 00 00 00-3F A9 05 00 00 00 00 00
0000000288	40 00 00 00 00 00 00 00-00 00 94 5A 00 00 00 00
0000000304	00 00 94 5A 00 00 00 00-00 00 94 5A 00 00 00 00
0000000320	33 20 C8 00 00 00 0C 33-06 C8 00 1A A6 63 33 10
0000000336	C8 00 D6 82 46 43 0E C8-00 A2 B8 F9 00 33 00 C8
0000000352	00 4E C3 1D 33 08 C8 00-B8 F4 14 43 2C C8 00 3C
0000000368	E7 6B FF 32 C8 30 9C 02-54 00 00 00 00 00 00 00
0000000384	B0 00 00 00 48 00 00 00-01 00 40 00 00 00 05 00
0000000400	00 00 00 00 00 00 00 00-2E 00 00 00 00 00 00 00
0000000416	40 00 00 00 00 00 00 00-00 F0 02 00 00 00 00 00
0000000432	08 E0 02 00 00 00 00 00-08 E0 02 00 00 00 00 00
0000000448	21 2F 14 73 00 00 00 00-FF FF FF FF 00 00 00 00
0000000464	FF FF FF FF 00 00 00 00-FF FF FF FF 00 00 00 00
0000000480	FF FF FF FF 00 00 00 00-FF FF FF FF 00 00 00 00

Şekil 30. MFT tablosu genel yapısı

REGİSTERY KAYITLARININ İNCELENMESİ

Registry, bir tür veri tabanıdır. Bu veri tabanı işletim sistemi ayarlarını ve işletim sisteminin yapılandırılması ile ilgili verileri içerir. Sadece işletim sistemi ile ilgili değil bilgisayara indirilen uygulamaların, kullanıcı ayarlarının, bilgisayar servislerinin bilgilerini ve donanımsal aygıtların bilgilerini içerir. registry kendi içinde key'lere ayrılır. Toplamda beş adet key bulunur. Bu key'ler System, Software, Security, SAM ve Default'tur. Bu dosyalara normal olarak bilgisayarda görünmezler ve bilgisayar kayıt defterinde yer alırlar. Registry dosyalarına ulaşmak için birden fazla yol vardır. Örneğin FTK Imager programında sırasıyla file > Obtain System Files > Options > Password recovery and all registry files seçenekleri seçilir ve registry dosyaları istenilen konuma çıkarılır. Şekil 31'de çıkarılan dosyalar yer almaktadır.



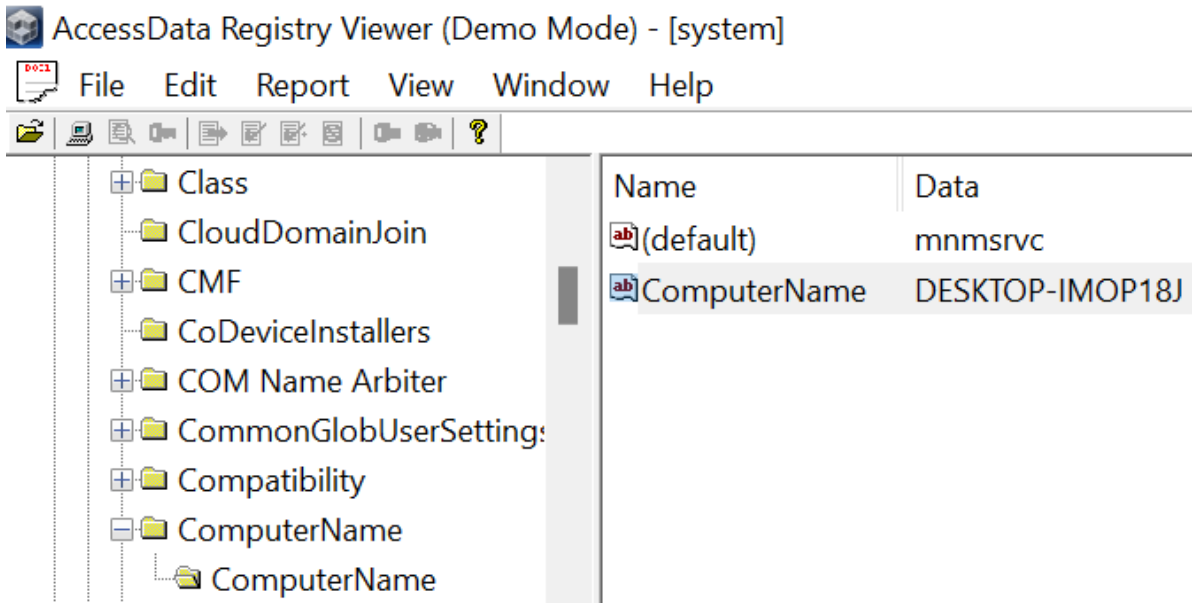
Ad	Değiştirme tarihi
Users	24.09.2022 17:14
default	15.09.2022 23:06
SAM	15.09.2022 23:06
SECURITY	15.09.2022 23:06
software	15.09.2022 23:07
system	15.09.2022 23:06

Şekil 31. Registry dosyaları

Bu dosyaların her biri farklı bilgiler içerir. Örneğin System dosyasında, sistem yapılandırmalarını içeren bilgiler yer alır. Bilgisayarın adı, sistemin kullandığı zaman dilimi bunlara örnek verilebilir. Software dosyasında, adından da anlaşılacağı gibi yüklenmiş olan uygulamaların ayarlarını ve işletim sisteminin sunduğu hizmet ayarları ile ilgili bilgileri içerir. Security dosyası, güvenlik ile ilgili yapılandırmaları ve ayarları içerir. SAM (Security Account Manager), güvenlik hesap yöneticisidir. Kullanıcının SID bilgisini, kullanıcı adı ve şifresini içeren bilgileri barındırır. Hardware kısmında ise sistemde olan donanımsal cihazların bilgilerini içerir ve saklı bir yapıdır.

Bu dosyaları Şekil 31’de gösterildiği gibi çıkarılsa bile direkt olarak açılmazlar. Dosyaların görüntülenmesi için bir program gereklidir. Örneğin Registry Viewer programı sayesinde bu dosyalar açılabilir ve içindeki dosyalar okunabilir. Bu durum Şekil 32’de gösterilmiştir. Registry Viewer ile System dosyası açılmış ve bu dosya sayesinde bilgisayarın adına ulaşılmıştır. Aynı şekilde Registry dosyalarından Software dosyasını kullanarak işletim sistemi ve sisteme ait sürüm öğrenilebilir. Bunun için Software > Microsoft > Windows NT > CurrentVersion seçilir ve istenilen bilgilere ulaşılır. Ve ya System > Controlset001 > Control > TimeZoneInformation seçenekleri seçilerek bilgisayarın kullandığı saat dilimine ulaşılabilir.

Sonuç olarak bir adli bilişim uzmanı bir delil elde ettiği zaman bu tarz temel bilgilere ulaşmak için Registry dosyalarından faydalanarak manuel analiz yapabilir.

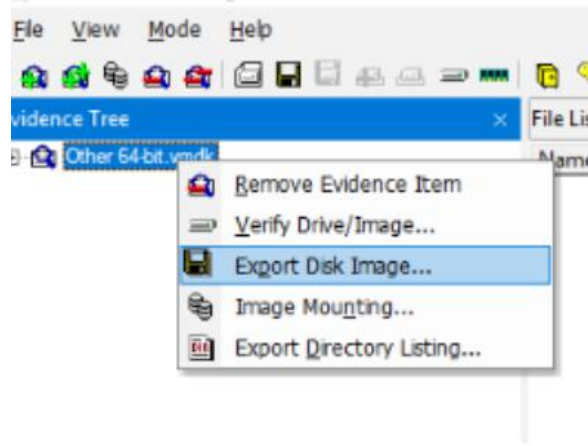


Şekil 32. Registry dosyalarının incelenmesi

SANAL MAKİNE İNCELENMESİ

Olay yeri incelemelerinde elde edilen bir bilgisayarda sanal makine var ise o da ayrı olarak incelenmelidir. Çünkü sanal makine farklı işletim sistemi ve dosya yapısına

sahip olabilir. İçindeki IP değeri, kullanıcı bilgileri gibi değerler ana bilgisayardan farklıdır. Dolayısıyla sanal makine üzerinden de suç işlenebilir ve detaylı bir şekilde incelenmesi gerekir. Detaylı bir şekilde incelenebilmesi için sanal makinenin ayrıca bir imajı alınmalıdır. Sanal makinenin imajının alınması için farklı uygulamalar mevcuttur. Örneğin FTK Imager programı ile bu işlem gerçekleştirilebilir. File kısmından Export Disk Image seçeneği yardımı ile VMKD uzantılı sanal makine imajı çıkarılır. Bu durum şekil 33'de gösterildiği gibidir. Ancak sanal makine imajı da diğer imajlarda olduğu gibi direkt olarak açılmazlar. Bunun için bir program gereklidir.



Şekil 33. Sanal makine imajının alınması

Bazı durumları ise adli bilişim uzmanlarına incelenmesi için hazır olarak bir sanal makine imajı verilir. İnceleme için çeşitli programlar mevcuttur. Örneğin Forensic Explorer (FEX) uygulaması, sanal makine incelemesi yapan programlar arasındadır. Hem Windows hem Mac cihazlarda çalışır. Live Boot ile sanal makinedeki kullanıcıya ait şifreler kırılabilir ve atlatılabilir, imaj içindeki programlar ve yazılımlar masaüstü düzeni modunda incelenebilir. Ayrıca bu kısım ile Windows geri yükleme noktasına geri dönülebilir ve sanal makinenin Registry dosyaları incelenebilir. Registry dosyalarından MRU List analizi yapılabilir. MRU List, kullanıcının son kullandıkları öğelerin geçmişi. Son açılan programlar ve web URL'leri gibi adli inceleme açısından önemli bilgiler içerir. MRU List yapılarına Registry dosyalarından ulaşılır. Registry dosyalarından Software > Microsoft > Windows > CurrentVersion > Explorer > RecentDocs ile son açılan dokümanlara ulaşılır. Bu ve bunun gibi birçok sanal

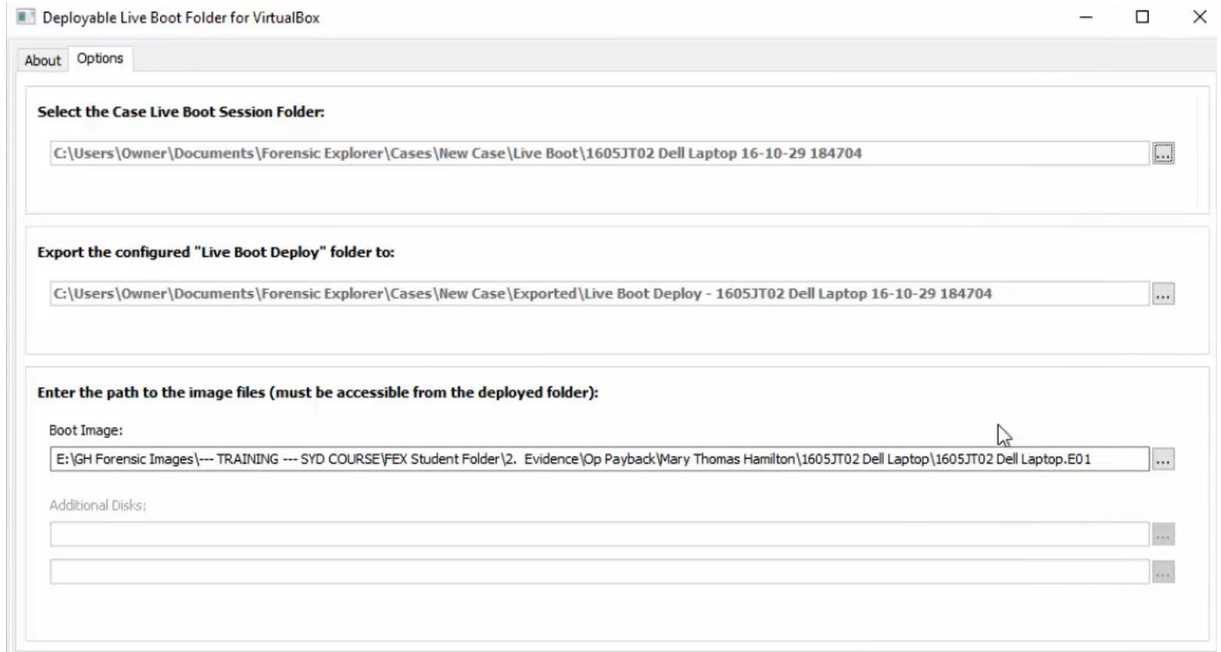
makine incelemeleri Şekil 33.1'de gösterildiği gibi FEX programının Live Boot kısmından yapılabilir.



Şekil 33.1 FEX-Live Boot

Sanal disk imajını şekil 34'de gösterildiği gibi Deployable Live Boot folder for Virtualbox seçeneğinden açılabilir. Sonrasında imaj dosyası eklenir ve incelenmek üzere bir sonraki aşamaya geçilir.

Sonuç olarak olay yeri incelemelerinde bir sanal makine ile karşılaşıldığı zaman FTK Imager ile imajı alınabilir ve Forensic Explorer programının Live Boot seçeneği ile adli incelemesi yapılabilir. Ardından mahkemeye sunulmak üzere hazırlanan rapora eklenerek delil çeşitliliği artırılabilir ve adli olayı aydınlatılabilir.



Şekil 34. Sanal disk imajının açılması

VİRÜSLÜ DOSYALAR

Olay yeri incelemelerinde virüslü bir dosya ve ya virüslü bir bilgisayar ile karşılaşılırsa ne olur?

Bir adli bilişim uzmanı olay yeri incelemelerinde delil niteliğinde olabilecek her şeyi olabildiğince incelemeli ve analiz yapmalıdır. Ancak bazı durumlarda problemler çıkabilir. Örneğin virüslü bir dosyayla ya da bilgisayarla karşılaşılması ve karşılaşıldığı durumda incelemelerinin nasıl olacağı önem arz eden bir durumdur.

Virüslü ya da virüslü olduğundan şüphelenilen bir disk ile karşılaşıldığı zamanlarda imaj alma işlemleri sırasında kesinlikle writeblocker kullanılmalıdır. Böylelikle imajın alınacağı hedef diske, sistemden virüs sızmamış olur. Writeblocker, adli kopyalama işlemlerinde yazma koruması sağlayan ve tek yönlü veri akışına izin veren bir sistemdir. Böyle bir diskin imajının alınması için Tableau TD2 donanımından yararlanılabilir. Tableau imaj alınırken kullanıcının yazma korumalı bir şekilde imaj almasına olanak sağlar.

Alınan imaj adli inceleme yazılımları ve programları ile normal bir şekilde incelenebilir. İncelenme sırasında, incelemenin yapıldığı bilgisayara virüs bulaşmaz. Adli bilişim uzmanları diğer imajları incelediği şekilde virüs içeren bir bilgisayarı veya programı inceleyebilirler. Ancak imaj dosyası Live modu ile (FEX, Live Boot vs.) çalıştırılması durumunda virüsün bulaşma ihtimali ortaya çıkar. Örneğin bir imajda e-mail gibi mesajlaşma uygulamaları ya da herhangi bir uygulama incelenecekse masa üstü canlandırması olmadan incelenmelidir.

NET OLMAYAN FOTOĞRAF VE VİDEOLAR

Bir olay yeri incelemesinde elde edilen delillerin manuel olarak ya da hazır programlar sayesinde incelenir. Elde edilen deliller arasında birden fazla dosya türü elde edilir. Bunlardan bazıları da fotoğraf ve videolardır. Fotoğraf ve videolar delil çıkarma ve olayı aydınlatma konusunda oldukça güçlü verilerdir. İnceleme esnasında elde edilen fotoğraflar, suçu aydınlatma görevi gören bir delil ise rapora eklenir ve hâkimin karar

vermesini kolaylaştırır. Ancak bazı durumlarda delil olabilecek fotoğraf ya da videolar bozuk, karanlık ve ya bulanık bir biçimde bulunabilir. Böyle durumlarda fotoğraf ve videonun düzeltilmesi gerekmektedir. Bunun için çeşitli programlar mevcuttur. Örneğin Amped5 programı video ve fotoğraflar üzerinde çeşitli düzeltme işlemleri gerçekleştirmeye yarar.

Örneğin trafik kazasına karışan bir araç kaçarken mobese kameraları tarafından çekilmiş olsun ancak plaka net değil ise aracın plakasını tespit ederken Amped5 uygulaması kullanılabilir. İçinde barındırdığı çeşitli filtrelemeler sayesinde fotoğrafın ve ya videonun yapısıyla oynayarak, bir Adli Bilişim uzmanının dosyayı kullanabileceği hale getirmesine yardımcı olur. Bu durumun bir örneği Şekil 35'te gösterilmiştir. Sol tarafta görünen fotoğraf, kameralara yakalanan orijinal fotoğraftır ve net olmadığı için plaka okunamamaktadır. Ancak sağ taraftaki fotoğraf uygulama sayesinde netleştirilmiştir. Bu durumda okunabildiği için olay ile ilgili aydınlatıcı bir veri olarak kullanılabilir.

Amped5 programı videoların da düzeltilmesi işlemini Şekil 35'te olduğu gibi yapabilir. Bunun için program videoları frame olarak böler ve fotoğraf gibi üzerinde oynanmasına olanak sağlar.



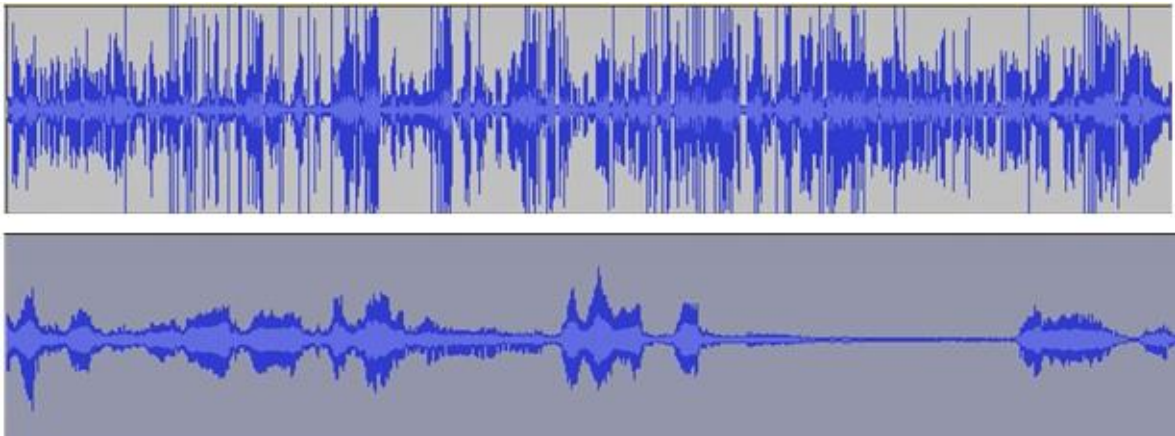
Şekil 35. Amped5 ile plakanın netleştirilmesi

NET OLMAYAN SES DOSYALARI

Olay yeri incelemelerinde fotoğraf ve video kadar ses dosyaları da delil niteliği taşır ve detaylı bir şekilde incelenmesi gerekir. Ancak bazen tıpkı fotoğraflarda olduğu gibi ses dosyaları da net olmayabilir. Bu durumdaki dosyaların gürültülerinden arındırılmaları gerekmektedir. Net olmayan ses dosyaları için Adli Bilişim uzmanları çeşitli programlar kullanırlar. Bu programlar lisanslı ya da lisanssız olabilir. Örneğin Audacity programı lisans gerektirmez ve net olmayan ses dosyalarını düzenler. Bunun için içinde çeşitli ayarlamalar ve filtreler mevcuttur. Adli bilişim uzmanı sesteki gürültülere göre hangi ayarlamalar yapacağını bilmelidir. Gerekli ayarlamalardan sonra ses dosyası, dosyanın sahip olduğu gürültü oranlarına göre farklı oranlarda gürültüyü azaltabilir.

Ses düzenleme programları ile düzeltilebilecek, kanıt niteliğinde birçok çeşit ses dosyası vardır. Örneğin net olmayan telefon konuşmaları, bazı güvenlik kameralarına takılmış olan sesler, ses kayıt cihaz ile alınan sesler, video çekildiği sırada delil olabilecek ancak anlaşılamayan sesler gibi birçok çeşit kaynaktan net olmayan ses verileri netleştirilip delil niteliğine ulaştırılabilir.

Şekil 36'da bir ortamda alınan ses kaydı vardır. Üst taraftaki ses orijinal ses dosyasına aittir ve şekilden de anlaşılacağı gibi gürültülü bir yapıdadır. Çevrede olan araba sesi, insan sesi ve şehrin gürültüsü ile birlikte net değildi ancak Audacity programı ile ses düzenlenmiş olup gürültülerinden arındırılmıştır. Gürültüden arındırılmış olan temiz ses dosyası ise Şekil 36'nın alt kısmında gösterildiği gibidir.



Şekil 36. Audacity ile ses gürültülerinin temizlenmesi

ÖRNEK VAKALAR SENARYOLAR

VAKA 1

Daniel ismi seri katil 15'ten fazla cinayet işledi ve polise işlediği cinayetleri itiraf eden mektuplar bırakıyordu. Ardından işlediği cinayetleri fotoğraflayarak ve yazarak bir USB içinde güvenlik kolluklarına alaycı mesajlarla gönderdi. Polis Daniel isimli seri katilin son işlediği cinayet olarak bilinen Rachel cinayetini araştırmak ve kanıt toplamak üzere olay yeri incelemesi başlattı.

ÇÖZÜM 1

Bu vakada, ilk olarak olay yerinin incelenmesi ve delillerin toplanabilmesi için mahkemeden arama izninin çıkarılması gerekiyordu. Mahkemeden olay yeri araması izni çıktıktan sonra olaya atanmış olan ve aralarında Adli Bilişim uzmanının da bulunduğu ekip olay yerine intikal ettiler. Olaydan kısa süre sonra Rachel isimli öldürülen kadının evine ulaştılar. Rachel kendi evinin yatak odasında ölü bulunmuştu. Olay yerine ulaşan ekip işlemlere başlamadan önce tüm alanı görebilecek şekilde kamera yerleştirdiler. Ardından olay ile ilgisi bulunabilecek olan dijital verileri toplamaya başladılar. Olay yerinde DELL marka olan bir adet açık bilgisayar ve tamamen kapalı LG markalı bir telefon buldular. Aynı zamanda katilin güvenlik güçlerine gönderdiği USB mevcuttu. Buldukları delilleri etiketlediler ve listeye eklediler. USB belleğin imajını Tableau TD2 donanımı kullanarak okuma yazma korumalı bir şekilde elde ettiler ve hash değerini imzalattılar. Kapalı bir biçimde olan ve şifresi olan telefonun şifresini UFED yazılımından faydalanarak etkisiz hale getirdiler ve root işlemini gerçekleştirdiler. Ardından yine aynı uygulama ile imaj aldılar ve hash değeri imzaladılar. Katil belli olmadığı için karşı tarafa bu değerler verilmedi. Ancak kayıt altına alındı. Diğer yandan açık olan bilgisayara yapılan tüm işlemler diğerleri gibi kayıt altına alındı. İlk önce Ram imajının alınabilmesi için tek yönlü aktarım yapan bir USB cihazda bulunan X-Ways Capture yazılımı ile RAM imajı alındı. Ardından Autopsy programı ile bilgisayarın imajı alındı ve hash değeri hesaplatıldı. İlk müdahale ve tespit aşamasından sonra mahkeme tarafından verilen delillerin incelenmesine yönelik zamana dâhilinde incelenmeler başlatıldı. Telefondan alınan imaj Oxygen programı ile

incelendi. Silinmiş veriler, en sık iletişim kurulan insanlar ve sosyal medya dökümleri gibi delil barındırabilecek alanlar incelendi. İncelemeler sonucunda normal olmayan bir görüşme ve kişiye rastlanmadı. İmajı alınan bilgisayarın incelenmesi için de tekrardan Autopsy uygulamasından yaralandılar. Var olan tüm dosyalar ve veriler incelendi. Konum bilgileri ve fotoğraflar analiz edildi. Silinmiş veriler arasında Daniel isimli katil ile çekilmiş bir fotoğraf mevcuttu ancak bu tek başına delil olabilecek bir veri değildi. Ardından uzmanlar katilin gönderdiği USB belleği incelemeye başladılar. Daha önceden imajı alınan USB belleği incelemek için FTK programından yararlandılar. Bellek içerisinde birkaç adet fotoğraf ve yazılı bir metin bulunmaktaydı. Silinmiş bir veriye rastlamadılar ancak var olan dosyaların metadata verilerine ulaşmayı başardılar. Katilin çekmiş olduğu fotoğraf dosyalarının metadata verileri katille ilgili birçok kanıt barındırıyordu. Metadata verilerinde, fotoğrafı çeken cihazın marka bilgisi, model bilgisi, çekildiği tarih ve konumu gibi bilgileri içeriyordu. Fotoğrafın çekildiği saat ile Rachel'in bilgisayarında bulunan ve Daniel ile çekilen silinmiş fotoğrafın saati arasında sadece yarım saat fark bulunuyordu. İnceleme yapan ekip bulmuş olduğu tüm kanıtları ve süreçleri rapora detaylı bir şekilde eklediler ve mahkemeye teslim ettiler. Rapor sonucu Daniel gözaltına alındı ve kısa süre sonra suçunu itiraf etti.

VAKA 2

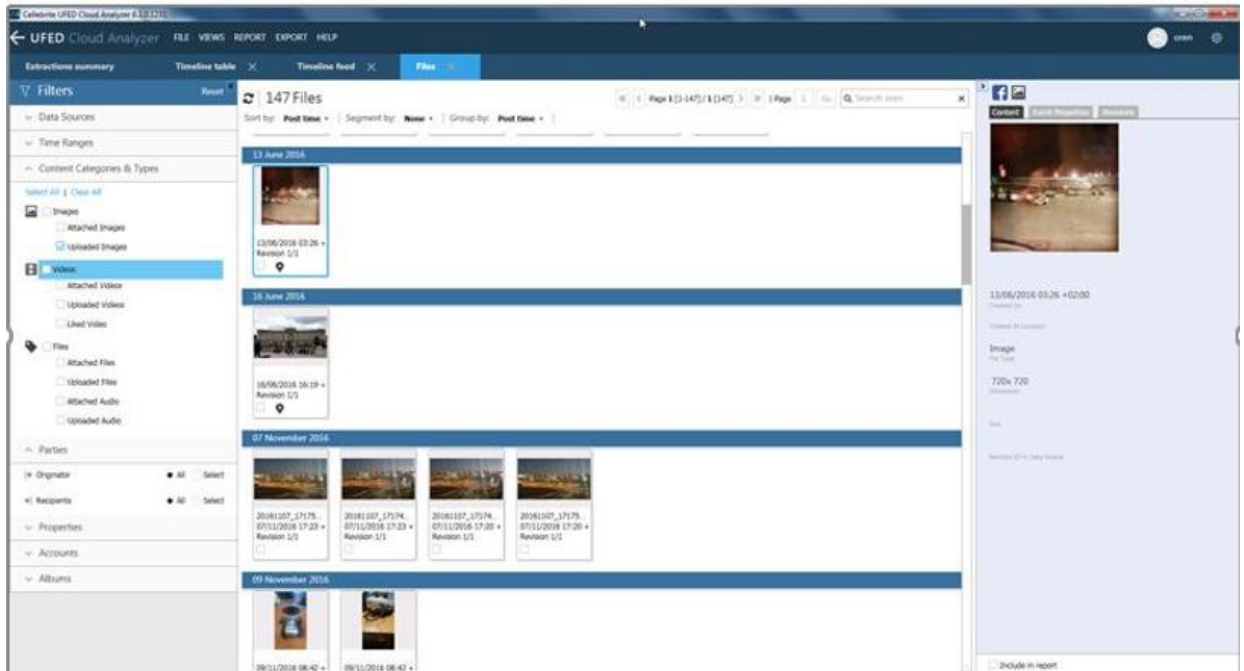
2017 yılında, Hüseyin K. ve Arda N. isimli hayvan ticareti yapan iki ortaklı. Yaptıkları ticaret sonucunda para paylaşımından anlaşılamayan ortaklar tartıştılar. Tartışmadan kısa süre sonra Hüseyin K. İsimli şahıs Arda N isimli şahsı darp etti ve kıyafetlerini çıkararak fotoğrafladı. Ardından evine dönen Hüseyin K. Çekmiş olduğu fotoğrafları bilgisayarına bir World dosyası içine attı ve altına parayı geri ödemediği takdirde fotoğrafı paylaşacağını yazdı. Ardından bu dosyayı yazıcı ile çıkarıp Arda N. İsimli şahsın evine gönderdi. Tehdit mesajını alan Arda N, durumu kolluk kuvvetlerine bildirdi ve Hüseyin K. hakkında suç duyurusunda bulundu.

ÇÖZÜM 2

Bu vakada ilk olarak kolluk kuvvetleri olayın gerçekleştiği ildeki Cumhuriyet Savcılığına bildiride bulundu. Bildiri sonucu CMK 119 maddesi yürürlüğe geçti ve şüpheli Hüseyin

K'nın evine arama yapılması ve delil elde edilmesine karar verildi. Bu olaya atanmış olan adli bilişim uzmanları olay yerine intikal ettiler. Evi arama işlemlerine başlamadan önce her açıdan çekim yapabilecek kameraları yerleştirdiler. Yapılan aramalar sonucunda bir adet Casper marka masaüstü bilgisayar, HP marka bir yazıcı ve Samsung marka bir telefon bulundu. Ortamda olan diğer teknolojik aletler (iki adet televizyon) olay ile ilgisi bulunmadığı için alınmadı. İncelenecek olan deliller numaralandırıldı ve delil listesine eklendi. CMK 134 gereği orijinal deliller üzerine analiz yapılamayacağı için incelenmek üzere alınan delillerden Casper marka masaüstü bilgisayarının sahip diski CRU Ditto donanımı ile imajı alındı. Şüpheli tarafından itiraf edilen şifre açıldıktan sonra UFED programı ile telefonun imajı alındı. Ardından telefon ve bilgisayar Hüseyin K kişisine iade edildi. Aynı zamanda alınmış olan imajların da bir kopyası şüpheli tarafa verildi. Ancak yazıcının bir imajı alınamadığı için el konuldu.

Elde edilen deliller güvenli bir şekilde laboratuvara götürüldü. Yazınının kutudan çıkarılması işleminden incelemenin bitme işlemine kadar olan süreç kayıt altında gerçekleştirildi. Yapılan inceleme sonucu yazıcının dâhili bir hafızasının olmadığı tespit edildi. Dolayısıyla buradan bir sonuca ulaşamadı. Ardından şüpheli Hüseyin K'nın telefonu incelenmeye başlandı. Zaten şifresi açılmış olan ve imajı alınmış olan telefon incelenme aşamasına geçirildi. İnceleme işlemleri için UFED programından yararlanıldı. UFED programının kategorileri arasında yer alan Images bölümünden mağdur Arda N'ye yapılan darp fotoğrafları bulundu.



Şekil 37. UFED ile fotoğrafların incelenmesi.

Diğer yandan incelenecek son delil olan masaüstü bilgisayarın diski incelenmeye başladı. İncelenme işlemleri için FTK programı kullanıldı. Yapılan incelemeler sonucunda FTK'nın imza analizi yapma fonksiyonları sayesinde uzantısı değiştirilmiş olan fotoğrafın orijinal haline ulaşıldı. Bu fotoğraf telefonda bulunan fotoğrafın kopyasıydı. Fotoğrafın EXIF bilgilerinden olay yerinin konumu ve saati tespit edildi. İncelenmenin ilerleyen aşamalarında ise mağdur Arda N'ye gönderilen tehdit belgesi silinmiş bir şekilde bulundu.

İnceleme işlemlerinin tamamı bittikten sonra bilirkişi raporu oluşturulmaya başlandı. Rapor; olayın türünü, şüpheli ve mağdur bilgilerini, olayın yerini, sunulan makamı ve elde edilen delilleri içeriyordu. Sonuç olarak raporda yazıcıdan bir bilgi elde edilemediği, telefonda fotoğraf ve arama kayıtlarının elde edildiği, bilgisayardan fotoğraf ve belgelerin elde edildiği konularına detaylıca değinilmiştir. Delillerin tespit edilme aşamasından olayın incelenme aşamalarına kadar olan her kısım detaylı bir şekilde rapora yazıldıktan sonra rapor mahkemeye sunulmuştur.

VAKA 3

2019 yılında Murat Y. ile boşanma aşamasında olan Emine T. dördüncü kattaki evinden düşerek öldü. Emine T'nin ailesi kolluk kuvvetlerine giderek Emine T'nin intihar etmediğini ve Murat Y'nin ittiğini iddia ettiler. Ardından Murat Y. ile ilgili suç duyurusunda bulundular. Kolluk kuvvetleri tarafından Murat Y. hakkında soruşturma başlatıldı. Murat Y. olayın gerçekleştiği zamanda farklı bir mekânda olduğunu iddia etti. Ardından hâkim kararı ile maktul Emine T'nin evine arama emri çıkarıldı.

ÇÖZÜM 3

Adli bilişim uzmanları Emine Y'nin ölmüş olduğu binayı gören güvenlik kamerasına hâkim kararı ile el koydu. Kamera, Emine T'nin düşmüş olduğu balkon tarafını görebilecek konumdaydı. Ardından Emine T'nin mutfağında bulunan ve Emine T'ye ait

olan telefona incelenmek üzere el konuldu. Diğer yandan yine hâkim kararı ile Murat Y'ye ait olan telefona da incelenmek üzere el konuldu. Murat Y'nin telefonunun imajı Oxygen Forensic uygulaması ile alındıktan sonra hash değerleri hesaplatıldı ve elde edilen imaj ve hash değerlerinin bir kopyası da şüpheli tarafa verildi. Sonrasında Oxygen Forensic uygulaması ile maktul Emine T'nin telefonunun imajı alındı. Son olarak Emine T'nin sokağında olan güvenlik kamerası görüntülerinin bir kopyası alındı. Ekipler ilk müdahale ve tespit aşamasından sonra inceme aşamasına geçtiler. İlk olarak güvenlik kamerası incelenmeye başladı. Olayın gerçekleştiği güne ve saate ait olan kamera kaydı incelenmeye başlandı. Ancak görüntüler tam olarak net değildi. Bunun için Amped5 programından faydalandılar ve gerekli düzenlemelerden sonra Şekil 38'de olduğu gibi görüntüde maktulün atlamadığı ve biri tarafından itildiği kanısına varıldı.



Şekil 38. Güvenlik kamerası görüntüleri

Ardından diğer cihazlar incelenmeye başladı. İmajı alınmış olan maktul Emine T'ye ait olan telefon Oxygen Forensic programı ile incelenmeye başlandı. Yapılan detaylı incelenmeler sonucunda, Murat Y, Emine T'ye Instagram uygulaması aracılığıyla tehdit mesajı attığı ortaya çıktı. Mesajın metadata verileri incelendiği zaman, mesaj Emine T'ye öldürülmesinden 2 saat önce atıldığı bilgisi elde edildi. Diğer yandan Murat Y'nin telefonu incelenmeye alındı. Oxygen Forensic ile incelenmeye başlanan telefonda delil olabilecek bir bulguya rastlandı. Şüpheli sorgu esnasında olay gerçekleştiğinde farklı

bir yerde olduğunu iddia etmişti Snapchat ile gönderilen fotoğrafların metadata verilerinden, olay saati civarlarında şüphelinin, Emine T'nin evinin yakınlarında olduğu tespit edildi. Elde edilen bulgular baştan sona rapora eklendikten sonra değerlendirilmek üzere hâkime sunuldu.

Kaynakça

- [1] Özocak, G. CEZA MUHAKEMESİNDE ELEKTRONİK DELİLLERİN TESPİTİ VE TOPLANMASI DETECTION AND COLLECTION OF DIGITAL EVIDENCES IN CRIMINAL PROCEDURE.
- [2] Muharrem, Ö. Z. E. N., & Özocak, G. (2015). Adli Bilişim, Elektronik Deliller ve Bilgisayarlarda Arama ve El Koyma Tedbirinin Hukuki Rejimi (CMK M. 134). *Ankara Barosu Dergisi*, (1).
- [3] Başlar, Y. (2019). Adli Bilişim Sürecinde Karşılaşılan Sorunlar ve Çözüm Önerileri.
- [4] https://tr.wikipedia.org/wiki/Adli_bili%C5%9Fim
- [5] <https://kernelblog.org/2020/03/adli-bilisimde-olay-yeri-mudahalesi/>
- [6] <https://bilirkisiraporlari.com/adli-bilisim-internet-suclari/>
- [7] [https://caneryenidunya.medium.com/ceza-muhakemesinde-delillerinde%C4%9Fferlendirilmesi-delil-yasaklar%C4%B1-ve-hukuka-ayk%C4%B1r%C4%B1-delillerin-ceza-bff814552eb4#:~:text=i\)%20Duru%C5%9Fmaya%20getirilip%20huzurda%20tart%C4%B1%C5%9F%C4%B1lm%C4%B1%C5%9F,de%C4%9Fferlendirme%20yasa%C4%9F%C4%B1%20kapsam%C4%B1nda%20bulunmamas%C4%B1%2C%20gerekir.](https://caneryenidunya.medium.com/ceza-muhakemesinde-delillerinde%C4%9Fferlendirilmesi-delil-yasaklar%C4%B1-ve-hukuka-ayk%C4%B1r%C4%B1-delillerin-ceza-bff814552eb4#:~:text=i)%20Duru%C5%9Fmaya%20getirilip%20huzurda%20tart%C4%B1%C5%9F%C4%B1lm%C4%B1%C5%9F,de%C4%9Fferlendirme%20yasa%C4%9F%C4%B1%20kapsam%C4%B1nda%20bulunmamas%C4%B1%2C%20gerekir.)
- [8] <https://tuncaybesikci.com/adli-bilisim-uzmanlarinin-dikkat-etmesi-gereken-hususlar/>
- [9] <https://www.adlibilisimuzmani.com/adli-bilisimde-olay-yerinde-ilk-mudahalede-genel-kurallar/>
- [10] <https://www.bilisimvehukuk.net/icerik/adli-bilisim-sureci/>
- [11] <https://www.adlibilisimuzmani.com/adli-kopya-alma-donanimlari-imaj-alma-donanimlari/>
- [12] <https://www.karel.com.tr/bilgi/wireshark-nedir-nasil-kullanilir>
- [13] [https://tr.wikipedia.org/wiki/Ping_\(a%C4%9F_arac%C4%B1\)](https://tr.wikipedia.org/wiki/Ping_(a%C4%9F_arac%C4%B1))
- [14] <https://www.difose.com.tr/portfolio/dolphin-data-recovery/>

- [15] <http://halilozturkci.com/adli-bilisim-dumpit-ile-windows-sistemlerde-hafiza-imaji-alma/#:~:text=Dumplt%20yaz%C4%B1l%C4%B1m%C4%B1%20Moonsols%20firmas%C4%B1%20taraf%C4%B1ndan,i%C3%A7in%20kullan%C4%B1labilecek%20%C3%BCcretsiz%20bir%20yaz%C4%B1l%C4%B1md%C4%B1r.>
- [16] <https://www.x-ways.net/capture/index-m.html>
- [17] <https://bilgegunluk.com/accessdata-ftk-forensic-toolkit-examiner/>
- [18] <https://www.difose.com.tr/forensic-explorer/>
- [19] <https://www.bigdataforensic.net/index.php/mobil-cihaz-inceleme-veri-kurtarma/165-cellebrite-mobil-cihaz-adli-inceleme-yazilimi-ozellikleri/>
- [20] <https://www.einvestigator.com/encase-forensic/#:~:text=Encase%20Forensic%20helps%20agencies%20conduct,and%20many%20flexible%20reporting%20options.>
- [21] <https://www.bigdataforensic.net/index.php/mobil-cihaz-inceleme-veri-kurtarma/158-oxygen-forensic-mobil-cihaz-adli-inceleme-yazilimi/>
- [22] <https://www.emt.com.tr/tr/markalar/oxygen-forensics-47>
- [23] <https://www.utahdatarecovery.com/flash-drive-repair-questions-answered/>
- [24] <https://getdataforensics.com/virtual-live-boot/>