DIFOSE

www.difose.com.tr

ADLİ BİLİŞİM HİZMETLERİ

"Her temas iz bırakır."

Edmond Locard-

-

DIFOSE

www.difose.com.tr

Başlarken

Bilgi ve iletişim teknolojilerinde görülen hızlı gelişmeler insan hayatını kolaylaştırıp iş verimliliğini artırırken günlük hayatımızdaki alışkanlıkları da değiştirerek bireyleri olduğu kadar toplumları da geri dönülemez bir biçimde bu teknolojilere bağımlı hale getirmiştir. Yaşanan bu hızlı gelişmelere paralel olarak hayatımızdaki dijital veriler en önemli varlıklarımız listesinde en üst sıraya yerleşmiş ve değerli olan her eşya gibi dijital verilerin de suç ve suistimale karşı korunması zorunlu hale gelmiştir. Nitekim kişisel veya kurumsal verilerin güvenliğinin yeterince sağlanmamış olması yetkisiz ve kötü niyetli kişilerin eline geçmesine ve hatta telafisi imkânsız zararlara neden olacağı aşikârdır.

Güvenlik sektöründe %100 oranında güvenliğin sağlanması çok zordur. Hele konu siber güvenlik ise öncelik sıralaması, sistemlere yönelik saldırıları önleyecek tedbirleri almak ve bu tedbirlerin uygulanmasını sağlamak olacaktır. Ancak, alınan pek çok tedbire rağmen siber güvenlik sistemlerinin aşıldığı bir olayın cereyan etmesi durumunda ise yaşanan olaya ait iz ve emareleri barındıran delilleri, gerek gelecekte yaşanması muhtemel bir siber olayı engellemek ve gerekse adli soruşturmalara dayanak oluşturmak için zarar görmeden usulüne uygun olarak elde etmek gerekmektedir.

DIFOSE ekibi, karşılaştığınız siber olayın türü ve büyüklüğü ne olursa olsun size en kısa sürede profesyonel destek vermek amacıyla Ankara ve İstanbul ofisleri ile hizmet etmeye hazırdır.

Vizyonumuz;

Müşterisinin kurumsal itibarı ve bilgi güvenliğine verdiği önemi her şeyin üzerinde tutan, güvenilir, dürüst ve sürekli kaliteli hizmetler sunan, bu bağlamda yeniliklere daima açık, çözüm odaklı çalışan, sürekli olarak fark ve değer yaratan, rakiplerinin her yönüyle örnek aldığı, Türkiye ve EMEA bölgesinde lider bir marka olmaktır.

Misyonumuz;

Uzun yıllara dayalı elde etmiş olduğumuz bilgi, beceri, tecrübe ve yüksek standartlardaki hizmetlerimizi ilgili yasal mevzuata uygun olarak yurt içi ve yurt dışındaki müşterilerimize sunmak ve Türkiye'de siber güvenlik ve adli bilişim sektörünün gelişmesine katkıda bulunmak.

Temel Değerlerimiz;

- Teslim aldığımız her işi en önemli, ilk ve tek işimiz gibi kabul etmek,
- Kabul ettiğimiz işi daima bilimsel ve etik değerler çerçevesinde çalışmak,
- Çalıştığımız her işi söz verdiğimiz sürede yerine getirmek, müşterimizin güvenini ve memnuniyetini en üst seviyede tutmaktır.

NEDEN FARKLIYIZ?

- Kolluk ve bilirkişi tecrübesi
- DIFOSE Adli Bilişim ve Veri Kurtarma laboratuvarı
- Güncel yazılım ve donanımlar
- Uluslararası deneyim ve referans
- Üniversitelerde akademik çalışmalar
- Resmi bilirkişilik ve uzman görüşü hizmetleri
- NATO, OSCE, UN, INTERPOL, Council of Europe, EC|Council, CompTIA, InfoSEC Global ve Logical Operations eğitim işbirliği
- İhtiyaca göre özel çözümler

Geçmişten

2013

- DIFOSE, Limited şirket olarak 27 Mayıs 2013 günü Ticaret Sicil Gazetesi'nde yayımlanan duyuru ile Çankaya-Ankara'da faaliyetlerine başladı.
- Adli Bilişim Laboratuvarı uluslararası standartlarda yazılım ve donanımlarla teçhiz edilerek hizmet vermeye başladı.
- Dünyaca tanınan GetData Pty. yazılım firması ile Forensic Explorer isimli adli bilişim yazılımını geliştirmek ve Türkçe sürümünü hazırlamak amacıyla anlaşma imzaladı. DIFOSE, Forensic Explorer adli bilişim yazılımın çözüm ortağı ve EMEA bölgesi distribütörü oldu.
- Forensic Explorer adli bilişim yazılımı Türkçe olarak yayımlandı.

2014

- DIFOSE, Ankara, Sherton Oteli'nde düzenlenen EMEA-Intelligence Fuarı'nda ilk kez görücüye çıkarak adli bilişim alanındaki çözüm ve hizmetlerini müşterilerine tanıttı.

2015

- DIFOSE, Ümitköy, Çankaya, Ankara adresindeki yeni binasına taşındı ve uygulamalı adli bilişim eğitimi vermek amacıyla DIFOSE AKADEMİ kuruldu.
- Azerbaycan, Birleşik Arap Emirlikleri, Nijerya ve Arnavutluk'ta adli bilişim alanında çeşitli eğitimler verdi.

2016

- DIFOSE, Dünyanın en büyük şirketlerinden birisi olan ARAMCO'ya Suudi Arabistan'ın Dammam kentinde eğitim verdi.
- Pakistan'da Pakistan Deniz Kuvvetleri ve Donanma Komutanlığı'na eğitim verdi.
- Suudi Arabistan'da Kral Abdülaziz Bilim ve Teknoloji Araştırmalar Kurumu'na (KACST) eğitim verdi.

2017

- DIFOSE, Moldova Kriminal Polisi'ne adli bilişim eğitimi verdi.
- Adli Bilişim ve Veri Kurtarma alanlarında ürünler üretmek amacıyla AR & GE bölümü kuruldu.
- Veri Kurtarma Laboratuvarı kuruldu. DIFOSE tarafından özel adli bilişim ve veri kurtarma bilgisayarı üretildi. DIFOSE tarafından uluslararası standartları karşılayan Clean Repair Box (DIFOSE Temiz Tamir Kutusu) üretildi.

DIFOSE Geleceğe

2021

- DIFOSE yeni yerleşkesi olan ODTÜ ASO Teknopark için sözleşme imzaladı.
- Adli Kopya Alma Cihazı projemiz KOSGEB tarafından AR&GE desteği aldı.
- DIFOSE uWiPeR Güvenilir Veri Silme Cihazı yurt dışına ihraç edildi.
- DIFOSE Mobil Cihaz Adli İnceleme Sistemi Hancom WITH firmasının Türkiye temsilcisi oldu.

2020

- Yerli tasarım, yerli üretim PWS (Portable WorkStation) üretildi ve ilk ihracaat Almanya'ya yapıldı.
- Yerli tasarım, yerli üretim uWiPeR güvenilir veri silme cihazı üretildi,
- Kurumsal Adli Bilişim ve Veri Kurtarma Eğitimleri icra edildi.
- Özel panel bilgisayar DIFOSE FPC v2 geliştirildi,
- Adaptör ve kablo setleri ailemize DIFOSE AKAS ve DIFOSE ChS (Şarj Seti) eklendi.

2019

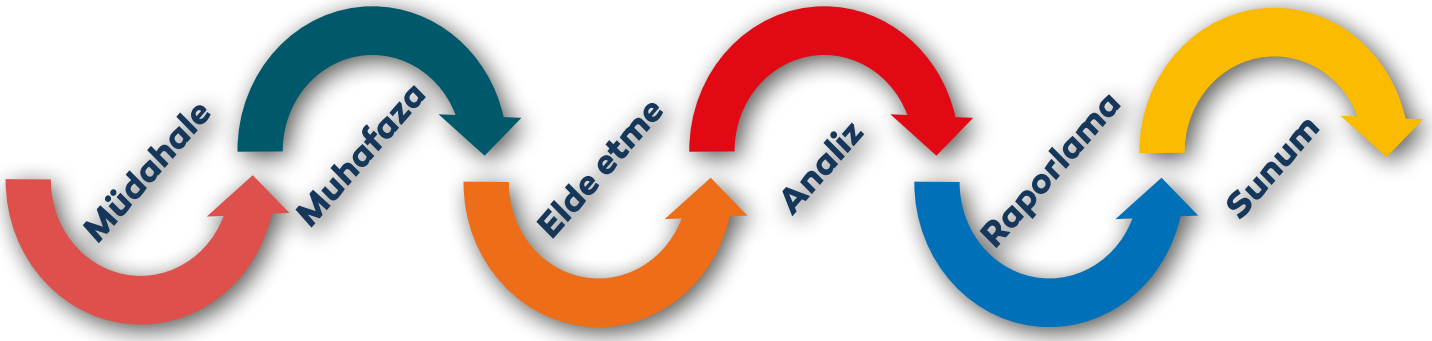
- Adli Tıp Kurumu, Jandarma Genel Komutanlığı ve Emniyet Genel Müdürlüğü'ne adli bilişim eğitimleri verdi.
- ICWC 4. Siber Savaş ve Güvenlik Konferansı'nda DIFOSE standı büyük ilgi gördü.
- Yerli şifre kırma sistemi DIFOSE PCU, özel panel bilgisayar DIFOSE FPC ve veri kurtarma adaptörü DIFOSE SPIDER'ın üretimi yapıldı.
- Adaptör ve kablo setleri DIFOSE AFAS, DIFOSE CFAS ve DIFOSE MFAS'ın üretimi yapıldı.

2018

- Makedonya'da Siber Suçlarla Mücadele Daire Başkanlığı'na eğitim verdi.
- Özbekistan Emniyet Genel Müdürlüğü'ne Adli Bilişim eğitimi verildi.
- İlk yerli yazma engelleme (write blocker) cihazı DIFOSE WB1'in prototipi yapıldı.
- İlk yerli veri kurtarma temiz tamir kabini DIFOSE CRB'nin üretimi yapıldı.

ADLİ BİLİŞİM

* Karşılaşılan bir siber olayda, bu olayın **hedefi**, **mağduru** veya farkında olmadan **faili** konumunda olabilirsiniz!
* Kişisel ya da kurumsal verileriniz yetkisiz kişiler tarafından ele **geçirilebilir**, **değiştirilebilir**, **yok edilebilir** ve hatta **çıkar amaçlı kullanılabilir!**
* İnternet ortamında şahsınız ya da kurumunuzu hedef alan **karalama amaçlı yayınlara** maruz kalabilirsiniz!
* Kişisel ya da kurumsal bilgisayar ve cep telefonlarınıza **zararlı yazılım bulaşmış ya da yüklenmiş** olabilir!
* Nedenini bilmediğiniz ya da tespit edemediğiniz bir **siber saldırı** yüzünden işiniz aksamış ve hatta tamamen durmuş olabilir!
* Şirketinize ya da kurumunuza ait **ticari gizli bilgi ve veriler** çalınmış ya da sızdırılmış olabilir!
* Şahsınız ya da kurumunuzla ilgili bir **soruşturma** ya da **dava dosyası** içeriğindeki teknik hususların incelenerek **raporlanmasına** ihtiyacınız olabilir!



Adli Bilişim, karşılaşılan bir bilişim olayında her türlü kayıt, iz, bulgu ve delillerin şüpheye meydan verilmeden, muhafazası, elde edilmesi, incelenmesi, analizi, raporlanması ve ilgili makamlara sunulması aşamalarından oluşan bir bilim dalıdır.

Bir bilişim olayında, olaya ilk müdahale ve kayıt, bulgu ve delillerin sağlıklı bir şekilde toplanması adli bilişimin en önemli safhasını oluşturur. Zira usulüne uygun, sağlıklı bir şekilde toplanmamış ve kayıt altına alınmamış bir delilin hukuken bir geçerliliği yoktur. Bu nedenle karşılaşılan bir bilişim olayının türü ve şekli ne olursa olsun adli bilişim uzmanları tarafından profesyonel cihaz, sistem ve yazılımlarla müdahale edilerek bulguların toplanması çok önemlidir.

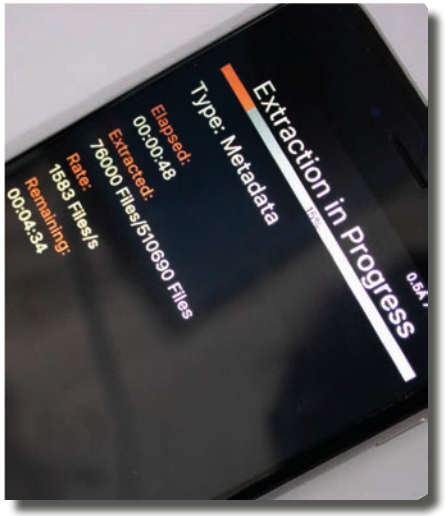
Karşılaşılan bir bilişim olayı, kasten ya da sehven oluşabilecek herhangi bir ihmal, suistimal ya da suça konu olabilir. Bu nedenle karşılaşılan olayın türü, oluş şekli, büyüklüğü ve etkilediği çevreye göre **idari soruşturma, tahkikat, inceleme** ya da **adli işlem** yapılabilir. Bu nedenle adli bilişim; sadece emniyet güçleri (kolluk), mahkeme ve savcılıklara iletilen bilişim suçlarını soruşturmak ya da kovuşturmak amacıyla müracaat ettikleri bir bilim dalından öte, bir bilişim olayına karışan kişi, kurum ve kuruluşların da olayın ortaya çıkartılması ve çözümü için müracaat ettikleri bir bilim dalıdır.

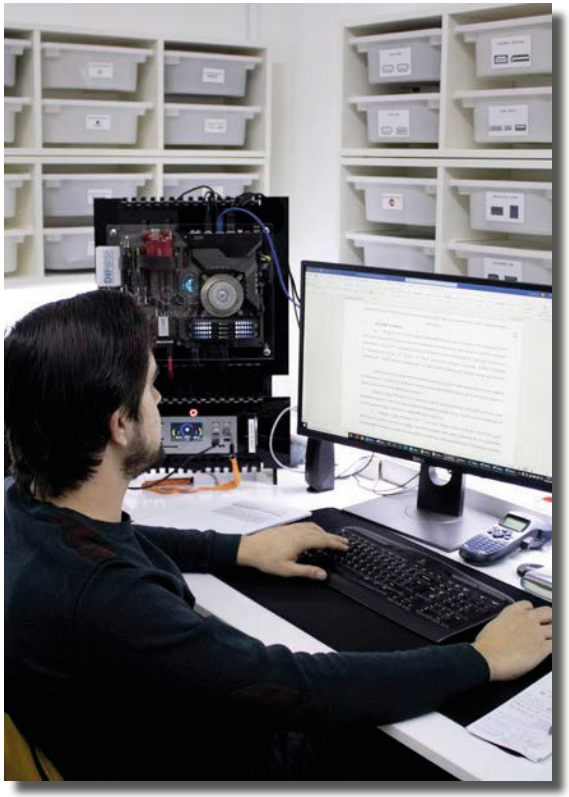
ADLİ BİLİŞİM

5N1K

Gerek adli bilişim ve gerekse bilişim güvenliği sektörlerinin en büyük ihtiyacı, karşılaşılan bir bilişim olayı, suiistimal ya da suç incelmesinde **“Kim, ne zaman, nerede, neyi, nasıl, ne şekilde ve niçin yapmış?”** sorularına cevap verebilecek imkân ve kabiliyete sahip olmaktır. Ancak, bu soruların cevaplarını bulmak için sistemlerin altyapısının müsait, gerekli inceleme ve analizi yapabilmek için ise bazı özel yazılım ve donanımların kullanılması gerekmektedir.

Bu alanda ihtiyacı karşılayacak her türlü dijital verilerin bulunduğu **sabit** ve **taşınabilir diskler, RAID sistemler, cep telefonu, SIM kart, tablet bilgisayar, USB bellek, hafıza kartları, çipler, CD/DVD/BlueRAY gibi optik medyalar, floppy disket, ZIP kartuş** ve **kasetler** üzerinde detaylı inceleme yapabilecek bir laboratuvarın kurulup hizmete alınmasına ihtiyaç vardır.





DIFOSE kendisine iletilen bir bilişim olayına ait bulguları adli bilişim laboratuvarında bulunan modern cihaz, sistem ve yazılımlar ile müdahale ederek hiçbir şüpheye meydan vermeden elde etmektedir. Elde edilen bulguların **incelenmesi**, **analizi** ve **raporlanması** özel durumlar hariç müşterinin bilgi güvenliği ve olayın gizliliği düşünülerek olay yerinde yapılmaktadır.

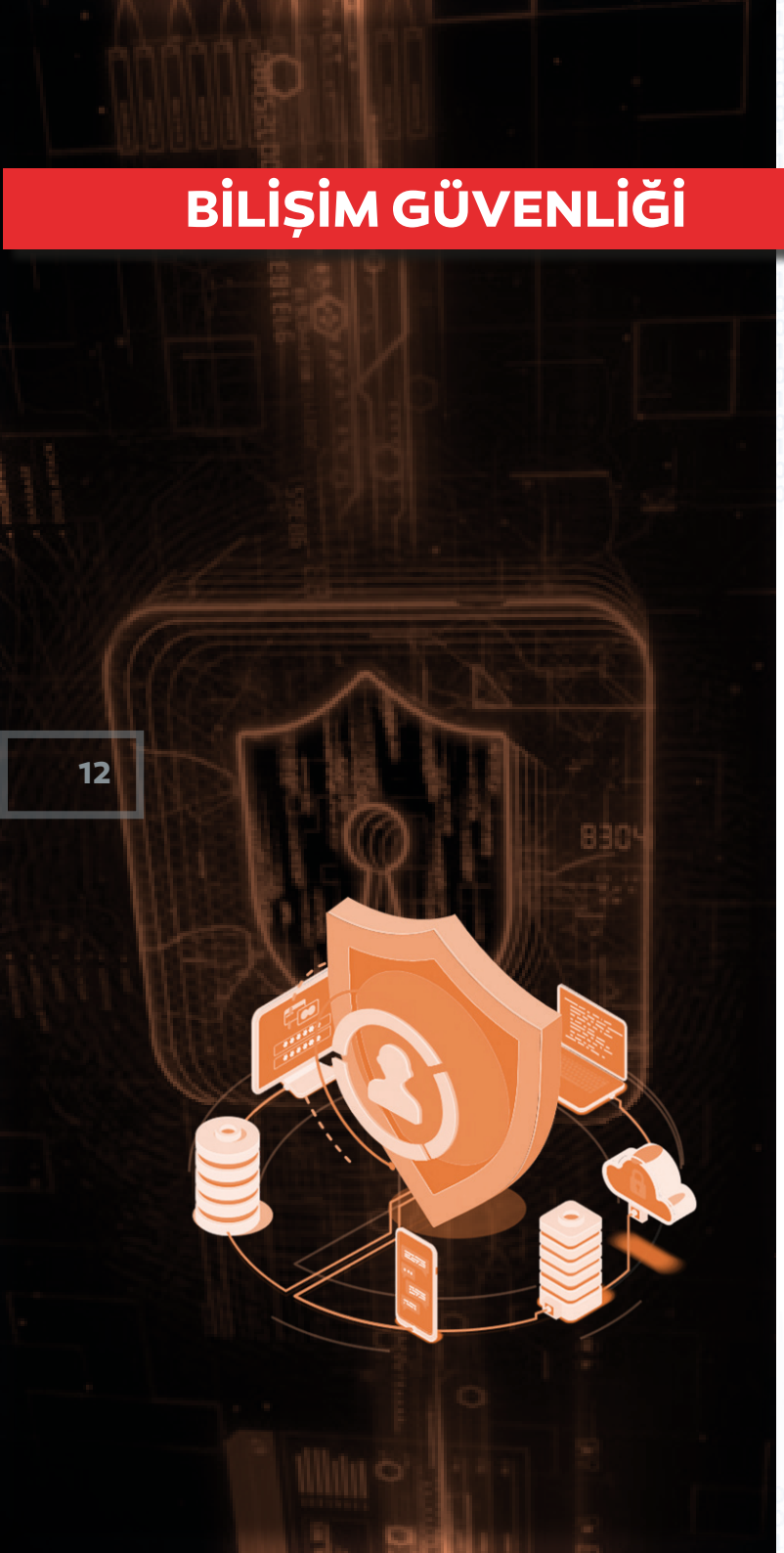
DIFOSE, hizmet prensipleri ve kalitesi gereği; vermiş olduğu tüm hizmetler için gizlilik anlaşması yaparak müşterisinin bilgi güvenliğini %100 oranında garanti altına almaktadır.

Meydana gelen olayın büyüklüğü ya da içeriği ne olursa olsun profesyonel bir adli bilişim danışmanlığı almak olayın çözümü açısından son derece önemlidir. Zira, ehliyetsiz kişiler tarafından yapılacak müdahaleler bulgu ve delillere zarar verdiği gibi olayın çözümünü de imkansız hale getirmektedir.

DIFOSE, yıllarını adli bilişim ve siber güvenlik alanına adamış uzmanları ve bu alanındaki yüksek standartları ile aşağıdaki hususlarda profesyonel danışmanlık hizmetleri sunmaktadır:

- **Bilişim olayına müdahale danışmanlığı (Hukuki, idari ve teknik destek sağlama),**
- **Bilişim olayı soruşturma ve inceleme,**
- **Dijital bulgu ve delillerin toplanması (Adli kopya-imaj alma),**
- **Bilişim olayı simülasyonu (Bilimsel test, gözlem ve deney yapma),**
- **Adli kopya inceleme ve analiz,**
- **Veri inceleme, karşılaştırma, analiz ve değerlendirme,**
- **Bilirkişi raporu hazırlama,**
- **Uzman mütalaası hazırlama,**
- **Soruşturma ya da dava dosyası içeriğindeki teknik hususların açıklığa kavuşturulması.**

BİLİŞİM GÜVENLİĞİ



Günlük hayatın hemen her alanında yaygın bir şekilde kullanılan ve pek çok alanda vazgeçilmez olan bilişim sistemleri üzerinde (siber uzayda) pek çok vaka yaşanmaktadır. Yaşanan bu vakalarda bilişim sistemleri hedef olduğu gibi, suç ya da suistimal aracı da olabilmektedir.

Bilgi hırsızlığı, endüstri casusluğu, zararlı yazılım bulaştırma, dijital veri manipülasyonu, sistemlere yetkisiz erişim, sistem içerisinde kalma, verileri değiştirme, silme gibi sonuçları çok ağır olan bu siber olaylara hayatın doğal akışı içerisinde her an rastlanılabilmektedir. İş hayatındaki kıyasıya rekabet, para kazanma ve başarma hırsı, çalışanların ekonomik tatminsizliği, işini kaybetme korkusu, husumet, kin, nefret gibi kişisel faktörler de siber uzaydaki bu vakaların oluşmasını tetiklemektedir.

Ancak, siber uzayda yaşanan bir suistimalde, olay devam ederken ya da olay bittikten sonra, adli bilişim metot ve teknikleri doğru, tam zamanında ve hukuka uygun bir şekilde uygulanırsa; olayın kaynağı, oluş şekli ve failleri ortamda bırakılan izlerin sağlıklı bir şekilde toplanması ve incelenmesi sonucunda ortaya çıkartılabilmektedir. Hiç şüphesiz ki, bu alandaki başarıyı artıran en önemli faktörler, siber olaylara müdahale etme tekniklerini uygulayarak dijital delillerin bozulmadan toplanmasını ve muhafaza altına alınmasını sağlamaktır.

Son derece hassas ve önemli bir konu olan siber olaylara müdahale edilmesi, muhtemel saldırı ve olayların etkilerinin azaltması ve ortadan kaldırmasına yönelik önlemlerin geliştirilmesi ve belirlenen aktörlerle paylaşılması için ulusal ve uluslararası düzeyde çalışmak üzere Telekomünikasyon İletişim Başkanlığı bünyesinde Ulusal Siber Olaylara Müdahale Merkezi (USOM, TR-CERT) oluşturulmuştur.

"Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ"i 11.11.2013 tarihli Resmi Gazete'de yayınlanarak duyurulmuştur. Bu tebliğe göre, herhangi bir kamu kurum ve kuruluşu ile diğer sektördeki kurum ve kuruluşlar kendi bünyelerinde **Siber Olaylara Müdahale Ekibi (SOME)** kurabilmekte ve bu alanda personel istihdam edebilmektedir. Bünyesinde SOME kuracak kurum ve kuruluşların kendi bilişim ve endüstriyel kontrol sistemlerinin büyüklük ve kritikliğini dikkate alarak meydana gelebilecek siber olaya müdahale edebilecek yeterlilikte personel ve teçhizatı hazırda bulundurması gerekmektedir.

Yapılması gereken ilk işlemin meydana gelen vakayı en kısa sürede tespit edip karşılık vermek olduğunu belirtmek gerekir. Herhangi bir zararlı yazılımın sistemlere bulaştığının tespit süresi ve doğru karşılık verme eyleminin gerçekleştirilmesi, bahse konu zararlı yazılımın neden olabileceği zararları minimize etmek açısından büyük önem taşır. Bu gerçekten hareketle, güvenlik yöneticilerinin tehditlere karşı yaklaşımlarını koruma ve önlemeden ziyade sürekli takip, tespit ve karşılık verme bağlamında yoğunlaştırmaları önem arz etmektedir.

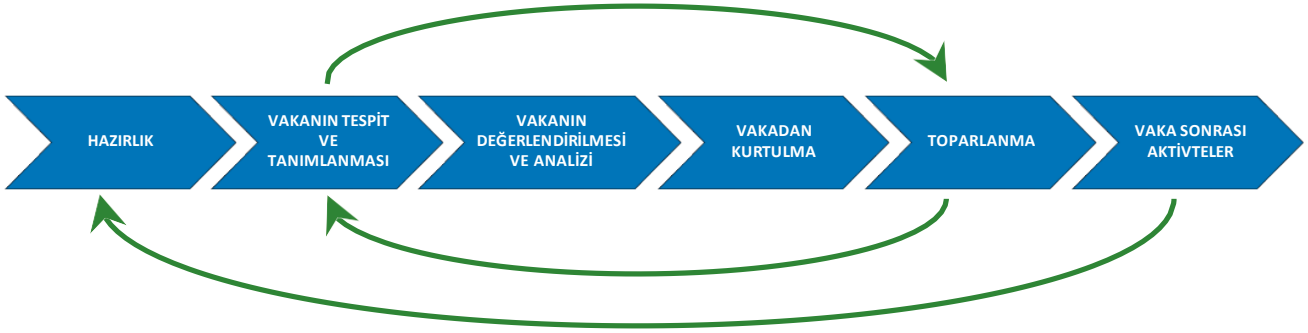
Meydana gelen bir vakaya müdahale edilmesi gerektiğinde, doğru süreçler, doğru personel ve doğru cihazlara sahipseniz, daha etkin bir şekilde olaya müdahale edebilirsiniz. Güvenlik vakaları meydana gelmeden önce kurumunuz olay yönetimini planlayıp uygulayacak imkân ve kabiliyete sahip olmalıdır. Bu planlama ve kabiliyet içerisinde güvenlik vakalarına müdahale için gerekli beceriler, roller, prosedürler ve cihazlar yer alır.

Bilgi sistemleriyle ilgili bazı açıklar güvenlik konularında kurumunuz için risk oluşturur. Risk yönetimi süreciniz kapsamında bazı güvenlik ve uyumluluk risklerini kabul edebilir, transfer edebilir, diğerlerini azaltabilir veya onlardan kaçınabilirsiniz. Açık taraması ve/veya sızma testi ile kurumunuzun bilgi sistemlerini ayrıntılı bir şekilde incelemek suretiyle, azaltmanız veya kaçınmanız gereken risklerin açık kaynaklarını çalışmalar, sorunları çözmek için sistemlerinizdeki açıklar hakkında bir yapılacaklar listesi üretir. Her bir açık için gerekli düzeltmeleri düzenli olarak belirleyip uygulayarak, kurumunuzun risklerini azaltmak veya bu risklerden kaçınmak suretiyle sistemlerinizi güçlendirebilirsiniz. Savunma ağırlıklı bir sistem yapılandırması oluşturduktan sonra, yapılandırmanın bekleneni vermesini temin etmek için sistemlerinizi sürekli olarak izlemeniz, test etmeniz ve gerekli düzenlemeleri yapmanız gerekir.

Kurumlar meydana gelen bir siber güvenlik olayına/vakasına karşı sıralanan amaçlara yönelik imkân ve kabiliyetlere sahip olmalıdır:

- Tehlikeyi veya saldırıyı mümkün olan en kısa sürede ve en etkin şekilde tespit etmek.
- Vakaya en kısa sürede müdahale etmek.
- Vakanın nedenini en kısa sürede tespit etmek.
- Vakadan en kısa sürede kurtulup normal çalışma moduna geçmek.

Meydana gelebilecek siber güvenlik vakalarına müdahale süreci birçok adımdan meydana gelir. Bu adımlar kurumdan kuruma değişebilir, ancak genel süreç aşağıda sıralandığı biçimdedir.



Güvenlik Operasyon Merkezi (SOC)

Güvenlik Operasyon Merkezi (Security Operation Center-SOC) işletme veya kurum güvenlik durumunun sürekli olarak takip ve analizinden sorumlu güvenlik uzmanlarının bulunduğu yerdir. SOC ekibinin görevi, teknolojik çözümler ve süreçlerle siber güvenlik vakalarını tespit ve analiz ederek karşılık vermektir.

Siber Olaylara Müdahale Ekibi (SOME-CISRT)

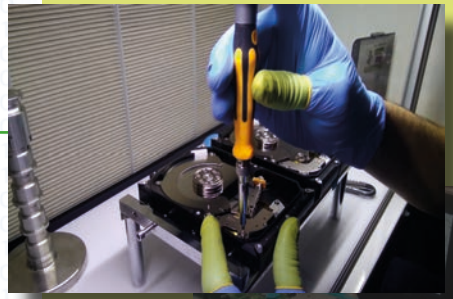
Kurumlar bilgi güvenliği vakalarını tespit ederek vakaları yönetmek için **Siber Olaylara Müdahale Ekipleri-SOME (Cybersecurity Incident Response Team-CISRT)** oluştururlar. SOME modeli belirlenirken kurum ihtiyaçları, yasal gereklilikler, maliyet ve personel uzmanlığı gibi hususlar dikkate alınmalıdır.

VERİ KURTARMA

Bilginin çeşitli amaçlarla üretildiği, işlendiği, aktarıldığı, paylaşıldığı ve depolandığı bir bilgi ve bilişim çağında yaşıyoruz. Bu nedenle bilişim sistemleri üzerinde saklanan bilgi ve verilerimiz en önemli varlıklarımızın arasında yer almaktadır.

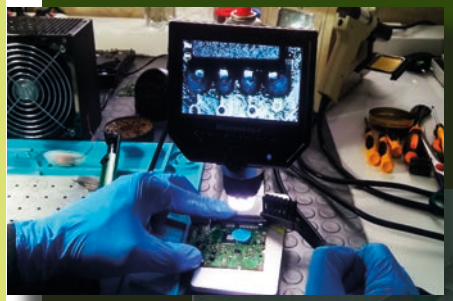
Bilişim sistemlerine virüs bulaşması, işletim sisteminin çökmesi, sistemlerin işlev görmemesi, sabit ve taşınabilir diskler, USB bellek ve hafıza kartları içerisindeki verilerin sehven ya da kasten silinmesi gibi olaylara hayatın doğal akışı içerisinde zaman zaman rastlanılmaktadır.

Bilgisayar, cep telefonu, USB bellek, hafıza kartı, taşınabilir disk ve diğer veri depolama aygıtları içerisinde yer alan verilerin silinmesi ya da bozulması veri depolama aygıtlarının fiziksel zarar görmesinden oluşabileceği gibi, sisteme bulaşan bir zararlı yazılımla da oluşabilmektedir.



Unutulmamalıdır ki, başarılı bir veri kurtarma hizmeti ileri seviye uzmanlık, tecrübe ve profesyonel donanım ve yazılımlarla yapılmaktadır. Başarılı bir veri kurtarma için, yaşanan ya da karşılaşılan sorun ne ise detaylı bir şekilde gözlemlenmeli ve zaman geçirmeden uzmanından teknik destek alınmalıdır.

DIFOSE uzmanları, karşılaşılan olayın türü ne olursa olsun, veri kaybının oluşmasını önlemek için sizleri doğru bir şekilde yönlendirerek gerekli olan bilgi ve teknik desteği sunmaktadır. Daha sonra, veri kurtarma için teslim alınan malzemeler detaylı incelenerek laboratuvar ortamında müdahale edilmek suretiyle verilerin kurtarılması sağlanmaktadır.



Dikkat etmelisiniz

Verileri silinen ya da zarar gören bilişim sistemi kesinlikle çalıştırılmamalı, sistem içerisine kesinlikle veri kopyalanmamalı, sisteme herhangi bir yazılım kurulmamalıdır. Ayrıca, fiziksel arızası bulunan başta sabit diskler olmak üzere diğer veri depolama aygıtları da her ne sebeple olursa olsun vidaları sökülerek ya da dış muhafazası çıkartılarak açılmamalıdır.

VERİ KURTARMA

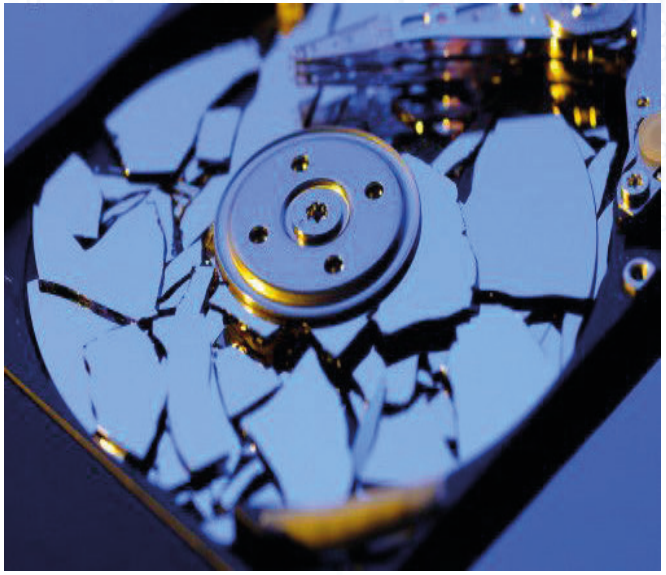
bir nedenden dolayı bilgisayar, cep telefonu, usb bellek, hafıza kartı, taşınabilir disk ve diğer veri depolama aygıtlarınızda bulunan verilerinize erişemeyecek olursanız bilgi ve tecrübenizi aşan yol ve yöntemleri sakın denemeyiniz!..

Arızalanmış bir hard diskteki sektörler nasıl okunursa okunsun önemli olan anlamlı bir yapı oluşturulacak ve dosyalar elde edilecek şekilde bu sektörlerin birleştirilmesidir. Bunun için özel yazılımlara ihtiyaç vardır. Daha sonra elde edilen dosyalar farklı bir ortama yazılarak kullanıcıya teslim edilir.

Fiziksel arızalı disklerden veri kurtarmak için uygulanan en gelişmiş yöntem arızalı parçaların çok dikkatli bir şekilde değiştirilmesi yöntemidir. Değiştirilecek parça gövdenin (HDA) içerisinde ise bu değişim işleminin belirli koşulları sağlayan temiz oda ortamında gerçekleştirilmesi gerekir. Kafanın yüzeye yaklaşık 1 mikro inç mesafede uçması gerektiği dikkate alındığında bir parmak izi veya ufacık bir partikülün tamir edilmiş olan hard diskin çökmesine ve veri kurtarma işleminin başarısız olmasına neden olacağı aşikardır. Bu durum disk üzerindeki verilerin daha fazla hasar görmesine neden olur. Parça değişiminin başarılı olabilmesi için arızalı parça yerine kullanılan yedek parçanın diskin modeline uygun olması gereklidir. Disk üretici firmalar ve bu firmalar için parça üreten tedarikçi firmalar dışarıya yedek parça vermemektedirler. Bu parçalar aynı özellikteki sağlam bir diskten elde edilmek durumundadır. Ancak kafa yapısının disk modeliyle olan sıkı ilişkisi ve sistem parametreleriyle ilgili hassas ayarlar yakın özelliklerdeki diskler arasındaki parça değişiminin dahi başarısız olmasına neden olur. Bu nedenle yedek parçalar özellikleri tamamen aynı olan diskten temin edilmelidir.

Veri ne zaman yok olur:

Mağara duvarlarındaki boyamalar, taşlara oyulmuş resimler ve deriler üzerindeki boyamalar yüzyıllarca bozulmadan kalır. Manyetik olarak kaydedilmiş veriler böyle değildir. Veriler dijital olarak doğmakta ve manyetik plaka ve teyplerde yaşamlarını devam ettirmektedir. Geçmişte, manyetik olarak kaydedilen verilerin 50 ila 100 yıl varlıklarını devam ettirebilecekleri tahmin ediliyordu. Ancak dijital veri ile ilgili iki temel problem vardır. Birincisi, kurtarma açısından bakıldığında dijital (sayısal) veri tamamen vardır veya hiç yoktur. Örnek olarak; yazılmış, boyanmış yada oyulmuş çalışmalar üzerinden zaman geçtikçe yavaş yavaş bozulur, oysa sayısal veri bir kere ECC'nin düzeltemeyeceği noktaya kadar bozuldu mu tamamen yok olmuş demektir. İkincisi, manyetik veriler insanların doğrudan okuyabileceği yapıda değildir, yani manyetik verileri okumak için makineler gerekir. Ortamdaki bilgileri okumak için tasarlanmış makine bozulduğunda manyetik veriler yerli yerinde duruyor olsa dahi veriler yok olmuş demektir. Ayrıca, sürücünü verileri tam olarak sağladığı durumda bu veriyi kullanan programın ve bu programın çalıştığı makinenin de düzgün olarak çalışıyor olması gerekmektedir.



Manyetik bilginin zamanla özelliğini yitirmesi genellikle ısısal bozulmaya bağlıdır. Kısaca açıklarsak, bir bit içerisinde manyetik olarak bir tarafa yönlendirilmiş (belki de) milyonlarca atom bulunur. Yıllar geçtikçe ısısal enerjiye (örneğin sıcaklık) bağlı olarak bit içerisindeki bazı atomlar manyetik yönlerini unuturlar. Bu durumda daha az sayıda atom veriyi korumaktadır, bu a daha az ısısal enerjinin etkisiyle bile biraz daha fazla atomun yönünü unutabileceği anlamına gelir. Belirli bir süre sonra "çiğ noktasına" ulaşılır ki bu durumda bit içerisindeki atomlar rasgele yönlenirler, artık veri kaybolmuştur. Bu durum "superparamagnetic" etki olarak bilinir.

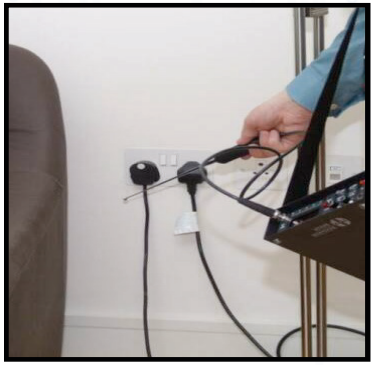
Yüzeysel veri yoğunluğu arttığı zaman her bir bit için manyetik olarak yönlendirilmiş atom sayısı azalacağından ısısal kararlılık hızlı bir şekilde düşer. Çalışma ortamındaki yüksek ısı da ısısal bozulmayı hızlandırabilir. Yazma işlemi esnasında bazen yazılan iz'e komşu iz'lerdeki bitlerde bozulmaya sebep olabileceği tespit edilmiştir. Genellikle bilinmez ancak birçok modern sürücü düzenli olarak bölgelerdeki bitlerde ısısal bozulma kontrolü yapar ve bozulma algıladığında o sektörü yeniden yazar.

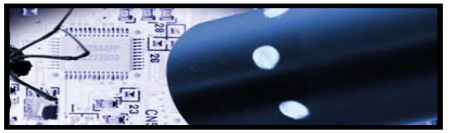
ELEKTRONİK ARAMA & TARAMA

Gelişen teknolojiye paralel olarak istihbarat elde etme şekli ve yöntemleri her geçen gün değişmektedir. Analog sistemlerin terkedilip yerine dijital sistemlerin gelmesi neticesinde istihbarat alanında kullanılan cihaz ve sistemler de aynı şekilde değişikliğe uğramıştır.

Özellikle iş hayatındaki **kıyasıya rekabet, kişiler arası çıkar, menfaat, anlaşmazlık, kin, husumet, baskı, tehdit, şantaj** gibi etkenler maalesef insanların yasal olmayan yol ve yöntemlere müracaat etmelerine neden olabilmektedir. Bunun sonucu olarak da; kimin kimi dinlediği ve izlediğinin tahmin bile edilemeyeceği bir çağda yaşadığımızı söyleyebiliriz. Bu durum ister istemez kişi ve kurumları **"Acaba biz de dinleniyor, takip ediliyor ve izleniyor muyuz?"** sorusunu sormaya, etrafındaki her türlü teknolojik cihaz ve sistemden şüphe duyarak bu sorunun cevabını aramaya yöneltmektedir.

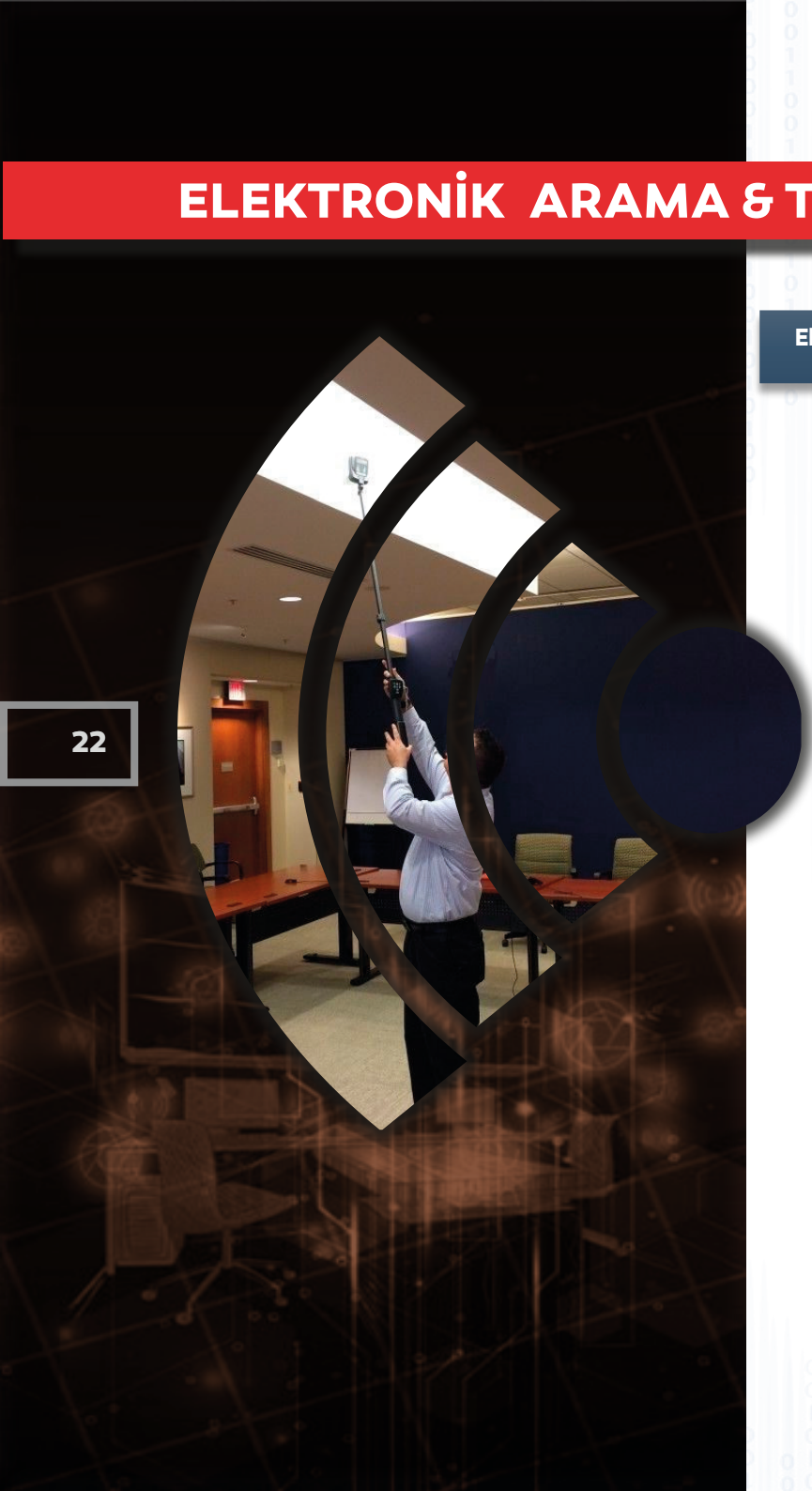
* Hayal edebileceğiniz her şey kayıt ortamı olabilir.
* Mikro ölçekli elektronik teknolojisi RF ve GSM vericileri her ortama yerleştirilebilecek hale getirmiştir.
* Yazılım tabanlı tehditler her geçen gün daha önemli hale gelmektedir.





Günümüzde gizli dinleme çok daha profesyonelce yapılmaktadır. Teknik personel bile olsanız, uzun süre gizli olarak izlenebilir ama fark edemeyebilirsiniz.

ELEKTRONİK ARAMA & TARAMA



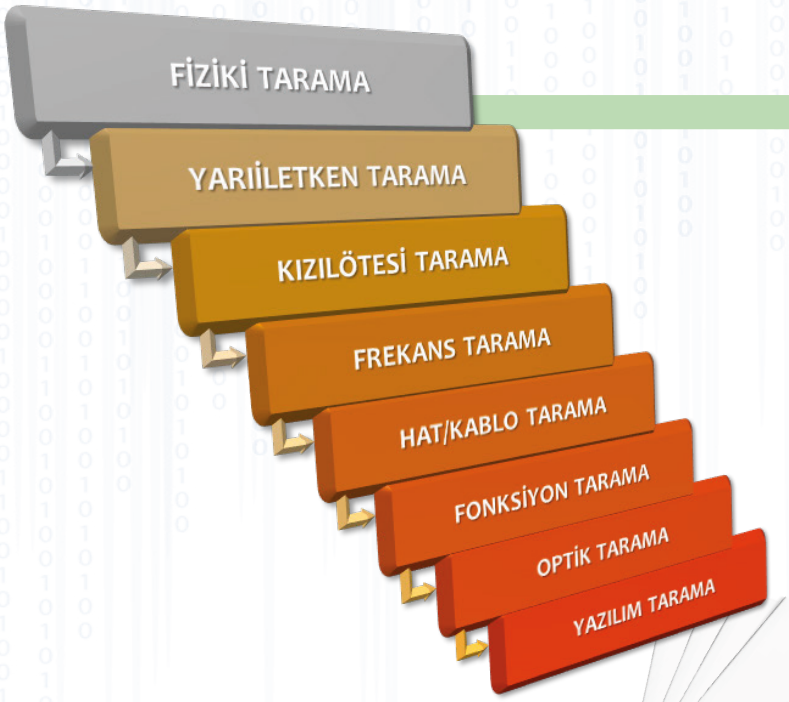
- Elektronik ve Fiziki Arama
- Raporlama
- Danışmanlık
- Eğitim
- Tedarik Uygulama

İstihbarata karşı koyma yöntemlerinin ön önemlisi olan fiziki ve elektronik arama yöntemlerinde başarı elde edebilmek için öncelikle güncel istihbarat imkan ve kabiliyetlerini tanımak ve bilmek gerekmektedir. Daha sonra ise istihbarat amaçlı kullanılan ileri teknoloji malzeme, cihaz ve sistemleri tespit edebilecek yol ve yöntemler hakkında önce bilgi ve daha sonra ise deneyim elde etmek gerekmektedir.

DIFOSE tarafından yıllarını bu işe adamış, güncel istihbarat imkan ve kabiliyetlerini sürekli inceleyen ve ekipmanlarını güncelleyen uzmanlar tarafından elektronik ve fiziki tarama ve kontrol faaliyeti bir sıra ve plan dahilinde yapılmaktadır.

Faaliyet esnasında, verilecek hizmetin sağlıklı bir şekilde yapılması için KURUM tarafından görevlendirilecek bir gözetmen refakatinde işlemlerin gerçekleştirilmesi ve ihtiyaç duyulan hususlarda yardımcı olunması talep edilmektedir.

Fiziki ve Elektronik Arama faaliyeti sonucunda yapılan işlemler ve elde edilen sonuçlar ile önerileri kapsayan detaylı bir Sonuç Raporu sunulur.



- **Aktif/Pasif Kayıt**
- **Aktif/Pasif Kablosuz Verici**
- **Kablolu Verici**
- **Saplama/Bölücü**
- **Uzaktan Algılama/ Dinleme/ Görüntüleme**
- **Ağa Sızma/Ağ Zafiyeti/Zararlı Yazılım**
- **GSM Aktif/Pasif İzleme**
- **Elektromanyetik Işınım ve Dalga Boyları**
- **Lazer Teknolojileri**

20 yıllık Teknik ve Elektronik Arama tecrübesi ile, bu konuda klasik hale gelmiş ekipmanlardan, günümüzün en son teknoloji ekipmanlarına kadar geniş bir laboratuvar ve saha ekipmanı envanteri mevcuttur.

Elektronik ve Fiziki Tarama Hizmeti bir süreç hizmeti olması nedeniyle, yapılacak protokol çerçevesinde periyodik dönemlerde (Aylık, 3 Aylık, 6 Aylık, Yıllık) yukarıda belirtilen akışa uygun olarak tarafımızdan denetim ve kontroller yapılmaktadır.

DIFOSE

AKADEMİ

DIFOSE Akademi olarak geleceğin adli bilişim uzmanlarını yetiştirmek amacıyla çalışıyoruz.

Kurumsal seviyede adli bilişim ve siber olaylara müdahale eğitimlerimizin yanında bireysel olarak katılım sağlanabilecek eğitimlerimiz kendi alanlarının uzmanları tarafından verilmektedir. Örnek ve yaşanmış olaylar ve çeşitli senaryolarla desteklenen eğitimlerimiz DIFOSE Akademi'nin erişiminde olan adli bilişim, veri kurtarma ve simülasyon laboratuvarlarımızda uygulamalı olarak verilmektedir. Ancak, talep edildiği takdirde eğitimler DIFOSE Akademi yerleşkesi haricinde başka bir merkezde ya da eğitimi talep eden kuruma ait uygun bir eğitim merkezinde de verilebilmektedir.

Eğitmenlerimiz


Yalkın DEMİRKAYA


Erdal ÖZKAYA

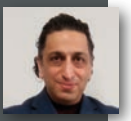

Ramon CRUZ


Richard BESHLIHAN


Şükrü DURMAZ


Raif SARICA


Timur ÖZCAN


Yılmaz DEĞİRMENCİ


Emre TINAZTEPE


Mehmet GÖKSU


Yiğit Emre ÇETİNKAYA


Onur SABAN


Samet YILMAZ


SAMİ KARACA

DIFOSE

AKADEMİ

ADLİ BİLİŞİM ATÖLYE EĞİTİMLERİ

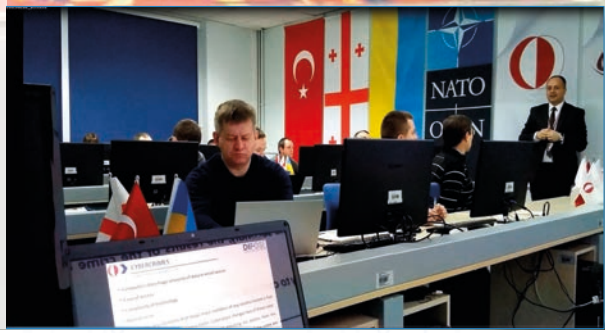
İyi bir adli bilişim uzmanı olabilmek için öncelikle bilişim suçu ve suistimlallerinin işleniş şekilleri ile bilişim güvenliği konusunda temel bilgiye sahip olmak gerekmektedir. Bu eğitimimizde, yıllarını adli bilişime adamış uzmanlarımız tarafından karşılaşılan bir bilişim olayına müdahale etme, bulgu ve delilleri usulüne uygun toplama, inceleme, analiz ve raporlama işlemleri için gerekli olan hukuki ve teknik bilgiler ile bu alanda kullanılan güncel yazılım ve donanımların temel ve ileri seviye eğitimleri verilmektedir.

VERİ KURTARMA ATÖLYE EĞİTİMLERİ

Sabit Disk, USB bellek ve mobil cihazlar üzerindeki veriler kasten ya da yanlışlıkla silinmiş olabilir. Bu durumda veri kurtarmak bir gereklilikse bir sıra ve plan dahilinde yapılması gerekenlerin bilinmesi de çok önemlidir. Özellikle silinmiş verilerin türü, niteliği, dosya imzası, dosya başlığı ve altlığı gibi bilgilerin bilinmesi gerekmektedir. Bu verilerin nereden ve nasıl elde edilebileceği, veri kurtarma ve veri kazıma arasındaki farklar ile veri kurtarma işlemindeki başarıyı etkileyen faktörler bu eğitimimizde detaylı olarak anlatılmaktadır.

DIFOSE UZMANLIK EĞİTİMLERİ

- Farkındalık Eğitimleri
- Yazılım Eğitimleri
- Uzmanlık Eğitimleri



Atölye Eğitimleri

- Temel Adli Bilişim
- İleri Adli Bilişim
- Dijital Delile İlk Müdahale ve Adli Kopya Alma
- Dosya Sistemleri Adli Analizi
  - MS Windows Adli Analizi
  - Linux Adli Analizi
  - MacOSx Adli Analizi
- Bilgisayar Ağlarında Trafik Kopyalama ve Paket Analizi
- Mobil Cihaz Adli Analizi
- Geçici Bellek İncelemeleri
- Zararlı Yazılım Adli Analizi
- DVR ve CCTV Sistemleri İncelemeleri
- Veri Kurtarma

Yazılım Eğitimleri

- Forensic Explorer
- X-Ways Forensics
- Oxygen Forensic
- Paraben Forensics
- CounterTack ResponderPro
- Savvius OmniPeek
- Maltego XL
- X1 Social Discovery
- Dolphin Data Recovery
- Passware
- Recover My Files
- Hex-Rays
- Detego
- HX Recovery For DVR

Farkındalık Eğitimleri

- Siber Olaylara Müdahale Ekipleri (SOME) Kurulumu ve Eğitimi
- Elektronik Arama Eğitimi
- Herkes İçin Kişisel Bilgisayar ve İnternet Güvenliği
- Avukatlar ve Hukukçular İçin Adli Bilişim
- İç Denetçiler İçin Adli Bilişim
- Uygulamalı Beden Dili, Mülakat ve Soruşturma Teknikleri
- Uygulamalı Kişisel ve Kurumsal Alanlarda Durumsal Farkındalık

* Eğitim öncesi tüm eğitim materyalleri kursiyerlerimize ücretsiz verilmektedir.

** Eğitim sonunda yapılacak değerlendirme sınavından %70 ve üzeri başarı sağlayanlara başarı sertifikası, diğerlerine ise katılım sertifikası verilmektedir.

DIFOSE

AKADEMİ

EĞİTİM REFERANSLARIMIZ (YURT İÇİ)

AR & GE ve ÜR & GE

Türkiye'de adli bilişim sektörünün en önemli sorunlarından birisi Türkçe ara yüze sahip yazılım ve donanımların yok denecek kadar az olmasıdır. Maalesef, bu alanda kullanılan yazılım ve donanımların tamamının ara yüzü İngilizcedir. Bu durum, kullanılan yazılım ve donanımların kullanımını yaygınlaştırma, geliştirme, teknik destek ve eğitim alanlarında bir takım sorun ve problemlere neden olmaktadır. Bir diğer husus ise, bu alanda kullanılan yazılımların eğitimini almak amacıyla yurtdışına personel gönderilmesi de ilave masraflara neden olmaktadır.

DIFOSE, Türkiye'deki adli bilişim sektörüne hem bir yenilik hem de %100 Türkçe adli bilişim yazılımı kazandırmak amacıyla 2013 Haziran'ında çalışmalara başlamıştır. Yapılan teşebbüsler sonucunda veri kurtarma alanında tüm dünyaca tanınmış olan Avustralya'nın GetData firması ile işbirliğine giderek tüm ara yüzü ve menüleri Türkçe olan ve Türkçe derlenen ilk adli bilişim yazılımı Forensic Explorer'ın çözüm ortağı olmuş ve sıra ile Forensic Imager, Mount Image Pro yazılımlarının Türkçe sürümlerini tamamlamıştır.

Adli İnceleme Panel PC
Forensic PC

DIFOSE FPC Kullanıcılara kullanım kolaylığı ve esneklik sağlar. Kullanıcının verilere daha hızlı erişmesini sağlamak için bir bilgisayarın tüm portları ve bağlantı arayüzlerine anında erişilebilir özellikte tasarlanmıştır. Adli çalışmalar için USB ve SATA donanımsal "Yazma Koruma" adaptörleri bulunmaktadır.

Özel ve sessiz parçaların bir araya getirilmesiyle oluşturulmuştur. Açık kasa mimarisi sayesinde ısınmaz ve çok sessizdir.

Adli Bilişim ve Veri Kurtarma Laboratuvarları için özel bir bilgisayar ihtiyacını karşılamak için tasarlanmıştır.

İhtiyaca özel farklı tasarımlarda üretilebilmektedir.

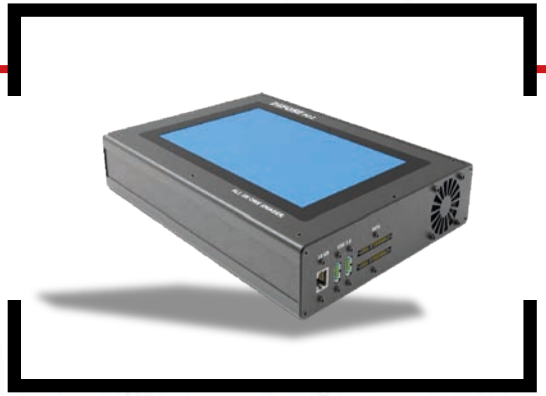
Parola Kırma Ünitesi
Password Cracking Unit

DIFOSE PCU, parola korumalı dosyalar ve şifreli alanları kırmak için kullanılan yazılımlarla bir bilgisayar ağı üzerinden kolayca entegre edilebilen ve kırma süresini azaltmaya yarayan ideal bir çözümdür.

Modüler tasarımı sayesinde ihtiyaca göre ölçeklendirilebilen bir çözüm sunar. Standart bir ünitede her biri 1 bilgisayar ve 8 GPU kartından oluşan toplam 8 modül bulunmaktadır.

Bilgisayar ağı üzerinden parola ve şifre kırmak amacıyla kullanılan ve GPU desteği bulunan Passware, Elcomsoft ve HashCat gibi yazılımlarla beraber kullanılabilmektedir.

200'den fazla dosya ve çeşitli alanların kırılması işleminde kullanılabilmektedir.



Adli Kopya Alma Cihazı
Forensic Duplicator

DIFOSE FD2, HDD, USB ve ağ depolama alanından alınan şüpheli sürücülerinin adli kopyasını oluşturan, amaca yönelik ve tam özellikli bir adli kopyalayıcıdır. Bir olay müdahalesi sırasında gereken işlevler için özellikle tasarlanmış ve üretilmiştir. Tüm veri yolları sistem açıldığında salt okunur olduğundan, veri depolama cihazında herhangi bir değişiklik yapmak mümkün değildir.

DIFOSE FD2, olay müdahale ve kanıt toplama uzmanlarının deneyim ve fikirleri ile tasarlanmış ve üretilmiştir ve tasarımı kullanıcılara kolaylık ve esneklik sağlar. Veri yolları kullanıcıların ihtiyaçlarına göre yerleştirilmiştir ve kullanıcılar 10,1 inç dokunmatik ekrandan gerekli fonksiyonları kolayca ve güvenli bir şekilde gerçekleştirebilir.

www.difose.com.tr

AR & GE ve ÜR & GE

DIFOSE, sadece ürün tedarik eden bir firma değil, müşterilerinin adli bilişim ve bilişim güvenliği alanlarında ihtiyaç duyduğu çözümleri en ekonomik ve en kısa sürede tamamlayan, gerçekleştirdiği ARGE ve ÜRGE çalışmaları ile Adli Bilişim alanında ihtiyaç duyulan yerli ürünler geliştiren bir çözüm ortağıdır.

Adaptör ve Kablo Setleri
Forensic Adapter and Cable Sets

DIFOSE CFAS:

Bilgisayar olaylarına müdahale ederken karşılaşılan çeşitli marka ve model disklerin uygun adaptör kullanılarak kopyalanması amacıyla tasarlanmış adaptör ve kablo setinden oluşan bir çözümdür. Karşılaşılan bir siber olayda en çok rastlanan sabit disklerin kopyalanmasını sağlayan adaptörlerinden oluşmaktadır.

DIFOSE AFAS:

Apple marka cihazlarda kullanılan veri depolama aygıtlarının bire bir kopyasını almak için gerekli olan adaptör ve kablo setinden oluşmaktadır. Adli bilişim uzmanlarının olay yerinde müdahale esnasında en çok ihtiyaç duyacakları adaptör, kablo ve araçların bir araya getirilmesi sonucu oluşmuştur.

DIFOSE MFAS:

Bir siber olaya müdahale esnasında karşılaşılan bir cep telefonunun kopya alma sistemine ya da bilgisayara bağlantısının sağlanması amacıyla kullanılmaktadır. Bu bağlantı esnasında gerekli olan çeşitli kablo ve adaptörlerden oluşmaktadır.

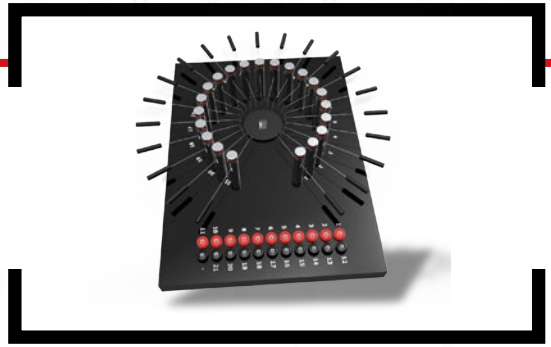
Yazma Koruyucu
Write Blocker

DIFOSE WB1, bir PC ile şüpheli sürücülerin adli kopyalarını HDD, USB ve bellek kartlarından alan, adli kopyalar yapan bütün olarak bir yazma engelleyicidir. Aynı zamanda canlı araştırmalar için tasarlanmış ve üretilmiştir. Sistem açıldığında tüm veri yollarının salt okunur olması nedeniyle, veri depolama cihazında yanlışlıkla değişiklik yapılması bile mümkün değildir.

Dünyada bugüne kadar üretilmiş taşınabilir ilk hepsi bir arada yazma engelleme cihazıdır.

Bir bilgisayara USB 3.0 (5 Gbps) bağlantı hızında bağlanır ve üzerinde bulunan veri yollarını sadece okuma özelliği ile bilgisayara bağlar ve yazma özelliğini bloke eder.

Monolit Okuyucu
Spider



Veri Kurtarma uzmanları her zaman NAND bellek yongalarla okuma sorunu yaşarlar. Bellek yongası boyutu çok küçükse, uygun alana lehimleme yapmak mümkün değildir.

Uzmanlarımızın deneyim ve bilgisinin ışığında üretilen DIFOSE SPIDER, NAND bellek yongalarına odaklanan veri kurtarma uzmanları için esnek bir çözüm sunmaktadır.

DIFOSE SPIDER ile, üzerinde bulunan 21 port sayesinde veri alanında kolayca okumak için uygun yer bulmak mümkündür.

Temiz Çalışma Kabinleri
Clean Repair Boxes

Sabit disklerin kafa, plaka ya da motor gibi parçalarının değiştirilmesi işlemi tozsuz bir ortamda fiziki müdahale gerektirmektedir. Veri kurtarma alanında çalışan uzmanların Laboratuvar ortamlarında temiz oda gerektirmeksizin stabil olarak yapacakları çalışmalar için DIFOSE CRB-L, laboratuvar dışında, olay yerinde ya da müşterinin tesislerinde yapacağı çalışmalar için ise taşınabilir nitelikte olan DIFOSE CRB-P Özel temiz kabinleri geliştirilmiştir.

AR & GE ve ÜR & GE

- Kullanıcı dostu
- Modüler yapı
- Dayanıklı & sessiz
- Güvenilir çözüm
- Esnek üretim
- Özel tasarım
- Güçlü destek
- Güçlü özellikler

Adaptör ve Kablo Setleri
Forensic Adapter and Cable Sets

DIFOSE AKAS:

DIFOSE AKAS olay müdahalelerinde karşılaşılan çeşitli veri ve güç bağlantı yoluna sahip cihazların *(sabit diskler, mobil cihazlar, hafıza kartları, bilgisayar çevre birimleri gibi)* bağlantısının yapılması güç ihtiyacının giderilmesi ve gerekli durumlarda kolaylıkla sökülebilmesi için tasarlanan adaptör, kablo, tornavida setinden oluşan bir çözümdür.

DIFOSE ChS:

DIFOSE Charge Seti, mobil adli bilişim olaylarına müdahale ederken çeşitli marka ve model mobil cihazlarda karşılaşılabilecek şarj ihtiyacının giderilmesi, cihazların bilgisayar bağlantısının yapılabilmesi amacıyla tasarlanmış adaptör ve kablo setinden oluşan bir çözümdür. En sık karşılaşılan mobil cihazlara ait kablolardan oluşmaktadır.

DIFOSE, Türkiye'de adli bilişim sektörünün gelişmesi ve hak ettiği yeri ve değeri bulması amacıyla kuruluşundan bu yana adli bilişim alanında kullanılan cihaz ve sistemlerde yurt dışına olan bağımlılığı azaltacak ve milli çözümler üretmeyi hedefleyen çalışmalarına devam etmektedir.

YERLİ ÜRETİM

TÜRKİYE'DE İLK VE TEK!
YERLİ TASARIM, YERLİ ÜRETİM

Güvenilir Veri Silme Cihazı
uWiPeR / sWiPeR

uWiPeR eşzamanlı olarak **3 adet USB 3.0** ve **1 adet SATA III**, **sWiPeR** ise **1 adet USB 3.0** ve **3 adet SATA II** taşınabilir ya da sabit diski bit-to-bit esasına göre güvenli olarak silebilir, silme sonucu oluşan raporu otomatik olarak görüntüleyebilir veya kaydedebilir.

Bilgi güvenliği, KVKK ve ISO 27001 gibi uluslararası standartlar gereği, kullanım amacını kaybeden kişisel ve kurumsal verilerin bir politika, prosedür ve süreç dahilinde güvenli bir şekilde silinmesi zorunluluktur.

Taşınabilir İş İstasyonu
PWS - Portable WorkStation

DIFOSE PWS kullanıcıların tüm işlemleri hızlı bir şekilde gerçekleştirmelerini sağlayan, gerek laboratuvar, gerekse saha çalışmalarına yönelik bir çözümdür. Güçlü bir bilgisayarın sunduğu tüm arayüzler ve bağlantılar mobil kullanım kolaylığı sağlayacak şekilde PWS'de sunulmaktadır.

AMD Ryzen™ 9 3950X 3.5GHz AM4 (16 Core, 32 Threads)
128 GB DDR4 3200 Mhz RAM
MSI Anakart
nVidia GT710
512 GB M.2 NVME SSD (Operating System)
2X1TB M.2 NVME SSD RAID 0 (Storage)
18.5 inch LED Full HD Ekran

TÜRKİYE'DE İLK VE TEK!
YERLİ TASARIM, YERLİ ÜRETİM

KOSGEB Destekli

Adli Kopya Alma Cihazı
Forensic Duplicator

DIFOSE, HDD, USB ve ağ depolama alanından alınan şüpheli sürücülerin adli kopyasını oluşturmak maksadıyla, olay müdahale ve kanıt toplama uzmanlarının deneyim ve fikirlerine dayanarak bir olay müdahalesi sırasında gereken işlevler için amaca yönelik ve tam özellikli yerli ve milli bir adli kopyalayıcı tasarlayarak proje çalışmalarına devam etmektedir.

İTHALAT & İHRACAT

DIFOSE müşterilerinin adli bilişim ve bilişim güvenliği alanındaki ihtiyaçlarını yerinde keşif ve gözlem yaparak tespit eder. Daha sonra ihtiyaca uygun ürün ve sistemleri yılların tecrübesi ile optimum seviyede planlar ve en kısa sürede tamamlayarak müşterisinin hizmetine sunar.
Aşağıda belirtilen alanlarda tedarik ettiği tüm ürünlerin kullanım kılavuzu, broşür ve garanti belgesini Türkçe olarak müşterilerine sunmakta, talep edilmesi halinde ise kurulum, danışmanlık, eğitim ve teknik destek hizmeti de vermektedir:

- Adli bilişim laboratuvar kurulumu ve projelendirilmesi
- Adli kopyalama cihaz ve sistemleri
- Adli bilişim bilgisayar ve iş istasyonu tasarımı
- Veri kurtarma donanım ve yazılımları
- Optik medya okuma ve kurtarma sistemleri
- Adli bilişim yazılımları
- Ağ adli analiz sistemleri
- Mobil cihaz adli inceleme sistemleri
- Chip okuma, kopyalama ve adli inceleme sistemleri
- Güvenli veri silme sistemleri
- Veri depolama aygıtı taşıma çantaları
- Bilişim güvenliği yazılım ve donanımları
- IT Audit (BT denetim) yazılımları
- Loglama sistemleri
- Elektronik keşif yazılımları
- Anti-Malware yazılımları

DIFOSE sadece ürün tedarik eden bir firma değil, müşterilerinin adli bilişim ve bilişim güvenliği alanlarında ihtiyaç duyduğu çözümleri en ekonomik ve en kısa sürede tamamlayan bir çözüm ortağıdır. Zira bizim için önemli olan, müşterilerimize ürün ve malzeme tedarik etmekten öte, tedarikini yapmış olduğumuz tüm çözümlerin ilk kurulum, bakım, onarım, iyileştirme ve güncelleştirme gibi önemli konuları teknik ekibimizle takip ederek müşterimizin memnuniyetini sağlamaktır.

Çözüm ortaklarımız

SERTİFİKALARIMIZ

T.C.
TÜRK PATENT ENSTİTÜSÜ

MARKA TESCİL BELGESİ

Marka No : 2013 98859 - Ticaret - Hizmet

DIFOSE

Marka Sahibi : DİFOSE BİLİŞİM BİLGİSAYAR EĞİTİM DANIŞMANLIK İTHALAT İHRACAT TİCARET LİMİTED ŞİRKETİ
TÜRKİYE CUMHURİYETİ
Mustafa Kemal Mah. 2131. Sok. 27/9 Çankaya 06520 ANKARA

Emtiası : 09 , 37 , 41 , 42 , 35
İlişiktedir.

Markaların Korunması Hakkında 556 Sayılı Kanun Hükmünde Kararnameye göre 03/12/2013 tarihinden itibaren ON YIL müddetle 05/09/2014 tarihinde tescil edilmiştir.

Prof. Dr. Habip ASAN
Enstitü Başkanı

TÜRK PATENT ENSTİTÜSÜ

DigiCert

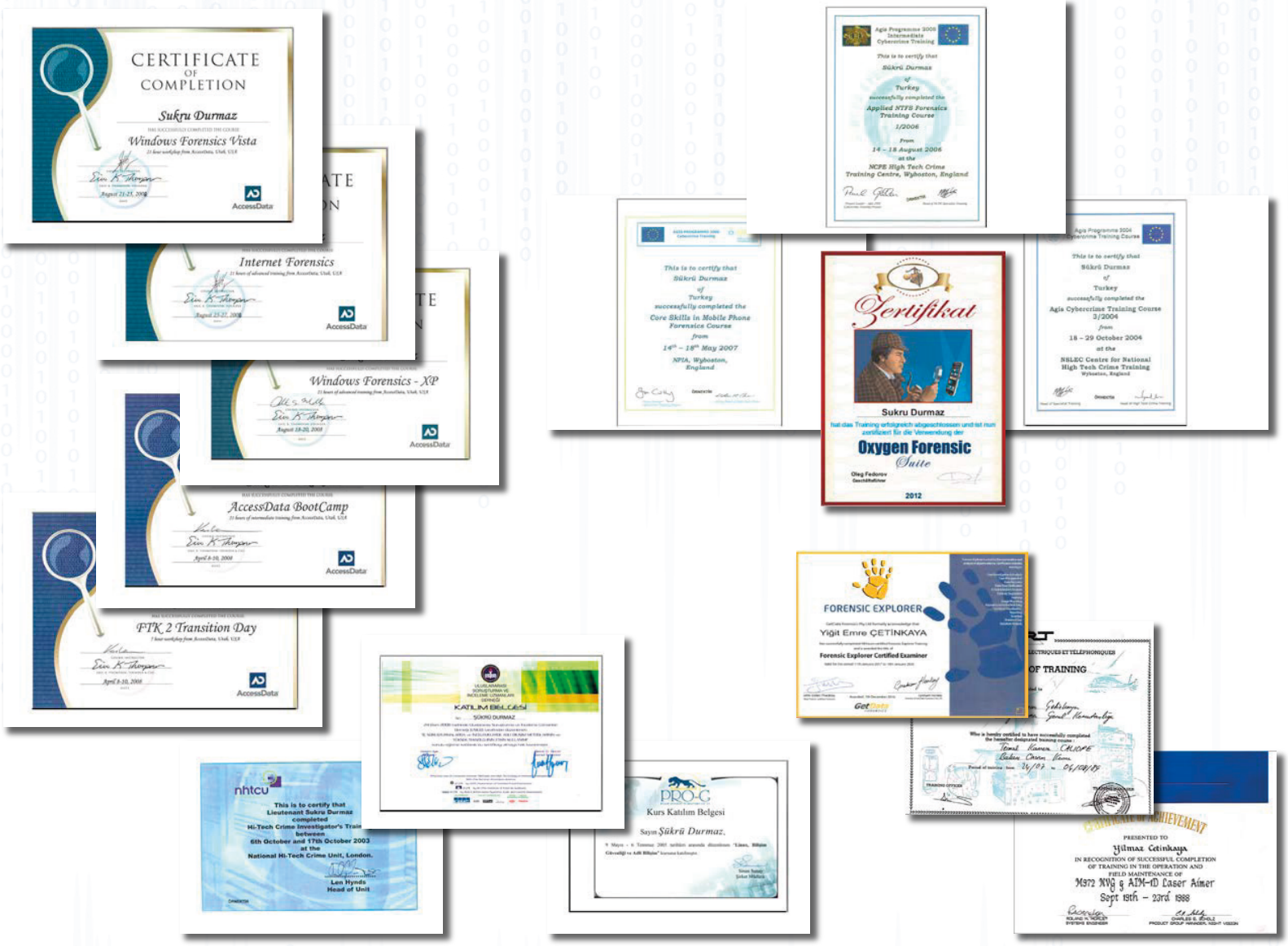
DİFOSE BİLİŞİM BİLGİSAYAR EĞİTİM DANIŞMANLIK İTHALAT İHRACAT TİCARET LİMİTED ŞİRKETİ

TS EN ISO/IEC 27001:2017

DigiCert

DİFOSE BİLİŞİM BİLGİSAYAR EĞİTİM DANIŞMANLIK İTHALAT İHRACAT TİCARET LİMİTED ŞİRKETİ

TS EN ISO 9001:2015


CERTIFICATE
OF
COMPLETION
Sukru Durmaz
Windows Forensics Vista
AccessData
Internet Forensics
AccessData
Windows Forensics - XP
AccessData
AccessData BootCamp
AccessData
FTK 2 Transition Day
AccessData
Agis Programme 2006
Intermediate
Cybercrime Training
This is to certify that
Sükrü Durmaz
of
Turkey
successfully completed the
Applied NTFS Forensics
Training Course
1/2006
From
14 – 18 August 2006
at the
NCPS High Tech Crime
Training Centre, Wyboston, England
This is to certify that
Sükrü Durmaz
of
Turkey
successfully completed the
Core Skills in Mobile Phone
Forensics Course
from
14th – 18th May 2007
NPIA, Wyboston,
England
Zertifikat
Sukru Durmaz
hat das Training erfolgreich abgeschlossen und ist nun
zertifiziert für die Verwendung der
Oxygen Forensic
Suite
Oleg Fedorov
Geschäftsführer
2012
Agis Programme 2004
Cybercrime Training Course
This is to certify that
Sükrü Durmaz
of
Turkey
successfully completed the
Agis Cybercrime Training Course
3/2004
from
18 – 29 October 2004
at the
NSLEC Centre for National
High Tech Crime Training
Wyboston, England
FORENSIC EXPLORER
Yiğit Emre ÇETİNKAYA
Forensic Explorer Certified Examiner
GetData
KATILIM BELGESİ
ŞÜKRÜ DURMAZ
nhtcu
This is to certify that
Lieutenant Sukru Durmaz
completed
Hi-Tech Crime Investigator's Train
between
6th October and 17th October 2003
at the
National Hi-Tech Crime Unit, London.
Len Hynds
Head of Unit
PRO-G
Kurs Katılım Belgesi
Sayın Şükrü Durmaz,
PRESENTED TO
Yilmaz Cetinkaya
IN RECOGNITION OF SUCCESSFUL COMPLETION
OF TRAINING IN THE OPERATION AND
FIELD MAINTENANCE OF
M972 NVG & AIM-D Laser Aimer
Sept 18th – 23rd 1988

DIFOSE

Bilişim Bilgisayar Eğitim Danışmanlık İthalat İhracat Ticaret Ltd. Şti.

ANKARA
Ümit Mah. 2481.Sok. Kafkas Sitesi No:6
06810 Ümitköy Çankaya

+90 312 219 56 16
+90 312 219 46 05
info@difose.com.tr

İSTANBUL
Esentepe Mah. Kelebek Sk. No:2 Marmara Kule Kat:10
D:79 34870 Kartal/İstanbul

+90 216 771 0797
+90 216 771 0597
info@difose.com.tr

www.difose.com.tr