|  |  |
| --- | --- |
|  | **CyberCrime@IPA**  **Avrupa Birliği/Avrupa Konseyi Sanal Suçlara Karşı Bölgesel İşbirliği Ortak Projesi**      **Adli eğitim**  **Hakim ve savcılar için sanal suçlar ve elektronik kanıt eğitimine giriş**  Eğitim kitapçığı ve eğitimci kılavuzu – Versiyon 1.0  Veri Koruma ve Sanal Suçlar Bölümü  İnsan Hakları ve Hukukun Üstünlüğü Genel Müdürlüğü  Strasbourg, Fransa  5 Nisan 2013  [**www.coe.int/cybercrime**](http://www.coe.int/cybercrime)  eu_coe_JP1 |
|  |

|  |  |
| --- | --- |
| İRTİBAT:  Veri Koruma ve Sanal Suçlar Bölümü  İnsan Hakları ve Hukukun Üstünlüğü Genel Müdürlüğü  Avrupa Konseyi, F-67075 Strasbourg Cedex (Fransa)  Tel +33 3 9021 4506  Faks +33 3 9021 5650  E-posta [alexander.seger@coe.int](mailto:alexander.seger@coe.int) | YASAL UYARI:  Bu teknik raporda ifade edilen görüşler, Avrupa Konseyi’nin, bu projeyi finanse eden kuruluşun ya da sözü edilen anlaşma Taraflarının resmi görüşlerini yansıtmak zorunda değildir. |

**İçindekiler**

[1 Giriş 4](#_Toc352944220)

[2 Genel Bakış 5](#_Toc352944221)

[2.1 Eğitimin amacı 5](#_Toc352944222)

[2.2 Bu eğitim neden gerekli? 5](#_Toc352944223)

[2.3 Eğitim programı 6](#_Toc352944224)

[3 Eğitimci Kılavuzu Nasıl Kullanılmalıdır? 6](#_Toc352944225)

[4 Eğitime Genel Bakış 7](#_Toc352944226)

[4.1 Eğitimin süresi ve hitap ettiği grup 7](#_Toc352944227)

[4.2 Eğitimi kim verecek? 7](#_Toc352944228)

[4.3 Eğitim nasıl verilecek? 8](#_Toc352944229)

[4.4 Eğitimin hedefleri 8](#_Toc352944230)

[4.5 Hedef öğrenciler ve eğitimciler grubu 8](#_Toc352944231)

[4.5.1 Öğrenciler 8](#_Toc352944232)

[4.5.2 Deneyim ön şartları 8](#_Toc352944233)

[4.5.3 Eğitimciler 8](#_Toc352944234)

[4.5.4 Deneyim ön şartları 8](#_Toc352944235)

[4.6 Kaynaklar 9](#_Toc352944236)

[4.6.1 Eğitim kaynaklarının şartları 9](#_Toc352944237)

[4.7 Değerlendirme 9](#_Toc352944238)

[4.8 Ders ve öğrenme amaçları 9](#_Toc352944239)

[5 Önemli Bağlantılar 13](#_Toc352944240)

[6 Ders Planları 14](#_Toc352944241)

[6.1 Ders 1.1.1 Eğitime Giriş 14](#_Toc352944242)

[6.2 Ders 1.1.2 Sanal Suçlara Giriş 17](#_Toc352944243)

[6.3 Ders 1.1.3, 1.2.2 & 1.2.5 - Teknoloji 29](#_Toc352944244)

[6.4 Ders 1.3.1 – Günlük Değerlendirme 55](#_Toc352944245)

[6.5 Ders 1.2.3 Suç eylemi olarak sanal suçlar – Yerel Mevzuat 56](#_Toc352944246)

[6.6 Ders 1.2.4 Yerel Usul Hukuku 81](#_Toc352944247)

[6.7 Ders 1.3.1 Günlük Değerlendirme 86](#_Toc352944248)

[6.8 Ders 1.3.2 & 1.3.3 Elektronik Kanıt 87](#_Toc352944249)

[6.9 Ders 1.3.4 Uluslararası İşbirliği 112](#_Toc352944250)

[6.10 Ders 1.3.5 Eğitimin Sonu 122](#_Toc352944251)

[7 Ölçüm 124](#_Toc352944252)

[8 Değerlendirme 124](#_Toc352944253)

# 1 Giriş

Dünyada toplumların bilgi ve iletişim teknolojilerine duydukları güven göz önüne alındığında hakim ve savcılar, sanal suçlarla ve elektronik kanıtlarla uğraşmak için hazırlıklı olmalıdır. Çoğu ülkede emniyet güçleri, sanal suçları araştırma ve elektronik kanıtların güvenliğini sağlamaya yönelik imkanlarını geliştirebilmiştir ancak aynısını hakim ve savcılar için söylemek pek mümkün değildir. Deneyimlere göre çoğu durumda hakim ve savcılar, sanal dünyanın yeni gerçeklikleriyle başa çıkmada zorluklarla karşı karşıya kalmaktadır. Dolayısıyla hakim ve savcıların sanal suçları takip etmesini, bu davalarda hüküm vermesini ve eğitim, paylaşım ve uzmanlaşma yoluyla elektronik kanıtlardan faydalanmasını sağlamak için özel çalışmalara ihtiyaç duyulmaktadır.

Bu çalışmaları desteklemeye yönelik bir konsept, Avrupa Konseyi tarafından Sanal Suçlar Projesi kapsamında, 2009 yılında Lizbon adli eğitim kurumları ağı ve çok paydaşlı bir çalışma grubu ile işbirliği yapılarak geliştirilmiştir.

Konseptin amacı, adli eğitim kurumlarının hakim ve savcılara yönelik olarak sanal suçlara ve elektronik kanıtlara dair eğitim programları geliştirmesine yardımcı olmak ve bu eğitimi normalde uygulanan ilk ve kurum içi eğitimlerin kapsamına dahil etmektir.

Hakim ve savcılara yönelik bu eğitim konseptinin amaçları şunlardır:

* Eğitim kurumlarının sanal suçlara dair ilk ve kurum içi eğitimleri uluslararası standartlara uygun olarak vermesini sağlamak
* Mevcut ve gelecekteki hakim ve savcıların mümkün olduğu kadar fazlasına sanal suçlar ve elektronik kanıtlarla ilgili temel bilgiler kazandırmak
* Önemli sayıda hakim ve savcıya ileri düzey eğitim vermek
* Hakim ve savcıların sürekli uzmanlaşma ve teknik eğitim çalışmalarını desteklemek
* Hakim ve savcılar arasında bir ağ aracılığıyla bilgilerin artırılmasına katkıda bulunmak
* Farklı eğitim girişimleri ve ağlarına erişimi kolaylaştırmak.

Avrupa Birliği ve Avrupa Konseyi’nin Katılım Öncesi Mali Yardım Aracı kapsamındaki Sanal Suçlar Bölgesel Ortak Projesi (Ceza Yargılamasında Bölgesel İşbirliği: Sanal suçlarla mücadelede kapasitelerin güçlendirilmesi)[[1]](#footnote-1) ile proje bölgelerindeki (Arnavutluk, Bosna Hersek, Hırvatistan, Karadağ, Sırbistan, “Makedonya Eski Yugoslav Cumhuriyeti”, Türkiye ve Kosova[[2]](#footnote-2)\*) eğitim kurumları, bu eğitim konseptini uygulamak üzere desteklenmektedir.

Bu bağlamda eğitim kurumları tarafından kullanılacak eğitim materyalleri oluşturulmaktadır ve bir “Eğitimcilerin Eğitim Programı” gerçekleştirilmiştir. Eğitim paketinin son versiyonu, “Eğitimcilerin Eğitim Programına” katılmış ve eğitimi kendi eğitim kurumlarında vermiş olan hakim ve savcılardan alınan geri bildirimleri dikkate almaktadır. Ayrıca son versiyon, özel olarak düzenlenen bir organizasyonda adli eğitim çalışma grubunun üyeleri ile eğitimciler tarafından da tartışılmıştır.

# 2 Genel Bakış

## Eğitimin Amacı

Bu eğitim, sanal suçlara ve elektronik kanıtlara ilişkin giriş seviyesindeki bilgileri hakim ve savcılara sunmak üzere tasarlanmıştır. Eğitimde, konular hakkında hukuki ve uygulamalı bilgiler sunulacak ve bu konuların, hakim ve savcıların günlük işlerinde nasıl etkiler yarattığına odaklanılacaktır.

Eğitimin sonunda hakim ve savcılar, şunlara dair temel bilgileri edinmiş olacaktır:

* Sanal suçlar ve elektronik kanıtlar
* Hakim ve savcıların bunlarla nasıl çalışabileceği
* Hangi maddi hukuk ve usul hukuku hükümlerinin ve hangi teknolojilerin uygulanabileceği, ve
* Acil ve etkili tedbirlerin nasıl alınacağı ve kapsamlı uluslararası işbirliğinin nasıl uygulanacağı.

Eğitimde şu konular yer alacaktır:

* Sanal suçlara giriş – eğilimler ve araçlar
* Sanal suçlarda kullanılan teknolojiler
* Yerel mevzuatta cezai suç olarak sanal suçlar
* Elektronik kanıt uygulamaları, usulleri ve mevzuatı
* Usul hukuku / yerel mevzuatta soruşturma tedbirleri
* Uluslararası işbirliği

## Bu eğitim neden gereklidir?

Hakim ve savcılar, suç işleyen şahıs ya da grupların soruşturulması ve yargılanmasında önemli bir rol oynar. Elektronik kanıtların söz konusu olduğu sanal suçları içeren olayların artmasıyla hakim ve savcıların, bu suçların doğasını anlamak ve uluslararası işbirliğinde sanal suç davalarını ele almaya yönelik olarak kullanılabilecek mevzuat ve araçlardan haberdar olmak üzere eğitilmesi gerekliliği de artmıştır.

Suçlular ve suç örgütleri genel olarak kendilerini ve faaliyetlerini ülke sınırları ile kısıtlamaz. Sanal suç, failin bir suç işlemek için bu sınırları aşmak zorunda olmadığı bir suç türüdür ve dolayısıyla bu suçların failinin soruşturulması ve kovuşturulması daha zordur. Bu, sanal suçlarla mücadelede daha güçlü uluslararası/bölgesel işbirliği ve kurumlar arası işbirliği ihtiyacını ortaya koymaktadır.

Sanal suç davaları çoğunlukla hızlı ve çok etkili bir uluslararası ya da bölgesel işbirliği gerektirir. Böylelikle faillerin zamanında soruşturulması ve kovuşturulması sağlanır. Sonuç olarak eğitim kurumları, 7/24 irtibat noktaları, MLA, Adli İşbirliği Faaliyeti, Adli İşbirliği Platformlarının vb. kullanımı dahil olmak üzere sanal suçların soruşturulmasında faydalanılabilecek uluslararası işbirliğinin araçları hakkında talimatlar içeren modülleri eğitim programlarına dahil etmek için çalışmalar yapmalıdır.

## Eğitim programı

Bu eğitim programı, sanal suçlara ilişkin eğitim çalışmaları yürütülürken eğitim kurumları tarafından dikkate alınacak temel bir araçtır. Bu dokümanın amacı, sanal suç davalarında yargılama ve soruşturma görevlerini yürüten hakim ve savcılara yönelik başlangıç eğitiminin gerçekleştirilmesinde proje ülkelerinde/bölgelerinde kullanılabilecek standart hale getirilmiş derslerin ya da modüllerin oluşturulması ve hazırlanmasına odaklanmaktır.

Hakimlerin eğitimine yönelik modül için önerilen şablon, yalnızca hakim ve savcıların eğitimi için bir temel hizmeti görür ve eğitimin nihai amacı değildir. Proje ülkeleri/bölgeleri, ulusal düzeydeki ihtiyaçları tartışmalı ve en kritik olarak belirledikleri sanal suç alanlarında özel ek eğitimler talep etmelidir.

Hazırlanan dersler, sunumların/oturumların başlıklarını/konularını ve eğitimciler tarafından yapılacak detaylı açıklamaları sunmaktadır. Eğitim, bir yandan eğitimin amaç ve hedeflerinin gerçekleştirilmesini sağlarken diğer yandan ulusal şartları yerine getirmek için tadil edilebilecek şekilde tasarlanmıştır. Bu, eğitim modüllerinin farklı ülkelerde de olsa tutarlı olmasını sağlayacaktır. Eğitimciler, her ülkedeki katılımcıların öğrenme deneyimini kolaylaştıracak çeşitli alıştırma ve tartışmaları kullanmayı düşünmelidir.

Temel Eğitim Modülü, bu modülü geçen hakim ve savcıların, sanal suçların doğasına, terimlere ve teknolojiye ilişkin temel bilgilere sahip olmasını sağlayacak şekilde oluşturulmuştur. Ayrıca bu modül, uluslararası işbirliği, elektronik kanıtlar, usul hukuku ve soruşturma tedbirleri vb. hakkında da temel bilgiler sunmaktadır.

Temel Modüle bir ek ve takviye olarak verilecek ileri eğitim modülü de olacaktır ve bu modül, konular hakkında daha ayrıntılı bilgiler sunacak ve temel modüldeki oturumlarda öğrenmeyi desteklemek için örnek olaylarından faydalanacaktır. İleri eğitim modülü, bilgisayar ve ağların işleyişi, sanal suçların ne olduğu, sanal suç mevzuatı, yargı alanı, soruşturma tedbirleri, elektronik kanıtlar ve uluslararası işbirliği hakkında pratikte uygulanabilecek ileri düzey bilgileri hakim ve savcılara sunmak amacıyla oluşturulacaktır.

# 3 Eğitimci kılavuzu nasıl kullanılmalıdır?

Bu kılavuzun amacı, eğitimin yapısı ve içeriğine ilişkin bilgileri eğitimcilere sunmaktır. Her bir dersin hedefleri, dersin hangi bilgileri kapsadığını özetlemektedir. Bu eğitim için eğitim metodolojisi hazırlanmıştır ve ilgili tüm eğitim destek materyalleri bu eğitim paketinde yer almalıdır. Bu kılavuzun amacı, eğitimin standardını korumak ve eğitimin verilişi sırasında tutarlılık sağlamaktır.

Bu derste, hakim ve savcıların görevlerini etkili bir şekilde gerçekleştirmeleri için gereken teknoloji bilgilerinin türü ve düzeyine dair rehberlik sunmaya çalışılmıştır. Ders, konuların eksiksiz bir analizi olduğu iddiasında değildir.

Eğitim geliştiricilerinin, hazırladıkları materyallerin mümkün olduğu kadar güncel olmasını sağlaması ve en son teknoloji konularını ve bunların eğitimin verileceği yerdeki yargı alanında hukuki, usul ve kanıtlarla ilgili kararlar üzerindeki etkilerini bu materyallere dahil etmesi tavsiye edilmektedir. Verilerin katı hal disklerinde ya da Web 2.0’da depolanması gibi ceza yargılaması sistemini etkileyecek teknolojik değişiklikler vardır. Bunlar, eğitim programlarına dahil edilmesi ve daha da yaygınlaştıkça güncellenmesi gereken önemli konular olacaktır.

Diğer programlarda da olduğu gibi, hakim ve savcılar için geliştirilen tüm eğitimler, özgün, ölçülebilir, başarılabilir, ilgili ve zamanlı olan net amaçlara sahip olmalıdır. Amaçların gerçekleştirilebilmesi için bu elzemdir. “Anlama” ve “bilme” gibi kelimelerle amaçların kullanımından kaçının çünkü bunlar kriterleri karşılamaz. Örneğin, bir konunun “bilinmesi” amacının gerçekleştirilip gerçekleştirilmediğini nasıl ölçersiniz? Ölçülebilir olan listeleme ya da tespit etme gibi kelimeleri kullanmak daha iyidir.

Bilgilendirme için örnek olayların kullanılması, bu tür bir eğitim için uygun görülmektedir ve yetişkinlere yönelik öğretim tarzlarında safi didaktik öğretimden daha faydalıdır.

Eğitim geliştiricisinin temel rolü, tüm öğrenim etkinliklerinin genel amacının ve özel amaçların gerçekleştirilmesini sağlamaktır. Bu bölümde bu sürece yardımcı olacak bazı bilgiler verilmektedir.

Bu eğitim ülkelere özel değil genel kapsamlı bir program olarak geliştirilmiş olmasına rağmen eğitimcilerin eğitim materyallerini daha etkili bir şekilde verebilmesi için bu materyalleri kişiselleştirmeleri önemlidir. Bilgilendirme için örnek olaylarının kullanılması, bu tür bir eğitim için uygun görülmektedir ve yetişkinlere yönelik öğretim tarzlarında safi didaktik öğretimden daha faydalıdır. Sözü geçen teknolojilerin fiziksel örneklerinin ve İnternetin kullanımı da öğrenmeyi destekleyebilir. Özellikle iç mevzuattaki maddi hukuk ve usul hukukuna ilişkin oturumlar, ulusal düzeyde dahil edilmesi gereken türden bilgilerin örnekleri olarak hazırlanmıştır. Eğitimciler, ülkelerinde eğitimi vermeden önce ulusal mevzuatlarının bu oturumlara dahil edilmesini sağlamaktan sorumludur.

# 4 Eğitime Genel Bakış



## Eğitimin süresi ve hitap ettiği grup

Bu eğitim, hakim ve savcılar için onların başlangıç eğitim programının bir parçası olarak 3 günlük bir program şeklinde tasarlanmıştır.

## Eğitimi kim verecek?

Eğitim, ülkelerin adli eğitim kurumlarındaki kurum içi eğitmenler tarafından verilmek üzere geliştirilmiştir. Gerekli durumlarda eğer adli merkezlerde gerekli uzmanlar mevcut değilse özel teknik konuların işlenmesi için konu uzmanlarının davet edilmesi tavsiye edilir. Bu temel seviyede bir eğitim olduğundan eğitimin tüm yeni hakim ve savcılara verilmesi beklenmektedir.

## Eğitim nasıl verilecek?

Eğitim, şu anda sahip olduğu yapısıyla, sınıf bazlı öğretime uygun olarak sınıf ortamında verilmek üzere tasarlanmıştır. Ancak gerekirse materyallerin uzaktan öğrenme veya e-öğrenme modüllerine çevrilmemesi için bir sebep yoktur. Yukarıda Bölüm 1’de açıklandığı gibi eğitimciler, ulusal düzeyde programa alıştırma ve diğer öğretim yöntemlerini dahil etmeyi düşünmelidir.

## Eğitimin hedefleri

Eğitimin hedefleri, eğitimcilerin bu hedefleri gerçekleştirmesi için çeşitli öğretim yöntemlerini kullanmasına olanak tanıyacak geleneksel bir şekilde yazılmıştır. Bu hedeflerin genel özellikleri şunlardır:

* **Belirli –** Hedefler, neyin gerçekleştirilmek istendiğini belirtmelidir.
* **Ölçülebilir** – Hedeflerin yerine getirilip getirilmediği ölçülebilmelidir.
* **Gerçekleştirilebilir** – Belirlenen hedefler gerçekleştirilebilir ve ulaşılabilir mi?
* **Gerçekçi –** Sahip olduğunuz kaynaklarla hedeflere gerçekçi olarak ulaşılabilir mi?
* **Zamanlı –** Belirlenen hedeflere ne zaman ulaşılmak isteniyor?

Buna dayanarak aşağıdaki eğitim hedefleri belirlenmiştir ve bunlar, eğitimin genel amacı ile birlikte okunmalıdır.

## Hedef öğrenciler ve eğitimci grubu

### Öğrenciler

Bu eğitim, hakim ve savcılara ilk görev dönemlerinde verilmek üzere tasarlanmıştır.

### Deneyim Ön Şartları

Hiçbir ön bilgi şartı yoktur.

### Eğitimciler

Bu eğitimi verecek olarak eğitmenler, bu eğitimin verileceği adli eğitim merkezleri tarafından istihdam edilmelidir.

### Deneyim Ön Şartları

Eğitimciler, sanal suç konuları/eğilimlerine ve ülkelerindeki sanal suç mevzuatına ilişkin olarak iyi düzeyde bilgiye sahip olmalıdır. Eğitmenlik deneyimi, öğretim bilgisi ve uygulamaları hakkında tecrübe şarttır.

## Kaynaklar

### Eğitim kaynaklarına ilişkin şartlar

Bu eğitimin bir eğitim sınıfı ortamında verilmesi için aşağıdaki ekipmanlar gereklidir:

* Beklenen sayıda öğrenci için uygun büyüklükte bir oda
* Windows 7 ve MS Office Professional kurulu olan bir dizüstü bilgisayar ya da PC
* Projektör ve perde
* İnternet erişimi (varsa)
* Bilgisayar donanımı örnekleri (varsa)
* “Ağ Savaşçıları” adlı video klip
* Budapeşte Sanal Suçlar Sözleşmesi ve açıklayıcı rapor
* EC OISIN tarafından finanse edilen e-kanıt kılavuzunun kopyası
* Beyaz tahta
* Beyaz tahta kalemleri (mavi, siyah, kırmızı ve yeşilden ikişer tane)
* 2 kağıt tahtası ve yeteri kadar kağıt
* Öğrenci not kağıdı ve kalemler
* Zımba, delgeç ve makas
* Raptiye ya da kağıtların duvarlara geçici olarak tutturulacağı başka bir ürün

## Değerlendirme

Bu pilot eğitimin bir parçası olarak öğrenci bilgilerinin değerlendirilmesi talep edilmemiş ve sunulmamıştır. Bu eğitimi ulusal düzeyde uygulayan ülkeler, değerlendirme yapmak isteyebilir. Her durumda eğitimciler, öğrenme hedeflerinin gerçekleştirilmesini sağlamak için eğitim sırasında sorular, küçük sınavlar ya da başka yöntemlerle öğrencilerin bilgilerini kontrol etmelidir.

## Eğitim ve ders hedefleri

| **Ders no.** | **Ders Başlığı** | **Hedefler** |
| --- | --- | --- |
| **1.1.1** | **Eğitime Giriş** | * Eğitmenlerin ve diğer katılımcıların tanınması * Eğitimin yapısı ve içeriğinin tanımlanması * İlgili idari görevlerin tespiti * Eğitimle ilgili belgelerin dağıtılması * Eğitim yeri için sağlık ve güvenlik konuları da dahil olmak üzere imkan ve usullerin açıklanması |
| **1.1.2** | **Sanal Suçlara Giriş** | * Farklı sanal suç türlerinin ve etkilerinin tespiti * Sanal suçların tehdit, eğilim ve araçlarının ve bu olguya verilen karşılıkların sayılması * Çoğu mevzuat ve uluslararası standarda göre suç türü olarak kabul edilen sanal suç kavramlarının açıklanması * Ulusal mevzuat ve başta Budapeşte Sözleşmesi olmak üzere uluslararası mevzuat arasında uyum sağlanmasına yönelik ihtiyaç ve bunun avantajlarının analizi |
| **1.1.3**  **1.2.2**  **1.2.5** | **Teknolojiye Giriş** | * Suçluların çeşitli internet uygulamalarını nasıl kullandıklarını belirleyebilecektir * Bir bilgisayar sisteminin bileşenlerinin sayılması * Farklı veri depolama cihaz çeşitlerinin tanınması üssel veri depolama kapasitesinin ceza yargılaması ile ilgili sonuçlarının değerlendirilmesi * Farklı bilgisayar işletim sistemlerinin tanınması * Ağların nasıl işlediğine dair temel bilgilerin açıklanması * İnternetin işlevlerinin açıklanması * En az 5 büyük İnternet uygulamasının tanınması * İnternetin günümüze kadar olan gelişiminin açıklanması * Farklı internet uygulamalarının ayırt edilmesi * Suçluların çeşitli internet uygulamalarını nasıl kullandıklarının belirlenmesi |
| **1.2.3** | **Yerel mevzuatta cezai suç olarak sanal suçlar** | * Maddi ceza hukuku hükümleri ve Budapeşte Sözleşmesi’ne göre suçları tarif etmek için kullanılan bazı temel faktörlerin sayılması * Maddi ceza hukuku hükümleri ve mevcut ulusal hukuka göre suçları tarif etmek için kullanılan bazı temel faktörlerin sayılması * Ulusal mevzuat ile başta Budapeşte Sözleşmesi olmak üzere uluslararası dokümanlar arasında uyum sağlanmasına yönelik ihtiyaç ve bunun avantajlarının analiz edilmesi * Sunulan örnek olaylar ile ilgili tartışmalara göre ilgili maddi hukuk hükümlerinin belirlenmesi. |
| **1.2.4** | **Usul Hukuku / Yerel Mevzuatta Soruşturma Tedbirleri** | * Budapeşte Sözleşmesi’nin usul hükümlerinin açıklanması * Ulusal hukuk kapsamındaki usul hükümlerinin açıklanması |
| **1.3.3**  **1.3.4** | **Elektronik kanıtların toplanması; usul ve soruşturma tedbirleri** | * Çeşitli elektronik kanıt türlerinin tartışılması * Elektronik kanıtların elde edilmesi ve bunlara gösterilecek muameleye ilişkin en iyi uygulama ilkelerinin açıklanması * Elektronik kanıtlara ait “cansız kutu”, “canlı veri” ve internet kaynaklarından kaynaklanan zorlukların belirlenmesi * Başka bir yargı alanından kanıtların elde edilmesine ilişkin zorlukların tespit edilmesi * Elektronik kanıtların gerçekliği, doğruluğu ve bütünlüğü açısından adli davalarda kabul edilebilirliğinin tartışılması * Budapeşte Sözleşmesi’nin usul hükümlerinin açıklanması. |
| **1.3.4** | **Uluslararası İşbirliği** | * İnternetin küresel boyutunun ve sanal suçların uluslararası boyutunun tanınması, * Uluslararası işbirliğinin öneminin açıklanması ve sanal suç alanında uluslararası işbirliği için mevcut araçların tanınması, * Uluslararası işbirliği için oldukça hızlı ve etkin kanallara olan ihtiyacın ve mevcut araçların, bunların kullanım yollarının, zaman çizelgelerinin ve etkinliklerinin belirlenmesi, * Yeni uluslararası işbirliği modellerinin uygulanmasına ilişkin uluslararası kuruluşların çalışmalarının anlatılması, * Budapeşte Sanal Suçlar Sözleşmesi’nin tartışılması, genel ilkelerinin, geçici önlemlerin ve 7/24 karşılıklı hukuki yardım ağının tanınması. |
| **1.3.5** | **Eğitimin Kapanışı** | * Eğitime ve etkinliğine ilişkin olarak uygun geri bildirimlerin sunulması * Avrupa Konseyi eğitim değerlendirme formlarının doldurulması * Katılımcıların konuya ilişkin bilgi ve becerilerini geliştirmek için almaları gereken bir sonraki eğitim düzeyini tespit edebilmesi. |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Avrupa Konseyi**  **Hakim ve Savcılar için Sanal Suçlar**  **Eğitim Kursu** | | | | | | | | | | | | |
| **Zaman programı – Modül 1** | | | | | | | | | | | | |
|  | **09:00 - 10:00** | | **10:00 - 11:00** | | **11:00 - 12:00** | | **12:00 - 13:00** | **13:00 - 14:00** | **14:00 - 15:00** | **15:00 - 16:00** | | **16:00 - 17:00** |
| **Gün 1** | **1.1.1**  **Eğitime Giriş ve Takdimler** | | | **1.1.2**  **Sanal Suç Tehditleri, eğilimleri ve mücadelelere Giriş** | | | | **ARA** | **1.1.3 Teknolojiye Giriş**  **Bölüm 1** | | | |
| **Gün 2** | **1.2.1**  **Günlük Değ.** | **1.2.2 Teknolojiye Giriş**  **Bölüm 2** | | | | **1.2.3**  **Yerel Mevzuatta Bir Suç olarak Sanal Suç** | | **ARA** | **1.2.4**  **Usul Hukuku ve Yerel Mevzuatta Soruşturma Tedbirleri** | | **1.2.5 Teknolojiye Giriş**  **Bölüm 3** | |
| **Gün 3** | **1.3.1**  **Günlük Değ.** | **1.3.2 Elektronik Kanıt**  **Uygulama ve Usul** | | | | **1.3.3**  **Elektronik Kanıt Usul ve Soruşturma Hukuku** | | **ARA** | **1.3.4**  **Uluslararası İşbirliği** | | **1.3.5**  **Katılımcıların Geri Bildirimi ve Eğitimin Kapanışı** | |

Kahve araları ve diğer aralar her eğitim gününde uygun zamanlarda verilecektir.

# 5 Önemli İrtibatlar

Aşağıdaki kişiler, eğitim ve içeriği hakkındaki tüm sorular için ulaşılabilecek irtibat noktalarıdır:

|  |  |
| --- | --- |
| Alexander Seger  Veri Koruma ve Sanal Suçlar Bölümü Başkanı  İnsan Hakları ve Hukukun Üstünlüğü Genel Müdürlüğü (DG-I)  Avrupa Konseyi,  F-67075 Strasbourg Cedex  Tel. +33 3 90 21 4506  Faks +33 3 90 21 56 50  [alexander.seger@coe.int](mailto:alexander.seger@coe.int) | Mustafa Ferati  Program Görevlisi  Veri Koruma ve Sanal Suçlar Bölümü İnsan Hakları ve Hukukun Üstünlüğü Genel Müdürlüğü (DG-I) Avrupa Konseyi 67075 Strasbourg Cedex, FRANSA Tel.: +33 (0)3 90 21 45 50 Faks: +33 (0)3 90 21 56 50  [Mustafa.Ferati@coe.int](mailto:Mustafa.Ferati@coe.int) |

# 6 Ders Planları

|  |  |  |
| --- | --- | --- |
| Ders 1.1.1 Eğitime Giriş | | **Süre: 90 Dakia** |
| **Gerekli kaynaklar:**   * Windows 7 ve MS Office Professional kurulu olan bir dizüstü bilgisayar ya da PC * Projektör ve perde * İnternet erişimi (varsa) * Bilgisayar donanımı örnekleri (varsa) * Beyaz tahta * Beyaz tahta kalemleri (mavi, siyah, kırmızı ve yeşilden en az 2’şer tane) * Kağıt tahtası ve yeterli kağıt * Öğrenci not kağıdı ve kalemler * Zımba, delgeç ve makas * Raptiye ya da kağıtların duvarlara geçici olarak tutturulacağı başka bir ürün | | |
| **Amaç:** Katılımcılara eğitim dersi, amaç ve hedeflerine duyulan ihtiyaç hakkında bilgi sağlamak. Etkinlik programı ve zaman tablosu hakkında yeterli bilgiye sahip olmalarını sağlamak. Dersin, sağlık, güvenlik ve idari ayrıntıları hakkında bilgi vermek. Katılımcıları eğitmenler ve diğer katılımcılarla tanıştırmak. | | |
| **Hedefler:**  Bu dersin sonunda katılımcılar:   * Eğitmenleri ve diğer katılımcıları tanıyabilecek, * Eğitimin genel amacını tartışabilecek, * Bu eğitimin neden gerekli olduğunu açıklayabilecek, * Eğitimin zaman tablosu ve etkinliklerinin bileşenlerini sayabilecek * Eğitim yeri için sağlık ve güvenlik usullerini sayabilecektir. | | |
| **Slayt no.** | **İçerik:** | |
| **Slayt 1 - 23** | **Giriş**  Bu, eğitimin açılış oturumudur. Bu oturum boyunca katılımcılar, eğitimciler ve diğer katılımcılar ile tanıştırılacaktır. Eğitimin amaç ve hedefleri öğretim yöntemleriyle beraber açıklanacaktır.  Eğitimci, katılımcıları eğitime katılmaları ve birbirleriyle kaynaşmaları konusunda teşvik etmek için ilk aşamada bazı kaynaştırma faaliyetleri gerçekleştirebilir. | |
|  | **PowerPoint (ya da başka bir tür sunum)**  Bu oturum için bir PowerPoint sunum hazırlanmıştır. Bu genel kapsamlı bir sunumdur ve bu eğitim ulusal düzeyde veriliyorken ele alınması gereken ulusal meseleleri dikkate almamaktadır. Eğitimci, bu sunumdaki bilgilerin, verildikleri yerle alakalı olmasını sağlamalıdır. | |
| **Slayt 2** | Bu slaytta sağlık ve güvenlik konuları ele alınmaktadır. Bunlar, eğitimin verildiği yere gore farklılık gösterecektir. Katılımcılara doğru bilgiler vermek eğitimcinin sorumluluğu altındadır. | |
| **Slayt 3** | Katılımcılara eğitimin arka planı sunulmaktadır. Bu eğitimin adı “Hakim ve Savcılar için Sanal Suçlar ve Elektronik Kanıt Eğitimine Giriş”tir. IPA (Katılım öncesi mali yardım aracı) bölgesinde Sanal Suçlar konusunda Bölgesel İşbirliğine dair Avrupa Birliği/Avrupa Konseyi Ortak Projesi’nin bir ürünü olarak geliştirilmiştir. | |
| **Slayt 4** | Oturumun amaçları aşağıda belirtilmektedir:   * Katılımcılara eğitim dersi, amaç ve hedeflerine duyulan ihtiyaç hakkında bilgi sağlamak. * Etkinlik programı ve zaman tablosu hakkında yeterli bilgiye sahip olmalarını sağlamak. * Dersin, sağlık, güvenlik ve idari ayrıntıları hakkında bilgi vermek. * Katılımcıları eğitmenler ve diğer katılımcılarla tanıştırmak. | |
| **Slayt 5** | Kişisel hedefler, eğitimin sonunda katılımcının yapabiliyor olması gereken şeylerdir. Bu hedefler, öğrencilerin edindikleri bilgileri sınamak ve öğrencilerin eğitimi değerlendirmesini sağlamak için kullanılabilir. Bu oturum sonunda öğrenciler,   * Eğitmenleri ve diğer katılımcıları tanıyabilir, * Eğitimin genel amacını tartışabilir, * Bu eğitimin neden gerekli olduğunu açıklayabilir, * Eğitimin zaman tablosu ve etkinliklerinin bileşenlerini sayabilir * Olay yeri için sağlık ve güvenlik usullerini sayabilir olmalıdır. | |
| **Slayt 6** | Bu eğitim gereklidir çünkü hakim ve savcılar, suç işleyen kişi veya grupların soruşturulması ve yargılanmasında önemli bir rol oynar. Elektronik kanıtların söz konusu olduğu sanal suçları içeren olayların artmasıyla hakim ve savcıların, bu suçların doğasını anlamak ve uluslararası işbirliğinde sanal suç davalarını ele almaya yönelik olarak kullanılabilecek mevzuat ve araçlardan haberdar olmak üzere eğitilmesi gerekliliği de artmıştır. | |
| **Slayt 7** | Eğitimin genel amacının katılımcılara başta açıklanması önemlidir. Bu, onların eğitimde bulunma nedenlerini anlamalarını sağlayacaktır. Eğitimin genel amacı, hakim ve savcılara sanal suç ve elektronik kanıt üzerine başlangıç seviyesinde bilgi vermektir. Eğitimde, konular hakkında pratik bilgilerin yanısıra hukuki bilgiler de verilecek ve bu konuların katılımcıların günlük çalışmalarını nasıl etkilediği hususuna da yoğunlaşılacaktır. | |
| **Slayt 8** | Eğitimin zaman tablosu da öğrencilere bu aşamada açıklanmalıdır. Bu, eğitimin, öğle yemeğinin ve diğer araların saatlerini ve her bir oturumun kısa bir açıklamasını içermelidir. Herhangi bir değerlendirmenin kursun kapsamına dahil edilmesi ya da kapsam dışı bırakılması bu aşamada halledilmelidir. Eğer bir değerlendirme varsa bu ayrıntılı bir şekilde açıklanmalı ve öğrencilerin çalışma açısından beklentileri de dikkate alınmalıdır. | |
| **Slayt 9 - 17** | Her bir oturumun ayrıntılı hedefleri bu slaytlarda verilmektedir. Bunlar, katılımcılara bu aşamada açıklanmalıdır. Her bir dersin temel içeriği açıklamada yer almalıdır. | |
| **Slayt 20** | Eğitimci ve öğrencilerin tanışması sonraki aşamadır. Öğrencilerin birbirleriyle ve eğitimcilerle etkileşime girmesini sağlamak için bu fırsatın kaçırılmaması önemlidir. Katılımcılardan, sınıfta tanımadıkları biriyle eşleşmeleri istenmelidir. Daha sonra eşlerinden şu sorulara cevap istemeleri konusunda yönlendirilmelilerdir:   * İsim ve ülke * Nerede çalıştıkları * Ne iş yaptıkları * Bir eğitimci olarak deneyimleri * Haklarında ilginç bir şey * “Bilgi sorularına” cevaplar: | |
| **Slayt 21** | “Bilgi soruları”, etkileşim oluşturmak ve eğitimcilerin teknoloji ve sanal suçlar kategorilerinin her birinde katılımcıların bilgi ve deneyimleri hakkında daha fazla bilgiye sahip olmaları için tasarlanmıştır. Bunlar, aşağıdaki slaytta belirtilmektedir. Katılımcılara, her bir kategorideki bilgi düzeylerini en iyi şekilde derecelendirdiği sorulmalıdır.  Eşler, aynı soruyu birbirlerine sormalıdır. Daha sonra yeni çalışma arkadaşlarını sınıfın geri kalanına tanıtmalıdır. Eğitimci, öğrenciler hakkında sunulan bilgileri not almalıdır. | |
|  | **Uygulama Alıştırmaları (eğer varsa)**  Bu oturumdaki tek uygulama alıştırması, öğrencilerin ve eğitimcilerin tanıştırılmasıdır ve bunun şartları önceki bölümde belirtilmektedir. | |
|  | **Bilgi Kontrolü**  Bu oturumda bilgi kontrolü yapılmayacaktır. | |
| **Slayt 23** | **Özet**  Eğitimci, oturumun öğrenme amaçlarının öğrenciler tarafından anlaşılmasını sağlamak için aşağıdaki konulardaki bilgileri özetlemelidir / sınamalıdır. Oturum sırasında uygun zamanlarda sorular için zaman ayırılmalıdır. | |

|  |  |  |
| --- | --- | --- |
| Ders 1.1.2 Sanal suçlara giriş | | **Süre: 120 Dakika** |
| **Gerekli kaynaklar:**   * Windows 7 ve Office 2010 kurulu olan bir dizüstü bilgisayar ya da PC * Projektör * PowerPoint Sunum | | |
| **Amaç:**  Bu dersin amacı, hem hukuki açıdan hem de yeni gerçeklikler açısından katılımcılara sanal suçlara dair genel bir bakış sunmaktır. Farklı ülkelerdeki arka plan senaryosunu ve uluslararası düzeydeki hukuki çerçeveyi kapsayacaktır. | | |
| **Hedefler:**   * Ders esnasında sanal suçların ne olduğu ve bunlar hakkında neden endişelenilmesi gerektiği katılımcılara açıklanacaktır. Sanal suçlara ilişkin tehdit, eğilim ve araçlar, hakim ve savcıların karşılaşacağı zorluklar olarak ifade edilecektir. Ayrıca bu olguya verilen ulusal ve uluslararası karşılıklar da bu oturumda açıklanacaktır. * Dersin sonunda katılımcılar, “sanal suçlar” ifadesinin içerdiği gerçeklikleri tanıyabilecek ve çoğu mevzuata ve uluslararası standartlara göre suç türleri olarak değerlendirilen kavramları anlayabilecektir. * Oturumda, sanal suçlarla ilgili en son gelişmelerden sonra temel ceza hukuku hükümleri ele alınacak ve Budapeşte Sözleşmesi’ne ve Avrupa Birliği düzeyindeki hukuki çerçeveye göre bu suçları tanımlamak için kullanılan temel faktörlerden bazıları değerlendirilecektir. * Bu son noktaya ilişkin olarak, ulusal mevzuat ve özellikle de Budapeşte Sözleşmesi olmak üzere uluslararası mevzuat arasında uyum sağlanmasına yönelik ihtiyaç ve bunun avantajları bu oturumda vurgulanacaktır. | | |
| **Slayt no.** | **İçerik:** | |
|  | **Giriş**  Bu dersin amacı, hem hukuki açıdan hem de yeni gerçeklikler açısından katılımcılara sanal suçlara dair genel bir bakış sunmaktır. Farklı ülkelerdeki arka plan senaryosunu ve uluslararası düzeydeki hukuki çerçeveyi kapsayacaktır. | |
| **Slayt 2** | **Gündem**  Sunumun 1. Bölümünde bilgi toplumunun yeni gerçeklikleri anlatılacak ve ağlarda ortaya çıkan yasa dışı faaliyetlere değinilecektir.  Sunumun 2. Bölümünde bazı uluslararası örgütlerin sanal suçlara tarihsel yaklaşımlarından bazıları belirtilecektir.  Sunumun 3. Bölümünde sanal suç kavramının içerdiği gerçekliğe ulaşmaya çalışılacaktır.  Sunumun 4. Bölümünde Budapeşte Sözleşmesi’nin ne olduğu açıklanacak ve sanal suçlarla mücadelede bu bağlayıcı uluslararası dokümanın önemi vurgulanacaktır.  Sunumun 5. Bölümünde bugünlerde önemli olan yasa dışı çevrimiçi faaliyetlerden bazılarına değinilecektir.  Sunumun 6. Bölümünde tüm sunumun başlıca konuları ele alınacaktır. | |
| **Slayt 3** | **Oturum Hedefleri**  Bu oturumun amacı, sanal suçlarla ilgili konuları genel bir bakış açısıyla ya da bir giriş olarak sunmaktır.  Sanal suç kavramı açıklanacak ve endişe edilmesini gerektiren sebepler tartışılacaktır. Sanal suçlara ilişkin başlıca tehdit, eğilim ve araçların yanı sıra bu olguya verilen ulusal ve uluslararası karşılıkları tartışacağız.  “Sanal suç” ifadesinin içerdiği anlamlara genel bir bakış sunulacaktır. Çoğu mevzuata ve uluslararası standartlara göre suç türleri olarak değerlendirilen kavramlardan bazılarının tanımı tartışılacaktır.  Tartışılacak en önemli konulardan bir tanesi de temel ceza hukuku hükümleri ve Budapeşte Sözleşmesi’ne ve Avrupa Birliği düzeyindeki hukuki çerçeveye göre bu suçları tanımlamak için kullanılan temel faktörlerden bazıları ile ilgilidir.  Ulusal mevzuat ve özellikle de Budapeşte Sözleşmesi olmak üzere uluslararası mevzuat arasında uyum sağlanmasına yönelik ihtiyaç ve bunun avantajlarının vurgulanması da önemlidir. | |
| **Slayt 4** | **1. Bölüm – Bilgi toplumu ve sanal suçlar** | |
| **Slayt 5 - 7** | İletişim ağları aracılığıyla bilgilerin edinilmesi ve yayılmasına dayalı sosyal ve ekonomik bir gelişim modeli olan bilgi toplumu, insanların günlük hayatına, iş yerlerine, evlerine ve birçok boş zaman faaliyetine nüfuz etmiştir.  Bu sosyal ve ekonomik çevrede dünyanın farklı kısımlarında yer alan insanlar arasındaki fiziksel mesafeler kaybolmuştur. Bazı çok iyi bilenen istisnalarla, bu yeni “açık dünyada” Devletlerin siyasi sınırları İnternet gezginleri arasında söz konusu değildir. Burada herkes, bilgileri nerede depolandığından bağımsız olmak üzere demokratik olarak edinebilir. Bu ayrıca tüm ekonomik aktörler arasında rekabet anlamına da gelir.  Bilgi serbest bir şekilde herkese açıktır. İnternet kullanıcıları, ağlar üzerinde egemenlik olmadığını hisseder. | |
| **Slayt 8** | İnternetin kullanımı dünyadaki her yere ve tüm insanlara yayıldığından suç artmaktadır ve suçlular yeni olağan suç faaliyetleri keşfetmektedir. Ağlar aracılığıyla işlenen suçlar, en ulusaşırı nitelikli suçlardır.  Bu özellik, bu suç faaliyetlerini araştıranlar için önemli zorluklar doğurmaktadır: dünyanın öteki ucunda kanıtlar, eğer derhal koruma altına alınmazsa kaybolabilir ve emniyet güçleri de siyasi sınırlara uygun davranmalıdır. Ayrıca suç soruşturmalarında uluslararası yardım talep etmek için hukuki işlemleri uygulamalı ve kamusal kanallardan faydalanmalılardır. | |
| **Slayt 9** | Bu bağlamda uluslararası yaklaşım elzemdir. Çok uluslu veya uluslararası yaklaşım, yalnızca ulusal veya hatta bölgesel bir yaklaşımdan daha faydalıdır ve olgunun küresel düzeyde anlaşılması, daha geniş bir boyut katar. Suç soruşturmalarında başarılı sonuçlar almak için emniyet güçleri (polis ve savcılık kurumları) arasındaki uluslararası işbirliği çok önemlidir. | |
| **Slayt 10** | Tüm gözlemciler, sanal suçların küresel bir olgu olduğu ve konusunda hemfikirdir ve küresel ağların sınırlar içermemesine ilişkin tek yeterli yaklaşım, yerel çalışmaların, sanal suçların küresel düzeyde kolaylaşması sorununu ele alabilecek özel uluslararası işbirliği türleri ve kanallarıyla tamamlandığı ortak yaklaşımdır.  Şu çok açıktır ki sanal suçlar, küresel boyutlara sahip küresel bir olgudur. Genellikle her yasa dışı faaliyet, birçok bölgesel bağlantıya sahiptir: Normalde failler, belirli bir ülkenin yargı alanlarında yer alırken bu faillerin eylemleri diğer birçok ülkedeki bilgisayarlara ve kurbanlara ulaşır.  Bu, diğer modern suç türlerinin ortak bir özelliğidir ancak genel olarak sanal suçların ve *e-kanıtların* doğasında vardır. Başta İnternet olmak üzere iletişim ağlarının genişlemesi sebebiyle dünyadaki herhangi bir ülkenin bu suç sorununa karşı tek başına hareket etmesi imkansızdır. | |
| **Slayt 11** | Modern toplumlar bilgi teknolojilerine bağımlıdır. Devletler, vatandaşlar ve ekonomiler şu anda İnternete bağlıdır. Bu, iletişim ağları içinde ağları kullanarak ya da ağlara karşı yürütülen ve yeni ortaya çıkan yasa dışı faaliyetler için çok verimli bir alandır. | |
| **Slayt 12** | Sanal suçlar her yerde *bilgisayar korsanlığı* ya da kötü amaçlı *yazılımların* (başta virüs ve solucanlar olmak üzere) yayılması veya *ortamlarda* bilgisayar saldırıları (*DoS* veya *DDos*) gibi olgularla tanımlanır. Ancak bugünlerde her sıradan yurttaşın bildiği gibi ağlarda çoğunluğu kazanç elde etme amacı taşıyan başka birçok yasa dışı faaliyet mevcuttur (Örneğin, normal dolandırıcılık ve bilgisayar dolandırıcılıkları). Ayrıca herkes, suç işlemek ya da suçların işlenmesini kolaylaştırmak için sanal ortamın ya da sanal ekosistemin kullanılmasına ilişkin imkanları bilir. | |
| **Slayt 13** | Hukuki ve akademik literatürde henüz tanımlanmamış olsa da “*sanal ortam*” ifadesi her geçen gün daha karmaşık bir hale gelmektedir. Teknoloji, ağlarda iletişi kurabilen ve verileri aktarıp kaydedebilen cihazların türlerini ve sayısını artırmaktadır. | |
| **Slayt** **15 ve 16** | **2. Bölüm - Uluslararası örgütler ve sanal suçlar**  Birçok uluslararası örgüt yıllardır sanal suçlar ve elektronik kanıtlarla ilgili meselelerle uğraşmaktadır. | |
| **Slayt 17 - 20** | Birleşmiş Milletler, sanal suçların tartışıldığı ortamlardan bir tanesidir. Birleşmiş Milletler Genel Kurulu, *Bilgi Teknolojilerinin Suç Amaçlı Kötüye Kullanımıyla Mücadele* ile ilgili resmi kararları 2000 yılından beri almaktadır (bunlardan ilki, Genel Kurul tarafından kabul edilen 55/63 no’lu Karardır. Bu Karar, bilgi teknolojilerini suç amaçlı kötüye kullanımı ile ilgilidir ve 4 Aralık 2000 tarihinde 81. genel kurul toplantısında kabul edilmiştir).  Bu resmi kararlar, bir Üye Devletin belirli faaliyetleri suç olarak kabul etmek ve sanal suçlular için *güvenli limanları* ortadan kaldırmak amacıyla yerel düzenlemeleri kabul etmesini sağlamaya yönelik ihtiyaca işaret eder.  “Küresel bir sanal güvenlik kültürünün oluşturulmasına” dair 64/211 no’lu (Mart 2010) BM Genel Kurul Kararı, ulusal çalışmalarla kritik bilgi altyapılarının korunması için ihtiyari bir öz değerlendirme aracı içerir. Kararda diğer konular arasında Devletlerin Budapeşte Sanal Suçlar Sözleşmesi gibi çerçeveleri dikkate alan suç mevzuatların kabul etmesi tavsiye edilmektedir.  Her beş yılda bir BM, Birleşmiş Milletler Suç Önleme ve Ceza Adaleti Kongresini düzenler. Bangkok’ta yapılan 2005 Kongresi ve Salvador’da (Brezilya) yapılan 2010 Kongresinde teknik yardım ve kapasite inşasına yönelik ihtiyaç konusunda anlaşmaya varılmıştır.  Yeni anlaşmalar geliştirmeye yönelik teklifler hakkında henüz fikir birliğine varılmamıştır. | |
| **Slayt 21** | Ekonomik Kalkınma ve İşbirliği Örgütü (OECD), sanal suçlar olgusuna ilişkin endişeleri Birleşmiş Milletler ile paylaşmaktadır. Ancak, OECD farklı bir yaklaşım geliştirmiştir. 1983’ten beri OECD, sanal suçlarla ilgili ulusal kanunlara yönelik ihtiyaç üzerinde çalışmaktadır ve buna ilişkin tavsiyeler yayınlamaktadır. OECD, uluslararası düzeyden ulusal düzeye benzer suç çerçeveleri içinde aynı suç gerçeklerinin nitelendirilebileceğini ifade etmektedir. | |
| **Slayt 22** | G8 Ülkelerinin yaklaşımı da birkaç adım ileriye giderek daha proaktif seçenekleri değerlendirmektedir. G8, uluslararası işbirliği senaryosunda bir referans haline gelmiş bir irtibat noktaları ağı oluşturmuştur. Bu, temelde gerektiğinde ulaşılabilecek ve acil adımların atılmasını kolaylaştırabilecek isimler listesidir.  G8, sanal suç konularının ele alınmasında bir öncü konumundadır ve Avrupa Konseyi’nin yanı sıra bu, sanal suçlarla mücadelede uluslararası düzeyde bugüne kadar geliştirilmiş en önemli çalışmadır. | |
| **Slayt 23 ve 24** | Avrupa Birliği (AB) de, sanal suçlara karşı tetikte görünmektedir. 2005’te AB, bilgi sistemlerine yönelik saldırılara ilişkin bağlayıcı bir doküman olan 24 Şubat 2005 tarihli Konsey Çerçeve Kararı 2005/222/JHA[[3]](#footnote-3)’yı uygulamaya koymuştur. Bu Çerçeve Karar, tüm Üye Devletlere belirtilen bazı suç eylemlerinin suç olarak kabul edilmesini dikte eder: bilgi sistemlerine yasa dışı erişim, yasa dışı sistem müdahalesi ve yasa dışı veri müdahalesi. Karar, ayrıca azmettirme, yardım ve yataklık ile teşebbüs eylemlerine atıfta bulunan kuralları da içerir.  Ayrıca, uluslararası işbirliğine ilişkin olarak Çerçeve Karar, tüm Avrupa Birliği Üye Devletlerinin haftada yedi gün 24 saat erişilebilir irtibat noktalarından oluşan mevcut ağdan faydalanılmasının sağlanması gerektiğini de ifade eder.  Çerçeve Kararı 2005/222/JHA, şu anda Ocak 2011’den beri revize edilmektedir (ilk kamu taslağı Ekim 2011’de yayınlanmıştır). | |
| **Slayt 25** | Ayrıca Avrupa Güvenlik ve İşbirliği Teşkilatı (OSCE) tarafından geliştirilen, sanal suçlara dair çalışmanın da dikkate alınması önemlidir.  OSCE, teşkilatın üyelerine tavsiyeler yayınlamaktadır. Karar No. 7/06 ile OSCE, katılımcı Devletlerin Budapeşte Sanal Suçlar Sözleşmesi’ne taraf olmayı dikkate alması gerektiğini ifade etmiştir. Bu karar ayrıca katılımcı Devletleri, G8 Devletleri tarafından yönetilen 24/7 Bilgisayar Suç Ağına katılmaları ve sanal ortamın suç amaçlı kötüye kullanımı ile mücadeleye ilişkin olarak uluslararası emniyet güçlerinin işbirliğinin düzene sokulması amacıyla uygun bir irtibat noktası belirlemeleri konusunda teşvik etmiştir. | |
| **Slayt 26** | Avrupa Konseyi, 1980’lerden beri sanal suçlar sorunuyla uğraşmaktadır. Hazırlık çalışmaları ve bağlayıcı olmayan hukuk tavsiyeleri, hukuki olarak bağlayıcı bir uluslararası anlaşmanın görüşülmesi kararına yol açmıştır: Budapeşte Sanal Suçlar Sözleşmesi (bu anlaşma daha sonra tartışılacaktır).  Avrupa Konseyi’nin yaklaşımı, aşağıdaki üçgenden oluşmaktadır:   1. Budapeşte Sözleşmesi gibi standartlar 2. Sanal Suçlar Sözleşmesi Komitesi tarafından uygulamanın takibi ve “izlenmesi” 3. Ülkelerin ceza yargılaması kapasitelerini oluşturmalarına yardımcı olacak teknik işbirliği. | |
| **Slayt 28 ve 29** | **3. Bölüm – Sanal suçlar nedir?** | |
| **Slayt 30** | **Bir kurban olarak teknoloji**  Bir suçun hedefi olarak teknoloji – Bu, gerçek “bilgisayar suçu” olarak görülmektedir ve bilgisayar korsanlığı, hizmeti engelleme saldırıları ve virüslerin dağıtılmasını içerir. | |
| **Slayt 31** | **Suça destek olarak teknoloji**  Suça destek olarak teknoloji, örneğin sahte dokümanlar üretmek, ölüm tehdidi ya da şantaj mesajları göndermek veya çocuk istismarı görüntüleri gibi yasa dışı materyalleri oluşturmak ve dağıtmak üzere geleneksel suçların işlenmesine yardımcı olmak için bilgisayarların ve diğer cihazların kullanılması durumudur. | |
| **Slayt 32** | **Bir iletişim aracı olarak teknoloji**  Bir iletişim aracı olarak teknoloji, örneğin şifreleme teknolojisinin kullanımıyla suçluların tespit edilme şansını azaltmak için birbirleriyle iletişim kurarken teknolojiden faydalanmasıdır. | |
| **Slayt 33** | **Bir depolama cihazı olarak teknoloji**  Bir depolama cihazı olarak teknoloji, diğer kategorilerin herhangi birinde kullanılan cihazlarda bilgilerin kasıtlı ya da kasıtsız olarak depolanmasıdır ve kurbanların, tanıkların veya şüphelilerin bilgisayar sistemlerinde tutulan verileri içerir. | |
| **Slayt 34** | **Bir suç tanığı olarak teknoloji**  Bir suç tanığı olarak teknoloji, bilişim cihazlarında toplanan kanıtların, açık biçimde ilgili olmadıkları kanıtları desteklemek üzere, örneğin, bir şüphelinin suçun işlendiği anda orada olmadığını ispatlamak üzere sunduğu kanıtları veya bir tanık tarafından öne sürülen bir iddiayı ispatlamak ya da çürütmek için kullanılabildiği zaman görülebilir. | |
| **Slayt 35** | **Teknoloji suçu?**  Bu slayt katılımcıların bugüne kadar anlatılmış olanları anladıklarını kontrol etmek üzere bir özet şeklinde kullanılabilir. Eğitmenin sadece başlığı okuyarak başlayıp, katılımcılardan Sanal Suç dediğimizde hangi suç türünü kastettiğimizi belirtmelerini istemesi tavsiye edilmiştir. Katılımcılardan gelecek soruları cevaplamak için veya örnek olarak kullanılmak üzere Budapeşte Sözleşmesi’nde açıklanan farklı suç türlerinin eğitmen tarafından önceden anlaşılmış olması faydalı olacaktır. | |
| **Slayt 36** | William Gibson 1984’te bir bilim kurgu romanı olan *Neuromancer’da,* İnternet ve diğer ağlara atıfta bulunarak siber uzay kelimesini kullandığından beri aynı önekle kullanılan benzeri ifadelerin sayısı artmaktadır. *Siber/sanal suç* dabunlardan biridir. Yaklaşık otuz yıl sonra da sanal suçlara dair literatürün genişlemesine rağmen hukuki metinlerde sanal suçun tam doğru bir tanımı üzerinde bir fikir birliğine varılamamıştır.  Sanal suçların gerçekten ceza hukukunun yeni ve ayrı bir alanı mı olduğu ya da sadece dijital ortamlara atıfta bulunan ceza hukuku hükümleri mi olduğu konusunda da anlaşmaya varılamamıştır. | |
| **Slayt 37 - 44** | Ancak, sosyolojik olarak konuşmak gerekirse sanal ortamlardaki suçlar, halihazırda önemli ve özerk bir gerçekliktir. Tüm Avrupa’da polis düzeyinde özel araştırma birimleri ve bazı özel savcılık birimleri vardır. Uluslararası kamu kuruluşları ve özel şirketler, iletişim ağları aracılığıyla ya da bu ağlar içinde işlenen yasa dışı ve zararlı suç eylemlerinin sonuçları hakkındaki endişeleri büyümektedir.  Hukukçular bu yeni gerçekliği ele almak isteğinden sanal suç ifadesi hakkında bir fikir birliğine varılamaz. Bazı yazarlar *bilgisayar suçlarına* ya da *bilişim suçlarına* atıfta bulunur. Diğerleri ise *yüksek teknoloji suçları* terimini tercih eder. Hepsinde konunun fazlasıyla genişletilmesi ya da uygun olmayacak şekilde kısıtlanması riski vardır.  Bilgisayarları içeren suçların ille de “yüksek teknoloji” içermesi gerekmez. Sanal ortamdaki suç faaliyetlerinin çoğu, göreceli olarak basit yöntemler kullanır ve bunların soruşturulmasında göreceli olarak daha az teknolojik sorun arz eder. Ancak, bu belki de yanlış bir sorudur çünkü bugünlerde herkes, bir bilgisayar sistemi aracılığıyla ya da içinde meydana gelen yeni bir sosyal gerçeklik/suç gerçekliği söz konusu olduğuna ilişkin olarak hemfikirdir.  Sanal suç, genellikle hem dar hem de daha geniş bir anlamda tanımlanır: normalde bu ifade, bir bilgisayar ya da ağın bir suçun temel bir parçası olduğu bir suç faaliyetini tarif etmek için kısıtlı bir şekilde kullanılır; ancak sanal suç, aynı bilgisayar ya da ağların yasa dışı bir faaliyeti mümkün kılmak için kullanıldığı diğer geleneksel suçları içerecek şekilde de kullanılır.  Bu bakış açısına göre, bilgisayarın suç faaliyetinin (örneğin, istenmeyen e-postalar gönderme, eşler arası ağlarda işlenen telif hakkı suçları) bir aracı olduğu sanal suçlar hakkında konuşmaktayız; bu, bilgisayar ya da ağın, yetkisiz erişim, kötü amaçlı kod vb. gibi bir suçun hedefi olduğu anlamdaki sanal suçtur; bilgisayar ya da ağın telekomünikasyon dolandırıcılığı gibi bir suç faaliyetinin yeri olduğu sanal suçtur; ve son olarak bilgisayar ya da ağların kullanımı yoluyla kolaylaştırılan sanal suçtur (örneğin, *Nijerya dolandırıcılıkları, bilgisayar korsanlığı, şifre avcılığı*, çocuk pornografisi, kimlik hırsızlığı vb.). İlk kategoride suçu işlemek için bilgisayar gerekirken son kategoride suç başka yollarla da işlenebilir ancak bilgisayar bunu kolaylaştırmaktadır.  Bu gerçekliklerden çok da uzak olmayan bazı *yeni çağ* suçları, ayırt edici özellik olarak yalnızca dijital ortamlarda işlenebilirliği içeren yeni geleneksel suç yöntemleridir.  Aslında bunlar, doğaları gereği sanal dünyanın dışında gerçekleşemez ve içinde meydana gelir. Bilgisayar dolandırıcılığı veya bilgisayarda sahte belgeler üretme bunun örneğidir.  Bazı diğer suç ihlalleri, bilgisayarların *ortam* olarak kullanılmasına rağmen başka şekillerde işlenen aynı suç türünden teorik olarak ayırt edilemeyen ve bir bilgisayar sistemi aracılığıyla işlenen suçlardır. Bunlar *çevrimiçi* suçlar olsa dahi bu özellik, suçu yeni bir suç türüne dönüştürmez. Dogmatik olarak bunların geleneksel ceza hukuku suçlarından ayırt edilmesini sağlayacak bir şey yoktur. Örnek olarak, elektronik bir gazete tarafından işlenen hakaret suçu ya da e-posta ile iletilen bir tehdit mesajı veya çevrimiçi bankacılık kullanılarak gerçekleştirilen para aklama suçu verilebilir.  Bu bağlamda daha da temel bir kategori söz konusudur: dijital kanıtlar meydana getiren geleneksel *çevrimdışı* suçlar. Örnek olarak “vurup kaçma” şakasını cep telefonu ile kaydeden ve bunu Youtube’de yayınlayan bir saldırgan verilebilir. Bu olay bir *sanal suç* olarak değerlendirilemese de sanal suçlarla ilgili aynı kanıt ve soruşturma konuları söz konusudur.  Ancak, normalde sanal suç olarak tanımlanan suç türü, bilgisayar ortamları ya da sistemlerini hedef alan suçların dahil olduğu kategoridir. Bu tür suçların klasik bir örneği olarak veri müdahalesi, hizmeti engelleme saldırıları gibi sistem müdahalesi veya hatta yasa dışı erişim verilebilir. Tüm bu ihlaller, bilgisayar verileri ya da bilgisayar sisteminin gizliliği, bütünlüğü ya da kullanılabilirliğine zarar veren ve bilgisayar sistemlerine karşı işlenen suçlardır.  Gerçek suç senaryolarında çoğunlukla bu kategorilerden birkaçı bir arada bulunacaktır. Bir suçlu, örneğin para ödemediği için (bilgisayarların araç olarak kullanıldığı yeni bir şantaj türü) bir şirketin web sitesine hizmeti engelleme saldırısı (bilgisayar sistemine karşı işlenen suç) düzenleyerek şirketi tehdit edebilir ve tehdit e-posta ile iletilir ancak pek tabii normal bir mektupla da gönderilebilirdi.  Ancak gerçek anlamda suç türleri artmaktadır ve geniş bir çeşitliliğe sahiptir: şifre avcılığı (phishing) ya da botnet kullanımı gibi tipik sanal suçlar artmakta ve kar amacı güdülen yaratıcı sanal suçlar koleksiyonu büyümektedir. Ayrıca, yazılım korsanlığı ve fikri mülkiyet hakları ile ilgili suçlar da önemli boyutlardadır. Çocuk pornografisi materyallerinin yayılması artmaktadır; İnternette aklanan paraların değeri de yükseliştedir. Genel olarak, organize suç örgütleri ve terörist örgütler gibi yasa dışı gruplar tarafından sanal imkanların kullanımında her gün artış yaşanmaktadır. | |
| **Slayt 46 - 49** | **4. Bölüm – Budapeşte Sanal Suçlar Sözleşmesi** | |
|  | Budapeşte Sözleşmesi olarak da bilinen Avrupa Konseyi’nin Sanal Suçlar Sözleşmesi (ETS 185) 23 Kasım 2001’de Budapeşte’de imzaya açılmış ve Temmuz 2004’te yürürlüğe girmiştir.  Nisan 2013 itibarıyla 39 ülke (Avrupa Devletleri, Avustralya, Dominik Cumhuriyeti, Japonya ve ABD) Budapeşte Sözleşmesi’ne taraftır. 10 ülke sözleşmeyi imzalamıştır (Avrupa ülkeleri, Kanada ve Güney Afrika) ve 8 ülke de sözleşmeyi kabul etmeye davet edilmiştir (Arjantin, Şili, Kosta Rika, Meksika, Fas, Panama, Filipinler ve Senegal). Başka ülkeler tarafından yöneltilen katılım talepleri de devam etmektedir.  Başka birçok ülke de Budapeşte Sözleşmesi’ni yerel mevzuata yönelik bir rehber olarak kullanmaktadır.  Anlaşma, bunu iç hukukuna entegre etmeye ve işbirliğine girmeye hazır tüm Devletler tarafından imzalanmaya açıktır.  Sözleşme, Devletlerin şunları yapmalarını şart koşar:   * Bilgisayar sistemlerine karşı (yasa dışı erişim, yasa dışı ele geçirme, veri ve sistem müdahalesi vb.) ve bilgisayarlar aracılığıyla (dolandırıcılık, çocuk pornografisi ve fikri mülkiyet hakları suçları gibi) işlenen suç eylemlerinin suç olarak kabul edilmesi. Önemli: anlaşma, teknoloji nötrdür ve teknoloji ya da teknikleri değil suçun işlenme şeklini kapsar (şifre avcılığı değil dolandırıcılık, bilgisayar korsanlığı değil yasa dışı erişim, dağıtık hizmet engelleme saldırıları değil sistem müdahalesi vb.). * Emniyet güçlerinin elektronik kanıtları güvence altına alması için gerekli araçların temin edilmesi (arama ve el koyma, hızlandırılmış koruma vb.). Önemli: bu tedbirler yalnızca sanal suçlar için değil bir bilgisayar sistemindeki elektronik kanıtları içeren tüm suçlar için geçerlidir. * Acil ve geçici tedbirler ve karşılıklı resmi yardımın yanı sıra 7/24 irtibat noktalarının kullanımıyla etkili uluslararası işbirliğine girilmesi.     Özellikle de usul hukuku araçları olmak üzere tüm bu tedbirler, insan hakları ve hukukun üstünlüğü şartlarını karşılamak içindir. Dolayısıyla Madde 15, (şartlar ve tedbirler) özellikle önemlidir.  Genel olarak, Budapeşte Sözleşmesi, Hükümetlerin bireyleri (sanal) suçlara karşı korumaya ilişkin müspet yükümlülüklerini yerine getirmesine ve aynı zamanda sanal suçlara karşı adımlar atarken bireylerin haklarına saygı göstermesine olanak tanır.  Bugüne kadar elde edilen kazanımlar:   * Dünya çapında yasal reformlar süreci * Ceza yargılaması tedbirlerinin artırılması * Taraflar arasında güven ve işbirliğinin artması * Küresel destek, küresel etki: 56 ülke onayladı, imzaladı, katılmaya davet edildi. En az 50 ülkeyle daha işbirliği * Kapasite oluşturmaya yönelik katalizör * Özel sektörde artan hukuki kesinlik ve güven * Siberuzay için davranış normlarının önemli bir unsuru * Siberuzayda insan hakları ve hukukun üstünlüğüne katkı * Sizi ve haklarınızı koruma | |
| **Slayt 51** | **5. Bölüm – Bazı yasa dışı çevrimiçi faaliyetler**  Bu bölümün amacı ağlarda geliştirilen bazı suç faaliyetlerini çok kısa bir şekilde tanımlamaktır. | |
| **Slayt 52** | Şifre avcılığı (phishing), birinin kendi kişisel bilgilerini göndermeye ikna edilmesi için kullanılan bir tekniktir. Bu bilgiler daha sonra hırsızlık ya da dolandırıcılık için kullanılabilir. Normalde failler, şifre ve diğer erişim belgeleri de dahil olmak üzere kişisel bilgileri elde ettikleri kurbanları kandırmak için e-posta mesajları gönderir. Bazen bu teknik, kullanıcıları kötü niyetli ve sahte web sitelerine yönlendirmek için de kullanılır. | |
| **Slayt 53** | SPAM (istenmeyen e-posta) gittikçe büyüyen bir sorundur. Milyonlarca istenmeyen e-postanın gönderilip yayılmasını içerir. Bu mesajları alanlar bundan kaçınamaz. Bazen bu mesajlar yalnızca pazarlama amaçlarıyla gönderilir. Ancak çoğunlukla bilgisayarlara bulaşacak kötü amaçlı yazılımların taşıyıcılarıdır.  Normalde mesajı gönderen, kurbanın tanımadığı ve mesajın gönderilmesi için bir talepte bulunmadığı ya da herhangi bir yetki vermediği bir kişidir. | |
| **Slayt 54** | “Kötü amaçlı” (malicious) ve “*yazılım*” (software) kelimelerinin birleşimi, genellikle bir bilgisayar sisteminin sahibi ya da kullanıcısının izni olmadan bu sisteme erişmek ya da zarar vermek amacıyla tasarlanan yazılımları ifade eden “kötü amaçlı yazılım” (malware) terimini oluşturmuştur. Kurban, e-posta ekleriyle ya da mesajlardaki resimlerle bilmeden bu kötü amaçlı yazılımları edinebilir.  Bu yazılımlar normalde saldırgan yazılımlardır. Kurbanın bilgisayarına onun izni olmadan yerleştirilip saldırgan işlem veya faaliyetler gerçekleştirirler. | |
| **Slayt 55** | Virüsler kötü amaçlı yazılımların özel bir örneğidir. Bir virüs genellikle kendini bir dosyadan diğerine kopyalayabilen ve belirli bir sisteme (bir sabit disk ya da başka bir veri depolama ortamı) yerleşebilen bir yazılımdır. Normalde virüs bulaşan dosya kopyalandığında ya da çalıştırıldığında yayılır. Tabii ki tüm bunlar, kurbanın izni ve hatta bilgisi olmadan ve bilgisayar sisteminde hasara sebep olmak amacıyla yapılmaktadır. | |
| **Slayt 56** | Solucan virüse çok benzerdir. Virüs gibi solucan da kendini kopyalama ve belirli bir sisteme yerleşerek onun kaynaklarını tüketme özelliğine sahiptir. Ancak bir ağ içinde yayılması ve bir dosyaya eklenme ihtiyacı duymaması açısından virüsten farklıdır. | |
| **Slayt 57** | Reklam (destekli) yazılımı da kötü amaçlı bir yazılımdır. Kullanıcının izni ya da müdahalesi olmadan otomatik olarak görüntülenen ya da ticari reklamlar indiren bir yazılımdır. Bazen diğer yazılımlarla birlikte ve ayrıca ücretsiz indirmeler aracılığıyla dağıtılırlar.  Reklam yazılımlarının bazı türleri daha tehlikelidir çünkü sistemi izleyerek İnternette ziyaret edilen siteler ve kullanıcı tercihleri gibi bilgileri edinirler. | |
| **Slayt 58** | Kötü amaçlı yazılımların en tehlikeli türlerinden birisi, sistemin kullanıcı tarafından kullanımını izlemek amacıyla kullanıcının izni olmadan sisteme yüklenen yazılımlara denilen casus yazılımlardır. Casus yazılımlar sistemin kullanıcısı hakkında bilgiler toplar. Yazılım, izleme faaliyetinden sonra otomatik olarak bu bilgileri üçüncü taraflara gönderir. Bu yazılımların amacı kurbanın bilgisayarında saklanıp bilgileri başka birine iletmektir. | |
| **Slayt 59** | Truva (Truva atı), Odysseus tarafından inşa edilip Truva şehrinin kapılarının içeriden açılması için şehre verilen ünlü attan esinlenilerek bu virüse adını vermiştir. Bu kötü amaçlı yazılım kullanıcının bilgisi olmadan kullanıcının sisteminde istenmeyen işlevler gerçekleştirir. Bu kötü amaçlı yazılım türü, verilerin yok edilmesine, güvenlik yazılımlarının etkisiz hale getirilmesine, bilgisayara uzaktan erişimin kolaylaştırılmasına (yetkisiz birilerinin bilgisayara erişim sağlaması için) ya da diğer kötü amaçlı yazılımların indirilip yüklenmesine sebep olabilir.  Truva Savaşı’nın ünlü atı gibi bu yazılım da bilgisayarı gizlice dışarıdan girilmeye açık hale getirmek üzere tasarlanmıştır. | |
| **Slayt 60** | Botnet (*robot ağı*), yasa dışı faaliyetlerde kullanmak amacıyla bir kişi ya da kurum tarafından kontrol edilen gizliliği ihlal edilmiş bilgisayarlar (*zombiler*) ağına verilen isimdir.  Bir botnet, sahibinin gönderdiği kötü amaçlı yazılımların sebep olduğu enfeksiyonla kurulur. Tüm enfekte bilgisayarlar, işlemlerin ağ içinde otomasyonunu mümkün kılan yazılım tarafından kontrol edilir. Ağın sahibi ağın faaliyetini kontrol eder ve gerekli olana kadar ağın pasif bir şekilde kalması talimatını verebilir.  Bir botnet, şahıslara spam ya da kötü amaçlı yazılım gönderme ya da altyapıya saldırma talimatı almış milyonlarca zombi bilgisayardan oluşabilir. Botnetler birçok suç amacına hizmet eder ve bu yüzden “sanal suçların İsviçre çakısı” olarak anılır. | |
| **Slayt 62** | **6. Bölüm - Özet** | |
| **Slayt 63** | Sanal suç nedir ve hakkında neden endişe edilmesi gerekir?  Sanal suçların tehditleri, eğilimleri ve araçları ile bu olguya verilen karşılıklar. *Sanal suç* ifadesi kapsamındaki gerçeklikler ve çoğu mevzuat ve uluslararası standartlar kapsamında suç türleri olarak kabul edilen kavramlar.  Ulusal mevzuat ile başta Budapeşte Sözleşmesi olmak üzere uluslararası dokümanlar arasında uyum sağlamaya yönelik ihtiyaç ve bunun avantajları. | |
|  | **Uygulamalı Alıştırmaları (eğer varsa)** Bu oturum için uygulama alıştırmaları öngörülmemektedir, çünkü bu alıştırmaları vermek için gerekli teknoloji düzeyi ve İnternet erişiminin her yerde mevcut olacağının garantisi yoktur.  Eğitimciler, gelecekte imkanların uygun olduğu bir ortamda verilen eğitimlere alıştırmalar ekleyerek öğrenmeye katkıda bulunmaya çalışabilir. | |
|  | **Bilgi Kontrolü**  Bu eğitimde yukarıdakilere ek olarak özel bir bilgi kontrolü şu anda öngörülmemektedir. Resmi bir değerlendirme talep edilmemiştir. | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ders 1.1.3, 1.2.2 & 1.2.5 - Teknoloji | | | | **Süre: 330 Dakika** |
| **Gerekli kaynaklar:**   * Windows 7 ve Office 2010 kurulu olan bir dizüstü bilgisayar ya da PC * Projektör * İnternet erişimi (varsa) * PowerPoint Sunum * Bilgisayar donanımı örnekleri (varsa) * “Ağ Savaşçıları” adlı video klip | | | | |
| **Amaç:** Bu oturum, hakim ve savcıların görevleri sırasında karşılaşacağı ve suçluların suç işlemek için ve emniyet güçlerinin bu suçları tespit etmek için kullandığı teknolojiler hakkında bilgiler sunmaktadır. Oturumun amacı, katılımcıların görevlerini daha etkili bir şekilde yerine getirebilmeleri için yeterli bilgileri kazanmasını sağlamaktır. | | | | |
| **Hedefler:**  Bu dersin sonunda öğrenciler:   * Bir bilgisayar sisteminin bileşenlerini sayabilecek, * Farklı veri depolama cihaz çeşitlerini tanıyabilecek, * Üssel veri depolama kapasitesinin ceza yargılaması ile ilgili sonuçlarını değerlendirebilecek, * Farklı bilgisayar işletim sistemlerini tanıyabilecek, * Ağların nasıl işlediğine dair temel bilgileri açıklayabilecek * İnternetin işlevlerini açıklayabilecek, * En az 5 büyük İnternet uygulamasını tanıyabilecek, * İnternetin günümüze kadar olan gelişimini açıklayabilecek, * Farklı internet uygulamalarını ayırt edebilecek, * Suçluların çeşitli internet uygulamalarını nasıl kullandıklarını belirleyebilecektir. | | | | |
| **Süre** | **İçerik:** | | | |
| 30 dakika  60 dakika  60 dakika  60 dakika  60 dakika  30 dakika  30 dakika | * Giriş ve açılış (Gündem ve Oturum hedefleri) * Bölüm 1 – Bilgisayarlar nasıl çalışır? * Bölüm 2 – İnternet nasıl çalışır? * Bölüm 3 – İnternet hizmetleri * Bölüm 4 – Diğer ilgili İnternet uygulamaları * Bölüm 5 – İnternet suçları * Bölüm 6 – Özet | | | |
| **Slayt no.** | **İçerik:** | | | |
|  | **Giriş**  **Hakim ve Savcılar için Teknoloji**  Bu oturumun amacı, daha geniş bir programın bir parçası olarak verilecek eğitim materyallerinin geliştirilmesi için eğitimcilere bir taslak sunmaktır. Teknoloji hızla değiştiğinden ve neredeyse doküman yayımlandığı anda ayrıntılı teknik özellikler güncelliğini kaybedeceğinden oturumlar çok kapsamlı olma imkanına sahip değildir. Hakim ve savcıların gördükleri davalardaki teknik konular hakkında yeterli bilgiye sahip olmasının sağlanması, adli sistemin adil bir şekilde yürütülmesi için elzemdir. Bu oturum, teknolojinin ilgili yönlerine ve ceza yargılaması sistemi ile ilişkisine genel bir bakış sunmaktadır. Uygun görülürse eğitimcilerin kullanabileceği bir kaynak olarak bir PowerPoint sunumu hazırlanmıştır.  Ağların nasıl işlediğinin katılımcılar tarafından net bir şekilde anlaşılabilmesi için Warriors of the Net (Ağ Savaşçıları) adlı video klip ek bir kaynak olarak verilmektedir. Bu video www.warriorsofthe.net adresinde şu dillerde yer almaktadır: İngilizce, Almanca, Fransızca, İbranice, Hollandaca, İsveççe, İtalyanca, Portekizce, Danca, Norveççe, Macarca, Çekçe, İspanyolca ve Ukraynaca.  Bu oturum, hakim ve savcıların görevleri sırasında karşılaşacağı ve suçluların suç işlemek için ve emniyet güçlerinin bu suçları tespit etmek için kullandığı teknolojiler hakkında bilgiler sunmaktadır. | | | |
|  | **PowerPoint**  Bu ders planını desteklemek ve eğitimciye bu dersin hedeflerini gerçekleştirmek için kendi materyallerini nasıl oluşturabileceğinin örneklerini sunmak için eğitim notları içeren bir PowerPoint sunumu hazırlanmıştır. Şunun unutulmaması gerekir ki güncel ve katılımcılara hitap eden öğrenme materyallerinin oluşturulması eğitimcinin sorumluluğundadır ve başka bir eğitimci tarafından hazırlanmış materyallere bel bağlanmaması gerekir. | | | |
| **Slayt 2 ve 3** | **Gündem**  Gündem slaytlarında oturumun bölümleri belirtilmektedir ve eğitimci, bu bölümleri işleyerek gerektiğinde belirli öğrenci grupları için önemi olan belirli yönlere dair ayrıntılara girmelidir. Eğitimci, materyallerin nasıl dağıtılacağını açıklamalı ve görüş alışverişi ve sorular için zaman ayırılacağını ifade etmelidir. Eğitimci, bu eğitimin etkileşimli olmak üzere tasarlandığına ve katılımcıların katkıda bulunmalarının beklendiğine vurgu yapmalıdır. Eğitimci, bir değerlendirme yapılıp yapılmayacağını ve uygulanacak geçiş notu hakkında bilgiler de dahil olmak üzere bu değerlendirmenin ne şekilde yapılacağını açıklamalıdır (Bu pilot programda değerlendirme yapılmayacaktır). | | | |
| **Slayt 4** | **Oturum Hedefleri**  Katılımcıların, dersin hedeflerinin neler olduğunu anlaması önemlidir. Bunlar, “akıllı” hedefler olmalı ve slayttaki bilgiler kullanılarak oturum başlamadan önce katılımcılara ayrıntılı bir şekilde açıklanmalıdır | | | |
| **5 – 54 arasındaki Slaytlar** | **1. Bölüm – Bilgisayarlar nasıl çalışır?**  Bu oturumun sonunda katılımcılar:   * Bir bilgisayar sisteminin bileşenlerini sayabilecek, * Farklı veri depolama cihaz çeşitlerini tanıyabilecek, * Üssel veri depolama kapasitesinin ceza yargılaması ile ilgili sonuçlarını değerlendirebilecek, * Farklı bilgisayar işletim sistemlerini tanıyabilecektir. | | | |
| **Slayt 5** | Teknolojinin suçlar üzerindeki etkisinin hakim ve savcılar tarafından tam olarak anlaşılması için kendilerine sunulan teknolojinin nasıl işlediğinin temellerine dair bir anlayış kazanmaları gerekir. Özellikle, en geniş anlamıyla adli bilişim yöntemlerini içeren davalarda bu bilgiler, genel bir bakış sağlayacak ve bilinçli kararların verilmesine olanak tanıyacaktır. Bu oturum, bilgisayarlar, bileşenleri, verilerin depolanması ve cihazlarda depolanan büyük miktarlarda verilerin etkilerine ilişkin olarak temel bir anlayış sunacaktır. Eğitimci bir kez daha bu oturumu olabildiği kadar etkileşimli hale getirmeli ve teknolojinin katılımcıların rolleri üzerindeki etkilerini ve bu kadar büyük miktarlardaki verilerin nasıl yönetilebileceği ve ceza yargılaması sistemine etkili bir şekilde nasıl dahil edilebileceğine dair konuları düşünmeleri için katılımcıları teşvik etmek üzere verilen bilgileri kullanmalıdır.  Eğer mümkünse eğitimci, bu oturumda bahsi geçen donanımların örneklerini katılımcılara gösterilmesi ve tanıtılması için edinmelidir.  Bu oturumda ele alınmayan başka birçok bileşen vardır, ancak dersin amaçları için en önemli olanlar dahil edilmiştir. Eğitim programlarının geliştirilmesi amacıyla burada ele alınmayan bileşenlerin, katılımcıların bilgi düzeyine bağlı olarak açıklanması önerilmektedir. Eğitimin çoğu katılımcısının, örneğin, bir klavye ve farenin ne olduğunu anlaması beklenmektedir ancak eğitimciler, katılımcıların bilgilerini olduğundan fazla görmemelidir. Listeye dahil edilebilecek öğeler şunları içerebilir: yazıcılar, tarayıcılar, web kameraları, modemler, hoparlörler, bilgisayarlı ve görüntülü telefonlar, çeşitli depolama cihazları, ağ bağlantıları ve Firewire ve USB gibi harici portlar.    Bilgisayar donanımları hakkında daha detaylı bilgi için, bu kavramların kolaylıkla anlaşılmasına büyük katkı sağlayacak fotoğraflar içeren şu adrese göz atın: <http://computer.howstuffworks.com/computer-hardware-channel.htm>. Buradaki bilgilerin eğitim programlarında kullanılması teklif edilirse bu bilgilerin sahiplerinden izin almayı unutmayın. | | | |
| **Slayt 6** | Bu slaytın amacı, teknoloji konusunda en bilgili insanların bile teknolojinin getireceği değişiklikleri öngöremediğini göstermektir. Katılımcılar, teknolojinin, onların rolleri üzerindeki etkisini anlamamakta belki de yalnız değildir ve bu slayttaki sözler, ceza yargılaması sistemindeki teknolojiden korkulmaması gerektiği ve bu teknolojinin gerekli tüm tedbirlerle birlikte benimsenmesi gerektiğine inanmaları için onları teşvik edebilir. | | | |
| **Slayt 7** | Eğitimci, bilgisayar bileşenlerinin açıklanmasına başlamadan önce giriş olarak bilgisayarların bağımsız bilgisayarlardan anaçatı uç birimlerle ağlar dünyasına nasıl geliştiğini kısa bir şekilde açıklamalıdır. | | | |
| **Slayt 8** | **Bilgisayar bileşenleri**  Bir bilgisayar, birçok bileşenden oluşur ve hakim ve savcıların bu bileşenlerin isim ve işlevlerini anlaması önemlidir, çünkü bunlar beyanlarda ve kanıtlarda geçecektir.  Her bileşen için kısa bir açıklama şu şekilde verilmektedir: | | | |
| **Slayt 9 ve 10** | * Anakart- Anakart aynı zamanda bilgisayarın sistem kartı olarak da bilinmektedir. Anakart, bir bilgisayarın merkezi devre kartıdır. Diğer tüm bileşenler ve çevre birimleri ona takılır. Anakartın görevi bunların arasında bilgileri iletmektir. Anakart, bilgisayar açıldığında çalıştırılan basit bir yazılım olan BIOS’u (Temel Giriş Çıkış Sistemi) barındırır. Bellek, CPU (Merkezi İşlem Birimi), ekran kartı, ses kartı, sabit disk, disk sürücüleri ve çeşitli harici portlar ve çevre birimleri gibi diğer bileşenler doğrudan ona bağlanır. * Genişletme Portları/Yuvaları – bunlar, bilgisayarın arkasında bulunan, ses kartı, video kartı, kablosuz ağ kartını vb. bağlayabileceğiniz yuvalardır. | | | |
| **Slayt 11 - 13** | * CMOS ve BIOS - CMOS ve BIOS anlam olarak çoğunlukla birbirinin yerine kullanılabilir; BIOS’u yazılım, CMOS’u da bu yazılımı çalıştıran donanım olarak düşünebilirsiniz. Anlamı Bütünleyici Metal Oksit Yarıiletken olan CMOS, genellikle “see-moss” (si-mos) olarak telaffuz edilir. CMOS, bilgisayarda çok düşük seviyeli işlevleri ve çok temel bilgisayar başlatma rutinlerini gerçekleştiren donanımdır. CMOS, bilgisayarın saatini muhafaza etmek gibi şeyler yapar ve BIOS’un görevini yapması için bilgisayar donanımlarının kalanına gerekli arayüzü sağlar. Çalışmak için çok az enerjiye ihtiyaç duyar. Anlamı Temel Giriş Çıkış Sistemi olan BIOS, genellikle “bye-oss” (bay-os) şeklinde telaffuz edilir. BIOS, bir kullanıcının bilgisayarın anakartında, CPU’sunda, belleğinde ya da diğer cihazlarda düşük seviyeli değişiklikler yapmasına olanak tanıyan bir arayüzdür. BIOS ayarları genellikle doğru ayarlanır. Adli bilişim yöntemi olarak BIOS’ta yapılan en yaygın değişikliklerden biri, bilgisayarın ön yükleme (başlatma) için cihazları arama sırasını değiştirmek için yapılır. Bir adli bilişim incelemecisi genellikle bir CD’de yer alan bir yazılımı kullanarak bilgisayarın sabit diskten değil CD’den başlaması için BIOS’u değiştirir ve böylelikle sabit diskten başlanarak ve sabit diske erişilerek verilerin değiştirilmesinden kaçınılmış olur. | | | |
| **Slayt 14** | * Güç Kaynağı – Güç Kaynağı Ünitesi, bir bilgisayarda gücü düzenler ve kasada yer alan bileşenlere dağıtır. Standart güç kaynakları gelen 110V ya da 220V AC’yi (Alternatif Akım) bilgisayarın bileşenlerini çalıştırmak için uygun olan çeşitli DC (Doğru Akım) voltajlarına dönüştürür. Güç kaynakları Watt olarak ifade edilen belirli bir güç çıkışına sahiptir. Standart bir güç kaynağı, genellikle 350 Watt civarında güç dağıtabilir. Bir PC’de ne kadar fazla bileşen varsa güç kaynağından çekilmesi gereken güç de o kadar fazladır. | | | |
| **Slayt 15** | * Merkezi İşlem Birimleri (CPU’lar) – CPU’nun anlamı bir bilgisayar sisteminin Merkezi İşlem Birimidir. İnsanlar çoğunlukla bilgisayarın kasasıyla CPU’sunu karıştırır. Ancak CPU, bilgisayarın dahili bir bileşenidir. Sistemin dışından görülemez. İlk CPU’lar 1960’ların başında kullanılmıştır. 1970’lerin sonunda entegre devrenin kullanılmasıyla daha küçük CPU’ların üretilmesi de mümkün hale gelmiştir. Bu sayede bilgisayarlar odaların tamamını kaplayan büyük ve hantal cihazlardan daha kullanışlı masaüstü ve dizüstü modellere evrilebilmiştir. Bilgisayarın türü ne olursa olsun CPU, program olarak bilinen depolanmış talimatlar dizisini yürüterek çalışır. Çoğu CPU, CPU’nun verileri oldukça hızlı ve art arda bulup getirmesi, şifresini çözmesi, yürütmesi ve geri yazması gerektiğini ifade eden von Neumann mimarisine uygundur. Profesyonel olmayan kişiler için CPU, bilgisayarın beyninden başka bir şey değildir, çünkü bilgisayarın yaptığı şeyler temelde CPU sayesinde gerçekleştirilir. | | | |
| **Slayt 16** | * Bellek – Bilgisayar belleği, her ne kadar hızlı bir şekilde erişilebilen geçici depolama birimlerini tarif etmek için kullanılsa da teknik olarak herhangi bir elektronik veri depolama birimidir. Eğer CPU her çalıştırıldığında verileri sabit diskten almak zorunda olsaydı bu çok yavaş bir işlem olurdu; bu yüzden, daha hızlı erişilebilmeleri için geçici bellekte çok fazla veri geçici olarak depolanır. Bu tür bir bellek, Rastgele Erişilebilir Bellek (RAM) olarak bilinir. CPU, RAM’den verileri ister, onları işler ve RAM’ye geri yazar. Bu saniyede milyonlarca kez gerçekleşir. Verilerin adli bilişim yöntemleriyle ele geçirilmesinde geçici belleğin anlaşılması önemlidir, çünkü bilgisayar sistemlerinin aranması ve bunlara el konulması işlemlerinin yaygın bir özelliği olarak bilgisayarın güç bağlantısı kesildiğinde bu veriler kaydedilmez. Artık Emniyet Güçlerinin bilgisayar aramaları sırasında güç bağlantısını çıkarmadan önce RAM’deki verileri ele geçirmeye teşebbüs etmesi daha sıklıkla gerçekleştirilen bir uygulamadır. Buna genel olarak “Canlı Veri Adli Bilişimi” denir. Kaybedilebilecek veri miktarı yalnızca birkaç sene öncesinin en büyük sabit diskinin boyutundan daha büyük olduğundan bu faaliyet daha sıklıkla gerçekleştirilmektedir. | | | |
| **Slayt 17** | * Evrensel Seri Veri Yolu (USB) – Çoğu bilgisayarda bulunan USB portları, fare, yazıcı, harici depolama cihazları ve cep telefonları gibi çok çeşitli cihazların bilgisayara bağlanmasını sağlar. Şu anda harici cihazların bilgisayarlara bağlanmasında kullanılan en yaygın yöntemdir. Tarihsel olarak, paralel ya da seri portlar gibi diğer bağlantı yöntemleri daha sorunluydu çünkü aynı anda bağlanabilecek cihaz sayısı için bir limit vardı ve veri aktarma hızı USB’ninkinden çok daha yavaştı. USB kullanarak bir bilgisayara 127 cihazın bağlanması mümkündür. USB cihazların kullanımının kolay olması, birçok adli bilişim araştırmasında öne çıktıkları anlamına gelir. | | | |
| **Slayt 18 - 20** | * Sabit Disk Sürücüler – Çoğu bilgisayar, en az bir sabit diske ve bazıları da birden çok sabit diske sahiptir. Anaçatı bilgisayarlar gibi büyük bilgisayarlar genellikle birçok sabit diske sahiptir. CCTV (kapalı devre TV) ve müzik çalarlar gibi diğer cihazların da büyük miktarlarda veri saklayan sabit disklere sahip olması artık oldukça yaygındır. Bu diskler, bilgilerin içinde tutulduğu ve verilerin kolaylıkla silinebileceği ve üzerine yeniden yazılabileceği sert tablalara sahiptir ancak diskin yapısı hatırlandığından sabit disk uzun süreler boyunca kullanılabilir. Veriler, tablanın yüzeyinde sektörler ve izler halinde depolanır. İzler, eş merkezli çemberlerdir ve sektörler, bir iz üzerindeki pasta dilimi şeklindeki parçalardır. Veriler, sabit diskte, aslında baytların (sekizlilerin) oluşturduğu bir grup olan dosyalar halinde depolanır. Programlar da dosyadır ve bunlar da kullanılmak üzere CPU tarafından çağrılır. | | | |
| **Slayt 21** | * Katı Hal Diski - Bazen katı hal bellek ya da elektronik disk olarak da anılan bir katı hal diski (SSD), geleneksel bir blok giriş/çıkış sabit disk sürücü ile aynı şekilde erişim sağlama amacıyla kalıcı verileri depolamak için katı hal belleği kullanan bir veri depolama cihazıdır. SSD’ler, dönen diskler ve hareket edebilir okuma/yazma kafaları içeren elektromekanik cihazlar olan sabit disk sürücüleri (HDD) ya da disket gibi geleneksel manyetik disklerden ayrılır. Bunların aksine SSD’lerde, verileri değişebilir olmayan çipler[1] içinde tutan mikroçipler kullanılır ve hareket eden parçalar yer almaz.[1] Elektromekanik HDD’lere kıyasla SSD’ler, genellikle fiziksel darbelerden daha az etkilenir, daha sessizdir, daha kısa erişim zamanı ve gecikme süresi sunar, ancak gigabayt (GB) başına daha pahalıdır. SSD’ler, sabit disk sürücüler ile aynı arayüzü kullanır ve bu yüzden çoğu uygulamada kolaylıkla onların yerine kullanılabilir. | | | |
| **Slayt 22** | * CD/DVD/Blu-Ray Diskler – Bu diskler, çeşitli miktarlarda veriyi depolayabilir ve genellikle müzik, video ya da bilgisayar dosyalarının dağıtım için depolanması amacıyla kullanılır. Örneğin bir DVD, CD ile aynı boyutta olmasına karşın CD’den yaklaşık 7 kat daha fazla veri depolayabilir. Yüksek çözünürlüklü içerikleri depolamak için kullanılabilen bir Blu-Ray disk, bir DVD’den 10 kat daha fazla veri depolayabilir. Başka bir deyişle yalnızca birkaç sene önce bir sabit diskte depolanması mümkün olmayan miktardaki verileri depolayabilirler. Her biri verileri sabit disklerden farklı bir şekilde depolar ve bunlar içinde yer alan veriler, sabit disklerde depolanan veriler kadar değişken değildir. | | | |
| **Slayt 23** | **Veri Depolama**  Bilgisayarlardan ya da cep telefonları gibi dijital cihazlardan elde edilen kanıtların ceza ve hukuk davalarında sunulması olağan bir durumdur. Teknoloji toplumda yayıldıkça daha fazla cihazın davalarda kullanılabilecek dijital kanıtlar içermesi normal hale gelecektir. Halihazırda evde kullanılan cihazlarda bu kanıtların aranması için inceleme yapıldığını görmekteyiz.  Dolayısıyla, hakim ve savcıların, dijital kanıtların bütünlüğü ve kabul edilebilirliğini etkileyen meseleleri anlaması hayati öneme sahiptir.  Bir başlangıç noktası olarak, verilerin nasıl depolandığı ve araştırmacılar tarafından nasıl kurtarıldığını anlamaları onlar için faydalı olacaktır.  Elektronik ya da dijital veriler, birçok farklı şekilde depolanır; bunlardan en iyi bilineni ve en geçerli olanı bilgisayarların sabit disklerinde yapılan depolamadır. Dijital kanıtların korunması ve sunulmasına yönelik tipik yaklaşımlar, statik bir durumda, başka bir deyişle, bir bilgisayar kapatıldığında ve veriler değişken bir durumda değilken cihazlar üzerinde yapılan incelemelere dayanır. Adli bilişim incelemecileri, bu kanıtlara uygulanacak muamelelere dair ulusal ve uluslararası kural ve şartları iyi bilir. E-Kanıtların Ele Geçirilmesi adlı bu tür bir kılavuz, Avrupa Komisyonu Oisin Programından alınan fon desteği ile geliştirilmiştir ve şu adreste bulunabilir: <http://www.e-evidence.info>. Bu kılavuz, çoğu emniyet gücünün çalışırken uyduğu genel ilkeleri tarif eder. Verilerin depolanma şekilleri ve kanıtların nasıl sunulduğunun hakimler tarafından net bir şekilde anlaşılması önemlidir. Bu, dijital veriler, depolama, bilgi bulma kavramlarının ve bu kanıtların ceza yargılaması sistemine getirilmesi için kullanılan araçların ve uyulan usullerin genel olarak anlaşılmasını gerektirir. Eğitimleri hazırlayan kişilerin öğrenme programlarında kullanabileceği, sabit disk bellekleri hakkında bilgiler içeren çeşitli kaynaklar mevcuttur. Bunun bir örneği şu adreste bulunabilir:  <http://www.storagereview.com/hard_disk_drive_reference_guide>. Bu dokümanda genellikle manyetik ortamlar, optik depolama ortamları, flaş bellek vb. gibi değişken olmayan depolama birimleri ele alınmaktadır.  Kanıtların Rastgele Erişilebilir Bellek (RAM) gibi değişken kaynaklardan ya da cep telefonları gibi verilerin daha uçucu (değişken) olduğu cihazlardan alınması artık daha yaygındır. Bu verilerin elde edilme şekilleri arasındaki farkların ve bunların kanıtların bütünlüğü üzerindeki etkilerinin hakimler tarafından anlaşılması gerekir. Uçucu verilerin elde edilmesinin önemi şudur ki cihaz kapatıldığında bu veriler genellikle kaybedilir ve içinde değerli kanıtların bulunabileceği büyük miktarlarda değerli bilgiyi elde etme şansı kaybolur. Bu bilgileri elde etmek için kullanılan teknikler, bu verilerin korunması ve kurtarılmasına yönelik genel ilkelere uygun olmalıdır. Ayrıca, uçucu verilerin, bir statik analizin gerçekleştirilmesi için kapatılamayan ağ bağlantılı sistemlerde elde edilmesi de tipik bir durumdur. | | | |
| **Slayt 24** | Bellek ve veri depolama – bu slaytta, verileri ve boyutlarını tarif etmek için kullanılan terimler ana hatlarıyla açıklanmaktadır ve bu slayt, katılımcıların farklı depolama cihazları ve kapasitelerinin ele alındığı oturumun sonraki bölümlerini anlaması için gerekli olacak bir giriş kısmıdır. | | | |
| **Slayt 25** | **İşletim Sistemleri**  Bilgisayar ve diğer dijital cihazların çalışması için bir işletim sistemi gerekir. Bir işletim sistemi, donanımların yazılım programları ile iletişimde bulunmasını sağlayan bir yazılım programıdır. Bir bilgisayar, işletim sistemi olmadan çalışamaz. Bilgisayarın ya da diğer dijital cihazların türüne bağlı olarak farklı türlerde işletim sistemleri mevcuttur.  Bugün en yaygın olarak kullanılan işletim sistemleri şu isimlerle bilinmektedir: Windows, Unix/Linux ve Apple Mac. Özellikle kişisel dijital yardımcılar ve cep telefonları gibi diğer türden cihazlarda kullanılan başka sistemler de mevcuttur. Bunlar çoğunlukla başlıca sistemlerin daha küçük versiyonlarıdır, ancak bazı daha küçük cihazlar için ısmarlama sistemlerin geliştirilmesi de artık daha yaygındır.  Bilgisayarlar için geliştirilen çoğu uygulama, belirli işletim sistemleri için yazılır ancak artık bu uygulamaların birden fazla platform için geliştirilmesi daha yaygın bir durumdur.  Hakim ve savcıların işletim sistemlerinin önemini anlaması ve farklı işletim sistemlerinin farklı şekillerde davrandığını bilmesi önemlidir. Bir eğitim geliştirmecisinin bu bölüm için belirtilen hedefleri gerçekleştirmek için işletim sistemleri hakkında yeterli bilgileri eğitime dahil etmesini sağlayacak birçok referans mevcuttur. Bu kaynaklardan birisi:  <http://en.wikipedia.org/wiki/Operating_systems> | | | |
| **Slayt 26 - 28** | İşletim Sistemleri – bu slaytlarda, işletim sistemlerinin amacına dair açıklamada bulunulmakta, bugün en yaygın olarak kullanılan işletim sistemleri belirtilmekte ve bu sistemlerin yaygınlığı hakkında istatistiksel bilgiler sunulmaktadır. Eğitimciler, bilgileri güncel tutmaları gerektiğini unutmamalıdır. Özellikle slayt 38’de bulunan bilgiler yılda bir güncellenmelidir. | | | |
| **Slayt 29** | **Dijital Cihazlar**  Dijital cihazlarla ilgili olan oturum, hakim ve savcıların potansiyel olarak kanıt içeren farklı türlerden cihazları tanıyabilmelerini sağlamak için tasarlanmıştır. Bundan sonra, cihazlarda ne kadar verinin tutulabileceğine ilişkin tartışmalar yapılacak ve veri miktarlarının ceza yargılaması sisteminde sebep olduğu zorluklara değinilecektir. | | | |
| **Slayt 30 - 38** | Bu oturumda yer alan slaytların sayısı fazladır ve eğitimciler, amacı gerçekleştirmek için bunlardan hangilerinin gerekli olduğuna karar vermelidir.  Ancak, kanıtların aranması, ele geçirilmesi ve incelenmesine ilişkin zorluklar açısından cep telefonu, flaş sürücü ya da bilgisayarlar gibi cihazlar arasındaki farklılıklar bu oturumda ele alınmamaktadır. Eğitimciler, bu öğrenme amaçlarını destekleyecek örnekleri kullanmayı düşünmelidir.  Eğitimin bu aşamasında katılımcılara birçok teknik unsur tanıtılacaktır ve slaytlardan bazılarının, anlaşılması çok zor olmayan bir bakış açısı kazandırması ve bazı ilginç örnekleri katılımcıların dikkatine sunması beklenmektedir.    Burada ele alınacak önemli noktalar, içinde verilerin depolanabileceği cihazların farklı nitelikleri ve bunların ceza yargılaması sisteminde sebep olduğu zorlukların boyutunu içerir. Eğitimciler, ceza davalarında alışılmadık cihazların önemli kanıt kaynakları olarak karşımıza çıktığı örnekleri kullanmayı da dikkate almalıdır. | | | |
| **Slayt 39** | **Bazı Farklı Bilgisayarlar**  Bu kısa bölüm, yukarıdaki bölümden hemen sonra gelir ve dijital cihazlara dair tartışmanın ek bölümüdür. Bir kez daha eğitimci, kanıtların geniş bir yelpazedeki çok çeşitli cihazlarda bulunabileceği ve karşılaşılabilecek tüm cihazların göründüğü gibi olmadığı mesajını vermek için gerekli olan sayıda slaytı kullanabilir.  Bu oturumun önemli bir özelliği, kanıt içerebilecek yüz binlerce sayfa dokümanı depolayabilen cihazlara erişim kolaylığıdır. | | | |
| **Slayt 40 - 45** | Burada ele alınacak önemli noktalar, içinde verilerin depolanabileceği cihazların farklı nitelikleri ve bunların ceza yargılaması sisteminde sebep olduğu zorlukların boyutunu içerir. Eğitimciler, ceza davalarında alışılmadık cihazların önemli kanıt kaynakları olarak karşımıza çıktığı örnekleri kullanmayı da dikkate almalıdır. | | | |
| **Slayt 46 - 54** | **Ne kadar veri depolayabilirler?**  Bu, dijital cihazlar hakkında verilen teknik bilgilerin, cihazlarda ne kadar bilgi saklanabileceği ve bunun sunulabilecek belgelerin miktarı açısından ne anlama geldiğine ilişkin olarak tercümesinin yapıldığı önemli bir oturumdur. Ayrıca, dijital kanıtların ve ürünlerinin bütünlüğü ve kabul edilebilirliği hakkında gerçekleştirilecek sonraki tartışmalara da bir giriş teşkil eder.  Verilen fotoğraflar, katılımcıların farklı cihazlarda depolanabilecek veri miktarlarını kıyaslamalarına yardımcı olmak için sunulmaktadır. Eğitimcilerin kendi ülkelerinde ilgili olabilecek diğer örnekleri de kullanması teşvik edilmektedir.  Açıklanması gereken başka bir önemli nokta da şudur ki bu cihazlar artık pahalı değildir ve çok büyük miktarlarda veriler farklı cihazlarda depolanabilir.    Eğitimciler, hakim ve savcıların çok büyük miktarlarda veri ya da basılı materyallerin etkili bir şekilde elden geçirilmesini esasen imkansız hale getiren kararlar verdiğinde meydana gelen zorlukları da vurgulamalıdır. | | | |
| **Slayt 55 - 81** | **2. Bölüm – İnternet Nasıl Çalışır?**  Bu oturumun sonunda katılımcılar:   * İnternetin günümüze kadar olan gelişimini açıklayabilecek, * İnternetin işlevlerini açıklayabilecek, * Farklı İnternet uygulamalarını ayırt edebilecek, * En az 5 büyük İnternet uygulamasını tanıyabilecek, * Suçluların çeşitli İnternet uygulamalarını nasıl kullandıklarını belirleyebilecektir. | | | |
| **Slayt 55** | Bu oturumda İnternetin tarihçesi, işleyişi ve İnternette mevcut olan hizmetler hakkında temel bilgiler ile katılımcılar tarafından İnternetin bileşenlerinin ayrımının yapılmasına, net bir şekilde tanımlanmasına ve ceza yargılaması sistemi üzerinde nasıl etkilere sebep olduğunun anlaşılmasına olanak tanıyan bilgiler verilmektedir. Eğitimciler, sunumda yer alan teknik verilere değer katmak için uygulamaya ilişkin örneklerin kullanılmasını sağlamalıdır. | | | |
| **Slayt 56 ve 57** | İNTERNET terimi, “bağlı ağ” anlamına gelen “INTERconnected NETwork” kelimelerinin kısaltılmışıdır. Birçok suç faaliyeti, İnternetin kullanımını gerektirir ve bu faaliyetler özellikle, bilgisayar korsanlığı, virüs dağıtımı ve kimlik hırsızlığı saldırılarının yanında dolandırıcılık gibi geleneksel suçları da içerir. Hakimlerin önlerine gelen bu tür davaları etkili bir şekilde idare edebilmeleri için İnternetin ve Dünya Çapında Ağ ve e-posta gibi uygulamalarının temellerini anlamaları gerekir. Aşağıda, derse giriş bölümü verilmektedir ve başarılı bir eğitim modülü için gerekli olan şablon sunulmaktadır. | | | |
| **Slayt 58 ve 59** | **İnternetin Tarihçesi**  İnternet ilk olarak 1960’larda ARPANET olarak hayatına başladı. Bu bilginin önemi hemen fark edilemeyebilir, ancak İnternetin asla güvenli olmak üzere tasarlanmadığı gerçeği, suçluların sistemleri kötüye kullanmasının nispeten neden bu kadar kolay olduğunu açıklayabilir. İlk fiziksel bağlantılar, 1969’da 4 adet üniversitedeki düğümler arasında oluşturulmuştur. İlk e-posta 1972 yılında gönderilmiştir ve ertesi yıl yeni bir iletişim protokolü olan ve şu anda İnternet iletişimlerinin üzerinde gerçekleştiği temeli oluşturan TCP/IP oluşturulmuştur. İnternetin şu anda bildiğimiz haliyle geliştirilmesi başlangıçta çok dikkat çekmedi çünkü yalnızca birbirleri arasındaki sınırlı ağ geçitlerinden hizmet alan birbirinden bağımsız ve ayrı ağlar mevcuttu. Bu, birçok farklı ağın üstün bir ağ çatısı oluşturmak üzere birbirine bağlanabildiği ağlar arası iletişim için bir protokol geliştirmek üzere paket anahtarlamanın uygulanmasına sebep oldu.  Bu sayede birbirine bağlılık güçlendi ve önce batı dünyasının gelişmiş ağları boyunca yayılarak dünyanın geri kalanına nüfuz etmeye başladı. Gelişmiş toplumlar ve gelişen dünya arasındaki farkın büyümesi bugün hala var olan sayısal uçuruma sebep oldu.    Bunun üzerine 1980’lerde İnternetin ticarileşmesi gerçekleşti ve özel olarak işletilen İnternet Servis Sağlayıcıları ortaya çıktı. Bunlar, aslen 1990’larda gelişen daha popüler erişimin meydana gelmesine imkan tanıdı. İnternet, ticaretin yanı sıra kültür üzerinde de çok büyük bir etkiye sahiptir. Artık elektronik posta (e-posta), sosyal paylaşım siteleri, metin bazlı tartışma forumları ve Dünya Çapında Ağ ile anında iletişim sağlanmaktadır. İnternet, ticaret ve daha büyük miktarlarda çevrimiçi bilgiyle büyümeye devam etmektedir. Web 2.0’ın çıkışı yakındır. | | | |
| **Slayt 60** | Eğitimci, katılımcılara onların ağ iletişimin temellerini ve kısıtlamalarını anlamalarına imkan tanıyacak bilgilerin verilmesini sağlamalıdır. Katılımcılar, yerel ve geniş alan ağlarını ayırt edebilmelidir. Bu slaytlarda temel bilgiler sunulmaktadır. Eğitimciler, örnekler vermeyi ve katılımcıların farklı ağ türlerini ve İnternetin nasıl geliştiğini tartışmaları konusunda onları teşvik etmeyi düşünmelidir. Port ve bant genişliği gibi yaygın olarak kullanılan ağ terimleri bu aşamada açıklanmalıdır. Katılımcılar, örneğin ev ya da iş yerlerindeki İnternet erişimlerini dikkate alarak kendi kişisel deneyimlerini düşünmeleri konusunda teşvik edilmelidir. | | | |
| **Slayt 61** | Yerel Alan Ağı (LAN) **–** Bir ev, ofis ya da binalar grubu (örneğin okul) gibi küçük bir coğrafi alanı kapsayan bir bilgisayar ağıdır. LAN’ların belirleyici özellikleri, çok daha yüksek veri transfer hızları, daha küçük coğrafi mesafe ve kiralık telekom hatlarına ihtiyaç duymamalarını içerir.  Geniş Alan Ağı (WAN)– Geniş bir alanı kapsayan bir bilgisayar ağıdır (yani, iletişim bağlantıları metropol, bölgesel ya da ulusal sınırları aşan tüm ağlar) ya da daha az resmi olarak tanımlamak gerekirse, yönlendiriciler ve kamu iletişim bağlantıları kullanan bir ağdır.    Sırasıyla bir oda, bina, kampüs ya da belirli bir metropol alanı (örneğin bir şehir) ile sınırlı kişisel alan ağları (PAN), kampüs alan ağları (CAN) ya da metropol alan ağları (MAN), Geniş Alan Ağlarının örnekleridir. WAN’ın en büyük ve en iyi bilinen örneği İNTERNET’tir. | | | |
| **Slayt 62** | Portlar– Ağ iletişimleri için bir uç nokta ya da “kanaldır”. Port sayısı, aynı bilgisayar üzerinde farklı uygulamaların birbirlerine müdahale etmeden ağ kaynaklarından faydalanmasına olanak tanır. Portlar ‘sanaldır’, içine giriş yaptığınız soketler DEĞİLDİR!  Bant genişliği– Bir telefon hattı, kablo hattı, uydu beslemesi vb. ile taşınabilecek bilgi miktarıdır. Bant genişliği ne kadar büyükse bağlantınızın hızı o kadar fazladır ve İnternet deneyiminiz daha hızlı indirmeli ve TV tarzı bir deneyime o kadar yakın olur. | | | |
| **Slayt 63** | Ağ Arayüz Denetimcisi (NIC)– Bir bilgisayar içinde kurulu olan ve bilgisayarın bir ağa bağlanmasına olanak tanıyan bir devre kartı ya da levhasıdır.    Ortam Erişim Kontrolü (MAC) adresi– Tespit edilmek için imalatçı tarafından çoğu ağ adaptörüne ya da ağ arayüz kartlarına (NIC) atanan ve özgün bir değer sağlayan yarı özgün bir kimlikleyicidir.    Ağ Merkezi– ya da yoğunlaştırıcı, birçok çift bükümlü ya da fiber optik ethernet cihazlarını birlikte bağlamaya ve bunların tek bir ağ segmenti olarak davranmasını sağlamaya yönelik bir cihazdır. Merkezler, OSI modelin fiziksel katmanında (katman 1) çalışır ve ‘katman 1 anahtarı’, terimi merkezin anlamını karşılayacak şekilde kullanılabilir. Dolayısıyla bu cihaz, çok portlu bir yineleyicinin bir türüdür. Ağ merkezleri, eğer bir çarpışma tespit edilirse tüm portlara bir uyarı sinyalinin gönderilmesinden de sorumludur. | | | |
| **Slayt 64** | Ağ Anahtarı **–** Bir merkeze çok benzeyen bir bilgisayar ağı oluşturma cihazıdır. Geçmişte içeriği adreslenebilir bellekte (CAM) yalnızca MAC adresleri aranabildiği zamanlarda anahtarlama yapmak için Katman 2 tekniklerini kullanmak daha hızlıydı. Üçlü CAM’nin (TCAM) ortaya çıkmasıyla bir IP adresini ya da MAC adresini arayıp bulmanın hızı eşitlendi.    Yönlendirici– Bir paketin varış noktasına doğru yönlendirilmesi gereken bir sonraki ağ noktasını belirleyen bir cihazdır. En az 2 ağa bağlanmalıdır. Akıllıdır ve yönlendirme tablaları üzerinde çalışır. Bir ağın ağ geçidinde yer alır. ‘Katman 3 anahtarı’ çoğunlukla yönlendiricinin anlamını tam olarak karşılamaktadır ancak bir anahtar gerçekte çok genel bir terimdir ve kesin bir teknik tanıma sahip değildir.    Sunucu– Bir ağda yer alan diğer bilgisayarlara bilgi ya da hizmetler sunan bir bilgisayar ya da cihazdır. Doğru yazılımlara sahip olunduğunda herhangi bir ağa bağlı bilgisayar bir sunucu olarak konfigüre edilebilir. Çoğu durumda, bu iş için tahsis edilen güçlü bir bilgisayarın “her zaman kullanıma hazır” olması gerekir. Bir bilgisayar, web sunucusu, e-posta sunucusu, dosya sunucusu, yazıcı sunucusu vb. gibi birkaç hizmeti birden çalıştırabilir. Ancak, iş uygulamalarında güvenlik sebepleriyle ve tüm arızaların etkisini en aza indirmek için farklı hizmetleri farklı makinelerde çalıştırmak daha akla uygundur. | | | |
| **Slayt 65 ve 66** | **İnternet Hakkında Temel Bilgiler**  İnternet, birçok farklı uygulamanın aynı anda çalıştırılabileceği bir altyapı olarak düşünülebilir. Eğer İnternetin herhangi bir kısmı arızalanırsa ya da yok edilirse, iletişim hala devam edebilir. Ne bir kurum, ne bir şirket ya da devlet, hiç kimse İnternetin sahibi değildir. Çoğunlukla öz düzenlemelidir. Aynı bağlantı teknolojisini kullanır.  İnternet gibi çoğu modern veri ağı “bağlantısız” ya da “paket anahtarlamalı” olarak tarif edilir. Trafik, küçük paketlere bölünür ve bu paketler göndericiden alıcıya kendi yolunu çizer. Bunlar aynı güzergahı izlemez ancak hedefe vardıklarında birbirleriyle birleşir. | | | |
| **Slayt 67 ve 68** | Eğitimciler, İnternette karşılaşılan farklı uygulamalar hakkında net açıklamalar yapmalı ve bunların nasıl temsil edildiğine dair anlaşılır örnekler vermelidir. Bu slaytta verilen genel açıklamaya ek olarak her bir uygulamanın örneklerinin gösterilmesi gerekmektedir.  Pek az İnternet protokolü vardır. Bunların içinde en önemlisi İnternet Protokolüdür (IP). İnternete bağlı her bilgisayar bunu kullanmalıdır. IP Adresi sizin İnternet ‘telefon numaranızdır’ ve IP adresi olmadan İnterneti kullanmanız mümkün değildir. Ağlar arasında iletişim kurmak için farklı uygulama ve hizmetler farklı protokolleri kullanır; bunlardan bazıları: HTTP – Hiper Metin Transferi Protokolü, SMTP – Basit Posta İletimi Protokolü, FTP – Dosya Transfer Protokolü ve NNTP – Ağ Haberleri Aktarma Protokolüdür. *Bunların IP üzerinden (yerine değil) çalıştığı söylenir.* | | | |
| **Slayt 69 ve 70** | Çoğu kişi İnternete bir İnternet Servis Sağlayıcı (İSS) ile bağlanır. Bunlar, yer kiralayan ticari kurumlardır. Kayıt tutarlar, ancak ne kadar süre boyunca? Verilerin İSS’ler tarafından ne kadar süreyle muhafaza edileceğini belirleyen ulusal ve uluslararası veri koruma hususları vardır. Bu tabii ki ceza yargılaması görevlilerinin bu kaynaklardan elde edilen kanıtları güvence altına alabilme imkanlarını etkiler. Bağlantı normalde şu yöntemlerden biriyle sağlanır: Çevirmeli, Geniş Bant (ADSL), ISDN, Kablolu, Kablosuz erişim noktası veya Uydu.  İnternete bağlantının nasıl sağlandığına ilişkin bilgiler sunulmalı ve katılımcılar, kendi deneyimlerini tartışmaları konusunda teşvik edilmelidir. İSS’lerin kayıtlar tuttuğu ancak veri koruma mevzuatının, İSS’ler tarafından bu kayıtların ne kadar süre ile tutulabileceğine dair kısıtlama getirdiği açıklanmalıdır.  İSS’lerin rolü ve yasal statüsü ve numaraları açıklanmalıdır. Bu, verilere erişim sağlama ve yasal ele geçirmeye ilişkin olarak İSS’lerle ilişki kurmanın önemini tartışmak için iyi bir fırsattır.    En basit anlatımı şudur ki İSS’ler İnternete erişimlerini, şahıs ya da kurumlara olmak üzere insanlara kiralar.    Her İSS, müşterileri hakkında belirli bilgileri saklar. Bu bilgilerin detayları ve miktarı İSS’ye bağlıdır ve ihtiyaca göre belirli saat ya da gün boyunca bu bilgiler saklanır.    Kayıt için kullanılan isim, adres ve diğer bilgileri,  Kayıt tarihini ve şahsın nasıl kayıt olduğu,  Kullanıcya özel e-posta adresleri veya ekran adları,  İSS’ye abone olmak için kullanılan kredi kartı gibi mali bilgileri,  Muhtemelen kullanıcı hakkındaki bazı yazılım bilgileri,  Hepsinden önemlisi kullanıcının çevrimiçi faaliyetlerinin tarih, saat ve süre gibi detaylarını öğrenmek mümkündür.  ZAMAN ÇOK ÖNEMLİDİR (Saat dilimi konuları bu oturumda daha sonra ele alınacaktır) Bir hesap almak için sahte bilgiler kullanmanın mümkün olduğu da belirtilmelidir.  Bir İSS şüpheli İnternet trafiğini durdurabilir mi? – EVET – ancak bu, kullanımı kaydetmeye ve neler olduğunu izlemeye yönelik özel ekipmanlara bağlıdır. Dolayısıyla insan gücü gerektirir. Ayrıca bunu yapmak için gereken yetkiyi de dikkate almamız gerekir. Herhangi bir durumda soruşturmanın ilk safhalarında İSS ile irtibata geçmek gerekir.  **Ağ Adresi Dönüştürme** – Kaynak ve/veya hedef IP adresinin bir güvenlik duvarı ya da yönlendiriciden geçerken yeniden yazıldığı bir tekniktir. En yaygın olarak, tek bir IP adresi ile İnternete erişim sağlamak amacıyla özel bir ağda çoklu hostlar için kullanılır.  Eğitim kursunun, ağ adreslemesinin biraz detaylı açıklamasını içermesi tavsiye edilmektedir ve özellikle şu bilgiler yer almalıdır: IP versiyon 4’te adresler 3 basamaklı 4 grup halindedir (32 ikilli adresleme) ve her grup 0 ile 255 arasında bir sayıdır; yani maksimum 256 tercih vardır. Her gruba Sekizli (28) denir ve bazı değerler rezervedir. IP adreslerinin nasıl elde edildiğinin detayları açıklanmalıdır. Bu, numaraların elde edildiği İkili numaralandırmanın görsel bir sunumuyla daha iyi bir şekilde gerçekleştirilebilir. Statik ve dinamik IP adresleri arasındaki farka ve bunun soruşturmalar üzerinde sahip olabileceği etkiye dair ek açıklamalarda bulunulmalıdır. IP versiyon 6’daki değişikliklerin ve İnternette IP adreslerinin tükenmesi sebebiyle bu versiyonda yapılan bu değişikliklere olan ihtiyacın açıklaması yapılmalıdır. | | | |
| **Slayt 71 ve 72** | İnternetin küresel bazda kullanımının boyutu önemli bir özelliktir. Burada sunulan iki slaytta, ilk olarak bilgilerin sunulmasına ilişkin iki farklı yöntemi ve ikinci olarak da farklı dillerin İnternet kullanımına sokulması ve oldukça kısa bir zaman dilimi içinde meydana gelen değişiklikler gösterilmektedir. Diğer zamanla ilgili bilgilerde olduğu gibi eğitimcinin, bilgilerin mümkün olduğunca güncel ve kaynakların mümkün olduğunca kabul edilmiş olmasını sağlaması gerekecektir. | | | |
| **Slayt 73** | **İnternet – Nasıl çalışır?**  Bu oturum, verilerin İnternette dolaştığının katılımcılar tarafından anlaşılması için tasarlanmıştır. Burada verilen bilgiler, bu özel dinleyiciler için gerekli olduğu şekilde çok temel bilgilerdir. | | | |
| **Slayt 74** | IP’de paketler çeşitli boyutlara sahiptir. Herhangi iki paketin kaynaktan hedefe aynı güzergahı izlemesi gerekmez. Alıcı bilgisayar, trafiği yeniden kurar ve eğer eksik paket varsa bunların yeniden iletilmesini talep eder.  Bunun avantajı ağın ilgili zamanda mevcut olan ihtiyaçlara bağlı olarak dinamik olarak tahsis edilebilen, paylaşılan bir kaynaktır olmasıdır. Dezavantajıysa, özel olarak ayrılmış bir bağlantı olmadığından hizmet kalitesinin garanti edilmesinin zor olmasıdır. Buna ilişkin olarak bazı IP üzerinden sesli iletişim hizmetleri, mükemmel ses kalitesi sunar. | | | |
| **Slayt 75 ve 76** | Bu slayttaki iki resim, trafiğin İnternette nasıl hareket ettiğinin eğitimci tarafından kolaylıkla açıklanmasını sağlamak için verilmiştir. | | | |
| **Slayt 77** | “Ağ Savaşçıları” adlı film, İnterneti açıklamaya yönelik mükemmel bir kaynaktır. İnterneti acemi kullanıcılara tanıtmak için harika bir araçtır. Yeni kullanıcıların İnternetin nasıl çalıştığını gözünde canlandırmasına yardımcı olur. Film 12 dakikadır. IP paketlerinin yönlendiricilerden, güvenlik duvarlarından ve Atlas Okyanusu’ndaki kablolardan geçerek ağda gerçekleştirdikleri yolculuk hakkındadır. [www.warriorsofthe.net](http://www.warriorsofthe.net/) adresinden ticari olmayan amaçlarla kullanılmak üzere ücretsiz olarak indirilebilir ve şu anda (Şubat 2010) şu dillerde mevcuttur: İngilizce, Almanca, İspanyolca, İbranice, Hollandaca, İsveççe, Fransızca, İtalyanca, Portekizce, Danca, Norveççe, Macarca ve Çekçe. İnternetin çeşitli ülke ve bölgelerdeki nüfuzu ve büyümesinin düzeyini tespit etmek için faydalı bir kaynak <http://www.internetworldstats.com/> adresinde yer almaktadır. Eğitimde katılımcıların İnternetin kendi ülkeleri üzerindeki etkisini değerlendirebilmesi için istatistiksel bilgilerin sunulması önerilmektedir. | | | |
| **Slayt 78** | Katılımcıları IP Adreslerini ve IPv4’ün kısıtlamalarını anlaması önemlidir. Bu, dinamik ve statik IP adresleri hakkında sonraki tartışmalar düzenlenirken yardımcı olacaktır. Bu basit bilgiler, İnternetin geleceği hakkındaki sonraki bölüme hazırlık için temel oluşturmaktadır. | | | |
| **Slayt 79** | Çoğu İSS, müşterilerinin hepsinin aynı anda bağlanmayacağını varsaydığından müşteri sayısından daha az sayıda IP adresine sahiptir. Adresleri dönüşüm sağlamak için dinamik IP adres tahsisi kullanın.  Aynı IP adresinin aynı günde farklı insanlar tarafından kullanılması oldukça muhtemel olduğundan şüphelilere karşı İSS kontrolleri yaparken zaman ve tarih (ve saat dilimi) kritik öneme sahiptir.  İSS’ler daha yüksek maliyetler karşılığında olmak kaydıyla statik IP adresleri de sunar (örneğin bir web sitesi için bir gerekliliktir). | | | |
| **Slayt 80 - 81** | İnternetin geleceği, sürekli olarak değişen bir tartışma konusudur, ancak IPv6’nın ortaya çıkışı, hayatımızı yaşama şeklimize ve ceza yargılaması sistemine birçok değişiklik getirecektir. Eğitimci, IPv6’nın neredeyse tüm cihazların kendi IP adresine sahip olmasını nasıl sağlayacağını ve bunun gelecekte soruşturmaların yürütülme şekli üzerinde etkilere yaratacağını açıklamalıdır.  İnternetin nasıl değiştiğinin ve bu değişikliklerin soruşturmaların yürütülme ve idare biçimi üzerindeki etkileri, ilgili dinleyicilere sunulmalıdır. Bant genişliği, ticaret ve kablosuz üzerindeki etkiler bunlara örnek olarak verilmektedir. | | | |
| **Slayt 83 - 111** | **3. Bölüm - İnternet hizmetleri** | | | |
| **Slayt 83** | Bu oturumda, özellikle Dünya Çapında Ağ ve E-posta gibi İnternette mevcut olan hizmetler hakkında daha fazla ayrıntıya girilmektedir. | | | |
| **Slayt 84** | İnternette mevcut olan hizmetler hakkında ayrıntıya girmeden önce ne kadar ülkenin şu anda bu hizmetlerden ulusal düzeyde faydalandığını değerlendirmek gerekir. Eğitimciler, İnternetin kısa bir süre içinde ulusal altyapı güvenlik konularında ne kadar önemli bir hale geldiğinin katılımcılar tarafından anlaşılmasını sağlamak için kendi ülkelerindeki kritik ulusal altyapının genel bir değerlendirmesini sunmalıdır. | | | |
| **Slayt 85** | **Dünya Çapında Ağ (WWW)**  Dünya Çapında Ağ (WWW), 1991’de Sör Tim Berners-Lee tarafından HTML (Hiper Metin İşaretleme Dili) icat edildiğinde doğmuştur. HTML, web sayfalarında kelime, resim ve sesleri birleştirmek için gerekli platformu sunmuştur. Web standartları Dünya Çapında Ağ Konsorsiyumu (W3C) tarafından oluşturulmaktadır. Aşağıdaki ifade, ismi bir nebze de olsa açıklamaktadır:  “W3 dünyasının görünümü, bağlantılarla birbirine işaret eden dokümanlarla ilgilidir. Bir örümceğin oluşturduğu yapıya benzerliğinden dolayı bu dünyaya Ağ (Web) denmektedir.” *(Tim Berners-Lee, Robert Cailliau; Dünya Çapında Ağ; Eylül 1992* | | | |
| **Slayt 86 ve 87** | WWW’ye erişim normalde, web sayfalarını bulmak ve görüntülemek için tasarlanmış bir yazılım programı olan bir Tarayıcının kullanımıyla gerçekleştirilir. Ocak 2012 itibarıyla en iyi bilinen tarayıcılar şunlardır: Mozilla Firefox, Google Chrome, Internet Explorer, Safari ve Opera. Eğitimciler, burada verilenler gibi istatistiklerin düzenli aralıklarla güncellenmesini sağlamalıdır. | | | |
| **Slayt 88 - 89** | Hyper Metin Aktarım Protokolü (HTTP) Web Tarayıcıları ve Web Sunucularının İnternette birbirleriyle iletişim sağlamak için kullandıkları ortak dildir.  WWW tarayıcıları çeşitli protokolleri desteklese de (örneğin FTP, NNTP, SMTP vb.) HTTP, web tarayıcıları ile birlikte en yaygın olarak kullanılan protokoldür. HTTP, TCP üzerinden basit bir talep/yanıt (RR) protokolüdür. Çoğu insan, WWW’nin aslında İnternet olduğu düşünür ve bunun sebebi de muhtemelen WWW’nin çoğu insan tarafından kullanılan uygulama olmasıdır. Suçluların bu kullanımdan faydalanması da sıklıkla görülen bir durumdur.  Bir eğitim programı geliştirilirken, eğitimin verildiği yerdeki yargı alanı ile ilgili durumlarda WWW’deki suç faaliyetlerinin örneklerinin verilmesine dikkat edilmelidir. | | | |
| **Slayt 90** | **Alan Adları ve IP Adresleme**  Bu bölüm, IP adreslerinin ve alan adlarının birbirleriyle ilişkisi hakkında fazla detaya girmeden IP adreslerine ve bunların ne anlama geldiğine ilişkin temel bilgileri katılımcılara sunmak için tasarlanmıştır. Teknik detayların, bu dersin kapsamının dışında yer aldığı düşünülmektedir. Eğitimcinin bunu, açıklaması mümkün olduğu kadar kolay getirmesi önemlidir. Verilen sunum materyallerinde bunun nasıl gerçekleştirilebileceği tespit edilmeye çalışılmaktadır. | | | |
| **Slayt 91 - 93** | Bu bölümde verilmesi gereken üç temel öğrenme noktası bulunmaktadır:   1. İlk olarak Tek Biçimli Kaynak Konumlayıcısının bir açıklaması ve nasıl yapılandırıldığı; 2. Statik ve IP adreslemenin anlatılması - Statik IP adresleri, kalıcı olarak tahsis edilir ve her zaman etkili bir şekilde çevrimiçidir.   Dinamik IP adresleri, her çevrimiçi oluşunuzda tahsis edilir, ancak çevrimdışı olduktan saniyeler sonra IP adresleri yeniden tahsis edilebilir.  Bu sebeple internet erişiminin tam saati önemlidir.   1. Bir IP adresiyle bir URL arasındaki ilişkinin açıklanması. Alan adları ve IP adresleri birbirlerinin yerine kullanılabilir. Eğer IP adresini biliyorsanız bunu adres satırına girerek aynı siteye bağlanmanız mümkündür.   Uygulamada normalde olan şey, kullanıcı dostu alan adını (www.open.gov.uk) girmeniz ve İnternet sistemindeki sunucuların bunu sizin için dönüştürmesi ve sizi doğru siteye göndermesidir.  İnternet Protokol Adreslerinde alan adı, normalde Noktalı Dörtlü gösterimi ile yazılan, noktalarla ayrılan dört adet 8 ikilli sayıların oluşturduğu özgün bir 32 ikilli numaraya dönüştürülür. Yukarıda verilen örnekte (212.140.189.10) bu dizideki tüm numaralar 0 ile 255 arasında yer almalıdır (yani toplam 256 alternatif). Verilen örnekte görüldüğü gibi son sayı 010 şeklide okunmalıdır ancak uygulama gereği bu 10 şeklinde kısaltılabilir. | | | |
| **Slayt 94** | **İzler**  Sanal suçların soruşturulması ile ilgili önemli bir unsur da araştırmacıların araştırma yapmak için İnterneti kullanırken hangi izlerin bırakılabileceğini anlamaktır. Bu yalnızca araştırmacılar için değil aynı zamanda soruşturma emri verebilen savcılar ve kanıtların kabul edilebilirliği açısından hakimler için de geçerlidir. Bu bölümde, çevrimiçi olmanın bir soruşturmaya ilişkin olarak sebep olabileceği risklerin katılımcılar tarafından anlaşılmasına imkan tanıyacak temel bilgiler verilmeye çalışılacaktır. | | | |
| **Slayt 95 - 98** | Sunum slaytlarında verilen bilgiler, web sitelerini ziyaret eden araştırmacılar da dahil olmak üzere herhangi biri tarafından geride hangi bilgilerin bırakıldığını göstermek için slaytlar arasında dolaşan katılımcılara bildirilmesi gereken temel bilgilerdir. Bu, araştırmacıların bu durumlarda kimliklerini korumasının sağlanması ile bazı yargı alanlarında bu soruşturmaların gerçekleştirilmesi için yerine getirilmesi gereken hukuki koşullar olabileceğinin tespit edilmesinin önemine bağlanmalıdır. | | | |
| **Slayt 101 - 104** | **E-posta**  Elektronik Posta ya da E-posta, dijital mesajları alıp göndermenin bir yöntemidir. Kullanıcılar, e-postanın doğrudan göndericinin makinesinden alıcınınkine aktarıldığını sanabilir ancak her mesaj, ömrü boyunca tipik olarak en az dört bilgisayardan geçer.   1. Kullanıcının kendi bilgisayarında bir mesaj oluşturulur ve İSS’nin giden SMTP (Basit Posta Aktarım Protokolü) posta sunucusuna\* gönderilir. 2. Giden İSS, e-postayı alıcının İSS SMTP posta sunucusuna iletir (SMTP – SMTP). 3. Alıcının posta sunucusu, alıcının gelen posta sunucusunu bulur (Posta Ofisi Protokolü veya POP3) ve mesajı alıcının posta kutusuna teslim eder. 4. Alıcı hesabına girer ve mesaj, alıcının gelen kutusuna alınır ve normal olarak posta sunucusundan silinir   *\* Posta sunucusu – postaları idare etmek için kullanılan özel bilgisayar* | | | |
| **Slayt 105** | Farklı türlerden elektronik postalar vardır;  E-posta - Geleneksel Outlook türü posta – SMTP ile gönderilir – POP3 ile alınır ve indirildiğinde bilgisayarınıza yerleşir  Web bazlı posta **-** POP3 posta – örneğin Outlook Express kullanırken – normalde oturum açtığınızda tüm yeni postaları makinenizdeki gelen kutusuna indirirsiniz; IMAP posta– ‘gerçek’ web-postası – makinenizden görüntülenir ancak uzaktaki bir sunucuda yerleşiktir – klasörlerin vb. içine atılabilir ama sadece çevrimiçiyken görülebilir. | | | |
| **Slayt 106 - 109** | **E-posta başlıkları**  E-postayı açıklarken e-postayı mektupla kıyaslamak genellikle kolaydır. E-posta mesajlarında bir başlık kısmı (zarf) ve ekleri ile birlikte bir gövde kısmı (mektubun kendisi) yer alır. Mesaj başlığı, gönderici, alıcı, IP adresleri, zaman damgaları vb. ile ilgili bilgiler içerdiğinden araştırmacılar için başlıca odak noktasıdır. Bu bilgiler, bir mesajın göndereninin bilinmediği durumlarda, örneğin e-posta ile iletilen bir fidye talebi durumunda mesajın göndereninin izlenmesine yardımcı olmak için kullanılır. Tam ya da uzun başlık, bir mesajın kaynağının izlenmesi için çok önemlidir ve bir mesaj teslim edildiğinde görünen başlıkla ilgili tüm bilgileri içeren uzun başlık arasındaki farkın hakimler tarafından anlaşılması gerekmektedir. E-posta, hakimlerin karşılaştığı en yaygın uygulamalardan birisidir ve eğitim tasarımcıları, farklı türlerden e-postalara ve bunlar hakkındaki kanıtların mesajların kendilerinden ve mesajların aktarımını sağlayan İnternet Servis Sağlayıcılarından doğru bir şekilde nasıl elde edilmesi gerektiğine ilişkin en güncel bilgilerin eğitimlerde yer almasını sağlamalıdır. Eğitim tasarımcılarının işine yarayabilecek, e-postalarla ilgili ek bilgiler şu adreste bulunabilir: <http://www.learnthenet.com/english/html/20how.htm> | | | |
| **Slayt 112 - 159** | 4. Bölüm – Diğer İlgili İnternet Uygulamaları  Dersin bu bölümü katılımcılara önceki bölümlerde yer almayan İnternet uygulamalarına dair genel bir bakış sunma amacıyla tasarlanmıştır. Bunlar, hedef kitlenin faaliyetlerinin normal seyri sırasında karşılaşacağı şeyler olduğundan gereklidir. Bu bilgiler, dersin amaçlarını destekleyecektir. Verilen ayrıntıların düzeyi, gerekli öğretim düzeyi için uygun olarak değerlendirilmektedir. Çok derin bilgiler sunulmaması için eğitimcilerin dikkat etmesi gerekmektedir çünkü bunlar, şu anda geliştirilen ileri düzey derste yer alacaktır. | | | |
| **Slayt 113 - 114** | **Çevrimiçi Depolama**  **Bulut Bilişim**  Bulut bilişim, hizmetleri veren sistemin fiziksel konumu ve konfigürasyonunun son kullanıcı bilgilerini gerektirmeyen bilişim, yazılım, veri erişimi ve depolama hizmetleri sunan teknolojilere yönelik bir pazarlama terimidir. Buna benzer nitelikte olan bir kavram, son kullanıcıların hizmeti sağlamak için gerekli donanım cihazlarını veya altyapıyı anlamalarına gerek olmadan enerji tükettiği elektrik şebekesidir. Bulut bilişim, İnternet protokollerine dayalı bilişim hizmetlerine yönelik yeni bir takviye, tüketim ve dağıtımı modelini tanımlar ve genellikle dinamik olarak ölçeklenebilir ve çoğunlukla sanallaştırılmış kaynakların teminini içerir. Bir yan üründür ve İnternetten sunulan uzak konumdaki bilişim sitelerine erişim kolaylığının bir sonucudur. Bu, kullanıcıların sanki programlar kendi bilgisayarlarında kuruluymuş gibi bir web tarayıcısı üzerinden erişebileceği ve kullanabileceği web bazlı araçlar ya da uygulamalar şeklinde olabilir. Bulut bilişim hizmeti sağlayıcıları, web tarayıcıları ve masaüstü ve mobil uygulamalardan erişilebilen uygulamaları İnternet üzerinden sunarken iş yazılımları ve verileri uzak bir konumda bulunan bir sunucuda depolanır. Bazı durumlarda mevcut uygulamalar bir ekran paylaşma teknolojisi ile sunulurken bilişim kaynakları, uzaktaki bir veri merkezi konumunda birleştirilir. Diğer durumlarda, tüm iş uygulamaları AJX gibi web bazlı teknolojiler kullanılarak kodlanmaktadır. Bulut bilişimin temelinde daha geniş bir kavram olan altyapı yakınsaması ve paylaşılan hizmetler yatar. Bu tür bir veri merkezi ortamı, işletmelerin daha kolay idare edilebilirlik ve daha düşük bakım maliyetleri ile uygulamalarını daha hızlı bir şekilde kullanmalarına olanak tanır. Bilişimin, bilişim kaynaklarını (sunucular, depolama birimleri ve ağ iletişimi gibi) dalgalı ve öngörülemeyen iş taleplerine göre daha hızlı bir şekilde ayarlamasına imkan verir. Çoğu bulut bilişim altyapısı, paylaşımlı veri merkezleri yoluyla verilen ve müşterilerin bilişim ihtiyaçları için tek bir erişim noktası olarak görünen hizmetlerden oluşur. Hizmet seviyesi anlaşmalarını yerine getirmek için ticari teklifler gerekebilir ancak daha küçük şirketler özel şartlara ilişkin olarak pek pazarlık etmez. Bulut bilişimin iş dünyası üzerindeki muazzam etkisi, federal ABD hükümetinin buluta bilişim altyapısını yeniden düzenlemenin ve bilişim bütçelerini azaltmanın bir yolu olarak bakmasını teşvik etmektedir.  (Kaynak: www.wikipedia.com)  Bulutta verilerin tespit edilmesi ve buradan verilerin toplanmasına ilişkin konular ve bu eylemlerin hukuki sonuçları bu dersin başka bir bölümünde ele alınmaktadır. | | | |
| **Slayt 115 - 116** | Eğitimci çevrimiçi depolamanın yaygınlığı hakkında bilgiler verebilir ve örnek olarak Google aramalarının sayısı ve belirli bir zaman dilim içerisinde bu sonuçların sayısı, çevrimiçi depolamaya olan ilgi hakkında fikir vermektedir. Ücretli ve ücretsiz hizmetler arasında ayrım yapılarak farklı çevrimiçi depolama türleri hakkında bilgiler sunulmalıdır. Suçluların bu tür bir depolama hizmetini kullanabileceği gerçeği net bir şekilde açıklanmalıdır. | | | |
| **Slayt 117 - 118** | Suçluların İnternet hizmetlerini kullanma yolları katılımcıların ilgisini çekiyor olmalıdır. Bu kullanımlardan biri, “gizli takas noktası” hakkındadır. Bu iletişim yönteminin düşük bir yakalanma riskiyle nasıl kullanılabileceğini anlamak oldukça kolay olduğundan bu, eğitimci tarafından açıklanmalıdır. | | | |
| **Slayt 119 - 120** | **Eşler arası (P2P)**  Eşler Arası hizmetler yıllardır yasa dışı dosyaların yanı sıra fikri mülkiyet haklarına tabi dosyaların paylaşılmasına olanak tanımaktadır. Eşler arası hizmetlerin istemcileri, bu faaliyetlere bulaşan suç çeteleri arasında popüler hale gelmiştir. İlk nesil eşler arası mimari, insanların dosyaları indirmek için bağlandığı merkezi bir sunucu kullanma ilkesi ile çalışmaktaydı. Bu, yasa dışı hizmetler sunanları tespit etmeyi ve ilgili konumu saptayıp hizmeti kapatmayı oldukça kolay hale getiriyordu. İkinci nesil eşler arası hizmetlerin istemcileri, aramayı daha kolay hale getirmek için mevcut dosyaların listesini tutanlardan dosyaların nerede mevcut olduğunu tespit eden süper düğümler olarak davrananlara kadar çeşitli bağlantı yöntemlerini kullanmaktadır.  Hakimlerin, birçok tür ceza ve hukuk davası ile ilgili olabilecek eşler arası faaliyetlerden haberdar olması gerekir. Derinlemesine bilgi gerekli değildirve eğitimciler, güncel bilgiler sunmak için şunun gibi sitelerden faydalanmalıdır: <http://ezinearticles.com/?How-Peer-to-Peer-(P2P)-Works&id=60126> | | | |
| **Slayt 121 - 122** | **Haber grupları**  Haber grubu terimi biraz yanıltıcı bir tarif olabilir, çünkü burada tartışmalar yer almaktadır. Bunlar Dünya Çapında Ağda yer alan tartışma forumlarından teknik anlamda farklıdır, ancak forumlarla benzer işlevlere sahiptir. Haber grubu sunucuları, bilgilerini düzenli olarak senkronize edeceklerine ilişkin olarak diğerleriyle anlaşmaya varan çeşitli kurumlar tarafından yönetilmektedir. Bu, kullanıcıların bir sunucuya mesaj atıp daha büyük bir izleyici kitlesi tarafından görülmesine olanak tanır. | | | |
| **Slayt 123 ve 124** | **Dosya Aktarım Protokolü (FTP)**  FTP, dosyaların bir bilgisayardan diğerine aktarılmasına olanak tanıyan güçlü bir protokoldür. İstemcide kurulu olan bir FTP programı ile istemci/sunucu bazında çalışır ve kullanıcının sunucudaki hizmet ve bilgilere erişim sağlaması için sunucu ile etkileşime girmesine olanak tanır. Bir kullanıcı bir dosyayı aktarmak istediğinde hedef sisteme bir TCP bağlantısı oluşturulur. Kullanıcı kimliği ve şifresinin iletilmesine izin verilir ve kullanıcının dosyaları ve gerekli eylemi belirtmesine olanak tanınır. Dosya aktarımı için onay verildiğinde aktarılacak veriler için başka bir TCP bağlantısı oluşturulur. Hakimlerin neden FTP hizmetlerinin varlığını bilmesi gerekir? Çünkü suçluların dosyaları birbirleriyle takas ettiği ya da FTP’nin İnternet Aktarımlı Sohbet (IRC) gibi diğer protokoller yoluyla gerçekleştirilen bir aktarım yöntemi olarak kullanıldığı durumlarda bu tür dosyaların kullanımıyla karşılaşabilirler. | | | |
| **Slayt 125 ve 126** | **İnternet Aktarımlı Sohbet (IRC)**  İnternet Aktarımlı Sohbet (IRC), aslında biraz modası geçmiş ancak iletişim kurmak ve dosya takas etmek için hala suçlular tarafından kullanılan bir telekonferans sistemidir. Birbirlerine bağlanan ve metin bazlı, sanal buluşma odaları olarak değerlendirilebilecek “Kanallarda” yayınlanan mesajları paylaşan bir dizi sunucu ile çalışır. Tartışma konuları listelenir ve IRC kullanıcıları, benzer fikirlere sahip insanlarla tartışmaya dahil olmak için aynı anda bir ya da daha fazla kanala bağlanabilir. IRC, İnternetteki en kullanıcı dostu hizmet değildir ve çoğunlukla daha deneyimli ve potansiyel olarak daha yaşlı kullanıcılar tarafından kullanılmaktadır. Suçlular tarafından kullanılan bir protokoldür ve hakim ve savcıların, bu protokolün işlevlerine ilişkin temel bilgilere sahip olması gerekir. | | | |
| **Slayt 127 - 132** | **Anında Mesajlaşma ve Sosyal Paylaşım**  Anında mesajlaşma ve sosyal paylaşım, dünya çapında diğer kullanıcılara anında ve kullanıcı dostu erişim sağlayan ve çok iyi bilinen örnekleriyle son yıllarda tercih edilen bir iletişim aracı haline gelmiştir. Bu sitelerin temel özelliği, kişisel profil oluşturabilme, kişinin kendisi hakkındaki bilgileri paylaşabilmesi ve yeni insanlarla tanışabilmedir. Fotoğraf, video ve müzik paylaşmak da mümkündür. Şahıslar tarafından yayınlanan kişisel bilgilerin miktarı, onları örneğin kimlik hırsızlığı ile uğraşan ya da çocukları kandırmaya yönelik planlı eylemler yapan suçluların hedefi haline getirebilir.  Eğitim materyallerinin geliştirilmesinde yardımcı olabilecek ek bilgiler şu adreste bulunabilir: http://communication.howstuffworks.com/how-social-networks- work.htm .  Anında mesajlaşma, paylaşılan istemciler kullanan iki ya da daha fazla kişi arasındaki gerçek zamanlı ve doğrudan gerçekleştirilen bir sohbet türüdür. Bu sohbet türü, bilinmeyen kişiler arasında iletişim sağlayan diğer sohbet türlerinin aksine bilinen kişilerle irtibatı içerir. Suçluların, anında mesajlaşmayı bir iletişim yöntemi olarak kullandığı bilinmektedir.  Eğitimci, sosyal paylaşım sitelerinin kullanımındaki artış hakkında istatistiksel veri şeklinde ek bilgiler verebilir. Belirli sitelerin büyümesi ve global etkisi örnek olarak verilmektedir.  Eğitimci, araştırmacıların kullanabileceği türden bilgilerin örneklerini vermeyi düşünmelidir. Faydalı olabilecek bazı örnekler sunumda verilmektedir, ancak eğitimciler, katılımcıların coğrafi konumu ile ilgili örnekler bulmaya çalışmalıdır. | | | |
| **Slayt 133 - 136** | **Çevrimiçi Oyunlar**  Çevrimiçi bir oyun, bir tür bilgisayar ağı üzerinden oynanan bir oyundur. Bu, neredeyse İnternet ya da ona eşdeğer bir teknoloji anlamına gelir ancak oyunlar her zaman teknolojinin son noktasını kullanmıştır: İnternetten önce modemleri ve modemlerden önce donanımla bütünleşik terminaller vb.  Çevrimiçi oyunların büyümesi, bilgisayar ağlarının küçük yerel ağlardan İnternete doğru genişlemesini ve İnternet erişiminin kendi büyümesini yansıtmaktadır. Çevrimiçi oyunlar, basit metin tabanlı oyunlardan karmaşık grafikleri ve aynı anda birçok oyuncunun bulunduğu sanal dünyaları içeren oyunlara kadar geniş bir çeşitlilik gösterir.  Birçok çevrimiçi oyun, çevrimiçi toplulukları birleştirerek bu oyunları tek kişilik oyunların ötesinde birer sosyal aktivite haline getirmiştir.  Eğitimci, oyun içeren suçların örneklerini sunmaya çalışmalıdır. Bunlar gittikçe yaygınlaşmaktadır ve çeşitli ülkelerdeki hukuki sonuçları dikkate almak faydalı olacaktır. | | | |
| **Slayt 137 - 146** | **İnternette Anonimlik ve İzlenebilirlik**  İnternette anonimlik, bu dersin temel düzeyinde ele alınacak önemli bir konudur. Bu terimler, hakim ve savcıların karşısına düzenli olarak çıkacaktır. Anonim hizmetlerin örnekleri, nasıl çalıştıklarına dair açıklamalarla birlikte verilmelidir. Anonim ve şeffaf iletim arasındaki fark açıklanmalıdır. Sunumda verilen slaytlar, eğitimcilerin kendi materyallerini oluşturmalarına yardımcı olabilir. Eğitimci, hem web hem de e-posta anonimlik hizmetlerinin örneklerini sunmalıdır. | | | |
| **Slayt 147 - 159** | **5. Bölüm - İnternet Suçları**  Dersin son önemli bölümlerinden biri olan bu bölümde eğitimci, açıklanan teknolojinin suç işlemede kullanılma yöntemlerini tespit etmeye çalışmalıdır. Gerçekten dünyada İnternet Suçu şikayetlerini alan tek ülke Birleşik Devletler’dir. İnternet Suçları Şikayet Merkezi tarafından sunulan istatistikler, sorunun ne boyutta olduğu konusunda en azından bir fikir vermektedir. Bunlar, eğitimci tarafından kullanılabilir ve güncel tutulmalıdır. | | | |
|  | ***Yatırım planları***  *Sanal alışveriş siteleri ya da yeni hizmet sağlayıcıları gibi ileri teknoloji gerektiren planlar için mali destek istemek amacıyla İnternetin kullanılması*    ***Kredi kartı planları***  *İnternetten yüksek değerli mallar satın almak için yasa dışı bir şekilde elde edilmiş kredi kartlarının kullanılması*  ***İş Fırsatları / Evde Çalışma Programları***  *Kurbanların evde çalışma programları ile ilgili bilgi ya da ürünler için peşin ödeme yaptığı iş fırsatlarının tanıtımını yapmak için kullanılan İnternet*  ***419 Dolandırıcılıkları***  *Batı Afrika dolandırıcılıkları – teslim yöntemleri değişmiştir – artık geleneksel posta ya da faks talepleri yerine elektronik postadır yoksa hiçbir şey değişmez – istenmeyen e-postalar gönderme yoluyla potansiyel olarak çok geniş erişim.*  ***İnternet Bankacılığı***  *Sadece bir bankanın web sitesini kopyalayın, web adresini birazcık değiştirin, yasal banka hizmetlerine link verin ve arada gerçekten inanılmaz bir yatırım fırsatına dahil edilmesini sağlamak için önemli tutarların aktarılmasını gerektiren yüksek getirili yatırımlara bir ya da iki link verin.*  ***Felaket Yardımı Başvuruları***  *Uzakdoğu’da Tsunami’nin meydana gelmesinden itibaren 1 saat içinde İnternette kurbanlar için yardım başvurusunda bulunulan birçok web sitesi ortaya çıktı ve bunlardan çoğu sahteydi.*  ***Bitkisel Viagra***  *Alternatif tıp tedavileri alanında müşterilere istenmeyen e-postalar (spam) atılarak tanıtılan ürünlerin çoğu hiçbir faydalı etkiye sahip değildir (tabi ürünler elinize geçerse) ve hatta bazıları kesinlikle tehlikelidir.*    ***Rus Gelinler***  *Doğu Avrupalı güzel kadınları ile irtibat ve Rus eyaletlerine ucuz ziyaretler sunan siteler*    ***Piyango***  *Piyangodan kazanılanları istemek için ödeme talebi ya da kazanmak için yardım talebi (çoğunlukla yabancı ülkelerin piyangoları ile ilgili)*  ***Şifre avcılığı***  *İyi bilinen kaynaklardan (banka ya da internet servis sağlayıcı gibi) geldiği süsü verilen ve kişisel bilgilerin doğrulanmasını talep eden e-posta mesajları*    Eğitimci, dersin verildiği bölgeden ilgili vakalar bulmaya çalışmalı ve bunları örnek olarak kullanmalıdır. Dersin sonunda eğitimci, katılımcıları internet suçlarına dair kendi bilgi ve deneyimlerini paylaşmaları konusunda teşvik etmelidir. | | | |
|  | **Uygulama Alıştırmaları (eğer varsa)**  Bu oturum için uygulama alıştırmaları öngörülmemektedir, çünkü bu alıştırmaları vermek için gerekli teknoloji düzeyi ve İnternet erişiminin her yerde mevcut olacağının garantisi yoktur.  Eğitimciler, gelecekte imkanların uygun olduğu bir ortamda verilen eğitimlere alıştırmalar ekleyerek öğrenmeye katkıda bulunmaya çalışabilir. | | | |
|  | **Bilgi Kontrolü**  Bu eğitimde yukarıdakilere ek olarak özel bir bilgi kontrolü şu anda öngörülmemektedir. Resmi bir değerlendirme talep edilmemiştir. | | | |
| **Slayt 160 - 162** | **6. Bölüm - Özet** | | | |
|  | Eğitimci, katılımcılara yönelik olarak aşağıda belirtilen hedeflerin gerçekleştirilmiş olduğundan emin olmak için şu noktalara ilişkin bilgileri özetlemeli / sınamalıdır:   * Teknolojinin suçlar üzerindeki farklı etkilerinin açıklanması * Bir bilgisayar sisteminin bileşenlerinin sayılması, * Verilerin bilgisayar sistemlerinde nasıl depolandığının açıklanması * Farklı bilgisayar işletim sistemlerinin tanınması * Ağların nasıl çalıştığına dair temel bilgilerin açıklanması * İnternetin işlevlerinin tarif edilebilmesi * En az 5 temel İnternet uygulamasının tanınabilmesi * İnternetin geçmişten günümüze kadar olan gelişiminin açıklanabilmesi * Farklı İnternet uygulamalarının ayırt edebilmesi * Suçluların çeşitli İnternet uygulamalarını nasıl kullandığının tespit edilmesi   Bu, grup tartışması, katılımcılara sorular sorulması, küçük sınavlar ya da başka yöntemlerle gerçekleştirilebilir.  Bu derste, hakim ve savcıların görevlerini etkili bir şekilde gerçekleştirmeleri için gereken teknoloji bilgilerinin türü ve düzeyine dair rehberlik sunmaya çalışılmıştır. Ders, konuların eksiksiz bir analizi olduğu iddiasında değildir.    Eğitim geliştiricilerinin, hazırladıkları materyallerin mümkün olduğu kadar güncel olmasını sağlaması ve en son teknoloji konularını ve bunların eğitimin verileceği yerdeki yargı alanında hukuki, usul ve kanıtlarla ilgili kararlar üzerindeki etkilerini bu materyallere dahil etmesi tavsiye edilmektedir. Verilerin katı hal disklerinde ya da Web 2.0’da depolanması gibi ceza yargılaması sistemini etkileyecek teknolojik değişiklikler vardır. Bunlar, eğitim programlarına dahil edilmesi ve daha da yaygınlaştıkça güncellenmesi gereken önemli konular olacaktır.    Diğer programlarda da olduğu gibi, hakimler için geliştirilen tüm eğitim dersleri, özgün, ölçülebilir, başarılabilir, ilgili ve zamanlı olan net amaçlara sahip olmalıdır. Amaçların gerçekleştirilebilmesi için bu elzemdir. “Anlama” ve “bilme” gibi kelimelerle amaçların kullanımından kaçının çünkü bunlar kriterleri karşılamaz. Örneğin, bir konunun “bilinmesi” amacının gerçekleştirilip gerçekleştirilmediğini nasıl ölçersiniz? Ölçülebilir olan listeleme ya da tespit etme gibi kelimeleri kullanmak daha iyidir. Özgün, ölçülebilir, başarılabilir, ilgili ve zamanlı amaçlar oluşturmaya yönelik bir rehber şu adreste bulunabilir:  [www.sheffield.ac.uk/.../Guide%20to%20setting%20objectives.doc](http://www.sheffield.ac.uk/.../Guide%20to%20setting%20objectives.doc)  Bilgilendirme için örnek olaylarının kullanılması, bu tür bir eğitim için uygun görülmektedir ve yetişkinlere yönelik öğretim tarzlarında sadece didaktik öğretimden daha faydalıdır.  Eğitim geliştiricisinin temel rolü, tüm öğrenim etkinliklerinin genel amacının ve özel amaçların gerçekleştirilmesini sağlamaktır. Bu bölümde bu sürece yardımcı olacak bazı bilgiler verilmektedir. | | | |
| **Potansiyel Ek Kaynaklar**  Elektronik kanıtlara ilişkin olarak eğitim materyallerinin geliştirilmesinde eğitimcilerin faydalanabileceği yayınlar, bunları hazırlayan kurumlar ve ülkelerle birlikte aşağıda verilmektedir. | | | | |
| **Kurum** | | **Ülke** | **Örnek belgeler** | |
| Uluslararası Standardizasyon Teşkilatı (ISO) ve Uluslararası Elektroteknik Komisyonu (IEC) | | Uluslararası | ISO/IEC 17025:2005 Test ve kalibrasyon laboratuvarlarının genel yeterlik şartları (18.10 Elektronik kanıt sınıfı, 01 Veri koruma, .02 Veri analizi)  ISO/IEC CD 27037 Bilgi teknolojisi – Güvenlik teknikleri – Dijital kanıtların tespiti, toplanması, edinilmesi ve korunmasına yönelik ana esaslar  ISO/IEC 9797-2:2011 Bilgi teknolojisi – Güvenlik teknikleri -- Mesaj Doğrulama Kodları (MAC) -- Bölüm 2: Özet fonksiyonu kullanan mekanizmalar | |
| Avrupa Adli Bilişim Kurumları Ağı (ENFSI) | | Avrupa Komisyonu | EA-5/03 Suç mahallinin araştırılması alanında ISO/IEC 17020’nin uygulanmasına yönelik rehberlik | |
| Polis Şefleri Derneği (ACPO)  PCeU  Galler Emniyet Güçleri  E-Suç Galler | | İngiltere, Galler ve Kuzey İrlanda  Galler | Bilgisayar Bazlı Elektronik Kanıtlar için İyi Uygulamalar Kılavuzu.  İlk müdahale ekibi kılavuzu: bilgisayarla ilgili olaylarda ilk müdahale için ilk müdahale ekibine yönelik bir kılavuz. | |
| ACPO | | İngiltere, Galler ve Kuzey İrlanda | Tavsiye ve İyi Uygulamalar Kılavuzu: İleri teknoloji/Bilgisayar Suçu Birimlerinin Yöneticileri için. | |
| ACPO | | İngiltere, Galler ve Kuzey İrlanda | Yönetici Kılavuzu: E-Suç Soruşturmalarının Yöneticileri için Tavsiye ve İyi Uygulamalar Kılavuzu. | |
| Britanya Standartlar Enstitüsü (BSI) | | Birleşik Krallık | ASTM E1732 – 11 Adli Bilişimle İlgili Standart Terminoloji  ASTM E1492 – 11 Kanıtların Alınması, Belgelendirilmesi, Depolanması ve bir Adli Bilişim Laboratuvarında Tutulmasına Yönelik Standart Uygulamalar | |
| Birleşik Krallık Akreditasyon Servisi (UKAS) | | Birleşik Krallık | Belgelendrime Kuruluşu akreditasyonu ile ilgili yayınlar | |
| Adli Bilişim Düzenleyicisi (FSR) | | Birleşik Krallık (İçişleri Bakanlığı) | Ceza Yargılaması Sistemindeki Adli Bilişim Uzmanları ve Çalışanları için Uygulama ve Davranış Kuralları  Adli Bilişim Grubu Tutanağı | |
| Mühendislik ve Teknoloji Kurumu (IET) | | Uluslararası (IET, IEE [Elektrik Mühendisleri Kurumu) ve IIE’den [Birleşik Mühendisler Kurumu] oluşmaktadır). | Yeni ortaya çıkan ve yerleşik teknoloji alanlarında standartların geliştirilmesi. | |
| Avrupa Sanal Suçlar Eğitim ve Öğretim Grubu (ECTEG) | | Avrupa Komisyonu (Europol) | ECTEG toplantılarının tutanakları | |
| Britanya Bilgisayar Derneği, Sanal Suçlar ve Adli Bilişim uzman Grubu | | Birleşik Krallık | Politika dokümanları | |
| ABD Adalet Bakanlığı | | ABD | Dijital Kanıtların Adli İncelemesi: Emniyet Güçleri için bir Kılavuz | |
| FBI/SWGDE | | ABD | Dijital Kanıtlar: Standartlar ve İlkeler | |
| ABD Ticaret Bakanlığı | | ABD | Cep Telefonu Adli Bilişim Kılavuzu | |
| Uluslararası Bilgisayar Kanıtları Teşkilatı | | Uluslararası | Dijital Kanıtlar Kılavuzu | |
| Avrupa Konseyi | | Avrupa Komisyonu | Sanal Suçlar Sözleşmesini imzalamak isteyen ülkeler için yasama ve usul şartları | |
| Interpol | | Uluslararası | Sanal Suçlar Kılavuzu | |
| Adalet Becerileri | | Birleşik Krallık | E-suçlara yönelik ulusal mesleki standartlar, dijital kanıtların idaresi, adli bilişim ve sanal suçlara ilişkin soruşturmalar için bilgi beceri standartları sunar. | |
| ABD Gizli Servisi (ABD İç Güvenlik Bakanlığı) | | ABD | Elektronik Kanıtların Ele Geçirilmesi için En İyi Uygulamalar  v.3A İlk Müdahale Ekipleri için Cep Kılavuzu | |
| Avrupa Komisyonu | | Avrupa Komisyonu | OISIN projesi 2002/OIS/014 “e-kanıtların” ele geçirilmesi | |
| Ulusal Adalet Enstitüsü (NIJ)  (Ulusal Teknoloji Standartları Enstitüsü (NIST) | | ABD | Elektronik Suç Mahalli Araştırması: İlk Müdahale Ekipleri için bir Kılavuz (2. Baskı) | |

|  |  |  |
| --- | --- | --- |
| Ders 1.3.1 – Günlük Değerlendirme | | **Süre: 30 Dakika** |
| **Gerekli kaynaklar:**   * Windows 7 ve Office 2010 kurulu olan bir dizüstü bilgisayar ya da PC * Projektör * PowerPoint Sunum | | |
| **Amaç:**  Bu oturumun amacı, önceki günlerde gerçekleştirilen faaliyetleri değerlendirmek, katılımcılardan geri bildirim almak ve oturumun hedeflerinin gerçekleştirilip gerçekleştirilmediğini kontrol etmektir. | | |
| **Hedefler:**  Dersin sonunda öğrenciler:   * Önceki günlerde gerçekleştirilen ve anladıkları faaliyetlerin alanlarını tespit edebilecek, * Bilgilerini istenen düzeye getirmek için gerekli olan materyalleri değerlendirmek için ihtiyaç duydukları alanları tespit edebilecektir. | | |
| **Giriş**  Bu oturum, öğrencilerin önceki günlerde öğretilen konuları anlayıp anlamadıklarını ve her bir oturumun her bir hedefini yerine getirip getiremediklerini kontrol etmelerine imkan tanımak için hazırlanmıştır. Ayrıca eğitimciye öğrencilerin bilgi düzeyini kontrol etme ve öğretim materyallerinin geliştirilebileceği alanları tespit etme imkanı vermektedir. | | |
| **Slayt no.** | **İçerik:** | |
| **Slayt**  **1 - 12** | **PowerPoint** (ya da başka bir tür sunum)  Bu sunumdaki slaytlar, eğitimcinin ve katılımcıların önceki gün faaliyetlerini değerlendirmelerine yardımcı olmak için verilmektedir. Eğitimci, gündemi ve hedefleri temel ölçüt olarak kullanarak bu faaliyetleri yeniden özetlemelidir. | |
|  | **Uygulama Alıştırmaları** (varsa)  Bu oturum için uygulama alıştırmaları hazırlanmamıştır. | |
|  | **Bilgi Kontrolü**  Eğitimci, oturumun boyutlarının her birinden ilgili sorular sorarak bilgi kontrolü gerçekleştirmelidir. | |
|  | **Özet**  Bu oturum, önceki gün faaliyetlerinin özeti olarak tasarlanmıştır ve ayrı bir özet gerekli değildir. | |

|  |  |  |
| --- | --- | --- |
| Ders 1.2.3 Suç faaliyeti olarak sanal suçlar – Yerel mevzuat | | **Süre: 90 Dakika** |
| **Gerekli kaynaklar:**   * Windows 7 ve Office 2010 kurulu olan bir dizüstü bilgisayar ya da PC * Projektör * PowerPoint Sunum | | |
| **Amaç:**  Bu oturumun amacı, sanal suçlara dair ulusal mevzuatı, açıklanan suç ihlallerinin türlerini ve ilgili ve yürürlükteki uluslararası hukuki çerçeveyi katılımcılara tanıtmaktır. | | |
| **Hedefler:**  Dersin sonunda öğrenciler:   * Sanal suçlara dair ulusal mevzuatı tanıyabilecek, * Ulusal mevzuatta belirtilen suç ihlallerini türlerini tespit edebilecek, * Uluslararası hukuki çerçeve senaryosu bağlamında sanal suçlara dair ulusal mevzuatın bazı özelliklerini tespit edebilecektir. | | |
| **Giriş**  Bu oturumun hedefi, hakim ve savcıların sanal suç davalarına ilişkin kovuşturma ve yargılamalarda yerel mevzuattaki yasal hükümleri etkili bir şekilde kullanmalarını sağlamak için onlara gerekli tüm temel bilgilerin sağlanmasıdır. Oturumun sonunda katılımcılar, yerel mevzuatta şunlara ilişkin yasal hükümleri tespit edebilecektir:   * Bilgisayar sistemlerinin ve verilerinin gizliliği, bütünlüğü ve kullanılabilirliğine karşı işlenen suçlar * Bilgisayar verileri ve sistemleri aracılığıyla işlenen suçlar * Suçlarla ilgili içerik   Bu oturum, Budapeşte Sözleşmesi’nin bir ülkenin (Portekiz) ulusal mevzuatına nasıl dahil edildiğinin örneğini öğrencilere sunmak için hazırlanmıştır. Eğitimcilerin, Portekiz ile ilgili bilgileri kendi ülkelerinin ilgili mevzuat bilgileriyle değiştirmeleri gerekecektir. | | |
| **Slayt no.** | **İçerik:** | |
| **Slayt 1 - 66** | **PowerPoint** (ya da başka tür bir sunum)  Bu bölümdeki slaytların içeriği, yerel eğitimlerin her birinde nelerin anlatılabileceğinin birer örneğidir.  İdeal olarak ulusal maddi hukuka dair oturumda imzalanan ya da kabul edilen uluslararası hukuk dokümanlarından ve bunların yerel hukuka aktarılmasını sonuçlarından bahsedilmelidir.  Ayrıca, ulusal hukuka göre suç türlerinin bir tarifi ve sonunda eğer mümkünse ulusal maddi hukukun muhtemel özelliklerinin bir tarifi verilmelidir. | |
| **Slayt 2** | **Gündem**  Bu oturum dört bölümden oluşmaktadır:   1. Birinci Bölümde, Budapeşte Sanal Suçlar Sözleşmesi’nin Maddi Ceza Hukuku kısmına odaklanılacaktır. 2. Ulusal Maddi Ceza Hukuku İkinci Bölümün konusu olacaktır. 3. Üçüncü Bölümde Örnek Olaylara odaklanılacaktır. 4. Son olarak tüm bölümlerin bir özeti Dördüncü Bölümde sunulacaktır. | |
| **Slayt 3** | Eğitimci şu noktaları işleyecektir:   * Maddi ceza hukuku hükümleri ve Budapeşte Sözleşmesi’ne göre suçları tarif etmek için kullanılan bazı temel faktörler. * Maddi ceza hukuku hükümleri ve mevcut ulusal hukuka göre suçları tarif etmek için kullanılan bazı temel faktörler. * Ulusal mevzuat ile başta Budapeşte Sözleşmesi olmak üzere uluslararası dokümanlar arasında uyum sağlanmasına yönelik ihtiyaç ve bunun avantajları. | |
| **Slayt 4** | * Sunulan örnek olaylar ile ilgili tartışmalara göre ilgili maddi hukuk hükümleri | |
| **Slayt 5 ve 6** | **Birinci Bölüm – Budapeşte Sanal Suçlar Sözleşmesi – Maddi Ceza Hukuku**  Sanal suçlara dair ilk uluslararası anlaşma olan Budapeşte Sözleşmesi, ceza soruşturmalarında uluslararası birliğini kolaylaştırmayı ve geliştirmeyi amaçlamaktadır.  Temel amaçlardan biri işbirliğini mümkün kılmak için Taraflar arasında maddi hukukun uyumunu sağlamaktır. Bu amaçla Budapeşte Sözleşmesi şunları tanımlar:   * Bilgisayar sistemlerinin ve verilerinin gizliliği, bütünlüğü ve kullanılabilirliğine karşı işlenen suçlar * Bilgisayarlar aracılığıyla işlenen suçlar | |
| **Slayt 7** | Bu bölümde sanal suçların en önemli kategorilerinden birisine değinilmektedir: Bilgisayar sistemlerinin ve verilerinin gizliliği, bütünlüğü ve kullanılabilirliğine karşı işlenen suçlar. Bu, dar anlamıyla sanal suçlar olarak anılabilir. | |
| **Slayt 8 ve 9** | Yasa dışı erişim suçu, bir bilgisayar sisteminin tamamına ya da herhangi bir kısmına hak ya da yetkisi olmadan erişim sağlayanlar tarafından işlenir. Bu eylem kasıtlı olmalıdır ve Budapeşte Sözleşmesi’nde Madde 2 kapsamında açıklanmaktadır.  Çoğunlukla bilgisayar sistemlerine korsan giriş (hacking) olarak anılır ve en yaygın bilgisayar suçlarındandır. Ancak, bilgisayar korsanlığı dışında yasa dışı erişim olarak sınıflandırılabilecek başka olgular da vardır. Aslında bilgisayar korsanlığı, normalde teknoloji aracılığıyla bir bilgisayar sistemine yasa dışı erişim eylemi olarak tanımlanır. Ancak, yasa dışı erişim, kullanılan teknolojiden veya hatta teknolojinin kullanılıp kullanılmamasından bağımsız olarak bir sisteme her türlü yetkisiz girişi kapsar. Buna örnek olarak bir failin bir şifreyi yasa dışı olarak ele geçirmesi verilebilir. Burada korunan hak, bilgisayar sisteminin ve verilerinin gizliliğidir. | |
| **Slayt 10 ve 11** | Budapeşte Sözleşmesi’nde Madde 3 kapsamında tarif edilen yasa dışı ele geçirme de kasıtlı bir ihlaldir. Teknik yöntemlerle bir bilgisayar sistemindeki bilgisayar verilerinin kamusal olmayan iletimlere haksız bir şekilde müdahalede bulunanlar tarafından işlenir.  Bu hüküm, bilgisayar verilerinin kamusal olmayan iletimlerinin bütünlüğünü korur ve yetkisiz bir şekilde engellenmesini suç sayar.  Bir bilgisayar sistemine ya da bu sistemden ya da bu sistem içindeki veri iletimleri, bugün ağlardaki en ilgili gerçekliklerdir.  Eğer ağ ve iletişim düzgün bir şekilde korunmuyorsa iletişimleri ele geçirmek teknik olarak çok kolaydır. İletişimlere yapılan bir ele geçirme, örneğin birinin hangi web sitelerini ziyaret ettiğini ya da gönderdiği ve aldığı e-posta mesajlarını ortaya çıkarabilir.  Dolayısıyla yasa dışı ele geçirme suçu ile ilgili hüküm, iletişim teknolojisinin savunmasızlığını ortaya koyarak kamusal olmayan iletişimlerin gizliliğini korur. | |
| **Slayt 12 ve 13** | Kasıtlı olarak ve hakkı olmadan bilgisayar verilerinin zarar görmesine, silinmesine, bozulmasına, değiştirilmesine ya da yok edilmesine sebep olanlar, Budapeşte Sözleşmesi Madde 4 uyarınca verilere müdahale suçunu işlemiş olur.  Verilere müdahale hükmü, yetkisiz müdahalelere karşı verilerin bütünlüğünü korur. Nasıl gerçek hayatta mal sahipleri, mal ve mülklerini diğerlerinin müdahalesinden uzak tutarak koruma hakkına sahipse verilerin sahibi de onları olduğu gibi tutma hakkına sahiptir. Bazı yargı alanlarında normal ve klasik hasar, verilere müdahaleyi de kapsarken diğerlerinde bilgisayar verilerine verilen zararı ya da veri müdahalesini ayrı ayrı değerlendirmeye ihtiyaç vardır.  Bu suç, ilgili verilerin (bilgisayar verileri) modern hayattaki büyük artışı ile ilgilidir. Bilgisayar verileri çok savunmasızdır ve kolaylıkla değiştirilebilir ya da yok edilebilir. Bu ceza hükmü, verilerin bütünlüğünü ve kullanılabilirliğini korur.  Veri müdahalesinin en sık vakalarından biri, kurbanın bilgisayarına haksız bir şekilde kendilerini kuran ve örneğin verileri silen virüslerin eylemleridir. | |
| **Slayt 14 ve 15** | Sistem müdahalesi, bir bilgisayar sisteminin işleyişinin engellenmesidir. Ciddi engelleme: Budapeşte Sözleşmesi Madde 5, ciddi olmayan engellemeleri kapsamamaktadır. Bu etki, eğer kasıtlı ve yetkisiz olarak işlendiyse bilgisayar verilerine giriş yapılması, bunların iletilmesi, zarar görmesi, silinmesi, bozulması, değiştirilmesi ya da yok edilmesinin sonucu olabilir. Bu özel boyut genel olarak örneğin ağın yöneticisi tarafından gerçekleştirilen güvenlik testlerini kapsamaz. Bu ihlal, bir ağın normal ve düzgün bir şekilde işleyişine müdahalede bulunabilen çok çeşitli eylemleri kapsar. Aslında Budapeşte Sözleşmesi, günlük hayatta iletişim sistemlerinin ve bilgisayar sistemlerinin önemini tanır. Bu sistemlerin kullanılabilirliği, kamusal, ekonomik ve sosyal faaliyetlerin normal işleyişi için çok önemlidir. Ancak bu suç türü, yalnızca hizmeti engelleme saldırıları gibi büyük ölçekli müdahaleleri kapsamaz. Sadece bir bilgisayara müdahale edilen küçük eylemler bile sistem müdahalesi olarak değerlendirilebilir. Tek bir e-posta adresini hedef alan *ileti bombardımanı* buna örnek olarak verilebilir. Aslında bir fail, bir bilgisayar sisteminin idare edebileceğinden daha fazla taleple bu sistemi hedef aldığında bu her zaman sistem müdahalesi suçu olarak değerlendirilecektir.  Bu suç hükmü, hem sistemin operatörlerini hem de son kullanıcıları kollayarak iletişim ağlarına erişimi korumayı öngörmektedir. | |
| **Slayt 16 - 19** | Budapeşte Sözleşmesi’nde belirtilen en karmaşık ihlallerden biri cihazların kötüye kullanımıdır – Madde 6.  Diğer suçlarda olduğu gibi, failin eylemi kasıtlı ve yetkisiz olmalıdır. Çok çeşitli faaliyetleri içerir ve bunların hepsi kötüye kullanılabilen cihazlarla ilgilidir.  Bu çok “yeni” bir suçtur ve 1989 Tavsiye Kararında yer almamaktadır. Ayrıca çok yenilikçidir - içinde tanımlanan gerçekler, önceden ulusal mevzuatların çoğunda bir suç olarak tanınmamıştır.  Temelde bir bilgisayar programı da dahil olmak üzere Sözleşmede anılan suçlardan herhangi birini işlemek amacıyla tasarlanan ya da uyarlanan cihazların üretimini, satışını, kullanım için teminini, ithalini, dağıtımını ya da başka bir şekilde kullanıma sunulmasını yasaklar.  Aynı ölçüde bir bilgisayar sistemine erişim sağlayacak bilgisayar şifreleri, erişim kodları ya da benzeri verilerin satışını da suç sayar. Bu hükümle Sözleşme, “suçları mümkün kılan ekipmanlara” ilişkin olarak gelişen ve artan öneme sahip “ikincil piyasayı” suç sayma ihtiyacını tanır: suç aletlerini çevrimiçi olarak satan bilgisayar korsanları, İnternette birçok yerde bulunabilen ev yapımı virüsler ve Truva Atı veya başka cihazlar kullanılarak çalınan şifrelerin toplu satışı. Bu demektir ki bir bilgisayar sistemine korsan giriş artık sadece vasıflı programcıların özel alanında değildir. Her “normal” suçlu, gerekli araçları ya da doğrudan çalınan şifreleri kolaylıkla satın alabilir. Suçlu satıcı çoğunlukla “müşteri hizmetleri” de sunar ve suçun işlenmesi için müşterisinin bilgisayarında gerekli ayarların yapılmasına yardımcı olur.  Madde 6’da en tartışılan ayrıntılardan biri, Sözleşmede Madde 2 ile 5 (yasa dışı erişim, yasa dışı ele geçirme, verilere müdahale ve sistemlere müdahale) arasındaki maddelerde belirtilen suçlardan herhangi birini işlemek amacıyla bir *cihazın* elde bulundurulmasını (yine kasıtlı ve yetkisiz olarak) suç sayan 1, b’ye atıfta bulunur.  Bu seçenek, bazı yargı alanlarında “hazırlık eylemleri” olarak anılan ve halihazırda ve bağımsız bir şekilde suç olarak sayılan eylemlere benzerdir. | |
| **Slayt 20** | Bilgisayarla ilgili suçlar, bir bilgisayar sistemi aracılığıyla işlenen suçlardır. Bu ihlaller, geleneksel suçların yeni türleridir, ancak yalnızca dijital dünyada işlenebilirler ve bu sanal dünyanın dışında işlenemezler. | |
| **Slayt 21** | Budapeşte Sözleşmesi Madde 7 kapsamında açıklanan bilgisayarla ilgili sahtecilik, özel bir sahtecilik türüdür. Çoğu ülkede sahtecilik, geleneksel bir suç ihlalidir. Ancak normalde somut nesnelerle ilgilidir ve bazen de bilgisayar sahteciliğini ya da bilgisayar verilerinin sahteciliğini suç saymak için kullanılamaz. Sözleşme’de Madde 7’de yer almasının sebebi de budur.  Bu noktada Sözleşme, geleneksel doküman sahteciliğine (somut dokümanlar) paralel bir suç tanımlamayı amaçlar. Ancak, bu durumda suçun nesnesi bilgisayar verileridir. Bu suç, verileri sanki orijinalmiş gibi değerlendirmek ya da hukuki amaçlar için kullanmak amacıyla bilgisayar verilerine giriş yaparak, bunları değiştirerek, silerek ya da yok ederek sahte verilerin oluşturulmasına yol açanlardır.  Bu suç da tabii ki kasıtlı ve yetkisiz eylemleri gerektirir. | |
| **Slayt 22** | Budapeşte Sözleşmesi Madde 8 kapsamında belirtilen bilgisayarla ilgili dolandırıcılık, dogmatik olarak ifade etmek gerekirse bir suç eylemi olarak geleneksel dolandırıcılıktan ayırt edilmesi zor bir suç türüdür. Ancak, gerçekte bu geleneksel suç türünün yeni ve bağımsız bir şeklidir. Yalnızca dijital ortamlarda işlenebilir.  Çoğu iç hukuk, geleneksel dolandırıcılığı suç sayar, ancak normalde bu, bilgisayarla ilgili durumlar için kullanılabilir değildir. Dolandırıcılık, bir kişinin sebep olduğu bir yalan ya da kasıtlı bir yanlışlıktır. Ancak çoğu zaman bilgisayar dolandırıcılığında bir kişinin doğrudan müdahalesi olmaz ve yalnızca bir bilgisayar sisteminin manipülasyonunun sonucudur. Bilgisayar dolandırıcılığı olarak anılan suç türünün tanımında bir fail olarak bir kişinin müdahalesinin yetkisiz bir şekilde bir ekonomik fayda sağlamak amacıyla verilerin uygunsuz bir şekilde manipüle edilmesiyle değiştirilmesinin sebebi de budur. Bu şekilde, dolandırıcılığın bir unsuru olarak başka bir kişinin kandırılması gerekliliği söz konusu değildir. | |
| **Slayt 23** | İçerikle ilgili suçlar, bilgisayar ya da ağların kullanımıyla daha kolay hale gelmiş olan suçlardır. Bu ihlal türleri başka yollarla da işlenebilir, ancak bilgisayar ve ağlar bunu daha kolay hale getirmiştir. | |
| **Slayt 24 - 26** | Budapeşte Sözleşmesi Madde 9, bu anlaşmanın en önemli yeniliklerinden birini ortaya koyar: bir bilgisayar sistemi aracılığıyla işlenen çocuk pornografisi eylemlerini suç sayar.  Çocuk pornografisi ticareti, İnternetin ortaya çıkışıyla önemli miktarda artmıştır. İletişim ve bilgi ağları, bu tür bir içerik arayanlar için çok sayıda avantaj ve imkanlar sunar. Ayrıca İnternette kullanıcılar, çocuk istismarı materyallerine çevrimiçi erişim sağlarken anonim kalabilir.  Çocuk pornografisi suçlarına ilişkin olarak tartışılması gereken ve Sözleşme metninde geniş bir şekilde ele alınan unsurlardan birisi şudur: çocuk pornografisi materyallerini yalnızca elinde bulundurmanın cezası. Madde 9, 1 bu tür materyalleri bir bilgisayar sistemi içinde yalnızca elinde bulundurmayı ve ayrıca sadece kişisel kullanım için bu tür görüntülerin satın alınmasını bir ihlal olarak tanımlar. Bu yaklaşım, konu üzerinde çalışan diğer uluslararası forumlar tarafından da yaygın bir şekilde kabul edilmektedir.  Aynı ölçüde tartışmalı başka bir konu da “sahte görüntülerin” suç sayılmasıdır. Sözleşme’nin maddeleri, yalnızca gerçek bir çocuğun cinsel ilişki sırasında görüntülerinin çekildiği durumları değil aynı zamanda örneğin tamamen bilgisayarla oluşturulmuş çocuk resimleri (örneğin cinsel faaliyeti gerçekleştiren bir yetişkinin vücuduna bir çocuk kafası yerleştirerek) ya da çocuk taklidi yapan (çocuk gibi davranarak veya giyinerek) yetişkinlerin (inandırıcı bir şekilde) resimleri gibi sahte çocuk gösterimlerini de kapsar.  Çocuk pornografisi materyallerinin yalnızca elde bulundurulmasının suç sayılması, bu konuda bir suç soruşturması gerçekleştirmeyi çok daha kolay hale getirmektedir, çünkü bu hüküm kapsamında bu tür materyalleri elinde bulunduran herkes yargılanabilir ve resimleri belirli bir şekilde kullanma niyetinin (örneğin satma) ya da bunların üretilmesine katkıda bulunma durumunun ispat edilmesi gerekmez. Bu ayrıca şüpheli pedofillerin bir çocuğa karşı dürtüleri ile hareket ettiklerine dair bir kanıt olmadan da cezalandırılabileceği anlamına gelir. Tabii ki polis ve mahkemeler, fiili ticaretin gerçekleştiğine dair kanıtlar olsun ya da olmasın çocuk pornografisi görüntülerinin şüpheli tedarikçilerini bu şekilde soruşturup mahkum edebilir.  Bu açıdan Avrupa Birliği’nin hukuki opsiyonunu da dikkate almak önemlidir. Avrupa Birliği, 29 Mayıs 2000 tarihli Konsey Kararından beri yıllardır çocuk pornografisi materyallerini yalnızca elde bulundurma eylemini suç sayma çalışmaları yapmaktadır. Daha yakın bir geçmişte, Konsey Çerçeve Kararı 2004/68/JHA’nın yerine geçen, Avrupa Parlamentosu’nun ve Konseyi’nın 13 Aralık 2011 tarihli ve 2011/92/EU no’lu, çocukların cinsel istismarı ve cinsel sömürüsü ve çocuk pornografisi ile mücadeleye dair Direktifi Avrupa Birliği’nden Üye Devletlerin, diğer yasa dışı eylemler arasında çocuk pornografisi görüntülerinin edinilmesi ya da elde bulundurulmasını suç sayması gerektiğini ifade eder (Madde 5, 2). Ancak aynı doküman, bu suç sayma talimatının, üreticinin, pornografik materyalleri yalnızca kendi özel kullanımı için elinde bulundurduğu durumlar için de geçerli mi olacağına karar verme takdirini Üye Devletlerin her birine vermektedir (üretimi amacıyla hiçbir pornografik materyaller kullanılmamış olması ve eylemde materyalin yayılması riski hiç bulunmaması şartıyla).  Avrupa Birliği’nin bu tercih hakkı, Budapeşte Sözleşmesi’nin bir bilgisayar sisteminde ya da bir bilgisayar verisi depolama ortamında çocuk pornografisi görüntülerinin üretilmesi, kullanıma sunulması, dağıtılması ya da iletilmesi, temin edilmesi ya da yalnızca elde bulundurulmasını suç sayan 9. Maddesine de kesinlikle uygundur. Ancak “temin etme” ya da “elde bulundurma” eylemlerinin dahil edilmesi, Sözleşme’nin Taraflarına hükmü kısmen ya da tamamen uygulama hakkı verir.  Bu opsiyon, Avrupa Konseyi tarafından yayınlanmış ve 2007’de imzaya açılmış Çocukların Korunmasına Dair Sözleşme (CETS 201) ile de pekiştirilmiştir. Bu anlaşmanın amacı, Taraflar arasında çocukların cinsel istismardan korumayı amaçlayan ceza hukuku hükümlerinin uyumlu hale getirilmesidir. Madde 20’ye göre diğer eylemlerin yanında “kendi ihtiyaçları ya da başkası için için çocuk pornografisi görüntüleri temin etme” ve “çocuk pornografisi görüntülerini elde bulundurma” eylemleri suç sayılmalıdır. | |
| **Slayt 27 ve 28** | Budapeşte Sözleşmesi, telif hakkı konularına dair suçlara ilişkin hiçbir hüküm içermemektedir.  Ancak, Sözleşme bu konuya ilişkin olarak kavramsal anlamda yeni düzenlemeler oluşturmasa da Sözleşme’nin 10. Maddesi buna atıfta bulunur. Sözleşme’de yalnızca gerçek dünyada telif haklarına önceki kuralların çevrimiçi ortam için de geçerli olması gerektiği vurgulanmaktadır: gerçek hayatta yasak olan bir şey çevrimiçi ortamlarda da yasak olmalıdır. Çevrimiçi ya da bir bilgisayar sistemi aracılığıyla gerçekleştirilen telif hakkı ihlalleri, gerçek dünyada gerçekleştirilmiş gibi cezalandırılmalıdır. Bu sebeple Sözleşme, halihazırda mevcut olan ve bu konuya ilişkin uluslararası anlaşma ve anlaşmalara atıfta bulunmaktadır (24 Temmuz 1971 tarihli Paris Anlaşması, Bern Sözleşmesi ve WIPO (Dünya Fikri Mülkiyet Örgütü) anlaşmaları). | |
| **Slayt 29** | Maddi ceza hukukuna atıfta bulunularak bu aşamada iki nihai konu dikkate alınmalıdır: biri yardım ve yataklığın cezalandırılması, diğeri de tüzel kişilerin cezai sorumluluğu.  Budapeşte Sözleşmesi’nin 11. Maddesi, Sözleşme’nin tüm Taraflarının iç hukukunda dikkate alması gereken yardım ve yataklı eylemlerini tarif etmektedir. Ancak, internet suçlarının çoğunlukla “çok taraflı” faaliyetler olduğunu, çoğunlukla farklı tarafların bu eylemlere anlaşılması zor derecelerde katkıda bulunduğu ve bu yüzden de kovuşturmanın potansiyel olarak zor olduğunu ifade etmektedir. | |
| **Slayt 30** | Son olarak Sözleşme’nin 12. Maddesi tüm Tarafların, tüzel kişilerin eylemlerini suç saymasını şart koşar. Bu önemli bir konudur. Aslında Avrupa Birliği’nde tüzel kişilerin faaliyetlerinin suç sayılması önemli ve çok tartışmalı bir konudur ve dolayısıyla Avrupa Konseyi’nin çerçevesinde yer almaktadır.  Hem Avrupa Birliği’nin hem de Avrupa Konseyi’nin bakış açıları, asgari olarak, şirketlerini temsil ederek ve onların çıkarına hareket eden temsilcilerin suç eylemleri için şirketlerin ve diğer teşekküllerin her türlü (cezai ya da değil) sorumluluğunu içerir. Buna ek olarak, şirketin ya da başka bir tüzel kişinin yasal bir temsilcisinin, onun kontrolü altında bulunması gereken bir kişi üzerinde denetim veya kontrolünün olmaması durumunda da Sözleşme’de tüzel kişilerin sorumluluğunun söz konusu olacağı Sözleşme’de belirtilmektedir.  Avrupa’daki bazı ülkeler, bir tüzel kişinin sorumluluğunu düzenlemek için ceza çözümlerinden ziyade özel kanun yollarını tercih etmektedir. | |
| **Slayt 32** | **İkinci Bölüm – Ulusal Maddi Ceza Hukuku** | |
| **Slayt 33 - 43** | Eğitimciler ulusal yasal hükümlere referansları buraya koyacaktır. | |
| **Slayt 44** | **Üçüncü Bölüm – Örnek Olaylar** | |
| **Slayt 45** | 1. **Örnek Olay 1**  * **Olgular / senaryo**   Bobby bir polis memurudur. Bir gece görevdeyken evinin önünde park etmiş bir Mercedes görür. Arabayı tanımaz ama karısının patronuna ait olduğundan şüphelenir. Polis merkezine telefon eder ve aracın kırmızı ışıkta geçtiğini bildirerek bilgisayar operatörü Mary’den Mercedes’in kime ait olduğunu söylemesini ister. Mary aracın gerçekten de karısının patronuna ait olduğunu doğrular.  *Bobby cezai bir suç işlemiş midir?*   * **Sorular**   *Bobby bir bilgisayar sistemine erişim sağlamış mıdır?*  *Bu erişim yetkili bir şekilde mi gerçekleştirilmiştir?*   * **Tartışma konuları**   Bilgisayara erişim sağlayan Bobby değil Mary’dir. Mary bilgisayardaki verilere erişim sağlama yetkisine sahiptir, dolayısıyla masumdur. Masum bir polis gibi davranarak verilere erişilmesini sağlayan Bobby’dir. Mary’ye yalan söylemiştir (bir sosyal mühendislik illüstrasyonu). Bu yasal bir erişim midir?  Hem Bobby hem de Mary polis bilgisayarına erişim hakkına sahiptir ancak bu hak, polis faaliyetlerine ilişkin olarak meşru bir sorgulama ile ilgili katı kurallara tabidir. Erişim bu yetkiyi aştığında bu bir suç teşkil eder mi?  Peki ya Bobby polis karakoluna gidip, Mary Mercedes’in sahibi hakkında meşru bir sorgulama yaparken onun omzunun üzerinde ekrandaki bilgileri görmeye başarırsa ne olur?  Bu omuz üzerinden bakma eylemi, Bobby’nin bilgisayar verilerine erişim sağlaması ile sonuçlanmıştır. Bobby’nin “niyetine” ilişkin olarak bazı sorular sorulabilir ve tabii ki erişim sağlamak için bilgisayar sistemini manipüle etmemiştir ancak yine de yetkisi olmadan erişim sağlamıştır (ancak bunu ispatlamak çok zordur).  Bu örnek olay, katılımcıların yetki (yetkisiz erişim) sorusunu düşünmeleri için tasarlanmıştır.  Katılımcılardan ayrıca Bobby’nin polis karakoluna gidip Mercedes’in sahibine ilişkin bilgileri bir kart dizin sisteminde araması durumunu düşünmeleri de istenebilir. Bu bilgiler, bilgisayardaki bilgilerle aynı konumda mıdır? Buradaki önemli nokta şudur ki korunan şey verilerin kendisi değil (Bobby’nin suistimali bir suç teşkil etse de bu, diğer veri koruma mevzuatlarıyla da korunabilir) verilerin depolandığı ortamdır.  Polisin bilgisayar sistemleri, şahıslarla ilgili muazzam miktarlarda kişisel bilgi ve birçok hassas bilgi barındırır. Bu verilere erişim yalnızca bundan meşru bir çıkarı olan kişilere verilmelidir. Birleşik Krallık’ta polis memurları ve polis bilgisayarı operatörleri, örneğin basının ilgilenebileceği bilgileri bulmak ya da görevi kötiye kullanan memurlar durumunda belirli bir kişi hakkında hangi bilgilerin bulunduğunu keşfetmek ya da belirli bir kişi ya da grubun aktif soruşturma altında olup olmadığını öğrenmek gibi kendi kişisel amaçlarıyla polis sistemlerine yasa dışı olarak erişim sağladıkları sıklıkla tespit edilmektedir. | |
| **Slayt 46** | 1. **Örnek Olay 2**  * **Olgular / senaryo**   Bir grup suçlu, bir banka güvenlik görevlisine yaklaşarak tuş kaydedici olarak bilinen bir cihazı bankadaki bazı terminallerin arkalarına yerleştirmesini ister. Bu cihaz kullanıcının tuş vuruşlarını kaydeder ve terminale erişimi olan birinin banka çalışanlarının kullanıcı hesaplarına girmesine imkan veren şifreleri ve diğer bilgileri alır.  Tuş kaydedici cihazın başka bir özelliği de terminalin kullanıcısı tarafından yapılan Skype telefon görüşmelerini kaydetmek üzere etkinleştirilmiş bir cihaz olmasıdır.  Suçlular ayrıca masanın üzerine terminal kullanıcısı tarafından yapılan ve kendisine gelen tüm telefonlar da dahil olmak üzere sesleri alan bir böcek yerleştirmişlerdir.  *Yasa dışı bir ele geçirme olmuş mudur?*   * **Sorular**   *Bir ele geçirme olmuş mudur?*  *Bu ele geçirme teknik yollarla mı gerçekleştirilmiştir?*  *Veriler bir bilgisayar sistemine ya da bir bilgisayar sisteminden mi iletilmiştir?*   * **Tartışma konuları**   Tuş kaydedici, terminalden iletilen verileri ele geçiren teknik bir cihazdır. Bu bir ele geçirme anlamına gelir ve kesinlikle yetkisizdir.  Peki ya Skype aramaları? Bu senaryoda verilerin, bilgisayardan iletilen diğer verilerle aynı hatta yolculuk yaptığı görünmektedir ancak kullanıcı bağımsız bir Skype telefonuna sahip olsaydı ne olurdu? Bu telefon bir bilgisayar sistemi teşkil eder miydi? Sözleşme, bir “bilgisayar sistemini” *biri ya da daha fazlası bir program uyarınca verileri otomatik olarak işleyen herhangi bir cihaz ya da birbirine bağlı veya birbirleriyle ilgili cihazlar grubu* olarak ve “bilgisayar verilerini”, *bir bilgisayar sisteminin bir işlevi gerçekleştirmesini sağlamak için uygun bir program da dahil olmak üzere olguların, bilgilerin ya da kavramların bir bilgisayar sisteminde işlenmesi için uygun bir şekilde herhangi bir gösterimi* olarak tanımlamaktadır.  Böceğin kullanımı da biraz zor bir durum teşkil edebilir. Bu bir ‘ele geçirme’ midir? Birleşik Krallık’ta mahkemeler, bir ele geçirmenin gerçekleşmesi için sinyalin ağda iletimi sırasında bir çeşit engelleme ya da soyutlamaya maruz bırakılması gerektiği yönünde değerlendirme yapmaktadır. Burada, cihaz hat üzerinde yerleştirilmiş olsaydı aynı bilgilerin elde edilmesi ile sonuçlanacaktı; buna karşın kayıt, iletimden bağımsız olarak gerçekleşmektedir.  Peki ya tuş kaydedici, çalışanlarının interneti uygun olmayan bir amaç için kullanıyor olabileceğinden endişe eden Şirket tarafından sisteme yerleştirilmiş olsaydı?  Çoğu telekomünikasyon sistemi hem kamusal hem de özel ağlarda gezinti yapar. İletişim, mülkünüzü terk ettiği noktada özel sistemden kamu sistemine geçer. Özel bir sistemin kontrolörü, bu sistemi kullanarak iletişimlere erişim sağlama hakkına sahiptir; o halde örneğin ev telefonunuzun hattı üzerinden yapılan görüşmeleri izleyebilir olmalısınız, ancak şu şartla ki bunu gerçekleştirmek için kullandığınız teknik cihazın sistemin özel tarafına bağlanmış olması gerekir.  Bu senaryo, katılımcıların, ele geçirmenin her unsurunu düşünmelerini ve bilgisayar verilerine, bunların iletimi sırasında teknik yollarla yetkisiz bir şekilde ele geçirildiğini fark etmelerini sağlamak üzere tasarlanmıştır.  Katılımcılar, bu hükmün, mesajın hitabı ya da hizmetin maliyeti ile bağlantılı bilgilerden ziyade iletişimlerin içeriğinin korunması için tasarlandığını net bir şekilde anlamalıdır. | |
| **Slayt 47** | 1. **Örnek olay 3**  * **Olgular / senaryo**   Bir suç çetesi, İnternet üzerinden dünyanın herhangi bir yerinden ulaşılabilen internet tabanlı bir e-posta sistemi kullanarak haberleşmektedir. Polisin müdahale edebileceğini düşünerek ya da bilgisayarlarında bulunursa kendilerini suçlu çıkartabilecek mesajları birbirlerine göndermek yerine bir ‘dead letter drop’ (alıcıya gönderilmeyen, ancak e-posta hesabına bırakılan e-posta) sistemi kullanırlar. Yaptıkları şey, mesajlarını asla göndermedikleri bir taslak şeklinde yazmaktır, çetenin diğer üyelerinin e-posta adresine erişmelerini sağlayan şifreleri vardır ve mesajı okuyup cevaplandırırlar.  *Eğer polisin taslak e-posta kutusuna erişmesi mümkün olsaydı, bu bir ele geçirme anlamına gelir miydi?*   * **Sorular**   *Mesaj iletilmekte midir?*   * **Tartışma konuları**   Çoğu devlet, bir iletişimin içeriğine ele geçirilmesi yetkisini vermeden önce polisin yüksek bir şüphenin varlığını aramasını şart koşar. Gerekli yetki olmadan kanıtların elde edilmesi, davanın durmasına ya da kanıtların kabul edilemez olmasına sebep olabilir.  Bilgisayarlar ve internet, e-posta, anında mesajlaşma, twitter vb. gibi çeşitli türlerde iletişimleri kolaylaştırır. Mesajlar, istenen alıcı tarafından alınmadan önce sıklıkla depolanacaktır. Henüz alınmamış bir mesaj hala iletim sürecinde olarak mı değerlendirilmelidir? Taslak mesajın istenen alıcı tarafından okunup okunmadığını bilmenin yolu yoktur. Kanunlar, e-postayı normal tasarlanma amacına uygun olarak kullananlara verdiği aynı korumayı e-posta ile normal iletişim yollarını bilerek altüst etmeye çalışanlara da vermeli midir?  Bu, suçluların birbirleriyle iletişim sağlamak için sıklıkla kullandıkları bir yoldur. Bir ele geçirmede bu mesajlara ulaşmaya çalışılıp çalışılmayacağı yerel mevzuata ya da yerel mahkemelerin tutumuna bağlıdır ancak katılımcıların şunu fark etmesi önemlidir ki eğer bu verileri elde etmek için Karşılıklı Hukuki Yardıma bel bağlamaları gerekirse talep yöneltilen devlet bunu bir müdahale olarak değerlendirebilir çünkü bir iletişimin içeriğine erişim sağlanmaya çalışılmaktadır ve gerekli adli yetkiyi almak için tesis edilmesi gereken daha yüksek bir hukuki eşik olacaktır. | |
| **Slayt 48** | 1. **Örnek olay 4**  * **Olgular / senaryo**   Polis memuru Bobby eşinin telefonu almış, şifresini tahmin etmiş ve henüz eşinin dinlemediği bir sesli mesajı dinlemiştir.  *Bu bir ele geçirme midir?*   * **Sorular**   Sesli mesaj hala iletim sürecinde midir?  Bilgisayar verilerine bir ele geçirme olmuş mudur?   * **Tartışma konuları**   Mesaj hedefine ulaşana kadar sistemde depolanmasa bile muhtemelen hala iletim sürecindedir. Mesaj muhtemelen telefon şirketinin sunucusunda dijital olarak depolanmaktadır ve bu yüzden Bobby, bilgisayar verilerine erişim sağlamıştır. Telefon bir bilgisayar mıdır? Muhtemelen evet, verilerin otomatik olarak işlenmesini sağlar. Arama yaparken telefonlar bulan polis memurları, bu mesajlara erişim sağlamak için gerekli yetkiye sahip olduklarından emin olmak için bunu dikkate almalıdır. Eğer alıcı mesajı dinlemiş ve kaydetmiş olsaydı da farklı olurdu. Bu senaryo, önceki senaryo ile benzeri konuları ortaya çıkardı. Bir arama emrini yerine getirirken hem açılmış hem de açılmamış e-postalar içeren bir bilgisayara el koyan memurlar için de aynı ölçüde geçerli olacak oldukça yaygın bir durumun ne olabileceğini göstermek üzere tasarlanmıştır. Ayrıca, Madde 3 kapsamında tespit edilen suçun, telefon, faks, e-posta ya da dosya transferi ile olmasından bağımsız olarak her türlü elektronik veri transferi için geçerli olduğunu göstermeye de hizmet etmektedir. | |
| **Slayt 49** | 1. **Örnek Olay 5**  * **Olgular / senaryo**   Bobby UFO’larla ilgilenmektedir ve Rus Hükümeti’nin 20. Yüzyıl başlarında Sibirya’ya inen bir uzay gemisini ele geçirdiğine inanır. Rus Hava Kuvvetleri tarafından yönetilen bir siteye bağlantı veren bir Rus Askere alma sitesini ziyaret eder. Hava Kuvvetleri sitesi şifre istemektedir, ancak şifre kırma aracını kullanarak siteye erişim kazanır. Sistemi keşfetmek için biraz zaman harcar ve birkaç dosya kopyalar. Faaliyetlerine ilişkin tüm günlük dosyalarını da Ruslar kimliğini tespit etmesin diye silmeye çalışır. Ana sayfayı da Hava Kuvvetleri amblemi yerine bir UFO resmi gösterecek şekilde değiştirir .  *Bobby bir suç işlemiş midir?*   * **Sorular**   Bu yetkisiz erişim bir Veri ya da Sistem Müdahalesi suçu teşkil eder mi?  Yetkisiz erişimin kanıtlarının silinmesi bir suç teşkil eder mi?  Suç yükümlülüğü oluşmadan önce bilgisayarın işleyişine ciddi bir zararın mı verilmesi gerekir?   * **Tartışma konuları**   Bu hükümlerin amacı, mal ve mülklerin bilinçli zarar vermeye karşı sahip olduğu korumanın aynısını bilgisayar verileri ve bilgisayar programlarına da sağlamaktır.  Bobby Hava Kuvvetlerinin sitesine erişim sağlama yetkisine sahip değildi. Site şifreyle korunmaktaydı. Dolayısıyla Bobby’nin bu siteye erişimi yasa dışı erişim suçu teşkil etmektedir.  Bobby verileri, günlük dosyalarını ve Hava Kuvvetleri amblemini sildi. Belki onun olmayan günlük dosyalarının oluşturulmasına sebep oldu ancak sistem bu faaliyetleri kaydetmek üzere konfigüre edilmişti. Bunları silme hakkına sahip değildi. Hava Kuvvetleri, sisteme kimin erişim sağladığını bilmek isteyebilir.    Ana sayfadaki görüntüyü değiştirerek sistemden hem veri silmiş hem de sisteme veri eklemiştir ki bu, önemli bilgilerin kaybolmasına sebep olması pek muhtemel olmamasına karşın Hava Kuvvetleri için bir utanç kaynağı olabilir. Ancak daha da önemlisi, Bobby yalnızca bilgi bulmak için sisteme erişim sağladığını ve yalnızca günlük dosyalarını ya da diğer önemsiz verileri sildiğini iddia etse de sistem yöneticisi, bu tür bir yasa dışı zorla girme eyleminin ardından verilerin bütünlüğüne güvenebilir mi?    Bir suçun bu şartlar altında işlenip işlenmediği yerel bir yorumlama konusu olacaktır. Bu ciddiyet eşiğinin henüz belirlenmemiş olmasından olabilir. Ancak, özellikle de erişim sağlanan site gizli ya da hassas veriler içeriyorsa veya örneğin bir nükleer enerji istasyonunun işletilmesinden sorumlu bir sistem durumunda bir şeyler yanlış giderse halkın tehlikeye atılacağı operasyonlarda kullanılıyorsa sistem yöneticisi, zorla girme eyleminin etkilerini tespit etmek için siteyi çevrimdışı konuma getirmek zorunda kalabilir.  Varsayalım ki Bobby’nin erişim sağladığı sistem, bir nükleer enerji istasyonunu işletmek amacıyla kullanılmaktadır; Madde 4 ve 5’te belirtilen suçlar, Ulusal Kritik Altyapıya bir saldırı anlamına gelen böyle bir zorla girme eyleminin ciddiyetini yansıtmak için yeterli midir? | |
| **Slayt 50** | 1. **Örnek Olay 6**  * **Olgular / senaryo**   Otomatik bir istenmeyen e-posta (spam) gönderme programı, her gün tüm dünyada binlerce kullanıcıya istenmeyen e-postalar gönderir. Eğer e-posta açılırsa, kullanıcının makinesine yazılım yüklenir. Yazılım kullanıcıların bilgisayarlarının çalışmasını engelleyen hiçbir şey yapmaz, kullanıcı bilgisayarlarından veri elde etmez, verileri silmez veya daha başka bir zarara neden olmaz, ancak, bu kullanıcı bilgisayarının artık, ‘bot kontrolör’ünün çok çeşitli faaliyetlerde kullanabileceği bir ‘Botnet’in bir parçasını oluşturan bir ‘Zombi’ olduğu anlamına gelir.  *Spam göndermekten sorumlu olan kişi tarafından Madde 4 veya 5’e aykırı bir suç işlenmiş midir?*   * **Sorular**   Kullanıcıların makinelerine yetkisiz bir erişim olmuş mudur?  Kullanıcıların makinelerindeki veriler değişikliğe uğramış mıdır?  Kullanıcıların makinelerine herhangi bir zarar gelmiş midir?   * **Tartışma konuları**   Hiçbir zarara sebep olunmamış olmasına rağmen yazılım, kullanıcıların makinelerindeki verilerde değişikliğe yol açmaktadır. Kullanıcıya hiçbir uyarıda bulunulmadığından ya da kullanıcı bilgisayarında değişiklik yapılmasına herhangi bir şekilde onay vermediğinden bu değişiklik yetkisizdir. İstenmeyen e-postaların gönderilmesi yasa dışı mıdır yoksa yalnızca rahatsız edici bir fiil midir? Yalnızca olumsuz bir etkiye sebep olduğunda mı yasa dışı sayılmaktadır?  Peki ya bu istenmeyen e-postalar, bir ek ve ekin açılması için “bunu seveceksiniz” yazan bir davet içerseydi ne olacaktı?  Alıcının verileri bilgisayarına indirmeyi seçtiği ve böylelikle buna onay verdiği konusu tartışılabilir. Ancak gerçek şu ki verilebilecek olan herhangi bir onay, bilinçli bir onay olmayacaktı ve olmadı. Tabii, bilinmeyen alıcılardan gelen ekleri açmayı seçenlerin bu riski göze aldığı da tartışılabilir.  Kullanıcının, bilgisayarının ‘botnet’in bir parçası olduğunu umursamaması herhangi bir fark yaratır mı?  İnternette gezinirken bilgisayarımıza girebilecek materyallerin niteliğine gerekli özeni göstermeden ancak web sitelerinin kendilerine verdikleri isimlere, dosyaların isimlerine ya da arama motorunun verdiği sonuçlara güvenerek siteleri ziyaret ederiz ve verileri indiririz. Bir resmin küçük görüntüsüne büyük görüntüyü görmek için tıklamak, kazanmaya çalıştığımız bir veri bilinçliliği ve verilerin niteliğine ilişkin tam bilinçli bir onayı işaret etmektedir. Edindiğimiz tam ekran görüntüsünün bir uçağın resmi olduğunu anlamak için bir arabanın küçük resmine tıklarsak bu verinin edinilmesine onay verdiğimiz söylenemez.  Bir web sitesine verilen bir bağlantıyı açmayı seçmek, birçok verinin indirilmesine yol açacaktır. Eğer site meşru bir siteyse bu verilerin çoğunluğu muhtemelen web sitesinin içeriği ile ilgili olacaktır ancak bir kısmı da üçüncü tarafların yerleştirdiği reklamlardan oluşabilir. Yine bilinçli bir tercih yaptık ve bunun internette yaygın bir uygulama olduğunu bilerek reklamı almak için dolaylı bir onay vermiş olduk. İnternet endüstrisinde yaygın bir uygulama, verileri kullanıcıların internet tarayıcısında ‘çerezler (cookies)’ bölümüne indirmektir.  Çerezler, kullanıcının internet göz atma tarihçesinin kaydedilmesi de dahil olmak üzere çeşitli işlevleri yerine getirir. Bir kullanıcıya, tarayıcısı üzerindeki çerez fonksiyonunu etkisiz hale getirme seçeneği verildiğinde bu seçenek, kullanıcının bu verilerin indirilmesine onay verdiği şeklinde yorumlaması için yeterli midir? | |
| **Slayt 51** | 1. **Örnek Olay 7**  * **Olgular / senaryo**   Bobby polis bilgisayar sisteminin kötüye kullanımından dolayı görevden alınan eski bir polis memurudur. Polis departmanından intikam almaya karar verir. Eski departmanına saatte 70.000 e-posta göndermesine olanak tanıyan bir e-posta programı kullanır. Polis memurlarının şefinden gelmiş gibi görünsün diye e-posta başlığını değiştirir ve böylece polisi e-posta sunucusunu meşru bir kaynaktan geldiğine inandırır. Polis sunucusu bu yoğun trafiği kaldırmaya elverişli değildir ve çöker.  *Bu bir sisteme müdahale suçu mudur?*   * **Sorular**   *Bir e-posta göndermek, bir bilgisayar sistemi olan e-posta sunucusuna erişimi ya da erişim çabasını içerir.* Bu sunucunun sahibi bu erişime ne derecede yetki vermektedir?  Eğer bir e-posta adresiniz varsa bu diğerlerini size e-posta mesajları göndermeleri için davet ettiğiniz anlamına gelmez mi?   * **Tartışma konuları**   Soru yerinde bir sorudur. Bobby bir sisteme erişim sağlamış ve veriler girerek sistemin çökmesine sebep olmuştur. Halkın erişimine açık bir e-posta adresine sahip olmak, adresin sahibinin mesajlar almaya dolaylı olarak onay verdiği anlamına gelir. Bobby, polisin her e-postanın alınışına onay verdiğini ve polisin sisteminin bu kadar çok mesajı kaldıracak kapasiteye sahip olmayışının onun suçu olmadığını öne sürebilir. Ancak gerçekten onay verilmiş midir? Bir evin sahibi, kendisine gönderilmiş mektupların posta kutusuna konması için postacıya dolaylı bir onay verir. Pizzacı broşürleri gibi önemsiz postalar almaya ilişkin olarak da dolaylı bir onay söz konusudur. Ancak ev sahibi, evin giriş kapısını açmasını engelleyecek kadar çok pizza broşürünü almaya onay vermez.  E-postanın göndereninin ayrıntılarını değiştirerek e-posta sunucusuna erişimin dolandırıcılık yoluyla sağlandığı da söylenemez mi? Bu yanıltıcı e-postaların alınmasına onay verilmemektedir.  Bu senaryo e-postaları ilgilendiriyorken, yöneltilen trafiği kaldıramayacak olan web sitelerini hizmeti engelleme saldırısıyla çökertmeye çalışanlar için bu ilke iyidir. Bir web sitesine bağlanma, kullanıcı bilgisayarı ile web sitesi arasında veri alışverişini gerektirir. Siteye bağlanmaya ilişkin dolaylı onayla ilgili benzeri konular, e-posta mesajlarına ilişkin tartışmalarda ortaya çıkmaktadır. | |
| **Slayt 52** | 1. **Örnek Olay 8**  * **Olgular / senaryo**   Bobby ayrıldığı karısının iş yerine bir e-posta gönderir. Başlığı bir arkadaşından gelmiş gibi değiştirir. E-posta, Bobby’nin karısının bilgisayarını kontrol etmesine olanak tanıyan ‘tüm alanlara erişim’ denen bir program içerir. Bobby programı kullanmaya fırsat bulamadan programın varlığı, izinsiz girişin kapsamının değerlendirmesini yapmak üzere sistemi kapatan sistem yöneticisi tarafından tespit edilir.  *Bobby Madde 5’e aykırı bir suç mu işlemiştir?*   * **Sorular**   Bobby sistemde tutulan verilerin bastırılmasına mı sebep olmuştur?  Bobby bir bilgisayar verilerinin işleyişini mi engellemiştir?  Bu verilerin bastırılması ya da sistemin işleyişinin engellenmesi yetkili bir şekilde mi gerçekleştirilmiştir?   * **Tartışma konuları**   Sistem yöneticisinin Bobby’nin e-postasına yanıtı, sistemin kullanıcılarına hizmetin engellendiği anlamına gelir. Dolayısıyla sistemde tutulan verilere erişim bastırılmıştır ancak buna karşın erişim kısıtlamasının geçici olması muhtemeldir. Suç, verilerin kalıcı olarak erişilemez/kullanılamaz olmasını gerektirmez.  Bir e-posta adresinin sahibinin, diğerlerinden veri alınmasına ne ölçüde onay verdiğini tartıştık.  Madde 5, bir ya da birden çok ve birbirine bağlı bilgisayar sistemi ile ilgilidir. İnternete bağlı tek bir bilgisayar, bir sistemin parçası mıdır?  Bobby’nin karısının iş bilgisayarının, bir sistemin parçası olması olmamasından daha muhtemeldir. Muhtemelen Yerel Alan Ağının (LAN) ya da Geniş Alan Ağının (WAN) veya kurum içi ağın bir parçasıdır. Bobby sistemin işleyişini engellemiş midir?  Bobby hizmeti engelleme saldırısından sorumlu olmadığını ve böyle bir olaya sebebiyet verme niyetinde olmadığını öne sürebilir ama aslında tam tersine, karısının neler yaptığını öğrenmek için sistemin çalışmaya devam etmesini istemiştir. Hizmeti engelleme saldırıları, bir internet sitesini çevrimdışı hale getirmek için genellikle yeterli değildir ancak hizmet sağlayıcıları, saldırının sistemleri üzerindeki etkisini ve diğer müşterilere yönelik rahatsızlığı en aza indirmek için siteyi çevrimdışı hale getirecektir.  Bu senaryoda Bobby’nin, Madde 5’e aykırı bir suç için gerekli niyete sahip olduğu gözükmemektedir ancak bu tabii ki suç sorumluluğundan kaçabileceği anlamına gelmez.  Bu, sanal suçluların diğerlerin bilgisayarlarına erişim sağlamak için sıklıkla kullandığı bir Truva virüsü örneğidir. | |
| **Slayt 53** | 1. **Örnek Olay 9**  * **Olgular / senaryo**   Kozmetiklerin hayvanlar üzerinde denenmesini protesto eden bir çevrimiçi internet “korsancılığı” grubu, kozmetik şirketleri ve kadın dergilerinin internet sitelerine karşı ‘Dağıtık Hizmet Engelleme’ ( DDOS) saldırıları düzenler. Grup internet siteleri aracılığıyla, grubun internet sitelerine saldırıları koordine etmesini ve böylece belirli bir sürede internet sitesine erişim sağlamaya çalışan trafiğin miktarını en üst düzeye çıkarmayı sağlayan ‘Supergun’ (Süper silah) adını verdikleri yazılımı dağıtır. ‘Supergun’ yazılımı esasen sistem yöneticileri tarafından sistemlerinin güvenliğini test eden bir araç olarak geliştirilmiştir. Ancak, yazılım hala tamamen aynı şekilde çalışırken, kullanıcı ara yüzü çok daha kolay kullanılacak şekle getirilmiştir ve artık grubun logosunu taşımaktadır.  *Supergun’ı karşıdan yüklemeye uygun hale getirmek bir suç mudur?*  *Supergun’a sahip olmak suç mudur?*   * **Sorular**   Supergun’ın meşru bir amaç için kullanılabileceği gerçeği bir davanın açılamayacağı anlamına mı gelir?  Supergun’ın karşıdan yüklemeye uygun hale getirilmesi bu yazılımın dağıtımı anlamına mı gelir?   * **Tartışma konuları**   Bu Maddenin ilgili olduğu suçlar yetkisiz erişim, yasa dışı ele geçirme, veri ve sistem müdahalesidir.  Yazılım esasen ikili kullanımdayken yani meşru bir işlevi varken şimdi kullanıcı arayüzü değiştirilmiştir. Bu, yazılımın elde bulundurulmasını vb. suç haline getirir mi?  Önceki örnek olaylarımıza bakarsak, Bobby’nin karısının bilgisayarına erişim sağlamak için kullandığı “tüm alanlara erişim” yazılımı meşru bir kullanıma sahiptir. Bunun gibi programlar, kullanıcıların kendi bilgisayarlarına uzaktan erişim sağlamasına olanak tanır. Peki ya Bobby’nin şifre kırma yazılımına sahip olması? Bu bir suç mudur? Niyetle ilgili sorular sorulabilir. Bu yazılımı elinde bulundurmaya ilişkin meşru sebebi nedir? Bu yazılımı bir suç işlemek için yerleştirmeye çalıştığını gösterecek herhangi bir kanıt var mıdır?  Bu suç, meşru yazılım tedarikçileri ve kullanıcılarının eylemlerini suç saymak üzere tasarlanmamıştır. Burada olduğu gibi kötü niyete dair kanıtlar olduğunda sorun belki de ortaya çıkmaz. Ancak sanal suçlara bulaşanlar da sıklıkla meşru internet faaliyetlerine katılır ve belki de bu yazılımları kullanan ve geliştiren endüstri çalışanlarıdır ancak fırsat olduğunda bu tür yazılımları suç faaliyetinin desteklenmesi için yerleştirmeye hazırlardır. Peki ya mağaza sahipleri? Belirli bir donanım ya da yazılıma ilişkin olarak bir müşterinin hangi niyete sahip olabileceğini nereden bilebilirler? Suçun sınırları çok mu muğlak? | |
| **Slayt 54** | 1. **Örnek Olay 10**  * **Olgular / senaryo**   Bir yazılım tedarikçisi bir şifreleme yazılımı üretmiştir. Yazılım sabit diski iki bölüme ayırır. Bu bölümlerden her biri erişim için bir şifre gerektirir ancak, yalnızca bir bölüm sıradan kullanıcılar tarafından görülebilirken ve gizli bölümün varlığı mevcut adli bilişim yazılımları kullanılarak tespit edilemez.  Üretici bu yazılımın, şifrelerini açıklamak zorunda bırakıldıkları bir durum yaşayabilecek herkes tarafından kullanılabileceğini iddia eder. Bu, gizli bölümdeki verilerin, görünen dosyanın şifresi açıklansa bile güvende olacağı anlamına gelir.   * **Sorular**   Bu yazılımın imalatı, üretimi, dağıtımı, kullanımı ya da elde bulundurulması cezai bir suç teşkil eder mi?   * **Tartışma konuları**   Hepimiz verilerimizi sürekli olarak güvende tutmak zorunda kalıyoruz. Böyle bir program, suç işleyenler ve bilgisayarlarının içeriğinin onları suçlu çıkarabileceğinden korkanlar için bariz bir şekilde faydalıyken program, onlar tarafından suç işlemek için değil kanıtları gizlemek için kullanılmaktadır.  Sanal suçlular, tespit edilmekten kaçınmak için, gerçek IP adreslerini ifşa etmeden internette gezinmek için anonimleştiriciler (IP numarasını gizleyen yazılımlar) de dahil olmak üzere diğer program veya sistemlerden ya da sabit diskin içeriğini silen kanıt yok edici programlardan faydalanabilir. | |
| **Slayt 55** | 1. **Örnek Olay 11**  * **Olgular / senaryo 3**   Nick kendi kurum içi ağı (intranet) olan büyük bir şirketin bilişim departmanında çalışmaktadır. Şirket politikası çalışanlarına şirketin bilgisayar ve internet bağlantısını kullanarak çevrimiçi alışveriş yapmayı yasaklar. Nick boş zamanlarında şirketin çevrimiçi ödemeler yapan çalışanları tespit edebilmesine ve disiplin soruşturmasında kanıt olarak kullanılmak üzere bu bilgiyi kaydetmesine imkan veren bir yazılım geliştirmeye başlar. Nick gerekli becerilere sahip değildir ve ‘Jupiter’ ile çevrimiçi irtibata geçer. Bir kullanıcının bilgisayarına indirildikten sonra o kullanıcı çevrimiçi ödemeleri gerçekleştirmeden kullanılanlara benzer bir çevrimiçi bir formu doldurmaya başladığında etkin hale gelen ve kullanıcı tarafından girilen verileri kaydeden bir yazılımı birlikte geliştirirler. Nick’in şirketi çok memnunken Jupiter bir Truva programı kullanarak yazılımı yerleştirmeye başlar.  *Nick bir suç işlemiş midir?*  *Şirket bir suç işlemiş midir?*  *Jupiter bir suç işlemiş midir?*   * **Sorular**   Cihaz temel olarak belirli cezai suçlar işlemek amacıyla mı tasarlanmış ya da uyarlanmıştır?   * **Tartışma konuları**   Sanal suçlular, suç işlemelerine olanak tanıyan ya da suç işlemelerine yardımcı olan çeşitli araçlara ulaşabilir. Kendi ‘bot’unuzu kurmanıza olanak tanıyacak kodu satın almak ya da bir ‘botnet’ satın almak veya kullanıcının ‘şifre avcılığı’ gibi çeşitli suç türlerini gerçekleştimesini sağlayacak bir botnet’e erişim satın almak mümkündür.  Jupiter, kendisinin ya da başkalarının kötüye kullanabileceği mali bilgileri kullanıcılardan elde etmek için bu programı kullanacaktır. Şirket büyük ihtimalle Nick’in bu yazılımı çalıştığı süre içinde geliştirmiş olduğunu düşünmektedir. Nick masumdur ve Jupiter’in güçlü bir suç aleti yaratmasına farkında olmadan yardım etmiştir. Ne Nick ne de Şirket, ceza için gerekli suç niyetine sahip değildir. Peki Jupiter bu programı çalışanlarının internet faaliyetlerini izlemek isteyen şirketlere pazarlasaydı farklı olur muydu? Jupiter yazılımın suçlular için bariz bir şekilde ilgi çekici olmasına karşın meşru bir amacı olduğunu öne sürebilir mi? | |
| **Slayt 56** | 1. **Örnek Olay 12**  * **Olgu / Senaryo**   Stefan ev bilgisayarında gerçekçi banka ödeme emirleri üretmek için ticari olarak satışı yapılan bir yazılım kullanmaktadır. Ödeme emrini bankasına götürür, banka belgenin gerçek olduğunu kabul edip Stefan’ın hesabına nakit aktarımı yapar.  *Stefan hangi suçu işlemiştir?*   * **Sorular**   Sahte ödeme emrinin üretilmesi bilgisayarla ilgili bir sahtecilik midir?  Bu suç yalnızca banka çalışanı tarafından ödeme emri orijinal olarak kabul edildiğinde mi tamamlanmış olur?   * **Tartışma konuları**   Banka ödeme emrinin üretilmesi bir bilgisayara gerçek olmayan verilerin girilmesini gerektirir. Yani bu belge, Stefan’ın lehine düzenlenmiştir. Ancak, bu yetkisiz bir şekilde mi yapılmıştır yoksa Stefan kendi bilgisayarında böyle bir doküman üretme hakkına sahip midir? Stefan, ödeme emrini bankayı dolandırmak için kullanma niyetine sahip olabilir ancak her ne sebeple olursa olsun bu belgeyi yazıcıda yazdıramaz. Belgenin kağıda basılıp basılmaması Stefan’ın sorumluluğuna ilişkin olarak bir fark yaratır mı?  Bu suç aslında bu tür bir senaryo üzerinde düşünmek için oluşturulmamıştır ancak eğer yerel mevzuat sahte bir banka ödeme emrinin üretimini suç saymıyorsa bu yönde bir fayda sağlayabilir. Bu suçların girişim gibi ikincil sorumluluk açısından değerlendirilmesi daha iyi olacaktır.  Bu suç gerçekte bir bilgisayar sistemini suç işlemeye yönelik bir mekanizma olarak kullananlara hitap etmektedir. Dolayısıyla iyi niyet çerçevesinde hareket ederken banka çalışanı, verilerin gerçek olduğunu kabul ederek Stefan tarafından temin edilen verilerin girişini yapar. | |
| **Slayt 53** | 1. **Örnek Olay 13**  * **Olgular / senaryo**   Stefan gençken ne kadar üstün yetenekli bir atlet olduğu konusunda arkadaşlarına her zaman övünür. Arkadaşları şüphecidir. Eski okulunun veritabanına ulaşmayı başarır ve kendisini okul atletizm takımının kaptanı ve bir çok madalya kazanmış olarak gösterecek şekilde kayıtları değiştirir  *Bu bilgisayarla ilişkili bir sahtecilik suçu mudur?*   * **Sorular**   Değiştirilmiş olan veriler herhangi bir yasal amaçla kullanılmayacaktır.   * **Tartışma konuları**   Stefan verileri değiştirmiş ve sahte veriler girmiştir. Bu erişim ve değişikliğin yetkisiz olduğu açıktır. Stefan’ın işlemiş olabileceği diğer suçlara bir kenara bırakırsak bilgisayarla ilgili bir sahtecilik suçu işlediği şüphelidir çünkü bu veriler yasal amaçlarla kullanılmayacaktır.  Sahtecilik suçu, mali ya da başka bir kazanç ile ilgili değildir. Bu suçlar bilgisayarla ilgili dolandırıcılık suçlarının sınırları içinde yer alır. Bu Madde, elektronik verilerin hukuki ilişkiler için çeşitli sonuçlara sebep olabilecek güvenliği ve güvenilirliğini temin etmeyi amaçlamaktadır. “Yasal amaçlar” terimi, yasal olarak uygun işlem ve dokümanlara işaret eder. | |
| **Slayt 58** | 1. **Örnek Olay 14**  * **Olgular / senaryo**   Bobby, Polis Teşkilatı’ndaki işini kaybettiği için ve de boşandıklarından beri karısına nafaka vermek zorunda olduğu için para kazanmanın başka bir yolunu aramaktadır. Her zaman hisse senedi alım-satımına ilgi duymuştur ve Belçika’da uranyum çıkarmak için özel izni bulunan Flanders Mining Inc. (Flanders Madencilik) adlı şirketin tanesi 1 Avrodan 1000 adet hissesini alır. Bobby, üyeleri de kendisi gibi borsaya ilgi duyan bir internet forumunun üyesidir. Bobby, Belçika hükümetinden bir arkadaşının Belçika’da önemli miktarlarda uranyum tespit edildiğini söylediğini belirten bir mesaj yollar. Bu duyuruyu takiben Flanders Mining hisse fiyatları hızla yükselişe geçer ve hafta sonunda her bir hisse 1000 Avro olur. Bobby daha sonra hisselerini satar.  *Bobby bir suç işlemiş midir?*   * **Sorular**   Bobby’nin mesajı asılsız mıdır?  Eğer mesaj asılsız ise başka bir kişi bunun sonucu olarak kayıp yaşamış mıdır?    Bobby ekonomik bir avantaj elde etmiş midir?   * **Tartışma konuları**   Eğer Bobby tarafından gönderilen mesaj asılsız ise bir suç işlemiş olabilir. Bir bilgisayara düzmece veriler girmiş ve hisse fiyatlarının yükselmesiyle kendisi için ekonomik bir kazanç elde etmiştir.  Verilerin girilmesiyle bunun etkisi arasında nedensel bağlantı var mıdır?  Bobby başka birinin kayıp yaşamasına sebep olmuş mudur? Hisselerin yanlış bir şekilde değer kazandığından ve büyük olasılıkla bir noktadan sonra düşmeye başlayacağından muhtemelen evet. Ancak hisse piyasasının aşırı şekilde oynak olduğu dikkate alındığında bir hissenin değeri, herhangi bir zamanda insanların buna ödemeye razı oldukları fiyat değil midir? Gerçekte herhangi birisi dolandırılmış mıdır? İnternette bu tür söylenti ve mesajlardan fazlasıyla yok mudur? Herhangi biri bu mesaja gerçekten inanacak ve bunun hisse fiyatını manipüle etmek için acemi bir girişim olduğunu göremeyecek midir? Bu, internetteki yalanları anlayamadığımız anlamına mı gelir? | |
| **Sliayt 59** | 1. **Örnek Olay 15**  * **Olgular / senaryo**   Stefan arabayla bankaya gider. Park yerinde yeterli bozuk parası olmadığını görür. Otomatik parkmetreye bir rondela atarak bir bilet alır.  *Stefan bir suç işlemiş midir?*   * **Sorular**   Parkmetre bir bilgisayar mıdır?  Parkmetrenin biletleri otomatik olarak üretmesi ve fiilen hiçbir insanın kandırılmamış olması fark eder mi?  Park biletinin statüsü nedir?   * **Tartışma konuları**   Parkmetre bir bilgisayardır. Park etme tarifesine göre ödenmesi gereken para tutarını hesaplayarak ve uygun süre ile bir bilet vererek bilgileri işler. Stefan, cihaza bozuk para atmak yerine rondela atarak sahte veri girmiştir. Madde 7, temin edilen verilerle bir insanın işlem yapmasını gerektirmez.  Bu şekilde park bileti alma eylemi sahteciliktir, bu bileti oluşturmak için kullanılan veriler sahtedir ve bir kişinin (park görevlisinin) bileti orijinal olarak değerlendirmesi ve Stefan’a park bileti vermemesi için oluşturulmuştur. | |
| **Slayt 60** | 1. **Örnek Olay 16**  * **Olgular / Senaryo**   Stefan yakalandıktan sonra polis, kendisinde çok sayıda üçüncü şahısa ait kredi kartı bilgisi bulunduğunu ortaya çıkarır.  *Bu verilere sahip olmak cezai bir suç mudur?*   * **Sorular**   Bilgisayar dosyaları hangi statüye sahiptir? Bunların sadece ikili kodlar dizisinden ibaret olmasına rağmen bunlar hukuka uygun ‘şeyler’ midir?   * **Tartışma konuları**   Birleşik Krallık’ta bir eşyaya dolandırıcılık amacıyla sahip olmak ceza gerektiren maddi bir suçtur. Bilgisayar dosyası da bir eşyadır. Tabii ki gerekli niyetin ispatlanması gerekir ancak bu tür verileri elde bulundurmanın meşru bir sebebi olduğunu ileri sürmek zordur.  Bu bir suç hazırlığı olarak değerlendirilebilir. | |
| **Slayt 61** | 1. **Örnek Olay 17**  * **Olgular / senaryo**   Adam, cinsel açıdan istismar edilen çocukların fotoğraflarını paylaşan özel bir çevrimiçi grubun üyesidir. Adam aynı zamanda bir ‘eşler arası’ dosya paylaşım grubunun da üyesidir ve çevrimiçi gruptan edindiği istismar edilen çocukların fotoğraflarını bu eşler arası paylaşılan klasörlere koyarak, eşler arası ağda bulunan diğer üyeler için erişilebilir kılar.  *Adam hangi suçları işlemiştir?*   * **Konular**   Üretim, temin ve dağıtımın tanımları.  Adam, internetten görüntü dosyaları indirmiştir. Bu fotoğrafların indirilmesi, üretilmesi ile denk tutulur mu? İndirme ve özellikle de bir görüntüyü bilgisayara kaydetme, televizyon seyretmek gibi değildir. İndirme eylemiyle yeni bir şey (bir dosya) oluşturulur. Dolayısıyla internette görüntülere bakma, yeni görüntülerin oluşturulmasına sebep olur. Savcılar bu kavramı faydalı bulabilir.  Eşler arası dosya paylaşım ağları, üyelerinin, ağdaki diğer üyeler tarafından kendilerinin kullanımına sunulan dosyalara erişim sağlamasına olanak tanır. Adam, görüntüleri paylaşılan klasöre koyarak bunları dağıtıma hazır hale getirmektedir. | |
| **Slayt 62** | 1. **Örnek Olay 18**  * **Olgular / senaryo**   Bill Kamboçya dönüşü havaalanında yakalanır. Dizüstü bilgisayarında Güney Doğu Asyalı oldukları görülen çocuklarla cinsel ilişkiye girdiğini gösteren çok sayıda görüntü bulunur.  *Bu görüntülerle ilgili olarak Bill hakkında dava açılabilir mi?*   * **Konular**   Yargı alanı.  Maddi suç seçimi, bir görüntünün elde bulundurulması ya da görüntünün üretimi.   * **Tartışma konuları**   Görüntülerin üretilmesine ilişkin olarak yargı alanı sorunları yaşanabilir çünkü görüntüler yabancı bir ülkede üretilmiş görünmektedir.  Elde bulundurma bir sorun olmamalıdır.  Tüm görüntüler ayrılmamış bir alanda bulunmuş olsaydı ne olurdu?  Elde bulundurma hem bilgi hem de kontrol gerektirir. Bill, silinmiş olan görüntülerin sabit diskte hala erişilebilir olduğunu biliyor ya da bilmiyor olabilir ancak teknik araçlara ve uzmanlığa sahip olmadıkça bu silinen görüntüleri asla kurtaramaz. Ancak, görüntülerin üretimi ya da geçmişte elde bulundurulmasına ilişkin olarak kovuşturma başlatmak savcıya kalır (yargı konularına tabi olarak).  Eğer görüntüler kumsalda oynayan 3-7 yaş aralığındaki çıplak çocukları içerseydi ve Bill nüdist olduğunu açıklayıp bu görüntülere bakmaktan cinsel haz aldığını kabul etseydi ne olurdu?  Bu görüntülerin yasa dışı olup olmaması yerel yorumlamalara göre değişen bir konudur. Birleşik Krallık’ta genellikle görüntülerin cinsel unsurlar içermesini şart koşarız ve fotoğrafçının güdüsünü dikkate almayız.  *Hangi görüntünün yasa dışı olduğuna kim karar verir? Bu suçun sınırları yeteri kadar net midir?* | |
| **Slayt 63** | 1. **Örnek Olay 19**  * **Olgular / senaryo**   WWW.Iuvfishin.com, olta balıkçılığına adanmış bir internet sitesidir. Site ABD'de bulunan sunucularda barındırılmaktadır. Sitenin sahipleri, sitenin saldırıya uğramış (hacklenmiş) olduğunu ve site içerisine bin adet çocuk istismarı görüntüsü yüklenip, yerleştirildiğini fark eder. Bu işlemin yapılış şekli, bu görüntülerin sitenin sıradan kullanıcıları tarafından görülemeyeceği anlamına gelir. Site fotoğraflara erişmiş olanların IP adreslerini kaydeder.  John’a ait olan IP adresi, ülkenizde polise verilmiştir. Polisler, John’ın adresini araştırır ve binlerce çocuk istismarı görüntüsü bulunan bilgisayarına el koyar. İnternet tarihçesi ve bu dosyalardaki verilerden, bu görüntülerin çoğunun internetten indirildiği açıktır.  *John hangi suçları işlemiştir?*   * **Sorular**   Görüntülerden John’un sorumlu olduğu nasıl ispatlanır?  Pedofili suçları ile suçlanan şüpheliler üzerindeki etki.   * **Tartışma konuları**   Görüntülerin gizlenmesine yönelik bu yöntem alışılmadık bir yöntem değildir. Gruplar, görüntülere bağlantıları yayınlar. Ancak, bir IP adresinin siteye nasıl bağlandığını anlamadan bir arama izni almak için yalnızca bu IP adresine bel bağlamak tehlikeli olabilir. Başka bir site tarafından yönlendirilerek tamamen masum kişilere ulaşıp hiçbir görüntüye erişim sağlayamayabilirler. Tabii ki birden fazla kez ziyarette bulunmuş ya da birkaç görüntüye erişim sağlamış da olabilirler.  Bir şahısın pedofil olmakla suçlanmasından önce gösterilmesi gereken özeni tartışmak için bu kullanılabilir. Bu suçlarla suçlanan kişiler arasında intihar oranı yüksektir. Tüm sanal suç davalarında olduğu gibi şüphelinin klavye başında doğru zamanda tespit edilmesi gerekir. Bir IP adresi, aynı adresteki birkaç şahıs tarafından kullanılabilir ya da kablosuz ağ, başka biri tarafından gasp edilmiş olabilir. Bu tür suçlamalar, masum bir kişi üzerinde yıkıcı etkilere sebep olabilir. | |
| **Slayt 64** | 1. **Örnek Olay 20**  * **Olgular / senaryo**   ABD’de polis, aylık abonelik ücreti ödeyenlere çocuk istismarı görüntüleri sunan siteleri barındıran bir internet sitesini kaldırmıştır. ABD makamları erişim için ödeme yapan bu kişilerden IP adresi, kredi kartı numarası, e-posta adresi, fatura adresi ve şifreler dahil olmak üzere çeşitli veriler elde etmiştir. Müşterilerden biri de Oswald’dır. Arama emri alındıktan sonra bilgisayarı incelenmiştir. Oswald “Kanıtların Ortadan Kaldırılması” adlı bir program kullandığından suçlayıcı hiçbir şey bulunamamıştır.  *Oswald bir suç işlemiş midir?*   * **Sorular**   Oswald asli bir suç mu işlemiştir yoksa ikinci dereceden bir sorumluluğa mı sahiptir?  Yargı alanı hakkında sorun var mıdır?  ABD web sitesinin tam olarak otomatik olması fark eder mi?  Kanıtların Ortadan Kaldırılması programının kullanımı hakkında neler söylenebilir?   * **Tartışma konuları**   Oswald, hiçbir görüntüyü elinde bulundurmamaktadır ve bu görüntülere bakmak için bir web sitesine erişim sağladığını ispatlayamayız ancak bu amaçla abonelik ücreti ödemiş olduğunu ispatlayabiliriz. Oswald başka bir kişiyi, ABD’deki web sitesi sahibini, çocuk istismarı görüntülerini dağıtıma hazır hale getirmesi ya da dağıtımını yapması için ikna etmek amacıyla para ödemiştir. Dolayısıyla bu bir suç teşkil eder mi?  ABD’li web sitesinin tam otomatik olması, kredi kartı bilgilerinin işlenmesinde fiilen hiçbir insanın görev almaması anlamına gelir. Durum böyle olsa bile işlem, mali olarak kar sağlayan bir kişi tarafından oluşturulmuştur ve bu kişi tarafından yönetilmekte ve sürdürülmektedir.  Bir kanıt yok etme programının kullanılması kendi başına yasa dışı değildir. Oswald polis soruşturması sırasında programı etkin hale getiremeseydi muhtemelen adalet yönetimi ile bağlantılı bir suç işlememiş olacaktı. Ancak Oswald hakkında dava açılırsa bu tür programların kullanımı mahkeme tarafından cezayı ağırlaştırıcı bir unsur olarak değerlendirilebilir. | |
|  | **Uygulama Alıştırmaları** **(eğer varsa)**  Bu oturum için uygulama alıştırmaları hazırlanmamıştır. | |
|  | **Bilgi Kontrolü**  Eğitimci, oturumun boyutlarının her birinden ilgili sorular sorarak bilgi kontrolü gerçekleştirmelidir. | |
| **Slayt 65 ve 66** | **Özet**  Eğitimci, aşağıdaki hususlara ilişkin olarak bilgileri özetlemeli / sınamalıdır:   * Maddi ceza hukuku hükümleri ve Budapeşte Sözleşmesi’ne göre suçları tarif etmek için kullanılan bazı temel faktörler. * Maddi ceza hukuku hükümleri ve mevcut ulusal hukuka göre suçları tarif etmek için kullanılan bazı temel faktörler. * Ulusal mevzuat ile başta Budapeşte Sözleşmesi olmak üzere uluslararası dokümanlar arasında uyum sağlanmasına yönelik ihtiyaç ve bunun avantajları. * Sunulan örnek olaylar ile ilgili tartışmalara göre ilgili maddi hukuk hükümleri. | |

|  |  |  |
| --- | --- | --- |
| Ders 1.2.4 Yerel usul hukuku | | **Süre: 90 Dakika** |
| **Gerekli kaynaklar:**   * Windows 7 ve Office 2010 kurulu olan bir dizüstü bilgisayar ya da PC * Projektör * PowerPoint Sunum | | |
| **Amaç:**  Bu oturumun amacı, elektronik kanıtlara ilişkin olarak ulusal hukuk ve ulusal düzenlemeler tarafından öngörülen araştırma/soruşturma tedbirlerini her ülkeden katılımcılara tanıtmaktır. | | |
| **Hedefler:**  Dersin sonunda öğrenciler:   * Elektronik kanıtlara ilişkin ulusal düzenlemeleri tespit edebilecek, * Ulusal hukuk kapsamında izin verilen araştırma tedbirlerini ve elektronik kanıtların toplanması ve korunmasının değer ve şartlarını tespit edebilecek, * Uluslararası hukuki çerçeve bağlamında elektronik kanıtlara ilişkin ulusal adli muamelelerin bazı özelliklerini tespit edebilecektir. | | |
| **Giriş**  Bu oturum, Budapeşte Sözleşmesi’nin bir ülkenin (Portekiz) ulusal mevzuatına nasıl dahil edildiğinin örneğini öğrencilere sunmak için hazırlanmıştır. Eğitimcilerin, Portekiz ile ilgili bilgileri kendi ülkelerinin ilgili mevzuat bilgileriyle değiştirmeleri gerekecektir. | | |
| **Slayt no.** | **İçerik:** | |
| **Slayt 1 - 29** | **PowerPoint (ya da başka tür bir sunum)**  Bu bölümdeki slaytların içeriği, yerel eğitimlerin her birinde nelerin anlatılabileceğinin birer örneğidir.  İdeal olarak elektronik kanıtlara dair oturumda, her bir Devlet imzalanan ya da kabul edilen uluslararası hukuk dokümanlarından ve bunların iç hukuka aktarılmasını sonuçlarından bahsedilmelidir.  Ayrıca, ulusal hukuk kapsamında izin verilen araştırma tedbirlerinin bir tarifi ve elektronik kanıtların toplanması ve korunmasının önemi ve şartlarına dair bir açıklama sunulmalıdır.  Dersin sonunda eğer uygunsa elektronik kanıtlara ilişkin ulusal adli muamelelerin olası özelliklerine değinilmelidir. | |
| **Slayt 2** | **Gündem**  Bu sunum üç bölümden oluşmaktadır:   * Birinci Bölümde, Budapeşte Sözleşmesi’nin usul hükümlerine değinilecektir. * İkinci Bölümde ulusal hukuk kapsamındaki usul hükümleri açıklanacaktır. * Üçüncü Bölümde önceki iki bölümün bir özeti sunulacaktır. | |
| **Slayt 3** | Oturumun sonunda katılımcılar, Budapeşte Sözleşmesi’nin usul hükümlerini ve iç hukuk kapsamındaki usul hükümlerini açıklayabilecektir. | |
| **Slayt 5** | **Birinci Bölüm - Budapeşte Sözleşmesi’nin usul hükümleri**  Sözleşme’nin en önemli ve ve kesinlikle altı çizilmesi gereken yönlerinden biri usul boyutudur. | |
| **Slayt 6** | Madde 14, Budapeşte Sözleşmesi’ne çok geniş bir kapsam katar. Buna göre Sözleşme, soruşturulan suç Sözleşme’de belirtilen suçlardan biri olduğu zaman, -açıkça- uygulanabilir olacaktır.  Ancak, iki oldukça geniş kapsamlı uzantıyı da içerir:   * usul kuralları bir bilgisayar sistemi aracılığıyla işlenmiş olan bütün suçların soruşturulmasında kullanılabilir; * kurallar, herhangi bir suçla ilgili elektronik kanıtların toplanması için de geçerlidir. Bu demektir ki her suç potansiyel olarak Sanal Suçlar Sözleşmesi’nin usul kuralları kapsamına girer. | |
| **Slayt 7 - 10** | Madde 16 ve 17 bilgisayar verilerinin hızlı korunması ve trafik verilerinin hızlı korunması ve açıklanmasını tanımlar. Her iki hüküm de çok yenilikçi ve son derece önemlidir.  Geleneksel kanıtlar nihayetinde uzun bir süre olay mahalinde kalacaktır, ancak dijital veriler (elektronik kanıtlar) çok uçucudur ve hızla kaybolabilir. Örneğin trafik verileri bir suçun failini belirlemek için çok yararlıdır. Ancak bu tür bilgi, veri saklama mevzuatını hayata geçirmediği takdirde, sistematik olarak kullanılmaz. Avrupa dışında birçok ülke henüz bu tür bir mevzuatı yürürlüğe koymamıştır. Bu nedenle, trafik verileri sadece eğer emniyet güçlerine bu tür geçici bilgilerin korunması emrini verme olanağı tanıyan yasal bir belge varsa elde edilebilir.  Dolayısıyla Madde 16, kanıtların tutmak ve verilerin ele geçirilmesi ya da ifşası için adli emirler almak üzere zaman kazanmak için “hızlı koruma” öngörür. Bu trafik verileri ya da içerik verileri için geçerli olabilir.  İnternetteki bir iletişim bir değil birden fazla hizmet sağlayıcıyı içerebilir. Emniyet güçlerinin bir iletişim yolu boyunca tüm sağlayıcılara istenen verileri koruma talimatı verebiliyor olması önemlidir. Dolayısıyla Madde 17 kapsamında, iletişim yolunun belirlenmesi için bir hizmet sağlayıcıya yeterli miktarda trafik verisinin ifşa edilmesi talimatı verilebilir.  Madde 16 ve 17’de, belirli bir soruşturmada ihtiyaç duyulan belirli verilere değinilmektedir. Bu, emniyet güçlerinin ihtiyaç duyabileceği düşünülerek hizmet sağlayıcıları tarafından tüm trafik verilerinin belirli bir süre boyunca saklanmasını gerektiren veri muhafaza düzenlemeleri ile karıştırılmamalıdır. Budapeşte Sözleşmesi böyle bir veri muhafaza hükmü içermemektedir. | |
| **Slayt 11 - 13** | Madde 18'in hükmü de oldukça ilginçtir. Buna göre, Taraflar'ın her biri, güvenlik güçlerine "sunma emri" verme imkanı ile birlikte yetki vermek üzere gerekli yasal tedbirleri almalıdır. Bu adli talimat, güvenlik kuvvetlerince vatandaşlara ve İnternet servis sağlayıcılarına yönelik olarak, yetkili makamlara kendi sorumlulukları altındaki bir bilgisayar sisteminde saklanan verileri veya abone verilerini temin etmelerini emretmek üzere çıkartılabilir.  Sözleşmeye göre veri sunma talimatında, istenen verilerin niteliği ve kapsamını belirtmelidir: soruşturmada ihtiyaç duyulan verilerin daha önceden tespit edilmesi gerektiği oldukça açıktır; bu nedenle belirli bir hedef olmaksızın yapılan incelemeler yasaklanmıştır. Bu yasal sınırın amacı bu tür yeni soruşturma yetkilerinin güvenlik güçlerince kötüye kullanılmasını önlemektir. Gerçek dünyada, nesnelerin veya belgelerin aranması ya da bunlara el konulması normalde sadece soruşturma altındaki olayla doğrudan ilişkili nesne veya belgelere yöneliktir. Dijital dünyada, eğer talimat bir donanımla birlikte gelen bilgilerin tümüne tam erişim iznini içerseydi, o bilgisayarda saklanan, genellikle soruşturma kapsamındaki suçla ilgisi olmayan ve (örneğin e-posta yazışmaları durumunda) üçüncü şahısları da ilgilendiren her türlü bilgiye erişime izin verilmiş olurdu.  Eğer Madde 16, ilk adımsa (verilerin korunması), korunan veriler ilgili makamlara ifşa edilmesi gerektiğinde Madde 18 de ikinci adımı teşkil eder. | |
| **Slayt 14 - 19** | Arama ve el koyma Budapeşte Sözleşmesi'nin 19. Madde’sinde açıklanmıştır.  Ulusal usul hukuku hükümlerinin çoğu arama ve el koymaya yönelik genel düzenlemeleri içerir, ancak bunların hepsi bilgisayarları arama ve bilgisayarlara el koymayı düzenleyen özel kurallara sahip değildir. Birçok yargı alanı yalnızca geleneksel arama ve el koyma uygulamalarıyla da gayet iyi idare edebilir. Ancak gerçek dünya, örneğin bilgisayar sistemlerinin birbirleriyle bağlantılı olmasının sebep olduğu, önceden bilinmeyen ve şu an dijital soruşturmalarda karşılaşılan zorluklar olduğunu göstermektedir.  Bu tür yeni sorunlarla karşılaşıldığından Budapeşte Sözleşmesi dijital dünyadaki arama ve el koyma uygulamalarını ele almak üzere belirli kurallar oluşturmuştur.  Örneğin, Madde 19.2'de, bir bilgisayar sisteminin aranması sırasında, soruşturma görevlilerinin aramanın bir başka bilgisayar sistemine doğru genişletilmesi sonucuna vardıkları durumlarda, aramanın varsayımsal olarak genişletilmesine ilişkin özel bir kural vardır. Sözleşme kapsamında, bir yetkili belirli bir bilgisayar sistemine veya bir parçasına yasal erişim sağladığında ve bu sistemin incelenmesi sırasında aranan verilerin, kendi ulusal sınırları içindeki bir başka bilgisayar sisteminde saklandığına dair makul bir inanca kapılırsa, o yetkili aramayı "süratle" diğer sisteme doğru genişletebilir.  Özellikle el koyma uygulamaları konusunda, yeni dijital ortama özgü olduklarından dolayı, altının çizilmesi gereken bazı somut konular vardır: fiziksel olarak bilgisayar verilerini ele geçirmenin çeşitli yöntemleri.  Çoğu mevzuat, yalnızca fiziksel dünyadaki arama işlemlerine özgü düzenlemelere sahip olduğundan, bilgisayar verilerine el koymaya uygun yeni ve daha etkin yöntemlere dair özel düzenlemelere sahip değildir.  Budapeşte Sözleşmesi, imzalayan devletlerden, bilgisayar verilerine yasal olarak el konulması sırasında özellikle şunlara imkan tanıyan mevzuatı yürürlüğe koymalarını talep etmektedir:   * 1. fiziksel olarak bir bilgisayar sistemine el koyma,   2. bu bilgisayar verilerini kopyalayıp bir kopyasını saklama (verilerin bir ana sunucuda saklandığı fiziksel olarak çıkartmanın imkansız olduğu ve ayrıca fiziksel olarak el koymanın o makineye erişim hakkı bulunan diğer insanların haklarını belirgin biçimde etkileyebileceği durumlarda önemlidir),   3. depolanmış ilgili bilgisayar verilerinin bütünlüğünü koruma ve son olarak,   4. erişilen bilgisayar sistemindeki bilgisayar verilerini erişilmez kılma veya silme.   Bu son hüküm, örneğin fiziksel el koymanın imkansız olduğu ama üçüncü bir şahısın verilere erişim elde etmesi durumunda fiili zararların doğabileceği durumlarda önemlidir.  Verilerin yalnızca kendi orijinal kayıtlarına el konulması hariç olmak üzere tüm bu usul olasılıkları, dijital ortamlara ilişkin özel tedbirlerdir. | |
| **Slayt 20** | Bazen araştırmacı, bir bilgisayar sisteminde depolanmış bilgilerden ziyade daha taze güncel ihtiyaç duyar. Trafik verilerinin *gerçek zamanlı* olarak toplanması, canlı soruşturmalara olanak tanır ve Budapeşte Sözleşmesi'nde Madde 20'de tanımlanmıştır. Bu tür bir müdahaleci tedbir, emniyet güçleri makamlarına teknik imkanlarıyla gerçek zamanlı olarak veri toplama ve kaydetme imkanı verecek uygun bir mevzuatı ve ayrıca hizmet sağlayıcılarının normal faaliyetleri içerisinde gerçek zamanlı olarak müşterilerinden trafik verilerini toplamaya ve kaydetmeye mecbur tutulmasına yönelik bir yetkiyi gerektirir.  Bu tarz bir soruşturma aracı, örneğin failin belirlenmesi amacıyla gerçek zamanlı olarak iletişimin kaynağını tespit etmede çok önemli olabilir. | |
| **Slayt 21** | Sonuncu ve aynı derecede önemli olarak Madde 21, içerik verilerinin ele geçirilmesini tanımlar. Trafik verilerinin yanı sıra bazen emniyet güçleri ve makamları bir suçun şüphelileri arasındaki iletişimin gerçek içeriğini bilmek zorundadır. Bazı ülkelerin zaten telefon dinlemelerine ilişkin hükümleri vardır ancak hepsi de yetkililere özellikle telefon dışındaki iletişimlere müdahale izni vermez.    Bu nedenle Budapeşte Sözleşmesi özellikle Madde 21’de araştırmacıların iletişim verilerine müdahale edip bunları kaydedebilmelerine imkan veren hükümler içerir.  Çok etkili bir soruşturma aracı olmasının yanı sıra, iletişimi izlenmesi/dinlenmesi aynı zamanda çok müdahaleci bir tedbirdir ve yalnızca ulusal hukuk tarafından ciddi suç olarak görülen bir dizi durumda Sözleşme şartlarınca izin verilir. | |
| **Slayt 23** | **İkinci Bölüm – Ulusal hukuk kapsamında usul hükümleri** | |
| **Slayt 24 - 31** | Eğitimciler, ulusal hukuk hükümlerine ilişkin referansları buraya yerleştirecektir. | |
|  | **Uygulamalı Alıştırmalar (eğer varsa)**  Bu oturum için uygulamalı alıştırma hazırlanmamıştır. | |
|  | **Bilgi Kontrolü**  Eğitimci, oturumun boyutlarının her birinden ilgili sorular sorarak bilgi kontrolü gerçekleştirmelidir. | |
| **Slayt 33 - 34** | **Özet**  Eğitimci aşağıdaki hususlara ilişkin bilgileri özetlemeli / sınamalıdır:   * Elektronik kanıtlara ilişkin ulusal düzenlemelerin açıklanması * Eğer varsa uluslararası çerçeveye değinilmesi * Ulusal hukuk kapsamında izin verilen soruşturma tedbirlerinin türlerinin ve elektronik kanıtların toplanması ve korunmasının önem ve şartlarının tartışılması * Uluslararası hukuki çerçeve bağlamında elektronik kanıtlara ilişkin ulusal adli muamelelerin bazı özelliklerinin tespit edilmesi. | |

|  |  |  |
| --- | --- | --- |
| Ders 1.3.1 – Günlük Değerlendirme | | **Süre: 30 Dakika** |
| **Gerekli kaynaklar:**   * Windows 7 ve Office 2010 kurulu olan bir dizüstü bilgisayar ya da PC * Projektör * PowerPoint Sunum | | |
| **Amaç:**  Bu oturumun amacı, önceki günlerde gerçekleştirilen faaliyetleri değerlendirmek, katılımcılardan geri bildirim almak ve oturumun hedeflerinin gerçekleştirilip gerçekleştirilmediğini kontrol etmektir. | | |
| **Hedefler:**  Dersin sonunda öğrenciler:   * Önceki günlerde gerçekleştirilen ve anladıkları faaliyetlerin alanlarını tespit edebilecek, * Bilgilerini istenen düzeye getirmek için gerekli olan materyalleri değerlendirmek için ihtiyaç duydukları alanları tespit edebilecektir. | | |
| **Giriş**  Bu oturum, öğrencilerin önceki günlerde öğretilen konuları anlayıp anlamadıklarını ve her bir oturumun her bir hedefini yerine getirip getiremediklerini kontrol etmelerine imkan tanımak için hazırlanmıştır. Ayrıca eğitimciye öğrencilerin bilgi düzeyini kontrol etme ve öğretim materyallerinin geliştirilebileceği alanları tespit etme imkanı vermektedir. | | |
| **Slayt no.** | **İçerik:** | |
| **Slayt**  **1 - 12** | **PowerPoint** **(ya da başka bir tür sunum)**  Bu sunumdaki slaytlar, eğitimcinin ve katılımcıların önceki gün faaliyetlerini değerlendirmelerine yardımcı olmak için verilmektedir. Eğitimci, gündemi ve hedefleri temel ölçüt olarak kullanarak bu faaliyetleri yeniden özetlemelidir | |
|  | **Uygulama Alıştırmaları (varsa)**  Bu oturum için uygulama alıştırmaları hazırlanmamıştır. | |
|  | **Bilgi Kontrolü**  Eğitimci, oturumun boyutlarının her birinden ilgili sorular sorarak bilgi kontrolü gerçekleştirmelidir. | |
|  | **Özet**  Bu oturum, önceki gün faaliyetlerinin özeti olarak tasarlanmıştır ve ayrı bir özet gerekli değildir. | |

|  |  |  |
| --- | --- | --- |
| Ders 1.3.2 ve 1.3.3 Elektronik Kanıtlar | | **Süre: 120 ve 90 Dakika** |
| **Gerekli kaynaklar:**   * Windows 7 ve Office 2010 kurulu olan bir dizüstü bilgisayar ya da PC * Projektör * İnternet erişimi (varsa) * PowerPoint Sunum * Bilgisayar donanımı örnekleri (varsa) * EC OISIN’in finanse ettiği e-kanıt kılavuzunun kopyası | | |
| **Amaç:** Oturumun amacı, elektronik kanıtlarla ilgili konuların (örneğin karşılaşılabilecek çeşitli türler, bunların soruşturmalar sırasında nasıl kurtarılacağı ve nasıl muamele göreceği ve ceza davalarında nasıl sunulacağı gibi) bilgisini hakim ve savcılara sunmaktır. Bu tür kanıtların diğer yargı alanlarından elde edilmesinin zorlukları hakkındaki bilgiler de sunulmaktadır. | | |
| **Hedefler:**  Dersin sonunda öğrenciler:   * Çeşitli elektronik kanıt türlerini tartışabilecekler, * Elektronik kanıtların elde edilmesi ve bunlara gösterilecek muameleye ilişkin en iyi uygulama ilkelerini açıklayabilecekler, * Elektronik kanıtlara ait “cansız kutu”, “canlı veri” ve internet kaynaklarından kaynaklanan zorlukları belirleyebilecekler, * Başka bir yargı alanından kanıtların elde edilmesine ilişkin zorlukları tespit edebilecekler, * Elektronik kanıtların gerçekliği, doğruluğu ve bütünlüğü açısından adli davalarda kabul edilebilirliğini tartışabileceklerdir. | | |
| **Süre** | **İçerik:** | |
| 30 dakika  30 dakika  60 dakika  60 dakika  30 dakika | * Giriş ve açılış (Gündem ve Oturum hedefleri) * Bölüm 1 – Elektronik kanıt nedir? * Bölüm 2 – Usuller ve İyi Uygulamalar * Bölüm 3 – Hukuki Konular * Özet | |
| **Giriş**  Bu oturumun amacı, daha geniş bir programın bir parçası olarak verilecek eğitim materyallerinin geliştirilmesi için eğitimcilere bir taslak sunmaktır. Teknoloji hızla değiştiğinden ve neredeyse doküman yayımlandığı anda ayrıntılı teknik özellikler güncelliğini kaybedeceğinden oturumlar çok kapsamlı olma imkanına sahip değildir. Hakim ve savcıların gördükleri davalardaki teknik konular hakkında yeterli bilgiye sahip olmasının sağlanması, adli sistemin adil bir şekilde yürütülmesi için elzemdir. Bu oturum, teknolojinin ilgili yönlerine ve ceza yargılaması sistemi ile ilişkisine genel bir bakış sunmaktadır. Uygun görülürse eğitimcilerin kullanabileceği bir kaynak olarak bir PowerPoint sunumu hazırlanmıştır.  Bu oturumda, hakim ve savcıların görevleri sırasında karşılaşacağı ve suçluların suç işlemek için ve emniyet güçlerinin bu suçları tespit etmek için kullandığı teknolojiler hakkında bilgiler sunulmaktadır.  Bu oturum, kaynak materyallerinin çoğunda “e-kanıtların ele geçirilmesi” adlı dokümandan faydalanmıştır. Bu doküman, OISIN programı kapsamında Avrupa Komisyonu’nun sağladığı finansmanla 2002/OIS/014[[4]](#footnote-4) referans no. ile oluşturulmuştur. Bu doküman yıllar önce oluşturulmuştur ve dolayısıyla bazı kısımları güncel değildir. Gereken yerlerde içindeki bilgiler bu eğitime dahil edilmek üzere güncellenmiştir. Doküman temel olarak emniyet güçleri ile ilgili kurumlara için oluşturulmuştur, ancak diğerleri, ilke ve usulleri ceza yargılaması sisteminde uygulayabilir. Bu doküman, e-kanıtların ele geçirilmesinin gerektiği tüm durumlarda uygulanabilir.  Her Üye Devlet, bu dokümanda önerilen tedbirleri yorumlarken kendi hukuki dokümanlarını ve düzenlemelerini dikkate almalıdır. Ayrıca her Üye Devlet, kendi uzman birimlerinin irtibat bilgilerini de eklemelidir.  Önerilen usulleri uygulamak isteyen bir kurum ya da kuruluş, kendi iç yapısına göre bireysel adımların / eylemlerin sorumluluğunu belirlemelidir. | | |
| **Slayt no.** | **İçerik:** | |
| Slayt 1 | **PowerPoint** (ya da başka bir tür sunum) | |
| **Slayt 2** | **Gündem**  Gündem slaytlarında oturumun bölümleri belirtilmektedir ve eğitimci, bu bölümleri işleyerek gerektiğinde belirli öğrenci grupları için önemi olan belirli yönlere dair ayrıntılara girmelidir. Eğitimci, materyallerin nasıl dağıtılacağını açıklamalı ve görüş alışverişi ve sorular için zaman ayırılacağını ifade etmelidir. Eğitimci, bu eğitimin etkileşimli olmak üzere tasarlandığına ve delegelerden katılımda bulunmalarının beklendiğine vurgu yapmalıdır. Eğitimci, bir değerlendirme yapılıp yapılmayacağını ve uygulanacak geçiş notu hakkında bilgiler de dahil olmak üzere bu değerlendirmenin ne şekilde yapılacağını açıklamalıdır (Bu pilot programda değerlendirme yapılmayacaktır). | |
| **Slayt 3** | Katılımcıların, dersin hedeflerinin neler olduğunu anlaması önemlidir. Bunlar, “akıllı” hedefler olmalı ve slayttaki bilgiler kullanılarak oturum başlamadan önce katılımcılara ayrıntılı bir şekilde açıklanmalıdır. | |
| **Slayt 6** | **Bölüm Bir – Elektronik kanıt nedir** | |
|  | **Elektronik kanıt türleri ve kaynakları**  **Örnekler**  Eğitimci, elektronik kanıtların türlerini tespit ederek ve katılımcıları konu hakkında bilgilerinin ayrıntılarını vermeye teşvik ederek grup içinde bir tartışma başlatmalıdır. Eğitimci, daha sonra tahta üzerinde altı çizilmiş olan türleri belirtmelidir. Eğer izleyiciler belirli kanıt türlerinin altını çizmezse eğitimci listeyi kendisi tamamlamalıdır. Liste, cansız kutu, canlı veri, bellek, İnternet gibi tüm kanıt türlerinin yanı sıra dersin teknoloji bölümünde ele alınanlar gibi kanıt kaynaklarını da içermelidir. | |
| **Slayt 8** | **Tanım**  Kanıtın tanımı, normalde ulusal mevzuatta yer almaktadır. Bu uluslararası bir kurs olduğu için genel bir tanım kullanılmıştır. Bu tanım Black’in Hukuk Sözlüğünden alınmıştır. Eğitimciler, bu dersi kendi ülkelerinde verirken bu tanımı ulusal tanımlarla değiştirmelidir.  Kanıt, ‘hukuki olarak bir davada, mahkemenin veya jürinin tarafların görüşü yönünde ikna edilebilmesi amacıyla; tarafların şahitler, kayıtlar, belgeler, beyanlar, somut nesneler vb. aracılığıyla sunduğu bir ispat türü ya da delil niteliğindeki unsurdur.’ Genel olarak elektronik bilgiler, adli davalarda kanıt olarak kabul edilebilir. | |
| **Slayt 9 ve 10** | Elektronik kanıtın uluslararası kabul görmüş hiç bir tanımı yoktur. Ancak, bütün ülkelerde *elektronik kanıta* bir şekilde atıfta bulunan kaidelerin yer aldığı düzenlemeler vardır.  “Tanıma” uygun yararlı örnek:  Elektronik bir cihazla depolanan ya da iletilen, araştırmaya/soruşturmaya ilişkin olarak değer taşıyan bilgiler ya da verilerdir.  [www.nij.gov/topics/forensics/evidence/digital/digital-glossary.htm](http://www.nij.gov/topics/forensics/evidence/digital/digital-glossary.htm)  Yine, mevcut olabilecek ulusal tanımların ülke içindeki eğitimlerin içeriğine dahil edilmesinin sağlanması eğitimcinin sorumluluğundadır.  Soruşturma ve yargılama sürecinde kanıtları doğru bir şekilde yorumlamak ve analiz etmek için modern suç türleriyle mücadelede uzmanların ve desteği gereklidir. | |
| **Slayt 12** | **Elektronik kanıtların kaynakları ve türleri**  Bu kursun teknoloji bölümünde belirtilen kanıt türleri ve kaynaklarının tüm listesini yeniden değerlendirmeye gerek yoktur. Eğitimci, bu oturumun başında oluşturulmuş olan listeyi kullanarak tekrar özet geçmelidir.  Kaynaklar, her türlü elektronik cihazı kapsar. Eğitimci, bu aşamada farklı cihazlardan elde edilen elektronik kanıtların önemini ve bunların davalarda oynadığı rolü tespit etmek isteyebilir.  Değerlendirilecek olan kanıt türleri şunları içerir:   * Statik Veriler * Canlı Veriler * İnternet Verileri | |
| **Slayt 13** | **Elektronik kanıtların özellikleri**  Elektronik kanıtların geleneksel kanıtlara kıyasla kabul edilebilirliğine ilişkin olarak ek zorluklara sebep olan birçok özelliği vardır. Çoğu durumda elektronik kanıtlar, diğer kanıtlarla aynı şekilde işlem ve muamele görür ve temel faktör, ortaya çıkan sorunların anlaşılması ve hakim ve savcıların, kanıtların elektronik özellikleri arasında ilişki kurabilmesidir.  Eğitimde verilen örneklerde görüldüğü gibi, belirtilen konulardan çoğu hem elektronik hem de geleneksel kanıtlarla ilgilidir ancak bazı farklılıklar vardır ve bunların bu aşamada vurgulanması gerekir.  Bu konular:   * **Uçuculuk**    + Kolaylıkla değiştirilebilir   + Uzun süre geçtikten sonra veriye ulaşım zorlaşabilir. * **Nitelik**    + Erişimi uzmanlık becerileri gerektirir   + Yorumlanması bilirkişi beyanı gerektirir   + Elde edilmesi ve erişilmesi için zorlayıcı gücün uygulanması gerekebilir veya kullanımı kısıtlanabilir * **Konum**    + Kanıt niteliğinde olmayan materyalle ayrılmaz bir şekilde bağlantılı olabilir   + Yetki/yargı alanı dışında olabilir * **Miktar**    + Kanıt materyallerinin belirlenmesi   + Kullanılmayan materyallerin belirlenmesi | |
| **Slayt 14** | **Kanıtlarla İlgili Konular**  Elektronik kanıtların özellikleri, altı çizilmesi gereken çeşitli meselelere sebep olur. Eğitimci, örnekler vererek bunları detaylı bir şekilde ele almalıdır.  Bu meseleler:   * + - Söylenti     - İş kayıtları     - Otomatik işlemler     - Birbirine karışmış kanıtlar     - Veri hacimleri     - Bilirkişi beyanı * **Hassas.** Bir bilgisayar sistemi tarafından işlenen bazı dijital veriler çok hassastır ve kolaylıkla silinebilir ya da değiştirilebilir. Bu özellik, yalnızca dijital kanıtların değerlendirilmesi için değil aynı zamanda bunların toplanması işlemi için de geçerlidir. Özel teknik tedbirler uygulanmadığı sürece sistem kapatıldığında genel olarak yalnızca RAM sistem belleğinde depolanan veriler kaybedilecektir. Sistem belleğinde depolanan bilgiler bir soruşturma için çok büyük öneme sahip olabileceğinden bu kanıtların toplanmasına ilişkin teknik, elektronik olmayan kanıtların toplanması işleminden farklı olabilir.      * **Kolaylıkla değiştirilebilir.** Dijital veriler kolaylıkla değiştirilebilir. Adli bilişimin en temel ilkelerinden birisi, dijital verilerin bütünlüğünün korunması gerekliliğidir. İşlemin eksiksiz bir şekilde belgelendirilmesinin ve bilgisayar verilerinin bütünlüğünün korunmasına yönelik yöntemlerin uygulanmasının sağlanması, şüphelinin kanıtlarla oynandığını iddia etmesini önlemek için elzemdir. Sonuç olarak, adli bilişim uzmanları, şüphelinin bilgisayarındaki dosyaların değiştirilmesine yol açan soruşturma işlemleri yerine daha sofistike işlemleri uygulamaya çalışmaktadır.      * **Merkezi olmayan depolama.** Geniş bantlı erişimin ve uzaktan depolama sunucularının kullanılabilirliği, bilgilerin depolanma şeklini etkilemiştir. Geçmişte araştırmacılar, bilgisayar verilerini ararken şüphelinin evine/işyerine odaklanabilirdi ancak bugün dijital bilgilerin fiziksel olarak yurt dışında depolanabileceği ve bu bilgilere gerektiğinde şüpheli tarafından yalnızca uzaktan erişim sağlanabileceği dikkate alınmalıdır. * **Teknik gelişimin hızı.** Teknik gelişim hızlı bir şekilde devam etmektedir. Önemli sayıda gelişme, adli inceleme konularına ilişkin olarak yeni zorluklar meydana getirmektedir. Bu gelişim, kanıtların toplanması işiyle meşgul olanların sürekli olarak eğitilmesini ve adli bilişim ekipmanlarının güncel tutulmasını gerektirir. İşletim sistemlerinin ve diğer yazılım ürünlerinin yeni versiyonları, soruşturmalarla ilgili olabilecek farklı veriler oluşturabilir. Geçmişte veriler disketlerde saklanırken bugün araştırmacılar, ilgili bilgilerin MP3 çalarlarda ya da USB depolama cihazına sahip saatlerde depolanabileceğini dikkate almalıdır. | |
| **Slayt 18 ve 19** | **Bölüm İki – Usuller ve İyi Uygulamalar** | |
|  | Ağırlıklı olarak, dersin bu kısmında e-kanıt kılavuzunda ele alınan konulara dayanmaktadır. Eğitimcinin dersi oluşturmasına yardımcı olmak için birçok ayrıntı sağlanmaktadır. Bunlar, eğitimci kılavuzunda ayrıntılarıyla verilmekte ve ilgili slaytlarda maddeler halinde özetlenmektedir. Eğitimci, hedeflerin yerine getirilmesini sağlamak için katılımcıların şartlarına bağlı olarak ne kadar ayrıntıya girilmesi gerektiğini değerlendirmelidir.  Kılavuz, elektronik kanıtların elde edilmesi gereken tüm durumlarda kullanılabilir.    Her Üye Devlet, bu dokümanda önerilen tedbirleri yorumlarken kendi hukuki dokümanlarını ve düzenlemelerini dikkate almalıdır. Ayrıca her Üye Devlet, kendi uzman birimlerinin irtibat bilgilerini de eklemelidir.  Önerilen usulleri uygulamak isteyen bir kurum ya da kuruluş, kendi iç yapısına göre bireysel adımların / eylemlerin sorumluluğunu belirlemelidir. | |
| **Slayt 20** | **GENEL İLKELER**  Elektronik kanıtlar toplanırken, şu genel ilkelere uymak son derece önemlidir:   1. Yerinde tanıklık, 2. Veri bütünlüğü, 3. Denetim izi, 4. Uzman desteği, 5. Görevlilerin eğitimi, 6. Yasallık ve ilkelere bağlılık.   Bu ilkeler sonraki bölümlerde açıklanmaktadır. | |
| **Slayt 21** | 1. **Yerinde Tanıklık**   İlke:*Görevli memur olay yerine asla yalnız başına katılmamalıdır*.    Bu tür bir faaliyete en az iki memur müdahil olmalıdır. Bu durum hem kişisel koruma sağlar, hem de olay yerinde daha fazla detay yakalanmasına yardımcı olur. Memurlar hareketlerini planlamalı ve koordine etmelidirler. Eğer beklenmeyen sorunlar ortaya çıkarsa, bunları çözmek de daha kolay olacaktır, çünkü “bir elin nesi var, iki elin sesi var” | |
| **Slayt 22** | 1. **Veri Bütünlüğü**   İlke:*Emniyet güçleri ya da bunların görevlileri tarafından gerçekleştirilen hiçbir eylem, daha sonradan mahkemede değerlendirmeye alınabilecek elektronik cihazların veya ortamların değişmesine sebep olmamalıdır.*    Elektronik cihaz ve veriler toplanırken bunların yazılım veya donanımında değişiklik yapılmamalıdır. Görevli memur olay yerinden toplanan malzemelerin bütünlüğünden ve dolayısıyla delil zincirinin oluşturulmasından sorumludur. | |
| **Slayt 23** | 1. **Denetim İzi**   İlke:*Elektronik kanıtlar toplanırken gerçekleştirilen tüm eylemlerin denetim izi ya da diğer kayıtları tutulmalı ve saklanmalıdır. Bağımsız bir üçüncü taraf, bu eylemleri inceleyebilmeli ve aynı sonuçlara ulaşabilmelidir.*  Üçüncü bir tarafın olay yerindeki ilk müdahale ekibinin eylemlerini yeniden düzenleyebilmesini olanak tanımak için bütün faaliyetler, mahkemede kanıt değeri taşıyabilmesi yönünden doğru bir şekilde kayıt altına alınmak zorundadır. Elektronik kanıtların elde edilmesine, depolanmasına, aktarılmasına ya da bunlara erişilmesine ilişkin bütün faaliyetler eksiksiz bir şekilde belgelenmeli, muhafaza edilmeli ve incelenebilir olmalıdır. | |
| **Slayt 24** | 1. **Uzman Desteği**   İlke:*Bir polis operasyonunda elektronik kanıtların bulunabileceği öngörülüyorsa görevli memur, uzmanları/bağımsız danışmanları zamanında haberdar etmelidir.*  Arama ve el koyma işlemleri uygulanacak soruşturmalarda dışardan uzmanlara danışmak gerekebilir. Bütün bağımsız uzmanlar bu ve buna benzer belgelerde ifade edilen ilkelerden haberdar olmalıdır. Bir uzman:   * + - Alanında gerekli uzmanlık ve deneyime,     - Gerekli soruşturma bilgilerine ve hukuki bilgilere,     - Gerekli bağlamsal bilgilere ve hukuki bilgilere, * Uygun iletişim becerilerine sahip olmalıdır (hem sözlü hem yazılı açıklamalar için). | |
| **Slayt 25** | 1. **Görevlilerin eğitimi**   İlke:*Olay yerinde hiçbir uzman bulunmuyorsa ilk müdahale ekibinin elektronik kanıtları aramayabilmesi ve bunlara el koyabilmesi için uygun bir şekilde eğitilmiş olması gerekir.*  İlk müdahale ekibinin elektronik kanıtları toplaması ve/veya elektronik bir cihazda ya da dijital depolama ortamında bulunan orijinal verilere ulaşması gereken istisnai durumlarda ekip, bu görevi düzgün bir şekilde yerine getirmek ve eylemlerinin uygunluğunu ve sonuçlarını açıklayabilmek için eğitim almalıdır. | |
| **Slayt 26** | 1. **Yasallık ve İlkelere Bağlılık**   İlke:*Davada görevli olan memur ve kurum, yasalara, genel adli ve usuli ilkelere ve yukarıda bahsedilen temel ilkelere bağlı kalınmasını sağlamaktan sorumludur. Bu, elektronik kanıtların elde edilmesi ve bunlara erişim sağlanmasında geçerlidir.*  Her Üye Devlet bu dokümanda önerilen önlemleri yorumlarken kendi kanuni düzenlemelerini ve belgelerini göz önünde bulundurmalıdır.  Uluslararası öneme sahip hukuki belgelerden biri olan Avrupa Konseyi Sanal Suçlar Sözleşmesi, halen Üye Devletler ile Sözleşmenin hazırlanmasına katılmış olan devletler tarafından imzalanmaya ve diğer devletlerin katılımına açıktır. | |
| **Slayt 28** | **Ele geçirme türleri**  Elektronik kanıtlara el koyma işleminin farklı seçenekleri, bu eğitimin önemli bir konusudur ve bu seçeneklerin hepsi farklı özellik, risk ve sonuçlara sahiptir. Eğitimci, bu seçeneklerin katılımcıların hakimlik ve savcılık görevleri üzerindeki etkilerini katılımcıların anlayabilmesi için ayrıntılı bir şekilde açıklanmasını sağlamalıdır. Aşağıdaki bilgiler, eğitimcilerin uygun materyalleri oluşturmasını sağlamak için verilmektedir.  Elektronik kanıtları ele geçirme işleminin beş genel türü vardır:   1. Elektronik ekipman ve depolama ortamlarına el koyma yoluyla ele geçirme 2. Tüm bellek içeriğinin kopyalanması yoluyla ele geçirme (görüntü alma ya da disk ikizleme) 3. Yedekleme belleği ortamlarına el koyma yoluyla ele geçirme 4. Seçili verileri kopyalama yoluyla ele geçirme 5. Kanıtların İnternetten ele geçirilmesi   Farklı ele geçirme türleri sonraki bölümlerde tartışılmaktadır. Şunun belirtilmesi gerekir ki farklı ele geçirme türlerini birleştirerek tek bir ele geçirme usulünü oluşturmak mümkündür. Örneğin, hem elektronik ekipmanlara hem de yedekleme belleği ortamlarına el koymak gerekli olabilir. | |
| **Slayt 29** | 1. **Elektronik ekipman ve depolama ortamlarına el koyma yoluyla ele geçirme**   Bu ele geçirme türü, aşağıdaki durumlarda uygun olabilir:   * El koyulacak fazla ekipman olmaması. Örneğin, bağımsız bir PC veya küçük bir ağ (örneğin, şüphelinin evinde); * El koyulan ekipmanların çalıştırılmaması/kullanılmaması sebebiyle yüksek bir mali ya da başka bir kayba uğrama riskinin bulunmaması; * İlgili suçun niteliği sebebiyle el koymanın mutlak surette gerekli olması; * El koyulacak ekipmanların destek sağladığı faaliyetleri durdurmanın gerekli/şart olması.   Bu tür bir ele geçirme işleminin avantajları şunlardır:   * Olay yerinde genellikle uzman desteği olmadan gerçekleştirilebilir; * Ele geçirme usulü genellikle fazla zaman almaz; * E-kanıtlar kontrol altına alınır; ve * E-kanıtlar kontrollü bir ortamda analiz edilebilir.   Bu tür bir ele geçirme işleminin dezavantajları ise şunlardır:   * Ekipmanların hasar görme riski bulunmaktadır; * Söz konusu suç ile ilgisi olmayan kişilere zarar verme riski bulunmaktadır; * Söz konusu suç ile ilgisi olmayan faaliyetleri engelleme riski bulunmaktadır.   **2. Tüm bellek içeriğinin kopyalanması**  Bazen görüntüleme/görüntü alma ya da disk ikizleme olarak da anılan bu tür bir ele geçirme işleminde harici bir depolama ortamlarındaki elektronik ekipmanların (ya da dijital depolama ortamlarının) bellek içeriklerinin birebir kopyasını oluşturmak için özel ekipmanlar kullanılır.  Bu tür bir ele geçirme işlemi aşağıdaki durumlarda uygun olabilir:   * Dikkate alınacak ekipman sayısının yüksek olması (örneğin, küçük ya da orta ölçekli bir işletme); * Ekipmanların çalıştırılmaması/kullanılmaması sebebiyle yüksek bir mali ya da başka bir kayba uğrama riskinin bulunması (örneğin, bilişim sistemi, şüpheli ya da üçüncü bir kişi için çok önemli olarak görülebilir); ve * İlgili suçun niteliği sebebiyle ekipmanlara el koymanın gerekli görülmemesi.   Bu tür bir ele geçirme işleminin avantajları şunlardır:   * Ekipmanların hasar görmesine ilişkin küçük bir risk; * Söz konusu suç ile ilgisi olmayan kişilere zarar vermeye ilişkin küçük bir risk; * Söz konusu suç ile ilgisi olmayan faaliyetleri engellemeye ilişkin küçük bir risk; * E-kanıtlar kontrollü bir ortamda analiz edilebilir.   Bu tür bir ele geçirme işleminin dezavantajları ise şunlardır:   * Olay yerinde özel ekipmanların kullanılması gerekir; * Olay yerinde genellikle **uzman desteğine** ihtiyaç duyulur; * Kanıtların bir kısmının gözden kaçırılmasına dair bir risk vardır, * Ele geçirme usulü zaman alır; ve * İlgili ekipmanlar kontrol altına alınmaz.     **3. Yedekleme belleği ortamlarına el koyma yoluyla ele geçirme**  Bu tür bir ele geçirme işlemi, özellikle dikkate alınacak çok büyük miktarlarda ekipman ve veri varsa tüm bellek içeriğinin kopyalanması yoluyla ele geçirme işleminin uygulandığı durumlara benzer durumlarda uygun olabilir (örneğin, büyük ağlar, ana bilgisayar ortamları).  Avantajları, bölüm 3.2’de anlatılan görüntü alma yoluyla ele geçirme işleminin avantajlarına benzerdir (hasar ya da zararlı eylemlere dair risk bulunmamaktadır). Ek avantajları ise şunlardır:   * Olay yerinde özel ekipmanların kullanılması gerekmez; ve * Olay yerinde zaman alan görüntü alma işlemlerinin gerçekleştirilmesi gerekmez.   Bu tür bir ele geçirme işleminin dezavantajları ise şunlardır:   * Olay yerinde genellikle **uzman desteğine** ihtiyaç duyulur; * Yerel sistem yöneticisinin desteğine genellikle ihtiyaç duyulur; * Kanıtların bir kısmının gözden kaçırılmasına dair bir risk vardır (çünkü yedek verilerin eksiksizliği genellikle önceden bilinemez), ve * İlgili ekipmanlar kontrol altına alınmaz.     **4. Seçili verileri kopyalama yoluyla ele geçirme**  Bu tür bir ele geçirme işlemi, yalnızca yukarıda bahsedilen ele geçirme türlerinin hiçbirisinin mümkün olmadığı istisnai durumlarda kullanılmalıdır. Seçilen (yani en ilgili) veriler, sonra analiz edilmek üzere kopyalanabilir. Olay yerinde genellikle **uzman desteği** olmak zorundadır.  Avantajları ve dezavantajları, yedek bellek ortamlarına el koyma yoluyla ele geçirme işlemininkilerine benzerdir. Ek bir dezavantajı, bilgisayar sisteminin tarihsel olarak yeniden yapılandırılmasının imkansız olmasıdır. Bu, ele geçirilen verilerin soruşturmaya ilişkin değerini önemli derecede kısıtlar. Ayrıca, bu şekilde ele geçirilen bilgilerin kanıt değerini korumak için özel önem gösterilmesi gerekir.   1. **Kanıtların İnternetten ele geçirilmesi**   Kanıtların İnternetten ele geçirilmesi, birçok soruşturma türü için çok önemlidir ve bunun etkili bir şekilde gerçekleştirilmesi için uzman bilgileri, becerileri ve kaynakları gerekir. Bu derste, bu veri toplama türünün ayrıntıları ele alınmayacaktır ancak genel ilkelerin, bu derste bahsedilen diğer ele geçirme türleri için geçerli olduğu gibi bu veri toplama türü için de geçerli olduğu ifade edilmelidir. İnternetten veri toplamanın farklı türleri vardır ve bunlar şu şekilde sınıflandırılabilir: 1) açık kaynak verilerin toplanması ve 2) gizli yollarla veri toplama. Bu konuya ilişkin olarak birçok hukuki ve usuli meseleler vardır ve bunlar kasten detaylandırılmamaktadır. Bu konunun, gelişmiş bir eğitim modülünde yer alması beklenmektedir**.** | |
| **Slayt 30 - 40** | **E- KANITLARI ELE GEÇİRME USULÜ**  Giriş bölümünde belirtildiği gibi bu belge, elektronik kanıtların aranması, tanınması, toplanması ve belgelendirilmesini içeren e-kanıt ele geçirme usulüne odaklanmaktadır. Bu usül, sonraki bölümlerde açıklanan aşağıdaki aşamalardan oluşmaktadır:   1. Ele geçirme hazırlığı (Bölüm 1), 2. Olay yerinin güvenliğinin sağlanması (Bölüm 2), 3. Olay yerinin belgelendirilmesi (Bölüm 3), 4. Kanıt toplama (Bölüm 4) ve 5. Paketleme, taşıma ve depolama (Bölüm 5).   Sonraki bölümlerde anlatılan usuller geliştirilirken bir bilişim ortamında arama yapmaya ilişkin olarak Avrupa Birliği Konseyi tarafından önerilen temel ilkelerin hepsi dikkate alınmıştır.   1. **Ele geçirme hazırlığı**   Bir arama izninin alınmasının amaçlandığı soruşturmanın başlangıç aşamasında dava ile ilgisi olabilecek herhangi bir e-kanıtın bulunmasının muhtemel olup olmadığı belirlenmelidir. Bu durumda sorumlu memur, yerel veri kurtarma birimini ve/veya bağımsız uzmanları olabildiği kadar çabuk bilgilendirmelidir. Verilecek ilk karar, hangi tür ele geçirme işlemlerinin uygulanması gerektiği ile ilgilidir (ele geçirme türleri Slayt 28’de açıklanmaktadır). El koyulacak bilişim sistemi hakkında mümkün olduğu kadar çok bilgi önceden ve uzman desteğiyle toplanmalıdır. Bu bilgiler örnek olarak şunları içerebilir:   * Bilgisayar donanımları/işletim sistemi/yazılımlar/uygulamalar ve depolama ortamları ile ilgili bilgiler, * İletişim ve ağ ile ilgili bilgiler (İSS[[5]](#footnote-5), telefon, faks, modem, LAN, ağ ekipmanları vb.), * Bilgisayar sisteminden ve/veya ağdan kimin sorumlu olduğu (örneğin, yerel bir yöneticisi varsa ya da dışarıdan bir şirket tarafından yönetiliyorsa), * Ne kadar ekipmana el konulmasının beklendiği (Bölüm 1’deki ele geçirme türü ile ilgili), * Ne kadar verinin kopyalanması gerektiği (Bölüm 2 ve 4’teki ele geçirme türleri ile ilgili), * Depolama ortamlarında sistem yedeği olup olmadığı (Bölüm 3’teki ele geçirme türü ile ilgili),   Hazırlık aşaması şu adımları içerir:   * E-kanıtların ele geçirilmesi işlemine ilişkin yetkilerin doğru bir şekilde alınmasının sağlanması (örneğin, yürürlükteki kanunlara uygun olarak bir arama izninin alınması); * El koyulacak bilişim sistemi hakkında olabildiğince çok bilgi elde edilmesi (yukarıya bakın); * Ekip üyelerinin seçilmesi (gerekirse bağımsız uzmanlar dahil); * Ekip üyelerine bireysel görevler verilmesi; * Ekip üyelerine görevlerini nasıl yerine getireceklerine dair bilgi verilmesi (ilgili temel eğitimi geçmiş olmalıdırlar); ve * Gerekli araç ve ekipmanların (lojistik) temin edilmesi.   Önceden de bahsedildiği gibi tüm faaliyetler kurum politikalarına ve AB’nin, devletin ve yerel idarenin kanunlarına uygun olmalıdır.  **Ele geçirme ekibinin üyeleri**  Eğer olay yerinde e-kanıtların bulunabileceği biliniyorsa ya da buna inanılıyorsa el koyma ekibi, bilişim ekipmanlarının ve e-kanıtların aranması ve bunlara el konulması görevleri için özel olarak eğitilmiş üyeleri de içermelidir. Bazı durumlarda bağımsız bir uzmana danışmak bile gerekli olabilir (Bölüm 4’e de bakın). Örneğin, eğer sistem dışarıdan bir şirket ya da yönetici tarafından yönetiliyorsa bu kişiyi bilirkişi olarak göreve dahil etmeyi düşünebilirsiniz (eğer bir şüpheli olarak değerlendirilmiyorsa). Asgari şart, ilk müdahale edenlerin kanıt içerebilecek elektronik ekipmanları toplamaya yönelik temel eğitime sahip olmasıdır.  Sorumlu bir kişi ekip üyelerini seçmeli ve el koyma usulü safhalarına göre bunlara görevlerini vermelidir (Slayt 30’un başlangıcına da bakın). Aşamalar ve ilgili görevler aşağıdaki bölümlerde açıklanmaktadır (Bölüm 2-5).  Tüm ekip üyeleri görevlerini nasıl yerine getireceklerine dair yeterli bir şekilde talimat almalıdır. Örneğin, diğer fiziksel kanıtları ele alırken uygulanan ilkelerin aynısının e-kanıtlarla meşgul olurken ne zaman uygulanması gerektiğini ve bazı özel tedbirlerin (örneğin, elektronik kanıtlardan parmak izi alırken alüminyum tozu kullanılmamalıdır) ne zaman alınması gerektiğini bilmelidirler. Belirli durumlarda bir uzman birim ile temasa geçmeleri ve dolayısıyla ilgili irtibat bilgilerini önceden elde etmeleri gerektiğini de bilmelidirler.  **Ele geçirme araç ve ekipmanları**  E-kanıtların toplanması için özel araç ve ekipmanlara ihtiyaç duyulabilir. Teknolojideki gelişmeler, ihtiyaç duyulan araç ve ekipmanlarda değişiklik yapılmasını gerektirebilir. Arama ve el koyma işlemleri sırasında aşağıdaki ekipmanlar/temel araç takımları faydalı olabilir ve bunlar, lojistikten sorumlu bir ekip üyesi tarafından hazır bulundurulmalıdır:   * Sökme ve çıkarma araçları:   + Tornavidalar (düz uçlu ve yıldız ve imalatçıya özel; örneğin, Hewlett Packard, Apple);   + Sökme-takma aletleri (altıgen somun, yıldız somun ve muhafazalı uçlu);   + Pense (standart ve iğne uçlu);   + Tel kesici (kablo kelepçelerinin çıkarılması için);   + Küçük cımbız; * Belgeler:   + Arama ve el koyma kaydı (tapu sicili);   + Etiketler ve bant (uçlar ve soketler de dahil olmak üzere sistemin bileşen parçalarının işaretlenmesi ve kimliklendirilmesi için);   + Kablo etiketleri;   + İbraz etiketleri (bağlamalı ve yapıştırmalı);   + Olay yerinde doldurulması gereken diğer formlar;   + Silinmeyen ve renkli işaret kalemleri (kaldırılan öğeleri kodlamak ve kimliklemek için);   + Kamera ve/veya video kamera (olay yerinin fotoğraflarını çekmek ve ekran üstü kumanda için); * Paket ve nakliye malzemeleri:   + Antistatik torbalar (toplanan devre kartları gibi ekipmanların korunması için; politen torbalar gibi statik elektrik oluşturabilen malzemelerden kaçınılmalıdır);   + Antistatik hava baloncuklu paket;   + Kablo kelepçeleri (kabloların sabitlenmesi için);   + Kanıt torbaları ve bant;   + USB cihazları, DVD’ler veya CD’ler gibi harici depolama ortamlarının paketlenmesi için kutular;   + Paketleme malzemeleri (strafor ya da küçük strafor taneleri gibi statik elektrik oluşturabilen malzemelerden kaçınılmalıdır);   + Sökülüp takılabilir kutular ya da çeşitli boylarda sağlam kutular (mümkün olduğunda orijinal paketleme kullanılmalıdır); * İletişim araçları: * Tavsiye ve danışmanlık almak için cep telefonu ya da diğer iletişim araçları (bilgisayar ekipmanlarına yakın bir konumda kullanılmamalıdır); * Yardım için irtibat bilgileri (Örneğin, uzman birimin telefon numaraları) * Diğer öğeler: * Bağlantı ayağı olan küçük bir fener; * Eldiven; * El arabası; * Büyük lastik bantlar; * Büyüteç; * Yazıcı kağıdı; * Tüm standart adli bilişim araçlarını içeren bir dizüstü bilgisayar * Ağ kabloları (Çift Bükümlü ve Çapraz) * Yeterli Sabit Disk kapasitesi (örneğin, TB’lik harici sabit disk sürücüleri) * Yazma Engelleme Donanımları (dizüstü bilgisayarınızda kanıtların önceliğinin belirlenmesi için) * Adli bilişim ön yükleme DVD’leri (eğer adli bilişim amaçları için kullanma eğitimi alınmışsa); * Ulaşım aracı (ekip üyeleri, el koyma araç ve ekipmanları ve el konulan kanıtlar için olay yerine ve olay yerinden)   **2. Olay yerinin güvenliğinin sağlanması**  İlk müdahale ekibi, olay yerinde bulunan bütün kişilerin güvenliğini ve hem geleneksel hem de elektronik tüm kanıtların bütünlüğünü sağlamalıdır.  Bu aşama şu adımları içerir:   * Suç mahallinin güvenliğinin sağlanması için göreve ilişkin politikaları izleyin: * Kanıtların (ekipmanlar ve güç kaynakları dahil) toplanacağı alanın etrafında tüm şahısları uzaklaştırın; * Bozulabilir verileri fiziksel ve elektronik olarak koruyun: * Bozulabilir veriler içeren her cihazı tespit edin, güvenliğini sağlayın, belgelendirin ve fotoğraflarını çekin; * Kanıtları değiştirmelerini ya da yok etmelerini önlemek için potansiyel şüphelileri ve diğer kişileri gözlemleyin; * Kanıtları değiştirmelerini ya da yok etmelerini önlemek için bilişim öğelerini gözlemleyin. * Toplanmayacak olan ilgili elektronik bileşenleri tespit edin ve belgelendirin; * Cihazlara bağlı olan telefon ve ağ hatlarını tespit edin, belgelendirin ve etiketleyin. * El koyulacak cihazlardan toplanması gereken başka kanıtların olup olmadığına karar verin (DNA, parmak izi, uyuşturucu, hızlandırıcı madde vb.); * Eğer varsa ilgili el kitabında o kanıt türü için belirtilen genel muamele usullerini izleyin; * İmha tekniklerini elektronik kanıtların kurtarılması gerçekleştirildikten sonrasına erteleyin; * E-kanıt kurtarma işlemi tamamlanana kadar gizli parmak izlerini toplayın (çünkü klavyeler, fareler, disketler, CD’ler veya diğer bileşenler gizli parmak izleri ya da korunması gereken başka fiziksel kanıtlar taşıyor olabilir); * Olay yerinden parmak izi toplamak için alüminyum tozu kullanmayın çünkü bu, ekipman ve verilere zarar verebilir. * Şunlar gibi elektronik olmayan ancak ilgili kanıtlar için olay yerini arayın: * Yazılı şifreler ve diğer el yazımı notlar, * Önceki sayfalarda yazılan yazıların izi kalmış boş sayfalar, * Donanım ve yazılım kılavuzları, * Takvimler veya günlükler, * Metin ya da grafik bilgisayar çıktıları, * Fotoğraflar ya da * Daha sonra gerçekleştirilecek şifre/parola kırma işlemleri için faydalı olabilecek, kişisel ilgiler hakkında bilgiler (çoğu şifre, doğrudan şahsi çevre ile ilgilidir; örneğin, araç plakası, eş/çocuklar, telefon numaraları, hobiler vb.) * Ön görüşmeler yapın; * Olay yerindeki tüm şahısları (tanıklar, failler veya diğerleri) ayırıp tespit edin ve giriş zamanındaki yerlerini kaydedin; * Bu şahıslardan bilgi alıp kaydetmek için bir kontrol listesi kullanın; * Kurum politikası ve yürürlükteki kanunlara uygun olarak şunlar gibi bilgileri şahıslardan alın: Cihazın/sistemin amacı (örneğin, muhasebe); * Olay yerinde bulunan cihazların/sistemlerin sahipleri ve/veya kullanıcıları ile şifreleri (aşağıya bakın), kullanıcı adları ve İnternet Servis Sağlayıcısı; * Sisteme, yazılımlara veya verilere erişmek için gerekli olan tüm şifreler. (Bir kişi birden çok şifreye sahip olabilir; örneğin, BIOS, sistem giriş, ağ ya da İSS, uygulama dosyaları, PGP ya da Truecrypt gibi şifreleme parolası, e-posta, erişim jetonu, programlayıcı ya da irtibat listesi.); * Tüm benzersiz güvenlik planları veya imha cihazları; * MySpace, Facebook ya da diğer sosyal paylaşım siteleri için hesap bilgileri. * Tüm alan dışı veri bellekleri; ve * Sistem üzerinde yüklü bulunan donanım ya da yazılımlar hakkında açıklamaların yer aldığı tüm belgeler.   **3. Olay yerinin belgelendirilmesi**  Olay yerinin belgelendirilmesi, **tüm ele geçirme usulü boyunca** devam eden bir süreçtir. Bilgisayarların, depolama ortamlarının, diğer elektronik cihazların ve geleneksel kanıtların yerini ve durumunu doğru bir şekilde belgelendirmek çok önemlidir. Bölüm 4’ten önceki ve sonraki bölümlerde nelerin belgelendirilmesi hakkında daha detaylı talimatlar verilmektedir. Bu bölümde bu talimatların yalnızca bir özeti verilmektedir.  Genel olarak aşağıdakiler belgelendirilmelidir ancak toplama safhasında ek belgeler de oluşturulabilir:   * Fiziksel olay yeri * Örneğin farenin konumu ve bileşenlerin yeri de dahil olmak üzere sistemin bir taslak planını çizin; * Tüm olay yerinin fotoğraflarını çekin, video görüntüsünü alın ve belgelendirin (mümkünse 360 dereceyi kapsayacak şekilde); * Bilgisayar sistemleri ve elektronik bileşenler/cihazlar/ekipmanlar * Aşağıdakilere ilişkin belgeleri hazırlayın: * Bulunan ilgili tüm ekipmanların ayrıntıları; örneğin, marka, model, seri numarası; * Bilgisayarların güç durumu (açık, kapalı ya da uyku modunda) da dahil olmak üzere elektronik kanıt içeren ya da sunan her bilgisayar sisteminin durumu ve yeri; * Bilgisayar sistemine ya da diğer cihazlara giren veya bunlardan çıkan tüm bağlantıları (kablo ya da kablosuz) belgelendirin; * İleride bir zamanda tam olarak takılmalarına olanak sağlamak için tüm port ve kabloların (çevre birim cihazlarına olan bağlantılar da dahil) etiketleyin; * Kullanılmayan portları “kullanılmıyor” ibaresi ile etiketleyin. Diğer depolama ortamlarını da tespit etmek için dizüstü bilgisayar yerleştirme istasyonlarını tespit edin. * Müdahale anında monitörün ayrıntılarını belgelendirin. * Bilgisayarın önünün yanı sıra monitör ekranının ve diğer bileşenlerin fotoğraflarını çekin; * Monitör ekranı üzerinde görünenleri yazılı olarak not alın; * Aktif programların görüntüsünü alın ya da monitör ekranı faaliyetinin belgelerini kapsamlı bir şekilde oluşturun * Toplanmayacak olan ilgili elektronik bileşenleri belgelendirin; * Olay yerinde bulunan insanlardan alınan bilgiler * İnsanlarla görüşmeler yapın ve cevaplarını belgelendirin/formları doldurun; * Aşağıdakilere ilişkin belgeler hazırlayın: * Aranan binalarda bulunan tüm şahısların bilgileri; * İlgili bilgisayar sistemini/ekipmanı kullanmış olan tüm şahısların bilgileri; * Bilgisayar kullanıcıları/sahipler/tanıkların yaptığı açıklamalar, yorumlar ve verdiği bilgiler. * Olay yerinde gerçekleştirilen eylemler * Gerçekleştirilen eylemin tarifi ve tam tarih ve zaman ile birlikte denetim izi/el koyma kaydını oluşturun.     **4. Kanıt toplama**  Bir bilişim sistemine, sadece olay yerinde bulunması sebebiyle el konulmamalıdır. Böyle bir tedbirin gerekçeleri olmalı ve bu tedbir ilgili suçla orantılı olmalıdır. Dolayısıyla, arama emrini veren kişi, bir unsurun araştırma ekibi tarafından toplanıp toplanmayacağına dair bilinçli bir karar vermeli ve bu araştırma için gerekçe teşkil eden makul bir şüpheye ya da yeterli kanıta sahip olmalıdır.  Elektronik kanıtlar, diğer tüm kanıtlarda olduğu gibi dikkatli bir biçimde ve kanıt değerlerinin muhafaza edileceği bir şekilde ele alınmalıdır. Bu, ilgili öğe ya da cihazın yalnızca fiziksel bütünlüğü ile değil aynı zamanda içerdiği elektronik verilerle de ilgilidir. Dolayısıyla belirli e-kanıt türlerinin özel bir şekilde toplanması, paketlenmesi ve taşınması gerekir. Hasarlara ya da elektromanyetik alanlardan (statik elektrik, mıknatıs, radyo vericileri ve diğer cihazların oluşturduğu) etkilenmeye karşı hassas olan e-kanıtlar yeterli bir şekilde korunmalıdır. E-kanıtlara, kurumun esasları ve yürürlükteki kanunlara uygun olarak el konulmalıdır. Aşağıdaki türlerden e-kanıtlar daha sonra ele alınacaktır:   * Bilgisayar sistemleri * Diğer elektronik cihazlar * Dijital depolama ortamları * Ağ ile ilgili bilgiler (konfigürasyon ve hizmetler/uygulamalar)   Elektronik/bilgisayarlı suçların araştırılmasında elektronik olmayan kanıtların (ya da klasik kanıtların) kurtarılması da çok önemli olabilir. Bu kanıtların toplanıp korunmasını sağlamak için özen gösterilmelidir. E-kanıtların daha sonra incelenmesi ile ilgili unsurlar farklı biçimlerde olabilir (örneğin, yazılı şifreler ve diğer el yazımı notlar, önceki sayfalarda yazılan yazıların izi kalmış boş sayfalar, donanım ve yazılım kılavuzları, takvimler, basılı materyaller, metin ya da grafik bilgisayar çıktıları ve fotoğraflar) ve ileride analiz edilmek üzere güvence altına alınmalı ve korunmalıdır. Bu unsurlar, çoğunlukla bilgisayar ve ilgili donanım unsurlarına yakın durur. Tüm kanıtlar, kurum politikaları ve yürürlükteki kanunlara uygun olarak tespit edilmeli, güvence altına alınmalı ve korunmalıdır.  **5. Paketleme, taşıma ve depolama**  Bilgisayarlar ve ilgili cihaz ve ekipmanlar, sıcaklık, nem, fiziksel sarsıntı, statik elektrik, manyetik kaynaklar ve hatta bazı eylemlere (örneğin, açma/kapama düğmesine basma) karşı duyarlı olan hassas elektronik ekipmanlardır. Dolayısıyla, e-kanıtların paketlenmesi, taşınması ve depolanmasında özel tedbirler alınmalıdır. Delil zincirini sağlamak için paketleme, taşıma ve depolama işlemleri yeterli bir şekilde kaydedilmelidir.  Genel olarak, tüm bilgisayar bileşenleri ve depolama ortamları azami dikkatle taşınmalıdır; aksi takdirde deneyimsiz kişiler bu ekipmanları taşırken e-kanıtlara zarar verebilir ya da bunları yok edebilir.     * Paketleme * Toplanan tüm e-kanıtların düzgün bir şekilde belgelendirilmesini ve paketlenmeden önce etiketlenmesini sağlayın. * Mümkün olduğunda toplanan e-kanıtları orijinal ambalajında taşıyın. * Eğer hiçbir orijinal ambalaj mevcut değilse antistatik ambalaj kullanın (örneğin, kağıt ya da antistatik naylon torbalar). Statik elektrik oluşturabilecek, standart naylon torbaları kullanmaktan kaçının. * Disket, CD-ROM ve kaset gibi depolama ortamlarını katlamayın, bükmeyin ya da çizmeyin. * Depolama ortamının yüzeyine yapışkan etiketler yapıştırmayın. Mümkün olduğunda depolama ortamlarının paketlenmesi için kutu ya da zarflar kullanın. * İçinde kanıtların bulunduğu tüm konteynerlerin düzgün bir şekilde etiketlenmesini sağlayın. * Eğer birden fazla bilgisayar sistemi toplanıyorsa her bir sistemi etiketleyin ki her biri bulunduğu şekilde yeniden kurulabilsin. * Taşıma * Elektronik kanıtları manyetik kaynaklardan uzak tutun. Radyo vericileri, hoparlör mıknatısları ve ısıtmalı koltuklar, e-kanıtlara zarar verebilecek unsurlardan bazılarıdır. * Ekipmanların sarsıntı ve darbelerden (yani mekanik hasar), ısıdan ve nemden korunmasını sağlayın. * Bilgisayarların ve konteynerler içinde paketlenmemiş diğer cihazların sarsıntı ve aşırı titreşimden kaçınmak için araç içinde sağlama alınmasını sağlayın. Örneğin, bilgisayarlar aracın zeminine yerleştirilmeli, monitörler ekran aşağı bakacak şekilde koltuklara yerleştirilmeli ve emniyet kemeri ile sağlama alınmalıdır. * Daha küçük ekipmanlar/depolama ortamları üzerine ağır objeler koymayın. * Mümkünse elektronik kanıtları uzun süreler boyunca araçlarda depolamayın. * Depolama * Kanıtların ilgili politikalara uygun olarak envantere alınmasını sağlayın. * Kanıtları aşırı sıcaklık ve nemden uzak, güvenli bir alanda depolayın. * Kanıtları manyetik kaynaklardan, nemden, tozdan ve diğer zararlı parçacık ya da kontaminantlardan koruyun. * Aşağıdaki özelliklere sahip, yeteri kadar güvenli bir depolama odası kullanın: * Erişim kontrolü, * Yangın koruma (örneğin, alarm, yangın söndürücüler, depolama alanında ya da çevresinde sigara içme yasağı), * Uygun sıcaklık ve nem * Manyetik kaynaklardan korunma (örneğin, yönsel radyo cihazlarından uzak).      * Aynı odada ya da çevresinde yanıcı malzemeler depolamayın (örneğin, temizlik maddeleri ya da kağıt istifleri). * Statik yükten kaçınmak için uygun zemin kaplaması kullanın. * E-kanıtları özellikle tavan boyunca içinden su boruları geçen odalarda depolamayın. * Tarih, zaman ve sistem konfigürasyonu gibi potansiyel kanıtların uzun süre depolama sonucunda kaybedilebileceği unutmayın. Piller sınırlı bir ömre sahip olduğundan herhangi bir pil arızasında veriler kaybolabilir. Dolayısıyla, ilgili personel, pillerle çalışan bir cihazla (örneğin, bir Kişisel Dijital Yardımcı ya da PC/CMOS) derhal ilgilenilmesi gerektiği konusunda bilgilendirilmelidir. | |
| **Slayt 42 - 51** | **Elektronik kanıtların araştırılması ve analizi**  **Adli Bilişim**  Adli bilişim terimi, dijital kanıtların aranması amacıyla bilişim ekipmanlarının sistematik analizini tarif etmek için kullanılır. Adli bilişim analizi, genellikle suç işlendikten sonra gerçekleştirilir. Normal soruşturmalara kıyasla bu analizin gerçekleştirilmesi, benzersiz zorluklara sahiptir çünkü bilgisayar teknolojisi sürekli olarak değişmektedir ve dijital formatlarda daha fazla bilgi depolandığından potansiyel kanıtların miktarı da artar. Kanıtların davalarda kullanılabilirliği üzerine odaklanılır. Bu, adli bilişim incelemelerinin yapılabilmesini bir dereceye kadar kısıtlar çünkü bu incelemeler, hukuki standartlara bağlıdır. Yeni teknik gelişmeler yeni adli bilişim araştırmalarına olanak tanısa bile bunların uygulanması, yeni araçların mevcut hukuki çerçevede yer alması şartı tarafından kısıtlanmaktadır.  **Adli bilişim uzmanlarının katılımının aşamaları**  Adli bilişim uzmanları yalnızca ceza davalarına katılmaz aynı zamanda hukuk davalarında, koruma stratejilerinin ve eğitimin geliştirilmesinde de önemli bir rol oynar. Ceza davaların ilişkin olarak adli bilişim uzmanlarının katılımı dört aşamada gerçekleşir:   * İlgili kanıtların tespiti. Adli bilişim uzmanları, soruşturma stratejilerinin tasarlanmasında önemli bir rol oynar. Emniyet güçlerinin soruşturmaya başlamadan önce soruşturma en iyi tekniğini belirlemesinde onlara destek olur. Buna ek olarak, danışman adli bilişim uzmanları, örneğin depolama cihazlarının bulunabileceği muhtemel yerleri tespit etmek için şüphelinin evindeki ağ altyapısını analiz ederek soruşturmalarda aktif bir rol oynayabilir. * Kanıtların korunması/toplanması/ele geçirilmesi. Dijital kanıtların toplanması işlemi, kanıtların fiziksel olarak depolandığı yerde ya da uzaktan gerçekleştirilebilir. Kanıtların toplanması için ilk adımları atan araştırmacılar (ilk müdahale ekibi), tüm soruşturma süreci için önemli bir sorumluluğa sahiptir. Eğer verilerin korunmasına ilişkin olarak kötü kararlar verirlerse önemli izlerin kaybolmasına yol açabilirler. Görevin zorluğuna ilişkin bir örnek, şüphelinin çalışan bilgisayarlarına ne yapılacağı meselesidir. İşletim sisteminin komutlarını kullanarak bilgisayarı kapatmak yerine elektrik bağlantısının kesilmesi genel olarak tavsiye edilen usuldür. Ancak suçlunun şifreleme teknolojisi kullandığı durumlarda elektrik bağlantısının kesilmesi dosyaların şifrelerinin çözülmesine yol açabilir. Dolayısıyla ilk müdahale ekibi, soruşturmanın odak noktasına göre bir karar vermelidir.   Adli bilişim uzmanlığı yalnızca ilgili verilerin depolandığı yerde meydana gelen soruşturmalarla ilgili değildir. Adli bilişim uzmanları, hizmet sağlayıcılarına sunulacak bir talep hazırlayarak da bir soruşturmaya destek olabilir ve yeterli bir olay tarihçesinin hazırlanmasında araştırmacılara yardımcı olabilir. Bunlar, toplanan kanıtların güvenilirliğini ispatlamak için gereklidir.   * Bilgisayar teknolojisi ve dijital kanıtların analizi. Sonraki aşama, dijital kanıtların ve el konulan donanımların analiziyle ilgili tüm yönleri kapsar. Genellikle tüm soruşturma sürecinin en karmaşık aşamasıdır. İlk müdahale ekipleri, çoğunlukla birkaç depolama cihazına birden el koyar. Depolama cihazlarından her biri, binlerce dosya içerebilir. Analiz edilmesi gereken veri miktarı da zaten araştırmacılar için büyük zorluklara sebep olur. Dolayısıyla, soruşturma için ilgili bilgilerin tespit edilmesi ve bunlar arasında bağlantı kurulması, adli bilişim uzmanlarının başlıca görevlerinden birisidir. Bu uzmanların görevleri, bir bilgisayar sistemindeki yasa dışı içeriğin aranmasından günlük dosyalarının analizine kadar çeşitli işler içerir. Bir sanal suç işlenirken suçlu tarafından gerçekleştirilen tüm işlemler iz bırakmaz. Ancak mevcut tüm kanıtların analiz edilmesiyle adli bilişim uzmanları suçun nasıl işlendiğini tespit edebilir. Üçüncü aşama ayrıca diğer hususların yanında soruşturmanın adımlarını ve kanıtları elde etmek için kullanılan yöntemleri içeren eksiksiz bir raporun sunulmasını da içerir.   **Adli bilişim incelemelerinin örnekleri**    Dört aşamada (özellikle de üçüncü aşamada) çoklu adli bilişim incelemesi yapmak mümkündür. Doğru araştırma tekniğinin seçilmesi, başta soruşturmanın odağında yer alan suçun türü olmak üzere çeşitli faktörlere bağlıdır.  En yaygın olarak kullanılan teknikler arasında şunlar yer alır:   * Donanım analizi. Eğer araştırmacılar bilgisayar donanımlarına el koyarsa adli bilişim uzmanları, sistemle ilgili bilgileri toplamak için donanımı analiz edebilir. Böyle bir araştırma, örneğin suçlunun bir bilgisayar sistemini İnternete bağlama imkanına sahip olup olmadığını ispatlamak için uygun olabilir. Donanım analizi, ayrıca sistemle ilgili bilgilerin bir kayıt işlemi esnasında aktarılması sebebiyle şüphelinin belirli bir donanım konfigürasyonunu kullandığı biliniyorsa da uygun olabilir. * Bilgisayar yazılımının işlevinin analizi. Donanımlar haricinde bilgisayar yazılımları da bir bilgisayar sisteminin çalıştırılmasında önemli bir rol oynar. Adli bilişim uzmanları, örneğin bir bilgisayar virüsünün ya da diğer kötü amaçlı yazılımların işlevlerini tespit edebilir. Ayrıca yazılım çalıştırma işlemlerini de yeniden düzenleyebilirler. Buna ek olarak, meşru ya da yasa dışı amaçlarla kullanılabilen (ikili kullanım) yazılımların üretimi ya da satışının yasaklanıp yasaklanmadığını belirlemek için de yazılım analizi önemli olabilir. * Şüphelinin bilgisayar sisteminde kurulu olan yazılımların analizi. Bir bilgisayar sisteminde kurulu olan yazılımların analizi, araştırmacılara soruşturma ile ilgili değerli bilgiler sağlayabilir. Bu özellikle dosyaları güvenli bir şekilde silmek için kullanılan şifreleme yazılımları ve araçlar için geçerlidir. Eğer bu yazılımlar şüphelinin bilgisayarında kuruluysa yapılacak araştırmalarda bu konular özel olarak ele alınabilir. * İlgili dijital bilgilerin tespiti. Bilgisayar verileri, farklı türlerde depolama cihazlarında depolanabilir. Hatta bir sabit diskte bile bir dosyayı kaydetmeye yönelik çeşitli imkanlar bulunur. Dolayısıyla ilgili kanıtların depolanma konumunun tespit edilmesi zorlu olabilir.   İlgili dijital bilgilerin tespit edilmesinde ek zorluklara sebep olan yeni trendlerden bir tanesi de uzak depolama birimlerinin kullanımıdır. Yukarıda bahsedildiği gibi, geniş bantlı erişimin ve uzak depolama sunucularının varlığı, bilgilerin depolanma şeklini etkilemiştir. Şüpheli, bu uzak depolama birimlerini kullanarak, emniyet güçlerinin uzak depolama hizmetlerinde depolanan bilgilere erişmesine olanak tanıyan bilgisayar donanımlarına el konulmasını önleyebilir. Bu durumda, şüphelinin uzak depolama hizmetlerini kullanıp kullanmadığını doğrulamak için adli bilişim analizinden faydalanılabilir.  İlgili dijital bilgilerin tespiti, dosyalarla sınırlı değildir. Şüphelinin bilgisayarında bilgileri bulmak için kullandığı yazılım araçlarının veritabanları da araştırma ile ilgili bilgiler içeriyor olabilir. Sistemde oluşturulan geçici dosyalar bile ceza davalarında kullanılabilecek kanıtlar içerebilir.   * Gizli dosyaların tespiti. Suçlular, emniyet güçleri tarafından dosyanın içeriğinin analiz edilmesini önlemek için bir depolama cihazındaki dosyaları saklamaya yönelik teknikleri kullanabilir. Bu özellikle yasa dışı içerikle ilgili soruşturmalarda geçerlidir. Adli bilişim araştırmalarında, gizlenmiş dosyalar tespit edilebilir ve analiz sonucunda bu dosyalara erişilebilir. * Silinen dosyaların kurtarılması. Eğer suçlular dosyaların güvenli bir şekilde silinmesini sağlamaya yönelik araçlar kullanıyorsa bu bilgilerin kurtarılması genel olarak mümkün değildir. Ancak, suçluların bu tür araçlardan haberdar olmadığı durumlarda dijital bilgilerin silinmesi, bu bilgilerin emniyet güçleri tarafından ele geçirilemeyeceği anlamına gelmez çünkü bu bilgiler özel adli bilişim yazılım araçları kullanılarak kurtarılabilir. * Şifrelenmiş dosyaların ve birimlerin deşifre edilmesi ve parolaların elde edilmesi. Suçlular her geçen gün şifreleme teknolojisini daha fazla kullanmaktadır. Bu teknoloji, emniyet güçleri için önemli güçlüklere sebep olmaktadır çünkü şifrelenmiş bilgiler erişime kapalıdır ve incelenemez. Adli bilişim analizi içinde şifrelenmiş dosyaların ve depolama cihazlarının şifresinin çözülmesine yönelik yaklaşımlar uygulanabilir. Ayrıca adli bilişim uzmanları, şifrelenmiş dosyalara örneğin bir tuş kaydedici kullanarak erişim sağlamak için stratejiler geliştirme açısından emniyet güçlerini destekleyebilir.   Suçlular, şifreleme araçları kullanarak yalnızca belirli bilgilere erişimi önlemez aynı zamanda parola koruma sistemleri de kullanır. Adli bilişim analizinde, emniyet güçlerinin parola koruma sistemlerine erişim sağlamasına imkan tanıyacak parola kurtarma araçları kullanılabilir.   * Dosya analizi. Bir depolama cihazında depolanan dosyalar, çeşitli şekillerde analiz edilebilir. Adli bilişim incelemelerinde örneğin dosyaların içeriğine odaklanılabilir. Şüpheli dosyaların elle incelenmesine ek olarak, adli bilişim araştırmaları, metin dosyaları için otomatik anahtar kelime aramalarını ve şüphelinin bilgisayarında bilinen görüntüler için otomatik arama yapan araçları içerebilir.   Önceden de bahsedildiği gibi, bilgisayar verileri üzerinde kolaylıkla oynama yapılabilir. Adli bilişim incelemeleri, bu tür oynamaları ve dijital dosyaların tahrifatını ortaya çıkarabilir.  Ayrıca, araştırmalarda üst veriler dikkate alınabilir. Bu tür analizlerle dokümanın son açıldığı ya da değiştirildiği zaman tespit edilebilir. Ayrıca üst veri analizleri, tehdit edici bir mesaj içeren bir dosyanın yazarını ya da çocuk pornografisi görüntüleri oluşturmak için kullanılmış bir kameranın seri numarasını tespit etmek için de kullanılabilir.   * Yazar analizi. Eğer İnternetteki bloglarda ya da forumlarda tehdit mesajları veya nefret söylemleri gönderilirse ve şüpheli bu mesajları bir İnternet kafeden gönderiyorsa ya da anonim iletişim hizmetleri kullanıyorsa günlük dosyalarının analizi, araştırmacıların metnin yazarına ulaşmasına yardımcı olamayabilir. Şüphelinin daha önce yazılar yazıp yazmadığını ve bu bağlamda şahsın tespit edilmesine yardımcı olabilecek bilgileri bırakıp bırakmadığını tespit etmek için sofistike dil analizi yardımcı olabilir. * Veri bütünlüğünün sağlanması. Önceden de ifade edildiği gibi, dijital kanıtların bütünlüğünün korunması, bu kanıtların mahkemede kabul edilebilirliği için çok önemlidir. Adli bilişim uzmanları, kanıtların toplanması sırasında dosyaların bütünlüğünün korunmasını sağlayabilir. Bu, bazı durumlarda emniyet güçlerinin donanımlara el koymak yerine ilgili dosyaları soruşturma süreci boyunca her türlü değişikliğe karşı bütünlüğü korunarak kopyalamasına olanak tanır. Bu özellikle depolama ortamlarının görüntülerinin oluşturulmasını içerir. * IP izleme. Suç işlemek için İnterneti kullanan suçlular (örneğin, çocuk pornografisi görüntüleri indiren ya da bilgisayar sistemlerine saldıran) çeşitli izler bırakır. İnternet sunucularında tutulan günlük dosyalarının incelenmesi gibi trafik verileri analizi, araştırmacıların İnternete bağlanmak için suçlu tarafından kullanılan bağlantılara ulaşmasını sağlayabilir. Eğer suçlu anonim iletişim teknolojileri kullanıyorsa bu araştırmalar zorlu olabilir. Ancak, bu durumlarda bile araştırmaların başarısı imkansız değildir. Bu tür araştırmalarda kullanılan araçlara örnek olarak, anonim iletişim hizmetleri kullanan bir şüpheliyi tespit etmek için ABD’de kullanılan adli bilişim aracı CIPAV (Bilgisayar ve İnternet Protokolü Adres Doğrulayıcısı) verilebilir. * E-posta analizi. E-posta çok popüler bir iletişim aracı haline gelmiştir ve dolayısıyla adli bilişimde önemli bir rol oynamaktadır. Bir tehdit mesajı içeren ya da yasa dışı içerik eklenmiş bir e-postanın göndereninin tespit edilmesinin nispeten kolay olduğu düşünüldüğünde suçlular, sahte kişisel bilgiler kullanılarak alınan ücretsiz e-posta adreslerini sıklıkla kullanır. Bu durumlarda bile başlık bilgilerinin ve e-posta hizmeti sağlayıcısının günlük dosyalarının incelenmesi, şüphelinin tespit edilmesine olanak tanıyabilir. * Mali işlemlerin izlenmesi. Çocuk pornografisi görüntülerinin satılması da dahil olmak üzere bazı suçlar mali işlemler içerir. Bu mali işlemleri gerçekleştiren ticari sistemler ve kurumlardan alınan veriler kullanılarak suçlunun tespit edilmesi mümkündür. Bunun bir örneği, Almanya’da ticari bir web sitesinden çocuk pornografisi görüntüleri indiren suçluların, o web sitesinde çocuk pornografisi görüntüleri satın almak için kredi kartlarını kullanan müşterileri tespit etmek için müşteri kayıtlarını inceleyen kredi kartı şirketleri tarafından tespit edildiği bir soruşturmadır. Eğer suçlular anonim ödeme yöntemlerinden faydalanırsa bu tür soruşturmalar daha zorlu olabilir. * Trafik verilerinin gerçek zamanlı olarak toplanması ve içerik verilerinin ele geçirilmesi. Adli bilişim soruşturmaları, işlenen veri aktarımının gerçek zamanlı olarak izlenmesini içerebilir. www.coe.int/cybercrime adresinde yer alan, Sanal Suçlara dair bu Avrupa Konseyi Projesi, araştırmacıların, bir soruşturmanın şüphelisinin eylemde bulunduğu anda işlemlere karşılık vermesine olanak tanır. * Halka açık hizmetlere ilişkin olarak izleme faaliyetleri. Telif hakkı korunan materyalleri ya da yasa dışı içerikleri değiş tokuş etmek için halka açık hizmetler kullanılabilir. Bu hizmetler, bir soruşturma dahilinde adli bilişim uzmanları tarafından izlenebilir. Bu, örneğin sohbet forumlarının gözlemlenmesini içerir. * Uzaktan adli bilişim. Şu anda uzaktan adli bilişim araçlarına yönelik ihtiyaç tartışılmaktadır. Bu, şüphelinin sistemi üzerinde yapılan araştırmalardan haberi olmadan canlı ve uzaktan kanıt toplama uzaktan izleme yapılmasını mümkün kılar.   Bu araştırmaların yapılması, yaygın bir şekilde kabul edilen standartlara ve metodolojilere dayanan özel eğitim ve iyi tanımlanmış usuller gerektirir.  **Adli bilişim incelemeleri nasıl yapılır?**  Adli bilişim araştırmalarının yürütülmesinde iki yol izlenmektedir:   * Elle yapılan işlemler: Soruşturma işlemlerini otomatikleştirmede teknolojiden faydalanılmasına rağmen adli bilişim büyük oranda elle yapılan işlemlere dayanır. Özellikle büyük miktarlarda veri içeren soruşturmalarda analiz araçlarının uygun olmadığı durumlarda bu tür elle yapılan işlemler uygulanabilir. * Analiz araçları: Özellikle anahtar sözcükle arama, silinmiş dosyalara yeniden ulaşma veya şifreli dosyaların şifresinin çözülmesi gibi işlemler gelişmiş adli bilişim analiz araçları kullanılarak otomatikleştirilebilir.   Soruşturmaların çoğunda işlemlerin otomatikleştirilmesi için elle yapılan işlemler adli bilişim yazılım araçlarıyla birleştirilmektedir.   * Kanıtların mahkemede sunulması/ibrazı. Genellikle davalarda fiili kanıt sunan tanıkların bilirkişi olmasına gerek yoktur. Ancak uzmanlar, ceza davalarında önemli rol oynayabilir. Adli bilişim uzmanları, dava sürecinde yer alan kişilerin, kanıtların nasıl ortaya çıktığını, kanıt toplama usullerini ve kanıtların değerlendirmesini anlamalarına yardımcı olur. Mahkemece gerekli görüldüğü takdirde bilirkişi raporu da verebilirler. | |
| **Slayt 52 - 59** | **Bölüm Üç – Hukuki Konular** | |
|  | **DİJİTAL KANITLARIN ELDE EDİLMESİNE İLİŞKİN ÖZEL SORULAR**  Ağlar üzerindeki, ağlara karşı ya da ağlar içindeki modern suç türleri, kanıtların toplanması ve analiz edilmesi ile mahkemede doğru bir şekilde yorumlanması için uzmanların ve ihtisas memurlarının desteğini gerektirir.  Bu tabii ki yeni değildir: yüzyıllardır uzmanlar hakimlere, savcılara ve avukatlara teknik soruları anlamalarında yardımcı olmaktadır. Örneğin, yüzyıllardır doktorlar, bir cinayetin tıbbi açıdan muhtemel sebebini belirlemek, açıklığa kavuşturmak ve değerlendirmek için görev almaktadır. Ancak dijital ortamlar, çözülmesi zor olan yeni ve farklı sorular ortaya çıkarmaktadır.  Aslında kalıcı teknik gelişmeleri her zaman yasal dokümanların sürekli revizyonu ve güncellenmesi izlemez ve usuli hukuki araçlar her zaman elektronik kanıtların toplanmasına ilişkin teknikleri meşrulaştırmaz  Diğer yandan, normalde hem emniyet güçlerinin hem de savcı ve hakimlerin ilk ve sürekli eğitiminde teknik gelişmeler gecikme olmadan izlenmez.  Bu senaryoda, anlayışları özel bilgilere bağlı olan yeni suç ihlalleri artarak ortaya çıkmaktadır. Teknik ekpertize yalnızcasSuç faaliyetlerini ispatlamak için ihtiyaç duyulmaz; aynı zamanda söz konusu suçun tam olarak ne olduğunu anlamak için de ihtiyaç duyulur. Cinayetin ne anlama geldiğini hepimiz anlarken ve ölüm sebebini tespit etmek için tıp uzmanlarına ihtiyaç duyulurken, “hizmet engelleme”, bilgisayar ağlarının belirli bir teknik anlayışı ile tanımlanan bir suçtur  Dünyadaki ülkelerin çoğunda elektronik kanıtlara dair özel düzenlemeler bulunmamaktadır. Bunlardan bazıları, örneğin iletişimin ele geçirilmesine yönelik özel kurallara sahiptir. Ancak genelde, önceden beri var olan kurallarla elektronik kanıtların toplanmasına dayalı hukuk sistemleri, halihazırda çevrimdışı dünya için geçerlidir. Bazı durumlarda mahkemeler, klasik kurallara uyum sağlayarak yeni kanıt gerçekliklerini kabul ederken diğer durumlardaysa bu söz konusu değildir. Bu tür durumlarda mevcut hukuki çerçeveye yeni hükümler eklenmelidir.  Birçok Avrupa ülkesi, elektronik kanıtlarla ilgili mevzuatı ve mahkemelerin elektronik kanıtları incelerken ve değerlendirirken kullanması gereken kriterleri henüz uygulamaya koymamıştır.  Elektronik kanıtların toplanması ve değerlendirilmesi hassas bir faaliyettir çünkü bu faaliyette normalde mahremiyet ya da iletişimin gizliliği gibi temel haklara dokunulur. Bazen hakim, bu haklara saygı gösterilip gösterilmediğini net bir şekilde anlayamaz.  Sanal suçlar globaldir. Suç olayları birden fazla ülkede ve yargı alanında aynı anda gerçekleşebilir. Sanal suçlar, doğası gereği uluslaraşırıdır. Bilgi ve iletişim ağlarında işlenen suçlar, ihlalin nerede gerçekleştiğinin ve davaya bakacak yetkili mahkemenin açıklığa kavuşturulmasına ilişkin olarak ciddi sorunlara sebep olmaktadır. Budapeşte Sanal Suçlar Sözleşmesi bunlarla ilgili tüm sorunları çözememektedir ancak bazı zor durumlar için çözümler bulmaya çalışmaktadır.  Sözleşmenin Tarafları, genellikler diğer vakalarda olduğu gibi kendi topraklarında işlenen suçları araştıracaktır. Ancak buna ek olarak Sözleşmede şu ifade edilmektedir: Taraflar, bir suç yurt dışında işlenmiş olsa bile söz konusu suç faaliyetinin gerçekleştiği yerdeki yerel kanunlara göre bir ceza gerektiriyor olması şartıyla kendi vatandaşlarını ilgilendiren davaları takip etmek ve görmek için kendilerini yetkili ilan etmelidir.  Bu önemli bir uygulama sorunudur. Bazı ülkeler evrensel yargı yetkilerini tanımlayan kanun hükümlerine sahip olmasına rağmen, bu genel ya da evrensel olarak kabul edilen bir ilke değildir.  Ancak, çoğu durumda genel kurallara göre hangi mahkemenin yargı yetkisine sahip olacağının belirlenmesi zor olabilir. Örneğin, bir bilgisayar suçu birkaç ülkede birkaç kurban üzerinde aynı anda işlenebilir ya da farklı yerlerden farklı failler tarafından işlenebilir.  Ceza yargılaması kuralları tüm ülkelerde uyum içinde olmadığından, Sanal Suçlar Sözleşmesindeki genel kurallara rağmen farklı ülkelerde yer alan iki mahkemenin tek bir suç üzerinde yargılama yetkisi iddia etmesi gayet mümkündür  Avrupa Birliği’nde özellikle dijital kanıtların toplanması ile ilgili önemli bir Yönerge çıkarılmıştır: Avrupa Parlamentosu’nun ve Konsey’in 15 Mart 2006 tarihinde çıkardığı Yönerge 2006/24/EC, halka açık elektronik iletişim hizmetleri veya halkın iletişim ağları hükmü ile bağlantılı olarak oluşturulan ya da işlenen verilerin muhafaza edilmesine dair Avrupa Birliğindeki ilk bağlayıcı dokümandır. | |
|  | **Uygulamalı Alıştırmalar** (eğer varsa)  Bu oturum için uygulama alıştırmaları öngörülmemektedir çünkü bu alıştırmaları vermek için gerekli teknoloji düzeyi ve İnternet erişiminin her yerde mevcut olacağının garantisi yoktur.  Eğitimciler, gelecekte imkanların uygun olduğu bir ortamda verilen eğitimlere alıştırmalar ekleyerek öğrenmeye katkıda bulunmaya çalışabilir. | |
|  | **Bilgi Kontrolü**  Bu eğitimde yukarıdakilere ek olarak özel bir bilgi kontrolü şu anda öngörülmemektedir. Resmi bir değerlendirme talep edilmemiştir. | |
| **Slayt 63 - 64** | **Özet:**  Eğitimci, şu hedeflerin oturum sırasında gerçekleştirilmesini sağlamak için bunlara dair bilgileri özetlemeli / sınamalıdır:   * Çeşitli elektronik kanıt türlerinin tartışılması, * Elektronik kanıtların elde edilmesi ve bunlara gösterilecek muameleye ilişkin en iyi uygulama ilkelerinin açıklanması, * Elektronik kanıtlara ait “cansız kutu”, “canlı veri” ve internet kaynaklarından kaynaklanan zorlukların belirlenmesi, * Başka bir yargı alanından kanıtların elde edilmesine ilişkin zorlukların tespit edilmesi, * Elektronik kanıtların gerçekliği, doğruluğu ve bütünlüğü açısından adli davalarda kabul edilebilirliğinin tartışılması.   Bu, grup tartışması, katılımcılara sorular sorulması, küçük sınavlar ya da başka yöntemlerle gerçekleştirilebilir.  Bu derste, hakim ve savcıların görevlerini etkili bir şekilde gerçekleştirmeleri için gereken teknoloji bilgilerinin türü ve düzeyine dair rehberlik sunmaya çalışılmıştır. Ders, konuların eksiksiz bir analizi olduğu iddiasında değildir. Gerekli yerlerde ek bilgi edinilebilir.  Eğitim geliştiricilerinin, hazırladıkları materyallerin mümkün olduğu kadar güncel olmasını sağlaması ve en son teknoloji konularını ve bunların eğitimin verileceği yerdeki yargı alanında hukuki, usul ve kanıtlarla ilgili kararlar üzerindeki etkilerini bu materyallere dahil etmesi tavsiye edilmektedir. Verilerin katı hal disklerinde ya da Web 2.0’da depolanması gibi ceza yargılaması sistemini etkileyecek teknolojik değişiklikler vardır. Bunlar, eğitim programlarına dahil edilmesi ve daha da yaygınlaştıkça güncellenmesi gereken önemli konular olacaktır. | |

|  |  |  |
| --- | --- | --- |
| Ders 1.3.4 Uluslararası İşbirliği | | **Süre: 90 Dakika** |
| **Gerekli kaynaklar:**   * Windows 7 ve Office 2010 kurulu olan bir dizüstü bilgisayar ya da PC * Projektör * PowerPoint Sunum | | |
| **Amaç:**  Bu oturumda uluslararası işbirliğinin öneminin hatırlatılması ve başta Budapeşte Sanal Suçlar Sözleşmesi olmak üzere sanal suçlar alanında uluslararası işbirliğine yönelik mevcut araçlara bir genel bakış sunulması istenmektedir. Bu, mevcut araçlara, bunların kullanılma yollarına, zaman çizelgelerine ve etkinliklerine bir giriş niteliğinde olacaktır. | | |
| **Hedefler**  Oturumun sonunda katılımcılar:   * İnternetin küresel boyutunu ve sanal suçların uluslararası boyutunu tanıyacak, * Uluslararası işbirliğinin önemini açıklayabilecek ve sanal suç alanında uluslararası işbirliği için mevcut araçları tanıyacak, * Uluslararası işbirliği için oldukça hızlı ve etkin kanallara olan ihtiyacı ve mevcut araçları, bunların kullanım yollarını, zaman çizelgelerini ve etkinliklerini belirleyebilecek, * Yeni uluslararası işbirliği modellerinin uygulanmasına ilişkin uluslararası kuruluşların çalışmalarını anlatabilecek, * Budapeşte Sanal Suçlar Sözleşmesi’ni tartışabilecek, genel ilkelerini, geçici önlemleri ve 7/24 karşılıklı hukuki yardım ağını tanıyacaktır. | | |
| **Slayt no.** | **İçerik:** | |
|  | **Giriş**  Bu oturumda, sanal suçlar içeren somut olayların soruşturulması için uluslararası işbirliğinin önemi vurgulanacaktır. Başta Budapeşte Sanal Suçlar Sözleşmesi olmak üzere uluslararası işbirliğinde kullanılabilecek araçlar açıklanacaktır. | |
| **Slayt 2** | 1. Sunumda Birinci Bölüm, sanal suçların uluslar arası boyutuna odaklanacaktır. Bu konuya daha önceden diğer oturumlarda da değinildiğinden bu çok kısa bir değerlendirme olacaktır. 2. İkinci Bölümde uluslararası düzeyde sanal suçlara verilen karşılıklardan bazıları belirtilecektir. 3. Sanal suçlara uluslararası karşılıklarla ilgili Üçüncü Bölümde Budapeşte Sanal Suçlar Sözleşmesi’nin rolü vurgulanacaktır. 4. Son olarak Dördüncü Bölüm Budapeşte Sözleşmesi’nde açıklanan uluslararası işbirliği araçlarına odaklanılacaktır. 5. Beşinci Bölümde tüm sunumun başlıca konuları yeniden değerlendirilecektir. | |
| **Slayt 3** | **Oturum Hedefleri**  Bu oturumun genel amacı İnternetin küresel boyutunu ve sanal suçların uluslararası ya da ulusaşırı boyutunu tanımaktır.  Uluslararası işbirliğine ve sanal suç alanında uluslararası işbirliği için mevcut olan araçlara değinilecektir.  Uluslararası işbirliği için oldukça hızlı ve etkin kanallara olan ihtiyaç vurgulanacak ve bu işbirliği için mevcut olan araçlar anlatılacaktır.  Yeni uluslararası işbirliği modellerinin uygulanmasına ilişkin uluslararası kuruluşların çalışmalarına genel bir bakış sunulacaktır.  Özellikle genel ilkele, geçici önlemleri ve 7/24 karşılıklı hukuki yardım ağı tanımlanarak Budapeşte Sanal Suçlar Sözleşmesi’nden bahsedilecektir. | |
| **Slayt 4** | **Birinci Bölüm – Sanal suçların uluslararası boyutu**  Çok kısa bir değerlendirme ile sanal suçların uluslararası boyutu yeniden ele alınacaktır. | |
| **Slayt 5** | İnternetin küresel düzeyde yayıldığı ve dünyadaki hemen hemen herkes tarafından erişilebilir ve kullanılabilir hale geldiği bariz bir olgudur.  Ağlar içinde suç oranı artmaktadır. Dolayısıyla sanal suçlara küresel bir olgu olarak yaklaşılmalıdır. Sanal suçlara ilişkin gerçeklik, bunun uluslararası boyutu tanınmadan tam olarak anlaşılamaz. | |
| **Slayt 6** | Bu bağlamda sanal suçlar, tüm suç türleri içerisinde en ulusaşırı olanıdır. Sanal suçların soruşturulmasında görev alanlar, görevlerinin etkin bir uluslararası işbirliği gerektirdiğinden haberdar olmalıdır. Aslında doğası gereği küresel olan sanal suçlara ilişkin soruşturmaların, böyle bir işbirliği olmaksızın başarılı olması pek olası değildir. | |
| **Slayt 7** | Somut olarak sanal dünyada bir suç işlendiğinde ceza yargılaması makamları, her şeyden önce çözmek zorunda oldukları çok zor sorularla karşılaşır.  İnternetin her yerde olduğu göz önüne alınırsa suçun konumunu tespit etmek her zaman kolay olmaz. Örneğin fail A noktasında hereket ederse ve hedef alınan kurbanın bilgisayarı B noktasında bulunuyorsa ancak suçlu tarafından kullanılan yasa dışı iletişim C noktasında bulunan bir sağlayıcı tarafından gerçekleştiriliyorsa ve tüm bu noktalar farklı yargı alanlarında yer alıyorsa emniyet güçleri yetkililerinin çözmesi gereken ilk sorun yargı alanı açısından suçun hukuki yeridir. Suçun işlendiği yerin hangisi olduğu net bir şekilde anlaşılmalıdır ki böylelikle uygulanabilir maddi hukukun ve yetkili yargı alanının (polis, savcı, hakim) hangisi olduğu olduğu tespit edilebilir.  Araştırmacı, kendi yetki alanına ve kendi bölgesel yetkinliğine saygı göstermelidir. Bu bakış açısına göre yargı alanı, suç soruşturmaları için bağlayıcı bir kısıtlama teşkil edecektir.  Bu gerçeklik iki çözülmemiş soru ortaya çıkarır.   * Bunlardan ilki, sınır ötesi araştırmalar ile ilgilidir: bir emniyet yetkilisi, acil olarak harekete geçmesi gerekiyorsa kendi ülkesinin dışında yasal olarak nasıl araştırma yapabilir? Eğer kanıtların hızla kaybolabileceğini düşünüyorsa başka bir ülkede bulunan kanıtları nasıl elde edip toplayabilir? * İkinci soru, “bulut” hizmetlerindeki araştırmalarla ilgilidir. Eğer veriler bir “bulut” hizmetinde depolanıyorsa bunların fiziksel olarak nerede bulunduğunu kimse bilmez. Bazı verilere ilişkin olarak ulusal yargı alanının hangisi olabileceğini kimsenin bilmemesi de mümkündür. Bir emniyet yetkilisi, “bulut” hizmetinde depolanan verileri, fiziksel olarak nerede olurlarsa olsunlar nasıl elde edip toplayabilir? | |
| **Slayt 9 ve 10** | **İkinci Bölüm – Sanal suçlara verilen uluslararası karşılık**  İnternet küresel olarak genişlediği ve bugünlerde potansiyel olarak dünyadaki herkes tarafından kullanıldığı için sanal suçlara küresel bir olgu olarak yaklaşılmalıdır. İkinci Bölümün amacı, pratik bir yaklaşımla Avrupa’da sanal suçlara karşılık vermek için atılan en önemli adımları tanımlamaktır. | |
| **Slayt 11 - 13** | İnterpol, üyeleri tüm dünyadan emniyet kurumları olan, çok iyi bilinen uluslararası bir kuruluştur. İnterpol, Ocak 2012 itibarıyla tüm kıtalardan 190 üyeyi içerir. Amacı, uluslararası polis işbirliğinin güçlendirilmesi ve kolaylaştırılmasıdır. Bu amaçla İnterpol, küresel bir polis iletişim sistemi organize etmiş ve özel veritabanları ve polis bilgisi analizleri geliştirmiştir.  İnterpol, sanal suç konularında duyarlılık gösteren ilk uluslararası kurum olmuştur. Aynı zamanda konunun uzmanlarından oluşan tartışma gruplarını 1995’te ilk düzenleyen kurumlardan birisidir. O zamandan beri İnterpol, dünyadaki polis ve diğer emniyet kurumlarının sanal suçlara mücadele etme yetilerini güçlendirmesine yardımcı olacak çalışmalar yapmaktadır.  Bu amacı gerçekleştirmek için İnterpol, üyelerine sürekli olarak yardım sunmaya çalışan bir irtibat noktası ağı (İnterpol Ulusal Merkezi Referans Noktaları – NCRP) oluşturmuştur. NCRP, Eylül 2011 itibarıyla dünyada 120 civarında referans noktasına sahipti. Bu referans noktaları, Budapeşte Sanal Suçlar Sözleşmesi’nin 35. Maddesi ile oluşturulan 7/24 irtibat noktalarının düzenini benimsemiştir. Sözleşmeye taraf olan bazı ülkelerde, İnterpol referans noktası aynı zamanda G8 irtibat noktası olarak da görevlendirilmiştir. Tüm G8 irtibat noktaları, bu ağa dahil edilmiştir. Bu yapının amacı, polisin bilgisayarla ilgili soruşturmalarda diğer ülkelerdeki uzmanları derhal tespit etmesini, acil yardım almasını ve kanıtları toplamasını sağlamaktır. Bu ağ, haftada yedi gün, günde 24 saat aktiftir.  NCRP’nin kapsamı, üyeleri arasında polis bilgilerinin ve istihbaratın paylaşılması ve teknik ve operasyonel destek sağlanmasıdır. Aslında NCRP’nin asıl amacı, tipik polis bilgilerinin özel ve uygun İnterpol kanallarıyla mümkün olduğu kadar çabuk paylaşılmasıdır. Bu bilgiler, şüpheli teröristlere, aranan kişilere, parmak izlerine, DNA profillerine, kayıp ya da çalıntı seyahat dokümanlarına, çalıntı motorlu araçlara, çalıntı sanat eserlerine vb. dair olabilir. İnterpol tarafından sağlanan ve potansiyel olarak önemli bu bilgi türleri, somut soruşturmalar için kesinlikle çok faydalıdır. Ancak tamamen ağın kapsamından dolayı ağ, örneğin bilgisayar verilerinin korunmasını, trafik verilerinin korunmasını ya da kanıt elde etmek ve bulunan kanıtları korumak için başka herhangi bir tedbiri acil olarak istemek amacıyla kullanılamaz. Başka bir deyişle bu özel İnterpol ağı tarafından sağlanabilecek işbirliği türü, genel İnterpol işbirliği için geçerli olan aynı ilkelere dayanmaktadır. | |
| **Slayt 14** | Avrupa Birliği, Budapeşte Sözleşmesi’nin destekleyicisidir ve hatta Sözleşme’nin tasarlanması sırasında gözlemci olarak katılımda bulunmuştur. O zamandan beri Avrupa Birliği, tüm Üye Devletleri Sözleşme’yi onaylamaları için teşvik etmiştir. Gerçekten de çok sayıda Üye Devlet Sözleşme’yi onaylamış ve hepsi de halihazırda imzalamıştır.  Tabii ki Avrupa Birliği’nde en güncel yaklaşımların dışında bile karşılıklı tanıma ilkesine dayanan çok çeşitli uluslararası işbirliği araçları mevcuttur. Avrupa sisteminin avantajlarından çoğu, her Üye Devletten adli makamlar arasındaki doğrudan temas imkanı ile ilgilidir. Bu imkana göre her hakim veya savcı, başka bir hakim veya savcıya doğrudan bir talep iletebilir. Bu, sanal suç konularında da kullanıma uygun, soruşturmalarla ilgili çok güçlü bir araçtır. | |
| **Slayt 15** | Ayrıca 2005’te Avrupa Birliği, diğer unsurların yanında sanal suç soruşturmalarına ilişkin olarak bir 7/24 irtibat noktası ağı ile ilgili bağlayıcı bir doküman olan, bilgi sistemlerine karşı düzenlenen saldırılara dair 24 Şubat 2005 tarihli Konsey Çerçeve Kararı 2005/222/JHA’yı kabul etmiştir. Bu Çerçeve Karar özellikle “mevcut irtibat noktaları ağı” ile ilgili kurallar içermektedir. Madde 11, 1’de tüm Avrupa Birliği Üye Devletlerinin, haftada yedi gün ve günde 24 saat aktif olan mevcut operasyonel irtibat noktaları ağından faydalanmasını sağlayacağı belirtilmektedir. Bu, belirtilen bazı suçlarla (bilgi sistemlerine yasa dışı erişim, yasa dışı sistem müdahalesi, yasa dışı veri müdahalesi, azmettirme, yardım ve yataklık ve teşebbüs eylemleri) ilgili olarak bilgi paylaşımını öngören bir hükümdür.  Çerçeve kararın maddelerinde belirtilmemesine karşı şu açıktır ki *mevcut ağ*, G8/Avrupa Konseyi ağıdır. | |
| **Slayt 16** | Europol, Avrupa Birliği’nin özerk bir kurumudur ve amacı Avrupa Birliği’nin her Üye Devletinin emniyet güçleri arasındaki işbirliğinin etkinliğinin geliştirilmesidir. Faaliyetleri, 1999’dan beri suçlu bilgilerinin analizinin kolaylaştırılması ve Üye Devletler arasında verilerin paylaşılmasını içermektedir. Sanal suçlar, Europol’ün en önemli faaliyet alanlarından birisidir. Diğer birçok imkanının yanında Europol, Budapeşte Sözleşmesi’nin spontane bilgilerle ilgili 26. Maddesinin hükümlerinin etkinliğini artırmak için mükemmel bir kanal olabilir.  Ocak 2013’te Europol bünyesinde Avrupa Sanal Suçlar Merkezi (EC3) kurulmuştur. | |
| **Slayt 17** | Eurojust’ın gelecekte nereye varacağını kimse bilmiyor ancak şu anda Eurojust, Avrupa Birliği’nin Üye Devletleri arasında adli (savcılık ve yargı düzeyi) işbirliğine yönelik önemli bir Avrupa Birliği kuruluşudur. Eurojust’ın kapsamı, kovuşturma işlemlerinden sorumlu ulusal makamlar tarafından yürütülen faaliyetlerin koordinasyonu aracılığıyla önemli suçlarla mücadelede uluslararası işbirliğidir.  Bu bağlamda Eurojust, çeşitli Üye Devletlerin yetkili makamları arasında koordinasyonu destekleme ve uluslararası karşılıklı hukuki yardımın ve suçluların iadesi ile ilgili taleplerin uygulanmasını kolaylaştırma yetkinliğine sahiptir.  Eurojust, Tampere Avrupa Konseyi tarafından sunulan öneriden sonra Aralık 2000’de tüzel bir kişilik olarak kurulmuştur ve 27 Üye Devletin her birinden bir temsilci almaktadır. “Bilgisayar suçları”, Eurojust’ın yetkinlik alanlarından birisidir. | |
| **Slayt 18** | Hala adli makamlar arasındaki işbirliğini artırarak ve kolaylaştırarak Avrupa Birliği’ndeki organize suçlar ve terörizm ile mücadele amacıyla faaliyet gösteren Avrupa Cezai Konular Yargı Ağı, Avrupa Birliği bünyesinde Haziran 1998’de kurulmuştur.  Aslında uluslararası adli işbirliği, her Üye Devletteki ulusal irtibat noktaları ve irtibat hakimlerinden sorumlu olan her Üye Devletteki merkezi makamlara dayalı bir adli irtibat noktaları ağıdır.  Avrupa Cezai Konular Yargı Ağı’nın kapsamlarından birisi, farklı adli kurumlar ve hukuki düzenler arasındaki uluslararası işbirliğini daha kolay hale getirmek için hakimlerin kullanabileceği gerekli bilgileri sunmaktır. Bu bağlamda Avrupa Cezai Konular Yargı Ağı, kullanıcıların karşılıklı hukuki yardım taleplerini almak ve uygulamak için her Üye Devletteki yetkili yerel makamı kolaylıkla tespit etmesine olanak tanıyan bir bilgisayar aracıdır.  Üye Devletler arasında adli işbirliğini kolaylaştırmak ve ayrıca adli işbirliğine ilişkin taleplerin hazırlanması için bu makamları desteklemek amacıyla yerel adli makamlar tarafından irtibat noktaları ile temasa geçilebileceği varsayılmaktadır.  Sınır ötesi işbirliğine yönelik taleplerin çok hızlı ve kolay bir şekilde sunulmasını sağlayan bu tür bir ağ, elektronik kanıtların toplanmasında çok değerli olabilir. | |
| **Slayt 19** | Avrupa Konseyi’nin Cezai Konularda Karşılıklı Yardıma Dair Avrupa Sözleşmesi, 1959’dan beri Budapeşte Sözleşmesi’nin arka planını oluşturmaktadır. Aslında Budapeşte Sözleşmesi, uluslararası işbirliğine dair tüm mevcut konuları kapsama niyetinde değildir; metin sadece yeni ve önceden var olmayan ya da daha hızlı kanallar ve işbirliği modellerine atıfta bulunur.  Avrupa Konseyi’nin Üye Devletlerinin hepsi (San Marino hariç) bu Sözleşme’yi onaylamıştır ve bu demektir ki Budapeşte Sözleşmesi’nin tüm Taraflarından 1959 Sözleşmesi’nin tek üye olmayan Tarafı Amerika Birleşik Devletleri’dir.  Bu gerçek, çoğu Avrupa Devleti ve Birleşik Devletler arasında uluslararası  Polis ve adli işbirliğine yönelik ortak bir hukuki çerçevenin ilk kez oluşturulması açısından Budapeşte Sözleşmesi’nin değerini gösterir. Bu özellikle önemli bir konudur çünkü Madde 14, 2, Sözleşme’nin uluslararası işbirliğine dair usulleri, Sözleşme’de Madde 2 ile 11 arasındaki maddelere uygun olarak tespit edilen cezai suçların yanı sıra bir bilgisayar sistemi aracılığıyla işlenen diğer cezai suçlar ve diğer tüm cezai suçların elektronik formattaki kanıtlarının toplanması için de geçerli olacaktır. | |
| **Slayt 21** | **Üçüncü Bölüm – Sanal suçlara verilen uluslararası karşılık: Budapeşte Sanal Suçlar Sözleşmesi** | |
| **Slayt 22 - 25** | Diğer derslerde de bahsedildiği gibi Budapeşte Sözleşmesi, 23 Kasım 2001 tarihinde imzaya açılmış ve Temmuz 2004’te yürürlüğe girmiştir. Nisan 2013 itibarıyla 57 Devlet, Sözleşme’nin ya tarafı veya imzalayıcısıdır ya da katılmaya davet edilmiş bulunmaktadır.  Sanal suç konularına dair soruşturmalarda Sözleşme’nin Tarafları, özellikle uluslararası işbirliği gerekli olduğunda yeni ve çok inovatif soruşturma araçları kullanma imkanı kazanmaktadır. Hakkında soruşturma yürütülen suç, Sözleşme’de belirtilen suçlardan birisi olduğunda ancak aynı zamanda eğer suç bir bilgisayar sistemi aracılığıyla işlenmişse veya suçun kanıtları dijital yollarla kaydedilmiş veya depolanmışsa da bu yeni imkanlar kullanılabilir. Bu, Sözleşme’de Madde 14’te belirtilmektedir.    Eninde sonunda tüm Devletlerin bu amacın ardında toplanacağı umuduyla uluslararası toplumun sanal suçlar ve elektronik kanıtlarla ilgili konularda evrensel bir anlaşma üzerinde anlaşmaya varmaya yönelik ortak çalışmalar gerçekleştirmesi bir ilk olmuştur. Bugün Sözleşme, sanal suçlara dair ilk ve tek bağlayıcı uluslararası doküman olarak varlığını sürdürmektedir.  Sözleşmeyi onaylayan ve Taraf olan her ülke, süreç içinde hem emniyet güçleri hem de yargı organları ile evrensel bir işbirliği *forumuna* çok değerli bir erişim kazanmaktadır.  Sözleşme, uluslararası işbirliği için yeni kanallar oluşturmaktadır. Hükümlerinden bazıları yüksek düzeyde yenilikçidir ve istisnaidir ancak sanal suçların yeni gerçekliklerine yönelik yeterli ve gerekli karşılıklar olarak değerlendirilebilmektedir.  Yine de Sanal Suçlar Sözleşmesi, uluslararası işbirliğine dair tek bağlayıcı uluslararası doküman olmayan çalışmamaktadır. Sözleşme’de Madde 23’te Sözleşme’nin suç konularında uluslararası işbirliğine dair mevcut diğer ilgili dokümanlar çerçevesinde uygulanabilir olacağı belirtilmektedir. Ayrıca Madde 27’de uygulanabilir uluslararası sözleşme ya da anlaşmaların mevcut olmaması durumunda uyulması gereken genel ilkeler açıklanmaktadır.  Diğer yandan şunun altının çizilmesi gerekir ki Sözleşme’nin maddelerinin getirdiği kurallar, Taraflar arasında önceki dokümanların hiçbirinin olanak tanımadığı yeni işbirliği araçları ve kanalları yaratmaktadır. | |
| **Slayt 27** | **Dördüncü Bölüm - Budapeşte Sözleşmesi – uluslararası işbirliği araçları**  Sözleşme’nin uluslararası işbirliğine ilişkin hükümleri, Sözleşme’de bölüm III’te açıklanmaktadır. Bu bölümdeki hükümlerin çoğu operasyonel ve usuli kurallardır ve diğer uluslararası sözleşmelerle de ortak yanlara sahiptir. Diğerleriyse çok daha yenilikçidir ve daha ayrıntılı bir şekilde ele alınmalıdır. | |
| **Slayt 28 ve 29** | Madde 26, bir Tarafın yetkililerinin ulusal bir soruşturma sırasında, elde ettikleri bilgilerden bazılarının başka bir Tarafın yetkililerine, bu devletten herhangi bir talep gelmesini beklemeden iletilmesi gerektiğini fark ettiğinde meydana gelen durumu tarif eder. Eğer bilgiler, Sözleşme çerçevesinde bir suça ilişkin olarak bir soruşturma başlatmak için faydalı ya da gerekli görünüyorsa bu gerçekleştirilebilir. Geçmişte karşılıklı yardımlaşmanın genellikle pasif olmasına karşın Sözleşme, daha proaktif bir yaklaşımı teşvik etmektedir. Ancak, Madde 26 paragraf 2’ye göre bilgilerin bu şekilde “kendiliğinden” temin edilmesi, örneğin gizlilik talebi ya da verilerin özel bir kullanımı gibi belirli koşullara tabi kılınabilir. | |
| **Slayt 30 - 32** | Madde 29, Budapeşte Sözleşmesi’nin en önemli hükümlerinden birisidir. Madde 29, bir bilgisayar sisteminde depolanan verilerin hızlı bir şekilde korunmasına ilişkin kuralları tanımlar. Verilerin hızlı bir şekilde korunmasına ilişkin yerel hüküm ile paralel bir çerçeveye sahiptir. Genel olarak bu hüküm, yüklenici bir Tarafın bir yandan bir arama, el koyma ya da benzeri bir tedbir için diğer Tarafa resmi bir yardım talebi sunmaya yönelik niyetini ifade ederken aynı zamanda verilerin hızlı bir şekilde korumaya alınmasını istemesine olanak tanır.  Bu durumda talebi alan taraf, kendi ulusal hukukuna uygun olarak istenen verileri korumak için gerekli özeni göstererek uygun bir şekilde hareket etmelidir. Daha önceden de bahsedildiği gibi, bu yeni bir uluslararası işbirliği aracıdır. Bu yeni araç, dijital ortamların özelliğinin sonucudur. Sınır ötesi yardım, herkesin bildiği gibi fazla zaman alır. Tedbirin hızlı özelliği, çok kısa süreler için tamamen silinebilecek bir şeyi koruma gerekliliğinin sebep olduğu bir ihtiyaçtır.  Şunun belirtilmesi gerekir ki bu, acil sebepler dolayısıyla yalnızca bir koruma tedbiridir ve korunan verilerin otomatik olarak ifşa edilmesini gerektirmez. Aslında ifşaya izin verilen durumlarda, her şeyden önce veriler yalnızca trafik verileri değilse buna olanak tanıyan çok dar kapsamlı kurallar vardır. Uygulamada verilerin hızlı bir şekilde korumaya alınması gerçekleştirilebilir ve daha sonra bu verilerin talebi yönelten tarafa ifşa edilmemesini gerektiren sebepler olduğu ortaya çıkabilir.  Şunun hatırlatılması gerekir ki, talebi alan taraf, verilerin korunmasının bir şartı olarak çifte suçluluğu şart koşamaz. | |
| **Slayt 33 ve 34** | Trafik verilerinin ifşası, Budapeşte Sözleşmesi’nde Madde 30 kapsamında açıklanmaktadır. Trafik verilerine ilişkin olarak Sözleşme metninde uluslararası işbirliğini kolaylaştıracak daha kolay bir model tarif edilmektedir. Usul hükümleri bölümünde hızlı ifşaya dair özel kurallar olmadığı gibi yerel düzeyde de hızlı ifşaya dair özel kurallar yoktur. Nitekim, açıkça ifade edilmese de Sözleşme, kanıtların hızlı bir şekilde korumaya alınması ve ifşasına ilişkin yerel hükümlerle uluslararası işbirliğini düzenleyen hükümler arasında bir uyum sağlar. | |
| **Slayt 35 ve 36** | Sözleşme’nin 31. Maddesinde depolanan bilgisayar verilerine erişime ilişkin karşılıklı yardıma dair genel bir kural tanımlanmaktadır. Bu madde ve bu maddede atıfta bulunulan Madde 23, sanal suçların takibatında tarafların azami seviyede işbirliği yapmasına yönelik genel bir istek ifade etse de yeni işbirliği görevleri oluşturulmamaktadır. Tüm işbirliği, geleneksel soruşturmalarda sınır ötesi işbirliğini düzenleyen mevcut anlaşmalara ve uluslararası dokümanlara tabidir.  Uygulamada Madde 31 sadece, zaten gerçek hayatta yıllardır geçerli olan genel kuralları sanal ortamlara getirmektedir. | |
| **Slayt 37 ve 38** | Madde 32, herhangi bir uluslararası işbirliği talebi olmadan başka bir Tarafın topraklarında fiziksel olarak bulunan bir bilgisayarda depolanmış kanıtları elde etmek için Sözleşme’ye Taraf bir devletin emniyet güçlerine verilen imkanı tanımlamaktadır. Bu, eğer somut bir soruşturma sırasında görevli yetkililer yabancı bir ülkede bulunan bir bilgisayardan ya da erişilmesine yasal olarak yetkili bir insan tarafından izin verilmiş bir bilgisayardan açık kaynak bilgiler almaya ihtiyaç duyarsa gerçekleştirilebilir.  Açık kaynak bilgilere ilişkin olarak şunun belirtilmesi gerekir ki bu “açık kaynak” araştırma, herhangi bir vatandaşın kendi inisiyatifiyle çoğu ülkede gerçekleştirebileceği bir şeydir. Dolayısıyla bu hüküm, sadece emniyet güçlerinin bunu gerçekleştirmesi ve aynı zamanda bu şekilde toplanan kanıtları geçerli olarak kabul etmesi için yetki vermeyi amaçlamaktadır.  Ancak, hükmün diğer tarafı çok yeni bir yaklaşım sunar. Fiziksel dünyada bu yeni imkana gerçekten eşdeğer bir unsur bulunmamaktadır: Geçmişte bir yetkili, başka bir ülkeye fiziksel olarak yolculuk yapıp yerel makamların yardımını isterdi. Kendi başına bir şey yapamazdı ve tüm soruşturma eylemleri, bu yabancı ülkenin ulusal makamlarının adına gerçekleştirilirdi.  Madde 32 ise tam tersini belirtmektedir. Buna göre tüm dünyadaki herhangi bir ülkeden herhangi bir emniyet yetkilisi, verileri ifşa etmeye yönelik meşru yetkiye sahip kişi meşru ve gönüllü onayını verirse “açık kaynak olmayan” bilgileri bile başka bir ülkeden alabilir. Bu soruşturma faaliyeti, bilginin depolandığı yerdeki yetki alanına sahip Devletten herhangi bir yetki alınmasını gerektirmez. Bazı Devletler, bu hükümden dolayı Sözleşme’yi barışçıl olarak değerlendirmez. Bunun egemenlik hükmüne aykırı olduğunu iddia ederler. Ancak, sınır ötesi soruşturmalar ya da “bulut” hizmetinde yapılan araştırmalara ilişkin karmaşık sorunlara herhangi bir teklif ya da başka bir çözüm getirilmemektedir. Gerçek hayat çoğu durumda şunu ortaya çıkarır ki geleneksel kanalları kullanarak uluslararası düzeyde sanal suçları araştırmak ya da bunlara ilişkin elektronik kanıtlar toplamak imkansızdır. Bunun sebebi şudur ki bu eylemin aldığı zaman, elektronik kanıtların uçuculuğu ve hassasiyeti ile uyumlu değildir. İşte bu yüzden davayla uğraşan bir emniyet yetkilisi tarafından yürütülen sınır ötesi bir soruşturma daha etkili olur.  Ancak diğer yandan, “bulut” hizmetlerine ilişkin olarak normal işbirliği kanallarını kullanmak gerçekten tamamen imkansızdır. Kullanıcılar (ve araştırmacı), polisin ihtiyaç duyduğu verilerin fiziksel olarak nerede depolandığını tam olarak bilmez. | |
| **Slayt 39 ve 40** | Madde 33, iletişimleri ele geçirmeye dair uluslararası işbirliği ile ilgilidir. Bu, yeni bir uluslararası işbirliği aracı değildir: diğer bağlayıcı uluslararası dokümanlar ona atıfta bulunur. Ancak Madde 33, özel bir kapsama sahiptir. Trafik verilerinin gerçek zamanlı olarak toplanması.  Diğer yandan Madde 33’te belirtilen en önemli kuralda, bu soruşturma tedbirinin uygulanmasının sınırlarından bahsedilir. Sınırlar, iç hukukta öngörülen koşullar ve usullerdir. Bu yüzden bu işbirliği modeli, trafik verilerinin gerçek zamanlı olarak toplanmasının benzer bir yerel davada mümkün olduğu aynı durumlarda her bir Devlet tarafından temin edilecektir. | |
| **Slayt 41 - 43** | Madde 35, Sözleşme’nin en önemli operasyonel hükümlerinden birisidir. Madde 35, tüm yüklenici Tarafların kalıcı olarak ulaşılabilir bir irtibat noktası (7/24 irtibat noktaları ağı) oluşturmasını şart koşar.  Bu irtibat noktalarının genel amacı uluslararası işbirliğini kolaylaştırmaktır. Diğer irtibat noktalarına teknik danışmanlık vererek, verilerin hızlı bir şekilde korunmaya alınması için düzgün bir mekanizmayı hareket geçirerek, acilen kanıtları toplayarak veya şüphelileri tespit ederek ve keşfederek bunu gerçekleştirebilirler.  Yüksek teknolojili suçlarla ilgili uzmanların oluşturduğu bu operayonel ağ, diğer ülkelerden ve yargı alanlarından uzmanlara suç soruşturmalarında uluslararası bağlantılarla yardımcı olmak üzere tasarlanmıştır. Yeni, hızlı ileri teknoloji suçlarının sebep olduğu yeni zorluklarla yüzleşmek istemektedir. Bazen bilgisayar suçlarına ilişkin soruşturmalarda şüphelilerin yerinin tespit edilip takibe alınabilmesi için elektronik verilerin çok hızlı bir şekilde korunması gerekir. Bu yeni ihtiyaç, hiçbir geleneksel uluslararası işbirliği kanalı ile karşılanamaz. Bu ağın katma değeri de burada yatar: resmi bir işbirliği talebi de bu gayriresmi yolu izlemek zorunda olsa bile bu ağ, yardım ve işbirliğini çok hızlı bir şekilde temin edebilir. | |
|  | **Uygulamalı Alıştırmalar (eğer varsa)**  Bu oturumu için uygulamalı alıştırma hazırlanmamıştır. | |
|  | Bilgi Kontrolü  Eğitimci, Eğitimci, oturumun boyutlarının her birinden ilgili sorular sorarak bilgi kontrolü gerçekleştirmelidir. | |
| **Slayt 45 ve 46** | **Özet**  Eğitimci, aşağıdaki hususlara ilişkin olarak bilgileri özetlemeli / sınamalıdır:   * İnternetin küresel boyutunun ve sanal suçların uluslararası boyutunun tanınması, * Uluslararası işbirliğinin öneminin açıklanması ve sanal suç alanında uluslararası işbirliği için mevcut araçların tanınması, * Uluslararası işbirliği için oldukça hızlı ve etkin kanallara olan ihtiyacın ve mevcut araçların, bunların kullanım yollarının, zaman çizelgelerinin ve etkinliklerinin belirlenmesi, * Yeni uluslararası işbirliği modellerinin uygulanmasına ilişkin uluslararası kuruluşların çalışmalarının anlatılması, * Budapeşte Sanal Suçlar Sözleşmesi’nin tartışılması, genel ilkelerinin, geçici önlemlerin ve 7/24 karşılıklı hukuki yardım ağının tanınması. | |

|  |  |  |
| --- | --- | --- |
| Ders 1.3.5 Eğitimin Kapanışı | | **Süre: 90 Dakika** |
| **Gerekli Kaynaklar:**   * Windows 7 ve Office 2010 kurulu olan bir dizüstü bilgisayar ya da PC * Projektör * PowerPoint Sunum * Katılımcı değerlendirme formları | | |
| **Amaç:**  Bu oturum, katılımcıların eğitime dair olarak geri bildirimler sunmasına ve eğitimcinin yapılabilecek iyileştirmeleri tespit etmesine yardımcı olmak üzere tasarlanmıştır. Ayrıca eğitimcinin, amaç ve hedeflere değinerek eğitimin içeriğini yeniden özetlemesi amaçlanmaktadır. | | |
| **Hedefler:**  Oturumun sonunda katılımcılar:   * Eğitime ve etkinliğine ilişkin olarak uygun geri bildirimler sunabilecek, * Avrupa Konseyi eğitim değerlendirme formlarını doldurabilecek, * Konuya ilişkin bilgi ve becerilerini geliştirmek için almaları gereken bir sonraki eğitim düzeyini tespit edebilecektir. | | |
| **Giriş**  Bu eğitimin önemli bir bölümüdür ve eğitimin içeriği ve eğitimin verilmesi için kullanılan metodolojiye ilişkin olarak öğrencilerden geri bildirim almak için kullanılmalıdır. Tüm değerlendirme formları, bu oturum sırasında doldurulmalı veya kesinleştirilmelidir. Eğitimci, eğitimin tüm oturumlarını yeniden özetlemeli ve hedeflerin gerçekleştirilip gerçekleştirilmediğini kontrol etmelidir. Oturum sona erdiğinde eğitimci, tüm geri bildirimlerin verilmesini ve gerekli olan tüm değişikliklerin eğitimde devam eden küçük bir düzeltme olarak ya da programlı ve büyük bir değişiklik güncellemesi sırasında uygulanmasını sağlamaktan sorumlu olacaktır. | | |
| **Slayt no.** | **İçerik:** | |
| **Slayt 1** | **PowerPoint** (ya da başka bir tür sunum)  PowerPoint sunumu eğitmene eğitimin tüm oturumları hakkında tartışmayı teşvik etmesine destek olmak amacıyla sağlanmıştır. Eğitmenin bu oturum başlamadan önce değerlendirme formlarını dağıtması gerekir. Bazı durumlarda değerlendirme formlarını eğitimin başında dağıtmak, eğitim ilerledikçe oturumlar hala katılımcıların zihinlerinde tazeyken doldurabilmeleri amacıyla uygun olabilir. Ayrıca, katılımcıların dersin sonunda bu formları tamamen doldurmama eğilimleri de söz konusu olabilmektedir | |
| **Slayt 2 ve 3** | Daha önceki tüm derslerde olduğu gibi bu derste de dersin başında belirlenen gündem ve oturum hedefleriyle benzer bir yol izlemelidir. | |
| **Slayt 4 - 21** | Zaman çizelgesi, eğitimin içeriğinin katılımcılara hatırlatılması için faydalı bir yoldur ve eğitmene yardımcı olmak için dahil edilmiştir.  Eğitmen, oturumların her biri için gündem ve oturum hedeflerini tekrarlamalıdır. Katılımcıların geri bildirim ve önerileri ileride kullanılmak üzere not edilmelidir. | |
| **Slayt 22** | Katılımcıların değerlendirme formlarını doldurmalarını sağlamak eğitmenin sorumluluğundadır. Eğitmen, doldurulan formları toplamalı ve eğitimdeki Avrupa Konseyi temsilcisine vermeli ya da ilk fırsatta Avrupa Konseyi’ne göndermelidir. | |
|  | **Uygulamalı Alıştırmalar** (eğer varsa)  Avrupa Konseyi değerlendirme formunun doldurulmasının dışında bu oturumla ilgili uygulamalı alıştırma mevcut değildir. | |
|  | **Bilgi Kontrolü**  Oturum, eğitimcinin geri bildirim aşamasında sorular sorarak öğrenciler tarafından edinilen bilgileri kontrol etmesi için uygundur. | |
|  | **Özet**  Eğitimciler, öğrencilerin geri bildirimler sunması için yeterli fırsatın verilmesini ve geri bildirimlerin toplanmasını sağlamalıdır. | |

# 7 Değerlendirme

Değerlendirme, bir eğitimin önemli bir bölümüdür ve katılımcıların öğrenme deneyimleri ile ilgili önemli geri bildirimlerini sunması gereken zamanda gerçekleştirilmelidir.

Bu eğitim, genel kapsamlı bir eğitim olarak geliştirilmiştir ve bu yüzden öğretim materyallerinin çoğu PowerPoint formatındadır ve bu tür bir eğitim ile normalde ilişkili olabilecek uygulamalı alıştırmalar düzeyinden yoksundur.

Bir değerlendirme formu hazırlanmıştır ve bundan sonraki bölümde yer almaktadır. Eğitimciler, eğitimin ileride verileceği zamanlar için iyileştirmelerin yapılabilmesi için formların doldurulmasını ve Avrupa Konseyi’ne gönderilmesini sağlamalıdır.

# 8 Ölçüm

Bu eğitim için hiçbir ölçüm talep edilmemiştir ancak özellikle eğitimin, ölçülen bir programın bir parçası olabileceği ülkelerde materyalleri gelecekte dağıtacak kişiler bunu yeniden değerlendirebilir. Eğer ölçüm uygulaması getirilirse o ülkedeki metodolojiler kullanılmalıdır.

**Ek**

**Eğitim materyalleri ve öğrenci materyalleri**

1. Katılım Öncesi Mali Yardım Aracı Kapsamında Avrupa Birliği/Avrupa Konseyi Sanal Suçlar Ortak Projesi (Ceza Yargılamasında Bölgesel İşbirliği: Sanal suçlarla mücadelede kapasitelerin güçlendirilmesi), sanal suçlara karşı etkili bir şekilde işbirliği yapmak için Batı Balkanlar ve Türkiye’nin ceza yargılaması makamlarının kapasitelerinin artırılmasını amaçlamaktadır. [↑](#footnote-ref-1)
2. \* Bu metin içerisinde toprakları, kurumları ve halkı kapsamında Kosova’ya yapılan tüm atıflar Birlşemiş Milletler Güvenlik Konseyi’nin 1244 sayılı Kararına uygun olarak ve Kosova’nın statüsüne halel getirmeyecek şekilde anlaşılacaktır. [↑](#footnote-ref-2)
3. http://eur-lex.europa.eu/LexUriServ/site/en/oj/2005/l\_069/l\_06920050316en00670071.pdf [↑](#footnote-ref-3)
4. http://register.consilium.europa.eu/pdf/en/03/st14/st14583.en03.pdf [↑](#footnote-ref-4)
5. internet Servis Sağlayıcı [↑](#footnote-ref-5)