Dosya Sistem Analizi Dersi
File System Forensic

Yrd. Doç. Dr. Erhan AKBAL

Dersin Amacı

- Bu ders, daha verimli bir adli inceleme yürütebilmenize ve verileri ve bunların nasıl depolandığını anlamamızı sağlar.
- Dijital soruşturma araçları, nispeten kullanımı kolay hale getirmiştir, çünkü soruşturma yapmak için gereken zamanı azaltmaktadır.
- Bununla birlikte, araştırmacının sonuçları tam olarak anlamayabileceği anlamına gelir.
- Soruşturmacı delilleri ve nereden geldiğini ifade etmek istediğinde bu sorun olabilir.

Dersin İçeriği

- Adli İncelemenin Temelleri
- Bilgisayar Temelleri
- Hard Disk Verilerinin Elde Edilmesi
- Volume Analizi
- PC Tabanlı Partitionlar
- Server Tabanlı Partitionlar
- Çoklu Disk Volümleri
- Dosya Sistem Analizi
- FAT Yapısı ve Analizi
- FAT Veri Yapıları
- NTFS Konsepti
- NTFS Analizi
- NTFS Veri Yapıları
- Ext2 ve Ext3 Konsepti ve Analizi
- UFS1 ve UFS2 Analizi
- HFS Dosya Yapıları ve Analizi

Dersin İşleyişi

- Bireysel Araştırma konusu ve varsa uygulaması
- Derste ve uygulamada verilen ödevler
- Vize ve Final Sınavı
- Devamsızlık

Dosya Sistem Tanımı

- Dosya sistemi disk üzerindeki dosyaların organize edilmesidir. Bir işletim sisteminin bir disk veya bölümleri üzerindeki dosyalarının izlerini bulmak için kullandığı yapı ve yönteme dosya sistemi (filesystem) denir.
- Ayrıca dosya sistemi terimi, dosyaların veya dosya sistemlerinin depolandığı bir disk veya disk üzerindeki bir bölümü tanımlamak için de kullanılabilir.
- En sade şekliyle, dosyaların kayıt ortamında düzen içinde olmalarını sağlar. Sonradan aradığımız bilgiye kolay bir şekilde ulaşmamız, dosyaları belli kriterlere göre gruplandırmamız (örn. klasörler) ve birtakım gelişmiş işlemler (paylaşım ve güvenlik gibi) dosya sisteminin görevidir.

Bölüm 1 Adli İncelemenin Temelleri

Giriş

- Dijital bir soruşturmanın odağı, bir olaya veya suça karışan bazı dijital cihazları incelemektir.
- Dijital cihaz ya bir fiziksel suç işlemek için ya da bir kanunu ihlal eden bir amaç için kullanılır.
- Birinciye örnek, bir şüpheli bir suçla ilgili veriler için İnternet kullanıp kullanmadığıdır.
- İkinci duruma örnek olarak bir saldırgan bir bilgisayara yetkisiz erişir, bir kullanıcıya ait materyali indirir veya bir kullanıcıyı tehdit eden bir e-posta gönderir.
- İhlal tespit edildiğinde, ihlalin neden meydana geldiği ve bunun nedenini kimin veya neyin sebep olduğu gibi sorulara cevap bulmak için bir soruşturma başlatılır.

Giriş

- Adli bilişim soruşturmaları, dijital olaylarla ilgili soruları yanıtlayan hipotezleri geliştirip test ettiğimiz bir süreçtir. Bu, bilimsel bir yöntem kullanarak yapılır; burada hipotez bulunur ve bulduğumuz hipotezi imkânsız olduğunu gösteren ek kanıtlar arayarak test eden bir hipotez geliştirilir.
- **Dijital delil**, bir hipotezi destekleyen ya da çürüten güvenilir bilgileri içeren öğelerdir.

Giriş – Örnek Senaryo

- Güvenlik açığı bulunan bir sunucuyu düşünelim. Bunun nasıl oluştuğunu ve kimin yaptığını belirlemek için bir soruşturma başlatalım. Soruşturma sırasında olayla ilgili yaratılan verileri bulmalıyız. Silinmiş günlük girişlerini sunucudan kurtarır, saldırı araçlarını bulur ve sunucudaki çok sayıda zayıf noktayı tespit ederiz. Bu verileri kullanarak, saldırganın hangi güvenlik açığına eriştiğini ve daha sonra ne yaptıklarını gösteren hipotezler hazırlarız.
- Daha sonra, güvenlik duvarı yapılandırmasını ve günlüklerini inceleriz ve hipotezlerimizdeki bazı senaryoların imkânsız olduğunu belirleriz. Çünkü bu tür ağ trafiği mevcut olamaz ve gerekli günlük girdilerini bulamayız. Bu nedenle, bir veya daha fazla hipotezi reddeden kanıtlar bulabiliriz.
- Kanıtlar inceleme kullanımları içindir ve bunların hepsinin bir mahkemeye girilemeyeceği durumlar olabilir.
- Yasal kabul edilebilirlik gereksinimleri ülke ve eyalete göre değişir ve hukuki dayanak olmadığında genel kanı konseptine odaklanılarak ve kendi yargı alanınızda gerekli ayarlamaları yapılarak inceleme yapılır.
- Aslında, dosya sistemlerine özgü yasal gereklilikler bulunmadığından genel yöntemler dosya sistemi için kullanılabilir.

Giriş

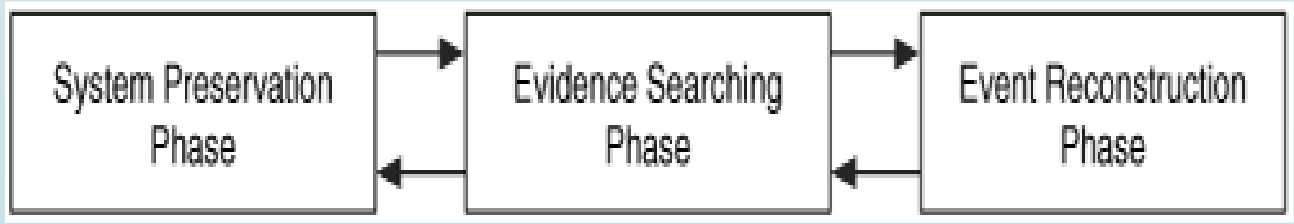
- Amerikan Miras Sözlüğü, adli tıpı bir sıfat olarak tanımlar ve "bir mahkemede soruşturma ve gerçeklerin veya kanıtların oluşturulmasında bilim veya teknolojinin kullanımı" şeklinde açıklar.
- Dijital kanıtların doğası bir araştırma sırasında teknolojiyi kullanmamızı gerektirir; bu nedenle dijital bir soruşturma ile dijital adli soruşturma arasındaki ana fark yasal gerekliliklerin getirilmesidir.
- Dijital bir adli inceleme, dijital nesneleri analiz etmek için bilim ve teknolojiyi kullanan bir süreçtir ve meydana gelen olaylarla ilgili soruları cevaplamak için kanunlarla ilişkili teorileri geliştirir ve test eder.
- Başka bir deyişle, dijital bir adli soruşturma daha sınırlı bir araştırma şeklidir.

Dijital Suç Senaryosu İnceleme Süreci

- Bir soruşturma yürütmenin tek bir yolu yoktur.
- Beş kişiden en son fincan kahveyi içen kişiyi bulmasını isterseniz muhtemelen beş farklı yaklaşımı göreceksiniz.
- Bir kişi fincandaki parmak izini inceler, diğeri mola odasının gündelik kamera bantlarını isteyebilir ve bir başkası en sıcak kahve bardağı ile insanları arayabilir.
- Doğru kişiyi bulduğumuz sürece ve süreçte herhangi bir yasayı ihlal etmediğimiz sürece, bazıları diğerlerinden daha verimli olmasına rağmen hangi işlemin kullanıldığı önemli değildir.

Dijital Suç Senaryosu İnceleme Süreci

- Dijital bir soruşturma için kullanılan yaklaşım fiziksel suç mahalinin soruşturma sürecine dayanmaktadır.
- Bu durumda, yazılım ve donanım tarafından oluşturulan dijital ortamı içeren dijital bir olay mahalline sahibiz.
- Süreç, sistemin korunması, kanıt araştırması ve olayın yeniden yapılandırılması olmak üzere üç ana safhaya sahiptir.



Dijital Suç Senaryosu İnceleme Süreci

- Bu süreç hem canlı hem de ölü sistemleri araştırırken kullanılabilir.
- Kanıt bulmak için işletim sistemini veya araştırılan sistemin diğer kaynaklarını kullandığınızda, canlı bir analiz yapılır.
- Ölü analizde kanıt bulmak için güvenilir bir işletim sistemi ve güvenilir uygulamalar kullanılarak analiz yapılır.
- Canlı bir analizle, yazılım yanlışlıkla veriyi gizleyebilir veya tahrif edebilir, çünkü yanlış bilgi alma riski taşırsınız. Ölü bir analiz daha idealdir, ancak her koşulda mümkün değildir.

Sistem Koruma Aşaması

- Soruşturma sürecinin ilk aşaması, dijital olay mahallinin durumunu korumaya çalıştığımız Sistem Koruma Aşaması‘ dır.
- Bu aşamada yapılan eylemler, soruşturmanın hukuki, ticari veya operasyonel gerekliliklerine bağlı olarak değişir.
- Örneğin, yasal gereklilikler sistemin fişini çekip tüm verilerin tam kopyasını almanıza neden olabilir. Diğer yandan, bir casus yazılım enfeksiyonu veya honeypot içeren bir durum olabilir ve hiçbir koruma yapılmaz.
- Kurumsal ya da askeri bir ortamda yapılan ve mahkemeye çıkmayacak olan soruşturmaların çoğunda, bu iki uç arasındaki teknikler kullanılmaktadır.
- Bu aşamanın amacı, üzerine yazılabilecek kanıt miktarını azaltmaktır. Veriler sistemden alındığında bu süreç devam eder, çünkü gelecekteki analizler için verilerin korunması gerekir.

Koruma Teknikleri

- Bu aşamanın amacı kanıt miktarını azaltmaktır, bu nedenle depolama cihazlarımıza yazabilecek işlemleri sınırlamak istenir. Ölü bir analiz için sistemi kapatarak tüm işlemleri sonlandırılır ve tüm verilerin çoğaltılmış kopyaları alınır.
- Canlı bir analiz için şüpheli süreçler sonlandırılabilir veya askıya alınabilir. Ağ bağlantısı kesilebilir (ölü bir bağlantı hakkında günlük iletilerini engellemek için sistemi boş bir hub'a veya anahtara takabilirsiniz) veya ağ filtreleri, failin uzaktaki bir sistemden bağlanamayacağı ve verileri kaldıramayacağı şekilde uygulanabilir.
- Delil araştırılırken üzerine yazılması durumuna karşın önemli veriler sistemden kopyalanmalıdır. Örneğin, dosyaları okurken, dosyaların özelliklerindeki sürelerin güncelleştirilmelerine neden olmadan önce son erişim sürelerinin bir kopyasını elde edebilmeniz için her dosyanın zamansal verilerini kaydedebilirsiniz.
- Ölü veya canlı analiz sırasında önemli veriler kaydedildiğinde, daha sonra verilerin değişmediğini gösteren bir şifreleme hash hesaplanmalıdır.
- MD5, SHA-1 ve SHA-256 gibi bir şifreleme hash, girdi verilerine dayalı çok büyük bir sayı üreten bir matematiksel formüldür. Giriş verilerinin herhangi bir biti değişirse, çıkış numarası dramatik bir şekilde değişir. Algoritmalar, aynı çıktıyı üreten iki girdinin bulunması son derece zor olacak şekilde tasarlanmıştır. Bu nedenle, önemli verilerinizin hash değeri değişirse, verilerin değiştirildiğini bilirsiniz

Kanıt Bulma Safhası

- Verileri korumak için gerekli önlemleri aldıktan sonra, delil araştırılması gereklidir.
- Olayla ilgili hipotezleri destekleyen veya çürüten veriler arıyor olduğumuzu unutmamalıyız.
- Bu işlem, tipik olarak, biliniyorsa, olayın türüne göre ortak konumların araştırılmasıyla başlar.
- Örneğin, Web tarama alışkanlıklarını araştırıyorsanız, Web tarayıcı önbelleğine, geçmiş dosyasına ve yer imlerine bakacağız.
- Bir Linux izinsiz girişini araştırıyorsanız, bir rootkit veya yeni kullanıcı hesapları bulmaya çalışabiliriz.
- Soruşturma devam ederken ve hipotez geliştirirken, onları çürütecek veya destekleyecek deliller aranması gerekir.
- Hipotezinizi çürüten kanıtlara bakmak, yalnızca hipotezinizi destekleyen kanıt aramaktan daha önemlidir.
- İki önemli adım, neye baktığımızı ve neyi bulmayı umduğumuzu belirlemektir.

Arama Teknikleri

- En çok kanıt arayışı dosya sistemi ve dosyaların içinde yapılır. Ortak bir arama tekniği, isimlerini veya adlarını kendi adlarına göre dosyaları aramaktır.
- Bir diğer yaygın arama tekniği, içeriklerindeki bir anahtar kelimeye dayalı dosyaları aramaktır. Dosyaları, son erişilen veya oluşturulduğu saat gibi zamansal verilerini temel alarak da arayabiliriz.
- Bir dosyanın içeriğinin MD5 veya SHA-1 hash değerini, Ulusal Yazılım Referans Kütüphanesi (NSRL) (http://www.nsrl.nist.gov) gibi bir karma veritabanı ile karşılaştırarak bilinen dosyaları arayabiliriz.
- Hash veritabanları, kötü veya iyi olduğu bilinen dosyaları bulmak için kullanılabilir.
- Bir diğer yaygın arama yöntemi, içeriklerindeki imzalara dayalı dosyaları aramaktır. Bu, birisinin adını değiştirmesine rağmen belirli bir türdeki tüm dosyaları bulmamızı sağlar.

Olay Yeniden Yapılandırma Aşaması

- Soruşturmanın son aşaması, bulduğumuz kanıtları kullanmak ve sistemde hangi olayların meydana geldiğini belirlemektir.
- Soruşturma tanımımız, sistemdeki dijital olaylarla ilgili soruları cevaplamaya çalışmaya başlamamızdır.
- Delil arama sırasında bir şirket politikasını veya yasayı ihlal eden birkaç dosya bulmuş olabiliriz ancak bu olaylarla ilgili soruları cevaplamamıza yeterli olmaz.
- Dosyalardan biri, onu indiren bir olayın etkisi olabilir, ancak aynı zamanda hangi uygulamanın indirildiğini de belirlemeliyiz. Web tarayıcısının bunları indirdiğine dair kanıt var mı yoksa kötü amaçlı yazılımdan kaynaklanıyor olabilir mi? (Küfür veya diğer dijital deliller bulunursa, birkaç durumda kötü amaçlı yazılımları bir savunma olarak kullanmıştır.)

Olay Yeniden Yapılandırma Aşaması

- Dijital olay yeniden yapılandırma aşamasından sonra, dijital olayları fiziksel olaylarla ilişkilendirebiliriz.
- Olayların yeniden yapılandırılması, yeteneklerine dayanarak hipotezler oluşturabilmeniz için sisteme kurulan uygulamalar ve işletim sistemi hakkında bilgi gerektirir.
- Örneğin, Windows 7'de Windows 10'dab farklı olaylar oluşabilir veya Mozilla Web tarayıcısının farklı sürümleri farklı olaylara neden olabilir.

Genel Kurallar

- Her soruşturma aynı prosedürü kullanmaz ve yeni bir prosedür geliştirmenizin gerektiği durumlar olabilir.
- Genel Kurallar
  - Koruma
  - İzolasyon
  - Korelasyon
  - Loglama

Koruma

- İlk kural, araştırılan sistemin korunmasıdır. Bu kural arkasındaki amaç, delil olabilecek herhangi bir bilgiyi değiştirmek istemediğiniz ve diğer tarafın mahkemeyi, delilinin üzerine yazdığınızı ikna etmeye çalıştığı bir mahkeme salonunda olmak istememizdir.
  - Önemli verileri kopyalayın, orijinali güvenli bir yere koyun ve veriler değiştirildiğinde orijinali geri yükleyebilmeniz için kopya üzerinden analiz edin.
  - Önemli verilerin MD5 veya SHA hash değerlerini hesaplayın, böylece daha sonra Veri değişmediğini ispatlayın.
  - Şüpheli verilere yazabilecek prosedürler sırasında bir yazma engelleme cihazı kullanın. Canlı analiz sırasında oluşturulan dosyaların sayısını en aza indirin, çünkü bunlar ayrılmamış alanlardaki kanıtların üzerine yazabilir.
  - Canlı analiz sırasında şüpheli sistemdeki dosyaları açarken dikkatli olun, çünkü son erişim zamanı gibi verileri değiştirmiş olabilirsiniz

İzolasyon

- İkinci kural analiz ortamını hem şüpheli verilerden hem de dış dünyadan izole etmektir.
- Kendinizi şüpheli verilerden ayırmak istiyorsunuz çünkü ne yapacağını bilmiyorsunuz. Şüpheli sistemden bir çalıştırılabilir dosya çalışması, bilgisayarınızdaki tüm dosyaları silebilir veya uzak bir sistemle iletişim kurabilir.
- Şüpheli sistemden bir HTML dosyası açılması, Web tarayıcınızın komut dosyalarını yürütmesine ve dosyaları uzaktaki bir sunucudan indirmesine neden olabilir.
- Bunların her ikisi de potansiyel olarak tehlikeli ve dikkatli olunmalıdır. Şüpheli verilerin izolasyonu, sınırlı işlevselliğe sahip uygulamalarda veya VMWare (http://www.vmware.com) gibi imha edildiğinde kolaylıkla yeniden oluşturulabilen sanal bir ortamdaki verileri görüntüleyerek uygulanır.

İzolasyon

- Dış dünyadan izolasyon genellikle dış dünyayla bağlantılı olmayan veya yalnızca sınırlı bağlantıya izin veren bir güvenlik duvarıyla bağlanmış bir analiz ağı kullanılarak gerçekleştirilir.
- Canlı analizle izolasyonun zor olduğunu unutmayın. Tanımı gereği, bir sistemi şüpheli olan işletim sistemini kullanarak analiz edeceğinizden, şüpheli veriden izole edilmemişsinizdir. Yaptığınız her eylem şüpheli verileri içerir. Dahası, sistemin dış dünyadan yalıtılması zordur, çünkü bu, ağ bağlantısının kaldırılmasını gerektirir ve canlı analiz genellikle sistemin aktif kalması gerektiği için oluşur.

Korelasyon

- Üçüncü kural, verileri diğer bağımsız kaynaklarla ilişkilendirmektir.
- Bu, sahte veri riskini azaltmaya yardımcı olur.
- Örneğin, çoğu sistemde zaman damgalarının kolayca değiştirilebileceğini göreceğiz.
- Bu nedenle, soruşturmada zaman çok önemli ise, günlük girdileri, ağ trafiğini veya dosya etkinliği sürelerini doğrulayabilecek diğer olayları bulmaya çalışmalısınız.

Loglama

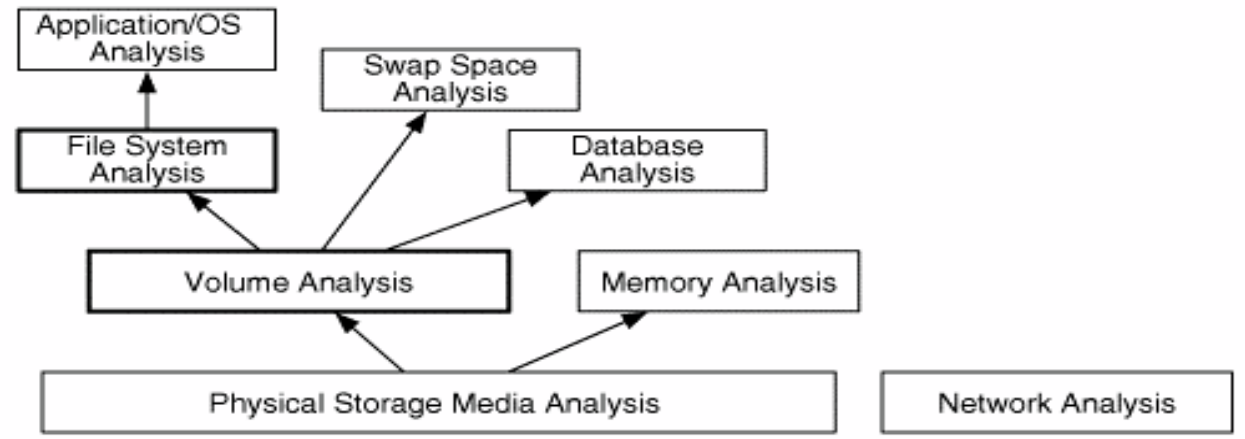
- Nihai kural, eylemlerinizi kaydetmek ve belgelemektir.
- Bu, hangi aramaları henüz gerçekleştirmediğinizi ve sonuçlarınızın ne olduğunu belirlemenize yardımcı olur.
- Canlı bir analiz yaparken ya da verileri değiştirecek teknikler icra ederken, yaptıklarınızı belgelemek önemlidir, böylece eylemleriniz nedeniyle sistemdeki değişikliklerin ne olduğunu belgeleyebilirsiniz.

Veri Analizi

Bu bölümde, dijital kanıt arayabileceğiniz yerler daraltılacak ve bu derste hangisinin daha sonra tartışılacağını belirtilecek. Ayrıca, hangi verilere diğerlerinden daha fazla güvenebileceğimiz gösterilecek.

Analiz Tipleri

- Sayısal verileri analiz ederken, insanlar tarafından tasarlanmış bir nesneye bakılmaktadır.
- Ayrıca, çoğu sayısal aygıtın depolama sistemleri ölçeklenebilir ve esnek olacak şekilde tasarlanmıştır ve katmanlı bir tasarıma sahiptir. Bu katmanlı tasarım farklı analiz türlerini tanımlamak için kullanılır.
- Tasarım katmanlarının altından başlarsak, iki bağımsız analiz alanı bulunur.
- Birincisi depolama aygıtlarına, diğeri de iletişim aygıtları tabanlı.



Volüm Analizi

- Uçucu olmayan depolamada kullanılan depolama aygıtları tipik olarak volümler halinde organize edilir.
- Volüm, bir kullanıcının veya uygulamanın yazabileceği ve okuyabileceği depolama konumlarının bir toplamıdır.
- Bu katmanda iki temel kavram vardır.
- Birincisi, tek bir partitionı daha küçük volümlere bölen bölümleme ve diğeri, birden fazla partitionı daha büyük bir volüm olarak birleştirdiğimiz yapıdır.
- Bu kategoriye örnek olarak DOS bölüm tabloları, Apple bölümleri ve RAID dizileri verilebilir.
- Disketler gibi bazı ortamların bu katmanda herhangi bir verisi yoktur ve tüm disk volüme dir.
- Dosya sisteminin veya diğer verilerin nerede olduğunu belirlemek ve gizli verileri nerede bulabileceğimizi belirlemek için verileri volume seviyesinde analiz etmeliyiz.

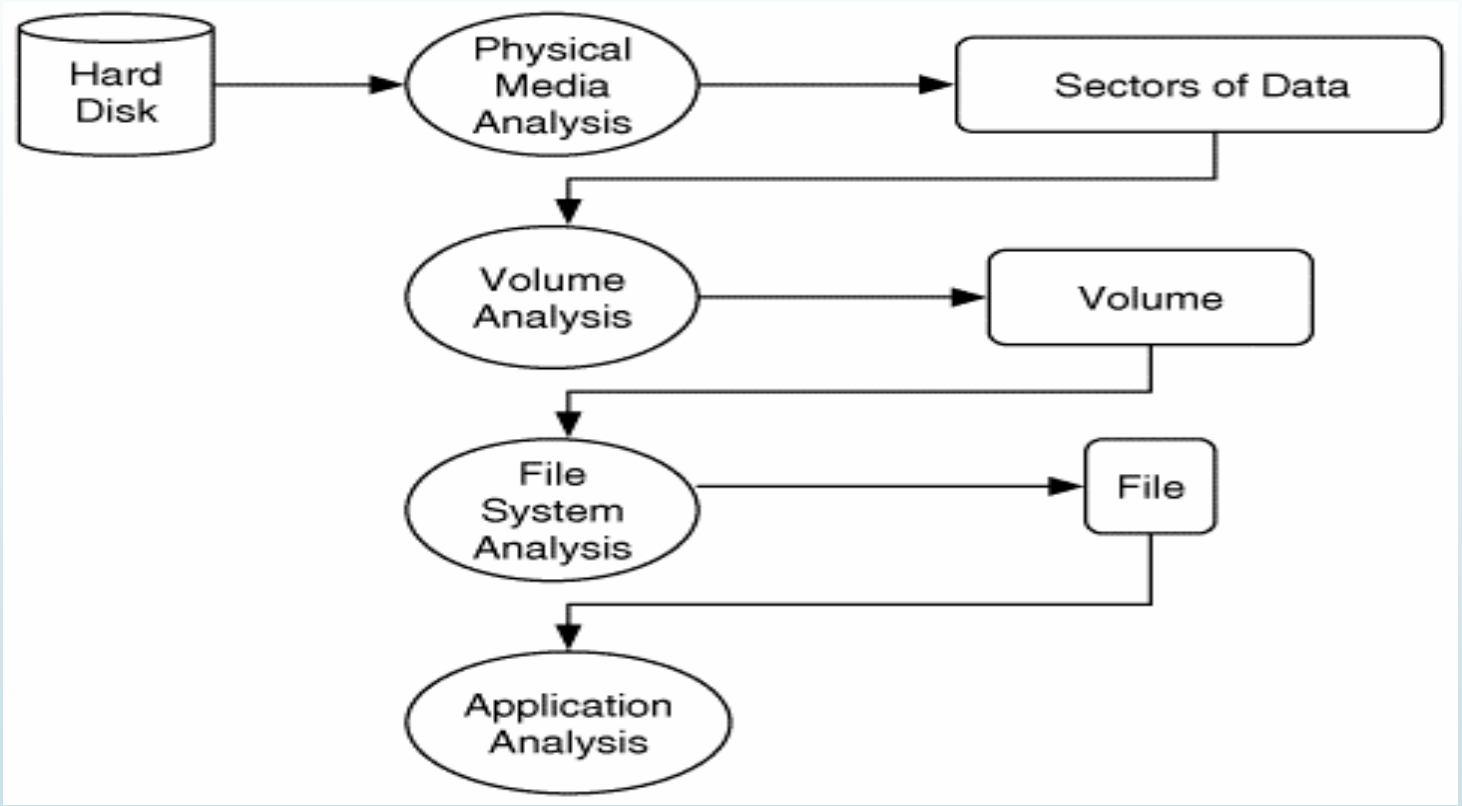
Dosya Sistem Analizi

- Her bir volume de her tür veri olabilir, ancak en yaygın içerik dosya sistemleridir.
- Diğer volumeler bir veritabanı içerebilir veya geçici bir saklama alanı olarak kullanılabilir.
- Dersin 3. bölümü, bir uygulamanın dosyaları oluşturmasına, okumasına ve yazmasına olanak tanıyan bir veri yapıları topluluğu olan dosya sistemleri gösterilecektir.
- Dosyaları bulmak, silinen dosyaları kurtarmak ve gizli verileri bulmak için bir dosya sistemini analiz etmek gerekir. Dosya sistemi analizi, dosya içeriği, veri parçaları ve dosyalarla ilişkili meta veriler olabilir.

Uygulama Analizi

- Bir dosyanın içeriğini anlamak için, uygulama katmanına atlamamız gerekir.
- Her dosyanın yapısı, dosyayı oluşturan uygulamaya veya OS'a dayanır.
- Örneğin, dosya sistemi perspektifinden, bir Windows kayıt dosyası bir HTML sayfasından farklı değildir, çünkü her ikisi de dosyadır. Fakat, çok farklı yapılara sahiptir ve her birini analiz etmek için farklı araçlar gerekmektedir.
- Uygulama analizi çok önemlidir ve burada hangi programların çalışmakta olduğunu belirlemek veya bir JPEG resminin ne olduğunu belirlemek için yapılandırma dosyalarını analiz etmek gerekebilir.
- Bu derste uygulama analizini kapsamamaktadır.

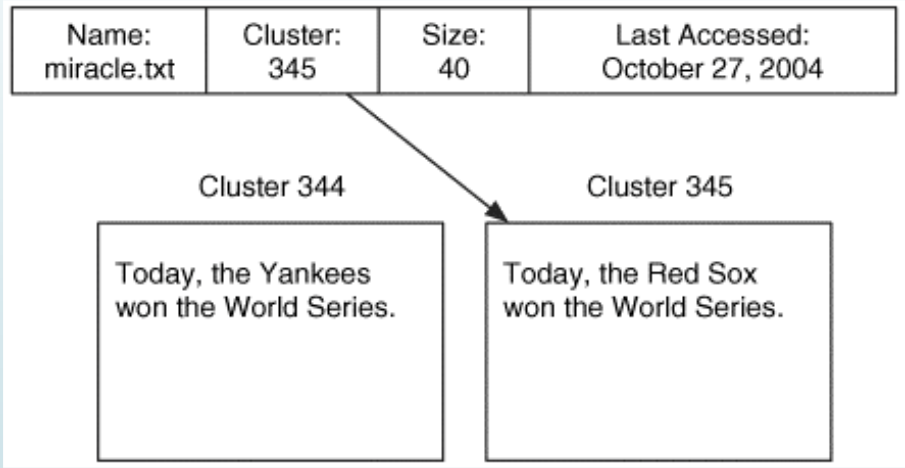
Analiz Süreci



Temel ve Gereksiz Veriler

- Daha önce tartışılan katmanlardaki tüm veriler bazı yapılara sahiptir ancak katmanın temel amacına hizmet etmesi için yapının tamamı gerekli değildir.
- Örneğin, dosya sistemi katmanının amacı boş bir birimi düzenlemektir, böylece verileri depolayıp daha sonra geri alabilmemiz mümkün olmaktadır.
- Dosya sistemi, bir dosya adını dosya içeriğiyle ilişkilendirmek için gereklidir. Bu nedenle, isim zorunludur ve dosya içeriğinin diskteki konumu çok önemlidir. Bunu Şekil 'de görüyoruz, burada miracle.txt adlı bir dosyaya sahibiz ve içeriği 345 numaralı adrese yerleştirilmiştir. Ad ya da adres yanlışsa ya da eksikse, dosya içeriği okunamamıştır. Örneğin, adres 344 olarak ayarlandıysa, dosyanın içeriği farklı olurdu.

Bu dosyayı bulmak ve okumak için ad, boyut ve içerik konumunun doğru olması gerekir, ancak son erişilen saatin doğru olması zorunlu değildir.



Temel ve Gereksiz Veriler

- Bu derste temel ve gereksiz veriler kavramı açıklanacaktır, çünkü temel verilere güvenebiliriz ancak gereksiz verilere güvenemeyebiliriz.
- Bir dosyadaki dosya içeriğinin doğru olduğuna güvenebiliriz, aksi takdirde sistemi kullanan kişi bu verileri okuyamaz. Son erişim zamanı doğru olabilir veya olmayabilir.
- OS, son erişimden sonra onu güncellememiş olabilir, kullanıcı zamanı değiştirmiş olabilir veya OS saati üç saat kapanmış olabilir ve yanlış saat saklanmış olabilir.
- İçerik adresinin numarasına güvendiğimizin bu adresteki gerçek içeriğe güvendiğimiz anlamına gelmediğini unutmayın.
- Örneğin, silinmiş bir dosyadaki adres değeri doğru olabilir, ancak veri birimi yeniden tahsis edilmiş olabilir ve bu adresteki içerik yeni bir dosya içindir.
- Gereksiz veriler çoğu zaman doğru olabilir, ancak bir olay çözümünde (yani, kurallar gereği) kullanıldığında bunları desteklemek için ek veri kaynakları bulmaya çalışılmalıdır.