

Türkiye'deki Hâkim ve Savcılar için siber suçların soruşturulması ve kovuşturulması esnasında elektronik delillerin ele alınması çalıştayı.

4. Oturum

iPROCEEDS-2

Funded
by the European Union
and the Council of Europe



EUROPEAN UNION

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

Oturumun Hedefi

Bu oturumun sonunda katılımcılar:

- Bir suç mahallinde delillerle karşılaşıldığında nelerin dikkate alınması gerektiğini analiz edebilecek
- Bir dijital suç mahalline girerken yapılması ve yapılmaması gerekenleri sıralayabilecek





Zorluk: Hız ve Kapsamlılık

➤ **Hızlı olmak istiyoruz çünkü:**

- ✓ Verileri kaybolmadan önce toplayabilmelisiniz
- ✓ Saldırganı daha fazla hasar vermeden açığa çıkarmalısınız

➤ **Daha kapsamlı olmak istiyoruz çünkü:**

- ✓ Tüm göstergeleri bulmalısınız
- ✓ Saldırganı açığa çıkarabilirsiniz

➤ Ama sakın unutmayın; ne kadar çok veri toplarsanız, onları analiz etmek de o kadar uzun sürer



Zorluk: Hız ve Kapsamlılık

- Etki: hıza odaklanma
- Etki: kapsamlılığa odaklanma
- İkisine de odaklanmalısınız ama nasıl?
- Çözüm: Otomasyon
- Amaç, inceleme görevlilerinin verimliliğini en üst düzeye çıkarmaktır
- Göstergeleri hızla bulun ve suçluları açığa çıkarın.



Elektronik Delil Kaynaklarının Hızlı Gelişimi

1. Elektronik deliller hemen hemen her tür soruşturmayla ilgili olabilir.
2. Elektronik cihazların türü ve sayısı her geçen gün artmaktadır



Doğru Usullerin, Süreçlerin ve Araçların Kullanımı

- Elektronik delillerin bir değeri olması için doğru şekilde ele alınması gerekir.
- Adli inceleme görevlileri tarafından kullanılan araçlar ve uygulanan usuller!
- Delillerin kabul edilebilirliğini doğru bir şekilde değerlendirmek üzere tanıklar ve tanıkların mahkeme önündeki beyanları
- Hâkimler, delil toplama, elde etme ve sunmada kullanılan teknikleri soracaktır.



Kabul Edilebilirliğe İlişkin Hususlar

Ulusal mevzuata uygun ve mahkemede kabul edilebilir dijital delillerin oluşturulması

- **Aslına Uygunluk**
- **Eksiksizlik**
- **Güvenilirlik**
- **İnanılrlık**
- **Orantıllılık**

Dijital suç mahallinde dikkat edilmesi gerekenler



Elektronik Delil Kaynakları



Camera



Lens



USB Veri Depolama Aygıtları

- Bařlanacak cihazlar için iletişim, bařlantı ve güç kaynağı protokollerini tanımlayan bir standarttır.



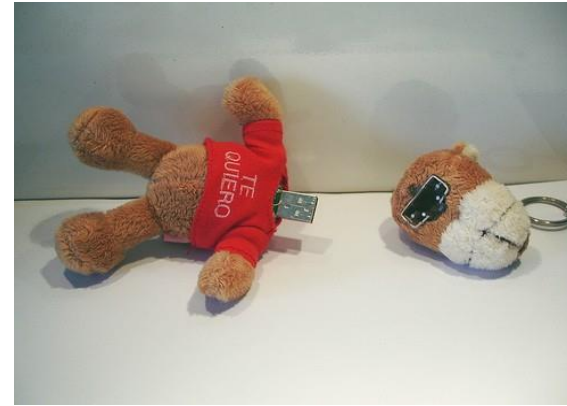
Bilgisayardaki USB Bařlantı Noktası



USB Depolama Aygıtları

USB Veri Depolama Aygıtları

- Suç mahallindeki hiçbir cihazı göz ardı etmeyin
- Cihazların görünüşü aldatıcı olabilir!!!!



USB Veri Depolama Aygıtları

- Cihazların görünüşü aldatıcı olabilir!!!!



USB Depolama Aygıtları





Potansiyel Deliller

- *Belgeler*
- *Fotoğraflar*
- *E-posta ve ekleri*
- *Veri tabanları*
- *Mali bilgiler*
- *İnternet tarama geçmişi*
- *Sohbet günlükleri*
- *Olay günlükleri*
- *GPS konumları*

**Soruşturma konusu
davaya yönelik
delil niteliği
taşıyabileceğinden,
herhangi bir kaynakta yer
alan hiçbir dijital delili göz
ardı etmeyin.**



Hazırlık

- Binaya giriş ve elektronik delillere el koyma için kanunlara uygun şekilde yetki alındığından emin olun (örneğin, ulusal hukuka uygun olarak arama emri veya başka izin alın).
- Ekip üyelerini (gerekirse dış uzmanlar dâhil) seçin ve onlara bireysel görevler atayın.
- Ekip üyelerini görevlerinin yerine getirilmesi konusunda bilgilendirin (ilgili temel eğitimi geçmiş olmaları gerekir);
- Gerekli el koyma araç ve gereçlerini temin edin.

Suç mahallinin güvenliĐinin saĐlanması

- Kişilerin emniyeti,
- Tüm delillerin bütünlüĐü,
- Elektronik deliller kolayca deĐiştirilebilir, silinebilir veya imha edilebilir.





Suç Mahallini Güvenli Kılmak için Yapılması Gerekenler

- Tüm kişileri delillerin toplanacağı alanın civarından uzaklaştırın;
- Kişisel ve taşınabilir cihazlar dâhil tüm elektronik cihazların güvenliğini temin edin;
- İzinsiz kişilerden gelen yardım veya teknik yardım tekliflerini reddedin;
- Zaten kapalıysa bilgisayarları veya elektronik cihazları kapalı bırakın;
- Uçucu verileri fiziksel ve elektronik olarak koruyun;



Suç Mahallini Güvenli Kılmak için Yapılması Gerekenler

- El koyulacak cihazdan başka delil gerekip gerekmediğine karar verin;
- Bozucu teknikleri elektronik delillerin kurtarılması tamamlandıktan **sonrasına** erteleyin;
- Görülmeyen izleri elektronik delillerin kurtarılması tamamlandıktan **sonra** toplayın;
- Ekipmana ve verilere zarar verebileceğinden suç mahallinden parmak izlerini toplamak için alüminyum tozu **kullanmayın**.



Suç Mahallinde Arama

- Suç mahallindeki elektronik olmayan ancak ilgili olabilecek delilleri arayın, örneğin:
 - ✓ Yazılı şifreler ve diğer elle yazılmış notlar,
 - ✓ Girintili yazının olduğu boş kağıt desteleri,
 - ✓ Donanım ve yazılım kılavuzları,
 - ✓ Takvimler veya günlükler,
 - ✓ Metin veya grafik bilgisayar çıktıları
 - ✓ Fotoğraflar veya
 - ✓ Daha sonra parola/şifre kırmak için yararlı olabilecek kişisel ilgi alanları hakkında bilgi.





Adli belgelendirme

- Tanım: Materyallere daha sonraki bir tarihte geri dönüp bulguların anlaşılması veya doğrulanması
- Özellikler: Açık, özlü ve ayrıntılı
- Amaç: Bunu okuyacak diğer kişilerin mantığınızı anlamasını sağlamak

Suç mahallinin belgelendirilmesi. Neler belgelenmeli?

- Her eylemin zamanını kaydedin;
- Delillerin listesi,
- Davayla ilgili tüm eylemlerin notları,
- İncelenen cihazlar (seri numaraları ve özel nitelikleri),
- Sonuçlar,
- Sonuçlarınızı destekleyen belgeler,
- Dava üzerinde çalışılan saatler,





Suç mahallinin belgelendirilmesi. Neler belgelenmeli?

- Müdahale sırasında monitörün durum detaylarını belgelendirin;
- Bilgisayarın ön tarafının yanı sıra ekranın ve diğer bileşenlerin fotoğrafını çekin;
- Ekranda görünenlerle ilgili yazılı notlar alın;
- Aktif programları videoya çekin veya ekran aktivitesinin daha kapsamlı belgelerini oluşturun;
- Toplanmayacak ilgili diğer elektronik bileşenleri belgeleyin.



El Koyma İle İlgili Genel Hususlar

- Suç mahallini sürekli olarak belgelendirin;
- Potansiyel bir şüphelinin doğrulanmamış tavsiyelerine uymayın;
- Bir bilgisayar ağıyla karşılaşılsa adli bilişim uzmanıyla iletişime geçin;
- Bazı cihazların kablosuz bağlantı üzerinden bağlanabileceğine dikkat edin;
- Herhangi bir ağ bağlantısı varsa el koyma esnasında bilgisayar sistemine erişilebileceğini ve sistemin manipüle edebileceğini unutmayın.

Bilgisayar donanımına el koyulmasıyla ilgili tavsiyeler

- Gösterge lambalarını kontrol edin;
- Ses gelip gelmediğini kontrol edin;
- Sıcaklığı kontrol edin;
- Özellikle taşınabilir bilgisayarlar için bekleme modunu dikkate alın.





Sorular

Monitörün gözlemlenmesi

1. Senaryo:

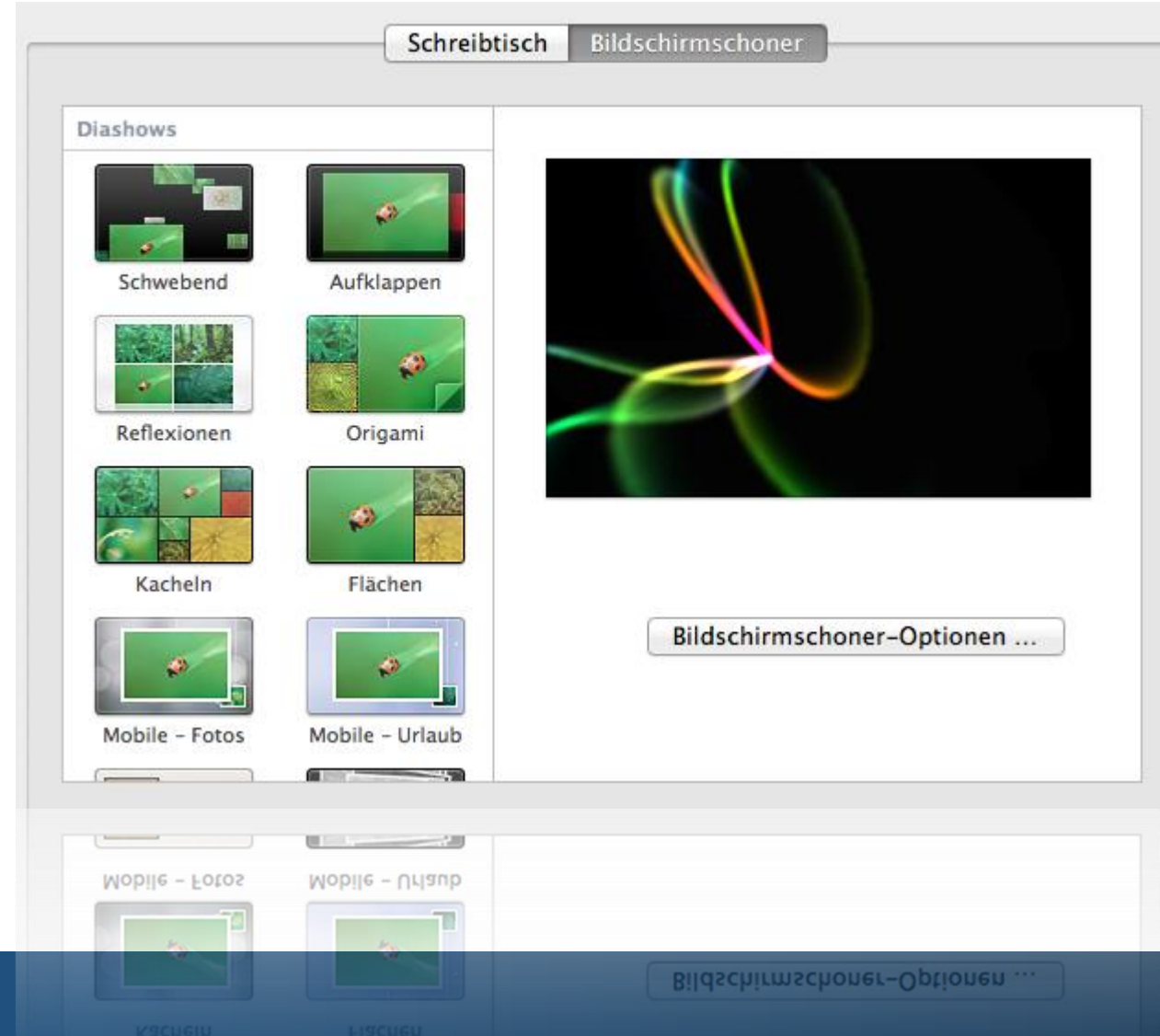
- Monitör açık ve iş ürünü ve/veya masaüstü görünüyor.
 - Müdahale sırasında monitörün durum detaylarını belgelendirin.



Monitörün gözlemlenmesi

2. Senaryo:

- Monitör açık ve ekran boş (uyku modu) veya ekran koruyucu (örn. bir resim) görünüyor.
 - Fareyi hafifçe hareket ettirin (düğmelere basmadan). Ekran değişip ve ürünü göstermeli veya bir şifre istemelidir.
 - Fare hareketi ekranda bir değişikliğe neden olmazsa başka herhangi bir tuşa basmayın veya fareye dokunmayın.
 - Müdahale sırasında monitörün durum detaylarını belgeleyin.



A Durumu – Bilgisayar Kapalı

- Sistemin kapalı olduğunu tespit ettiniz; **sakın açmayın!**
- Güç kablosunu hedef ekipmandan çıkarın (prizden **kapatmayın**) ve bunu yaptığınız zamanı kaydedin.
- Taşınabilir bir cihazı ele alıyorsanız pil takımını da çıkarın.



B Durumu – Bilgisayar Açık

- Sistemin açık olduğunu tespit ettiniz; **sakın kapatmayın!**
- Bir uzmanla iletişime geçmeyi deneyin.
 - Uzman varsa tavsiyelerine uyun.
 - Uzman yoksa bir sonraki talimatla devam edin.
- Klavyeye veya diğer giriş aygıtlarına **dokunmayın.**
- "Canlı veri senaryosu"na devam edin





Canlı veri incelemesi nedir?

- Canlı veri incelemesi (CVİ), çalışmakta olan (canlı) bir dijital sistemden verilerin mahkemede kullanılmak üzere adli olarak elde edilmesi ve/veya analizidir.
- Cihazlar kapatılmadan önce **uçucu verilerin** toplanmasının gerekli olduğu durumları ele alır.



Canlı veri incelemesi ne zaman yapılır?

Canlı veri incelemesi şu durumlarda kullanılır:

1. Bilgisayarın kapatılmasının delilleri erişilemez hale getirebileceği durumlar.
2. Disk şifrelemesi kullanılıyor ve kurtarma anahtarı yoksa.
3. Çevrim içi/uzaktan disk depolama kullanılıyor ve bilgisayar kapatıldığında erişim kaybedilecekse.



Canlı veri incelemesi ne zaman yapılır?

Canlı veri incelemesi şu durumlarda kullanılır:

4. Bilgisayarın kapatılması pratik değildir:

Örnek: Büyük kuruluşlardaki üretim sunucuları

- Amazon, eBay, Salesforce vb.
- Büyük parasal kayıplar



Canlı veri incelemesi ne zaman yapılır?

5. Kritik veriler muhtemelen yalnızca Rastgele Erişimli Bellekte bulunduğunda (uçucu olduğunda). Örneğin;

- Anlık mesajlaşma konuşmaları
- Kullanıcı tarafından yazılan şifreler
- Deşifre edilmiş dosyalar veya metin
- Pano içeriği



Canlı veri incelemesi ne zaman yapılır?

6. İstihbarat bilgilerine hızlı bir şekilde ihtiyaç duyulduğunda:
 - Hayatı tehlikede olan mağdurun yerinin tespit edilmesinin öncelikli amaç olduğu kaçırma vakaları (Olaya Müdahale)
 - Şüphelinin bilgisayarında bomba tehdidi için bir yer belirleme ihtiyacı



Canlı veri incelemesi ne zaman YAPILMAZ?

1. Kritik veriler veya bilgiler başka bir yolla elde edilebildiğinde.
2. Gerekli veri veya bilgiler zaten elde edildiğinde.



Canlı veri incelemesinin etkisi

Ne Yapacağız?

- Eylemlerimiz sonucunda değişecek her şeyi önceden bilemeyiz... Bu durumda ne yapacağız?
 - ✓ Uçuculuk sırasına uyarız
 - ✓ Öncelikle en az müdahaleci eylemleri gerçekleştiririz
 - ✓ Öncelikle en değerli delilleri toplarız
 - ✓ Her şeyi belgeleriz



Canlı Veri İncelesinde Dikkat Edilmesi Gereken Hususlar

- Hedef bilgisayarda bu programların/araçların olup olmadığını kontrol edin:
 - ✓ Bulut Şifreleme; örn: Cloudflogger
 - ✓ Steganografi, örn: StegHide
 - ✓ Bulut Depolama, örn: Google Drive
 - ✓ Şifreleme, örn: Truecrypt
 - ✓ Sohbet, ör: ICQ
 - ✓ Denkler arası (P2P) paylaşım, örn: uTorrent
 - ✓ Kripto para cüzdanları, örn: Bitcoin Core QT
 - ✓ Şifre kasaları, örn: 1Password
 - ✓ Delil karartma, örn: CCleaner
 - ✓ Anonimlik, örn: Tor Tarayıcısı
 - ✓ Uzaktan erişim istemcileri, örn: TeamViewer

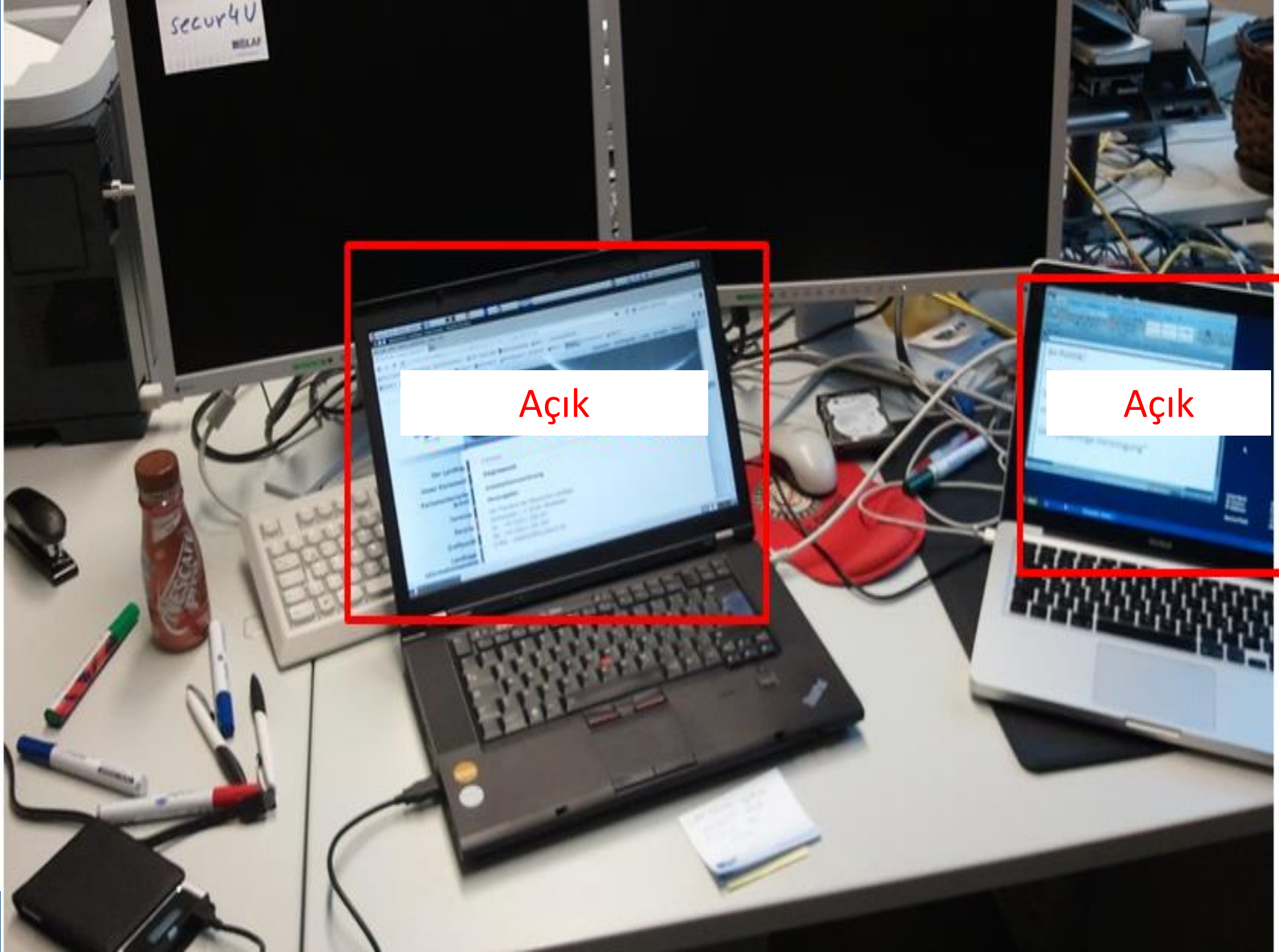
Ekrandaki göstergeler

- Dijital delillerin imha edildiğini gösteren işaretler için ekranı kontrol edin. Örneğin "sil", "biçimlendir", "kaldır", "kopyala", "taşı", "kes" veya "süpür"
- Hangi pencerelerin açıldığını belgeleyin.
- Kullanılan şifrelemeye yönelik göstergeleri bulmaya çalışın (sonraki slaytlara bakın).
- Kullanılan bulut hizmetlerine ilişkin göstergeleri bulmaya çalışın (sonraki slaytlara bakın).
- Anlık mesajlaşma pencereleri veya sohbet odaları gibi diğer bilgisayarlar veya kullanıcılar ile aktif veya devam eden iletişime dair göstergeleri bulmaya çalışın.
- Kameraların veya web kameralarının (webcam) aktif olduğuna dair göstergeleri bulmaya çalışın.



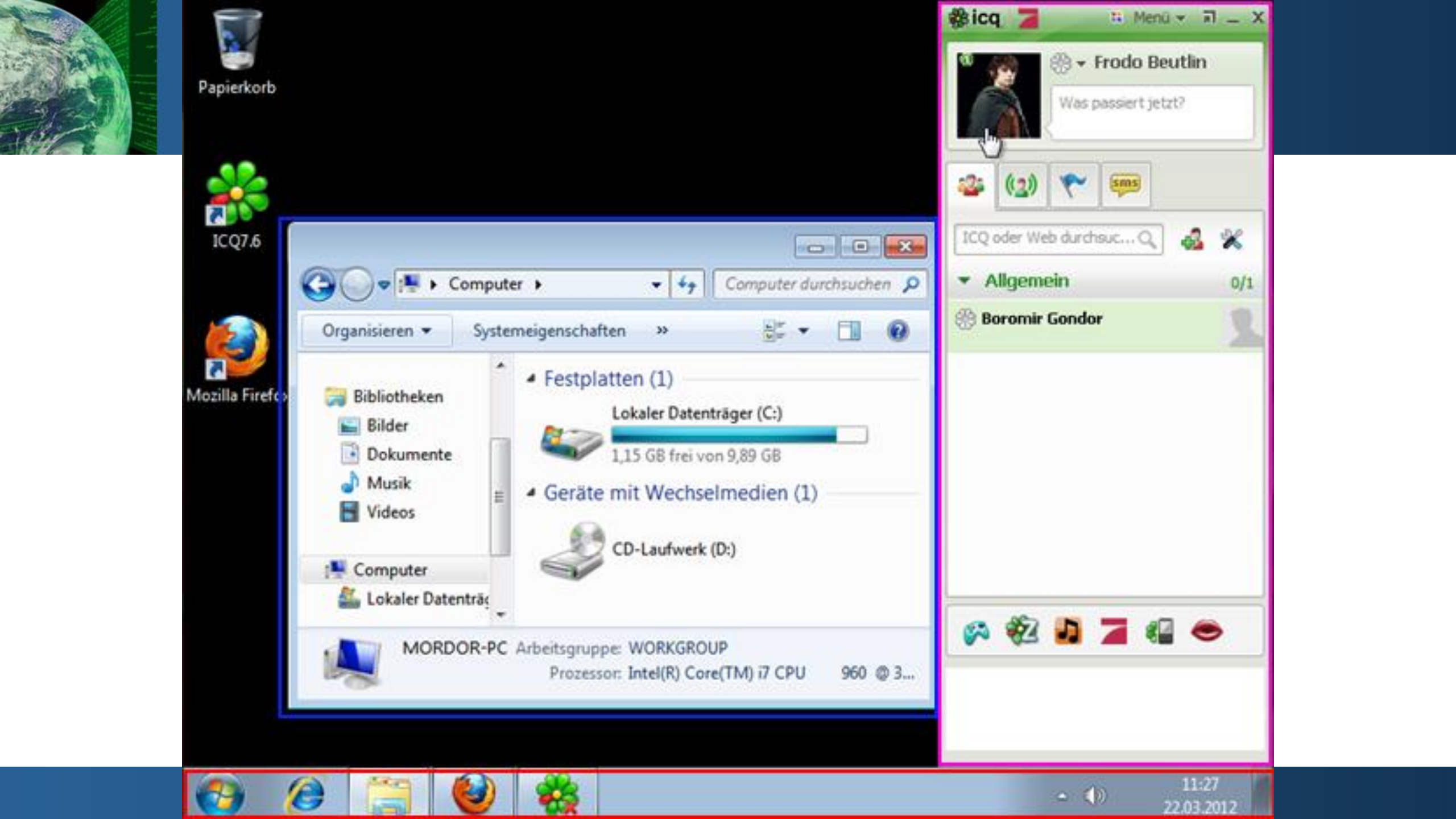


**Birkaç örneğe
göz atalım**



Açık

Açık



Papierkorb



ICQ7.6



Mozilla Firefox

Computer

Computer durchsuchen

Organisieren Systemeigenschaften

Bibliotheken

- Bilder
- Dokumente
- Musik
- Videos

Computer

Lokaler Datenträger

Festplatten (1)

Lokaler Datenträger (C:)

1,15 GB frei von 9,89 GB

Geräte mit Wechselmedien (1)

CD-Laufwerk (D:)

MORDOR-PC Arbeitsgruppe: WORKGROUP

Prozessor: Intel(R) Core(TM) i7 CPU 960 @ 3...

icq Menü

Frodo Beutlin

Was passiert jetzt?

ICQ oder Web durchsuc...

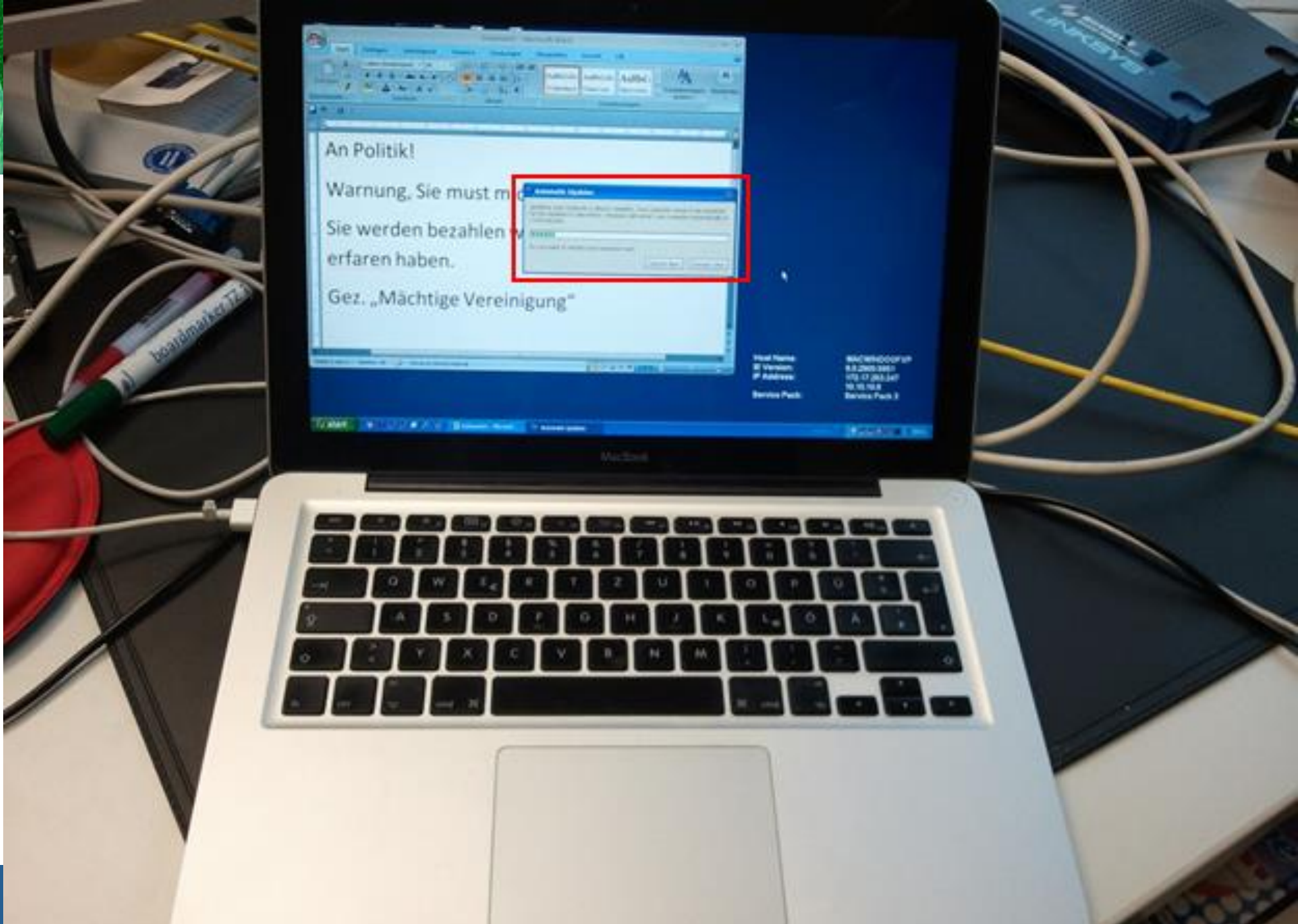
Allgemein 0/1

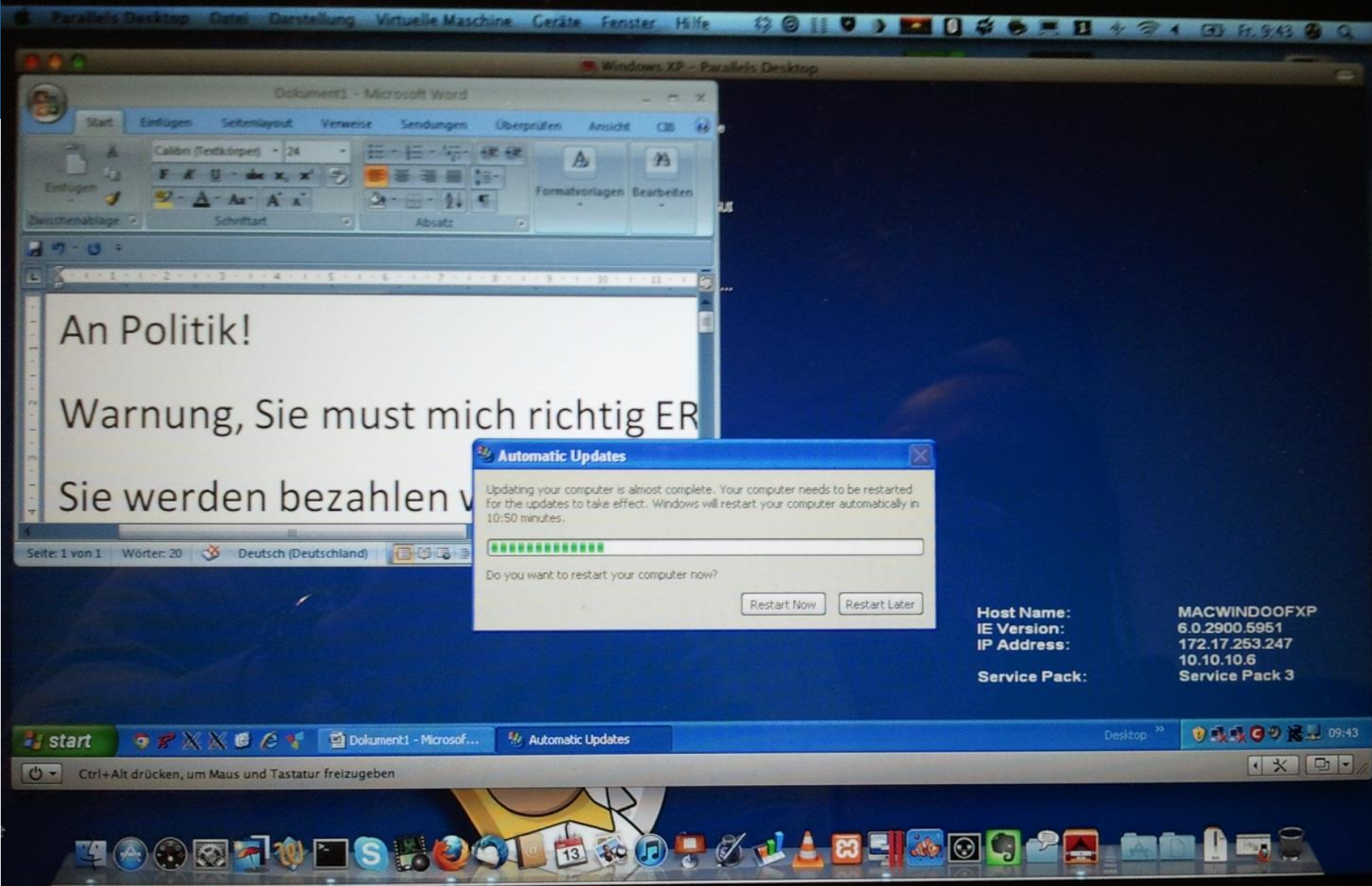
Boromir Gondor

Game Z Music ICQ7.6



11:27
22.03.2012





MacBook

Etiketleme

- Tüm cihazları ve kablo bağlantılarını etiketleyin
- Depolama aygıtlarının yüzeyine yapışkan etiketler yapıştırmayın. Depolama aygıtlarının ambalajlanması ve etiketlenmesi için kutular, torbalar ve zarflar kullanın.



Ambalajlama ve Taşıma

- Elektronik deliller sıcaklığa, neme, fiziksel şoka, statik elektriğe, manyetik kaynaklara ve hatta bazı eylemlere (örn. açma/kapama) karşı hassas olabilir.
- Elektronik deliller dikkatle ele alınmalı ve cihazlara el koyulurken uygun torbalar ve kutular kullanılmalıdır.



Taşıma

- Elektronik delilleri manyetik kaynaklardan uzak tutun (örn. radyo vericileri, hoparlör mıknatısları, ısıtmalı koltuklar).
- Ekipmanın şok ve çarpmalardan (yani mekanik hasardan), ısıdan ve nemden korunduğundan emin olun.



Depolama tesisleri

Yeterince güvenli ve aşağıdakilere sahip bir depolama alanını kullanın:

- Uygun erişim denetimi,
- Yangından koruma (örn. alarm, yangın söndürücüler, depolama alanında veya yakınında sigara içme yasağı),
- Sıcaklık ve nem,
- Manyetik kaynaklardan (örn. yönlü radyo cihazlarından uzakta) koruma.







Sorularınız var mı?

