



## 2011 Yılı Adli Bilişim Eğitim Programları

### 1) Eğitim Adı: **Adli Bilişim Analizine Giriş**

**Açıklama:** Teorik ve pratik temelli bu eğitimle Adli Bilişim için kavramların ve delil toplama-saklama metodların öğrenilmesi ve analizde kullanılan yazılım ve donanım tanıtılması. Bilişim suçlarıyla ilgili yasal içeriğin öğrenilmesi. Bilgi teknolojileriyle ilgili, sabit disk-CD-DVD-Ram ve taşınabilir bellek-cep telefonu-digital kamera ortamlarında delil aramak için temel gereklilikler.

**Kazandırılacak beceri:** Ticari uygulamalar, Winhex (Alman), Encase-FTK (ABD), Helix (ABD) ve açık kaynaklı FCCU (Belçika Polisi), Deft-Caine (İtalyan Polisi), Spada (Avustralya Polisi), TSK Sleutkit-Pyflag (ABD), en iyi adli bilişim yazılımlarının üstünlük ve zayıflıklarının tanıtılması. Çeşitli ara birimlerle e01, AD, aff, dd, whx adli imaj alma.

**Eğitim süresi:** 4 gün, **Eğitim ücreti:** 1.885 ABD \$ + KDV

### 2) Eğitim Adı: **Dijital Delillerin, Elektronik Keşif ile Olay Örgüsünün Çıkarılması**

**Açıklama:** Daha önceki adli imajları alınan ortamlarda, özet (MD5, SHA1 hash) kontrolü ve Winhex, Encase, FTK, FCCU, Caine, Deft, Spada, Pyflag, TSK Autopsy-Sleutkit adli bilişim yazılımlarıyla, uygulamalı olarak delillerin adli imajlarda elektronik keşfi ve olay örgüsünün çıkarılması. Silinen ve yeniden biçimlendirilen sabit disk-CD-DVD-RAM ve taşınabilir bellek-cep telefonu-digital kamera ortamlarından ve alınan adli imajlarından veri kurtarılması.

**Kazandırılacak beceri:** Ticari uygulamalar, Winhex (Alman), Encase-FTK (ABD), Helix (ABD) ve açık kaynaklı FCCU (Belçika Polisi), Deft-Caine (İtalyan Polisi), Spada (Avustralya Polisi), TSK Sleutkit-Pyflag (ABD), adli bilişim yazılımlarıyla e01, AD, aff, dd, whx adli imajların incelenmesi. Adli bilişimin incelemesi raporunun yazılması.

**Eğitim süresi:** 4 gün, **Eğitim ücreti:** 2.100 ABD \$ + KDV

### 3) Eğitim Adı: **Ağ Temelli Adli Bilişim ve Log Analizi**

**Açıklama:** Açıklama: Adli imajı alınan diskler üzerinde güvenlik duvarı, uygulama ve sistem kayıtlarıyla ilgili FW-IDS-IPS- loglar da araştırma yapılması, internet çerezleri (MSN-Gmail-Hotmail-Yahoo-Facebook-Twitter)- ziyaretçi kayıtlarının araştırılması. 5651 sayılı yasa ile ilgili bilgilendirme.

**Kazandırılacak beceri:** Ağ trafiğinde taşınan veriye paket analizi yapılması. 5651 yasal gerekliliğin anlaşılması.

**Eğitim süresi:** 3 gün, **Eğitim ücreti:** 1.425 ABD \$ + KDV



**GÖKTÜRK Bilgi Teknolojileri ve Bilişim Analizi Denetim Yatırım Danışmanlığı Ltd .**

**Adres:** İnönü mah. Çayır sk.No: 83 D: 6 Harbiye- Şişli / İstanbul **Tel:** 0 212 291 83 46 **VoIP/Skype:** turkishforensic  
**Beyoğlu Vergi Dairesi:** 406 0303 872 **İTO Sicil:** 665985 **Ziraat Bankası TL Hesabı IBAN:** TR47 0001 0006 8756 4882 1350 01  
**e-posta:** [info@turkishforensic.com](mailto:info@turkishforensic.com) **http:** [www.turkishforensic.com](http://www.turkishforensic.com)



#### 4) Eđitim Adı: **Sanayi Casusluđunu Tespit**

**Açıklama:** İmajı alınan diskler üzerinde gizli yazılımlar ve bilgisayarlardan kurum verileri çalma tekniklerinin anlatılması ve uygulamalı tespiti.

**Kazandırılacak beceri:** Botnet, truva atı, steganografiye karşı koymak için anti sanayi casusluđu uygulamalarının kullanımı ve adli biliřime karşı kullanılan teknikler ve güvenli veri silme (Wipe) deneyimi.

**Eđitim süresi:** 3 gün, **Eđitim ücreti:** 1.425 ABD \$ + KDV

#### 5) Eđitim Adı: **Steganografi**

**Açıklama:** Sanayi casusluđu için kullanılan dışarıya veri sızdırma yazılımları ve tekniđi hakkında bilgi verilmesi, kullanılan yazılımların ve tespit yöntemlerinin uygulamalı tanıtılması.

**Kazandırılacak beceri:** Jpeg, VoIP, mp3 ve çeřitli ofis dosyaları içine gizlenmiř sanayi casusluđu verilerinin tespiti.

**Eđitim süresi:** 3 gün, **Eđitim ücreti:** 1.425 ABD \$ + KDV

#### 6) Eđitim Adı: **řifre Çözme ve Kırma Teknikleri**

**Açıklama:** Veri ve bilgi güvenliđi için çeřitli algoritmaların tanıtılması, çözülmesi, kırılması. Bellekten RSA,AES anahtarlarının bulunması.

**Kazandırılacak beceri:** John Ripper, Opcrack, Backtrack, DNA, Brotforce, RSA, AES, MD5, SHA1, PGP, Truecrypt kullanımı ve tersine mühendislik uygulamaları.

**Eđitim süresi:** 5 gün, **Eđitim ücreti:** 2.375 ABD \$ + KDV



**GÖKTÜRK Bilgi Teknolojileri ve Biliřim Analizi Denetim Yatırım Danıřmanlıđı Ltd .**

**Adres:** İnönü mah. Çayır sk.No: 83 D: 6 Harbiye- řiřli / İstanbul **Tel:** 0 212 291 83 46 **VoIP/Skype:** turkishforensic  
**Beyođlu Vergi Dairesi:** 406 0303 872 **İTO Sicil:** 665985 **Ziraat Bankası TL Hesabı IBAN:** TR47 0001 0006 8756 4882 1350 01

**e-posta:** [info@turkishforensic.com](mailto:info@turkishforensic.com) **http:** [www.turkishforensic.com](http://www.turkishforensic.com)



## 7) Eğitim Adı: **EnCase Computer Forensics I**

**Açıklama:** Guidance şirketinin dünyaca ünlü adli bilişim uygulaması Encase için, resmi ders rehberine (Study Guide) uygun olarak hazırlanan 1.aşama eğitimi. Türkçe ders içeriği ve anlatım. Özel İngilizce kavramların açıklanması, resmi Encase belgeli soruşturmacı (Certified Examiner) sınavına hazırlık için, resmi hazırlık kitabından (the Official EnCe Study Guide) örnek soruların çözülmesi.

**Kazandırılacak beceri:** Bilgisayar Nasıl Çalışır, NTFS-FAT Dosya Sistemi, EnCase Forensic Metodolojisi, EnCase Forensic Konsepti, Adli Disk İmajı Alma, Ön İnceleme, anahtar sözcük-Keyword Oluşturma, Arama, Temel Bookmark Yapısı, Dosya Türleri ve imza-başlık Analizi, özet-Hash Analizi, adli imajların Restore Edilmesi, EnCase olay Arşivleme, Restore Forensic İmajların Doğrulanması, Timeline Yapısı, Silinen delil Tespiti ve Kurtarılması (Veri Kurtarma)

**Eğitim süresi:** 4 gün , **Eğitim ücreti:** 1.885 \$ (ABD)+ KDV

## 8) Eğitim Adı: **EnCase Computer Forensics II**

**Açıklama:** Guidance şirketinin dünyaca ünlü adli bilişim uygulaması Encase için, resmi ders rehberine (Study Guide) uygun olarak hazırlanan 2.aşama eğitimi. Türkçe ders içeriği ve anlatım. Özel İngilizce kavramların açıklanması, resmi Encase belgeli soruşturmacı (Certified Examiner) sınavına hazırlık için, resmi hazırlık kitabından (the Official EnCe Study Guide) örnek soruların çözülmesi.

### **Kazandırılacak beceri:**

EnCase de Olay Oluşturma ve İmaj ekleme, Veri Kurtarma Temel Prensipleri, Master Boot Record ve bölüm kayıtları, Encase Sanal Dosya Sistemi (VFC) Modülü, EnCase Fiziksel Disk Benzetimi (PDE) Modülü, NTFS Dosya Sistemi, Compound Dosyalar, Windows Registry, Grep komutu ve Arama Yapma, Filtre Oluşturma, Windows Sistemlerde İnceleme, Link Dosyaları, e-posta ve İnternet Geçmişi, Flash Card ve Benzeri Donanımların İncelenmesi, Metadata Analizi, Adli Bilişim Analizi Raporunun Hazırlanması.

**Eğitim süresi:** 4 gün, **Eğitim ücreti:** 1.885 \$ (ABD)+ KDV



**GÖKTÜRK Bilgi Teknolojileri ve Bilişim Analizi Denetim Yatırım Danışmanlığı Ltd .**

Adres: İnönü mah. Çayır sk.No: 83 D: 6 Harbiye- Şişli / İstanbul Tel: 0 212 291 83 46 VoIP/Skype: turkishforensic  
Beyoğlu Vergi Dairesi: 406 0303 872 İTO Sicil: 665985 Ziraat Bankası TL Hesabı IBAN: TR47 0001 0006 8756 4882 1350 01

e-posta: [info@turkishforensic.com](mailto:info@turkishforensic.com) http: [www.turkishforensic.com](http://www.turkishforensic.com)



## Hakkımızda

řirketimiz, lkemizde birok nemli maddi ve manevi talepli dava iin adli biliřim incelemesi yaptı. Havacılık sektrnde İnter Havayolları iin yaptığımız incelemede 1 milyon ABD doları tutarında řirket iin ynetici yolsuzluđunun ortaya ıkarılması, e-ticaret sektrnde, Altivi.com řirketinin aık artırma satıř sistemine hile karıřtranların tespit edilmesi, zel sektrde tek seferde incelen en byk adli biliřim incelemesi, halen devam eden zel sektr ve kamu davalarındaki (200 bin e-posta, 100 bilgisayar ve sunucu logları vb) nemli mřterilerimiz iin adli biliřim alıřması yapmaktayız.

Gemiř dnemde, Gamze zelik-Gkhan Demirkol davası da bizim incelediğimiz ve davanın seyrini deđiřtiren adli biliřim alıřmasıdır.

Amerika Birleřik Devletlerinde, Las Vegas'ta dzenlenen bilgi gvenliđi konferansları, Blackhat ve Defcon, Baltimore'da yapılan dnyanın en nemli Adli Biliřim konferansı DFRWS, dnyanın en byk biliřim fuarı Cebit Hannover'a katılan tek Trk řirketiyiz.

Amerikan Savunma Bakanlıđı'na bilgi teknolojileri konusunda iř yapan Booz Alen grubunun Wetstone řirketinden, ieriden saldırı teknikleri konusunda, 2008 yılında Las Vegas'ta 4 gnlk uygulamalı Hacking BootComp for Investigators eđitimi sonucunda, Certified Hacking Investigator belgesi ve Inside Hacking & Malware eđitimlerini tamamladık. 19 yıllık bilgi teknolojileri tecrbesiyle, son 7 yıldır sadece bilgi gvenliđi ve adli biliřimle ilgili alıřmalar yapan ve sektrn ilklerinden olup, bilimsel konferanslar iin makale ve bildirimlerle de sektrn geliřimine katkı da bulunuyoruz.

Daha fazla bilgi iin, Tbitak-UEKAE-Bilgem, **Ulusal Bilgi Gvenliđi Kapısı** <http://www.bilgiguvenligi.gov.tr/siber-savunma/index.php> ve **Linkedin**, Cenk Ceylan profil bilgilerine <http://www.linkedin.com/pub/cenk-ceylan/19/698/2b4> ulařılabilir.

*İhtiyacınız olan adli biliřim eđitimi iin, uluslararası lekteki bilgi birikimi ve mřteri deneyimlerinden kaynaklı gerek olay incelemeleriyle, uygulamalı stratejik bilgiler vereceđimizi hatırlatırız.*



**GKTRK Bilgi Teknolojileri ve Biliřim Analizi Denetim Yatırım Danıřmanlıđı Ltd .**

Adres: İnn mah. ayır sk.No: 83 D: 6 Harbiye- řiřli / İstanbul Tel: 0 212 291 83 46 VoIP/Skype: turkishforensic  
Beyođlu Vergi Dairesi: 406 0303 872 İTO Sicil: 665985 Ziraat Bankası TL Hesabı IBAN: TR47 0001 0006 8756 4882 1350 01

e-posta: [info@turkishforensic.com](mailto:info@turkishforensic.com) http: [www.turkishforensic.com](http://www.turkishforensic.com)



### ŞARTLAR

1. Katılımcıların bilgisayar sistemleri için donanım tanıtabilme ve yazılımları yönetebilme seviyesinde Windows ve Linux bilgilerinin olması gerekir. Sistem yöneticisi olması tercih edilir.
2. Virtual Box, VWware vb. Sanallaştırma yazılımlarını kullanabilmeleri beklenir. Talep halinde, EGM-Jandarma-TSK için kendi adli bilişim laboratuvarlarında canlı sistemlerde eğitim verilebilir.
3. TCP / IP protokolü, sabit disk yapısı ve işletim sistemi dosya sistemi hakkında bilgi sahibi olması. (Fat16,32, NTFS, ext3-ext4, swap vb.)
4. USB-CD-DVD'den önyükleme yapabilen ve USB, PCMCIA, PCIx gibi ara birimleri olan dizüstü / masaüstü bilgisayarlara sahip olmak.
5. Eğitim ortamı kurum tarafından sağlanacaksa, sunum cihazı, yazı tahtası, masa ve internet erişimi, kesintisiz güç kaynağı bulunmalı.
6. Katılımcıların öğle yemeği şirketimiz tarafından karşılanacaktır. Müşterinin yerinde eğitim isteniyorsa, şehirlerarası ulaşım, konaklama ve yemek ihtiyacı kurum tarafından karşılanır.
7. Eğitimler sabah 09:00 da başlayıp, 17:00 de biter. Cumartesi ve Pazar günleri mesaiye dahildir.
8. Eğitim için verilecek olan ders içeriği çeşitli yazılımlar, sunum dosyaları ve bilimsel makaleler CD-DVD ortamındadır. İçerik, katılımcılar dışında paylaşılamaz, çoğaltılamaz. Eğitim dili ve içerik TÜRKÇE'dir. Encase yazılımı için 6.sürüm, dikkate alınır.
9. Eğitim için iş anlaşması imzalanırken, ücret %40 peşin alınır. Kalan %60 eğitim sonunda, 1 hafta içinde alınır. Kamu kurumlarından ödeme beyanı, yönetim onaylı olarak kurumsal e-posta ve üst yönetim imzalı olarak alınır.
10. 3 kişiyi geçen katılımlarda, eğitim yeri müşteri tarafından karşılanmak kaydıyla, 5 kişi dahil %10, 6-10 kişi arasında % 20 indirim uygulanır.
11. Karşılıklı gizlilik sözleşmesi ile öğrenilen sırlar güvenceye alınır.

**Bilginize,  
Saygılarımla,**

**Cenk CEYLAN  
Bağımsız Bilgi Güvenliği Danışmanı, Adli Bilişim Analizi Uzmanı**



**GÖKTÜRK Bilgi Teknolojileri ve Bilişim Analizi Denetim Yatırım Danışmanlığı Ltd .**  
Adres: İnönü mah. Çayır sk.No: 83 D: 6 Harbiye- Şişli / İstanbul Tel: 0 212 291 83 46 VoIP/Skype: turkishforensic  
Beyoğlu Vergi Dairesi: 406 0303 872 İTO Sicil: 665985 Ziraat Bankası TL Hesabı IBAN: TR47 0001 0006 8756 4882 1350 01  
e-posta: [info@turkishforensic.com](mailto:info@turkishforensic.com) http: [www.turkishforensic.com](http://www.turkishforensic.com)