

Siber Güvenlik Uzmanı
Burak BOZKURLAR*

Av. İdris Tefvık GÜLEÇ**

DİJİTAL DELİL

ve

CEZA SAVUNMASI

TEORİDEN UYGULAMAYA

TEKNİK, HUKUKİ VE STRATEJİK REHBER



* İstanbul Üniversitesi Açık ve Uzaktan Eğitim Fakültesi (AUZEF) Acil Yardım ve Afet Yönetimi (AYAY) Lisans Tamamlama Programı / Ders Veren Uzman

** Av. İdris Tefvık Güleç – İstanbul Barosu

İÇİNDEKİLER

ÖNSÖZ	iii
-------------	-----

İÇİNDEKİLER.....	v
------------------	---

BÖLÜM 1

AVUKAT İÇİN DİJİTAL DELİLİ OKUMA

1.1. Dijital Delil Karşısında Hukukçunun Değişen Rolü	1
1.2. Dijital Veri, Teknik Bulgu ve Hukuki Delil Ayırımı.....	2
1.3. “Cihazda Bulundu” Ne Anlama Gelir?	3
1.4. Dijital Delilde Kaynak Sorunu	4
1.5. Dijital Delilin Bütünlüğü	4
1.6. Muhafaza Zinciri: Delilin Yolculuğunu Okumak.....	5
1.7. Bilirkişi Raporu Mutlak Gerçek Değildir	6
1.8. Yazılım Çıktısı ile Bilirkişi Kanaati Arasındaki Fark	6
1.9. Zaman Bilgisinin Sorgulanması	7
1.10. Tek Dijital İzden Fail Sonucuna Ulaşma Problemi	8
1.11. Alternatif Hipotezleri Sorgulamak	8
1.12. Dijital Delile İtirazın Amacı.....	9
BÖLÜM SONU – MÜDAFİ İÇİN 10 TEMEL SORU	10

BÖLÜM 2

DİJİTAL DELİLİN GÜVENİLİRLİĞİNİ SORGULAMAK

Hash, Adli İmaj, Write Blocker ve Muhafaza Zinciri

2.1. Dijital Delilde Güvenilirlik Problemi	11
2.2. Orijinal Materyal ve Adli Kopya.....	11
2.3. Adli İmaj Nedir?.....	12
2.4. Write Blocker Nedir?	13
2.5. Hash Değeri Nedir?	14
2.6. Hash Varsa Sorun Yok mudur?	15
2.7. Hash Bulunmaması Delili Otomatik Olarak Geçersiz Kılar mı?.....	15
2.8. MD5, SHA-1 ve SHA-256 Meselesi	16

2.9. Hash Uyuşmazlığı Ne Anlama Gelir?	17
2.10. Muhafaza Zinciri	17
2.11. Muhafaza Zincirindeki Her Eksiklik Delili Geçersiz Kılar mı?	18
2.12. Canlı Sistemlerde Write Blocker Problemi	18
2.13. Mobil Cihazlarda Adli Kopya Problemi.....	19
2.14. Kullanılan Adli Bilişim Aracının Güvenilirliği.....	20
2.15. Bilirkişi Raporunda Aranması Gereken Teknik Bilgiler	21
2.16. UYGULAMALI ÖRNEK: EKSİK BİLİRKİŞİ RAPORUNU OKUMAK.....	22
2.17. MÜDAFİ İÇİN DİJİTAL BÜTÜNLÜK KONTROL LİSTESİ.....	23
2.18. İTİRAZ DİLİ NASIL OLMALIDIR?	24
2.19. BÖLÜM SONU	24

BÖLÜM 3

IP ADRESİ, CGNAT VE LOG KAYITLARINA İTİRAZ

3.1. IP Adresinin Ceza Muhakemesindeki Yeri	27
3.2. IP Adresi Neyi Gösterir?	27
3.3. IP Adresi = Fail Değildir	28
3.4. Statik ve Dinamik IP Adresi.....	29
3.5. Zaman Bilgisi Neden Kritik?.....	29
3.6. Saat Hangi Saat?.....	30
3.7. NAT Nedir?	31
3.8. CGNAT Nedir?	31
3.9. Port Bilgisi Neden Bu Kadar Önemlidir?	32
3.10. Hedef IP ve Kaynak IP Ayrımı.....	33
3.11. Log Kaydı Nedir?	33
3.12. Log Kaydı Bir İşlemin Başarılı Olduğunu Her Zaman Gösterir mi? ..	34
3.13. Abonelik ile Kullanıcı Arasındaki Fark.....	35
3.14. Ortak Wi-Fi Ağları	35
3.15. VPN Kullanımı	36
3.16. Proxy ve Tor	37
3.17. Zararlı Yazılım ve Ele Geçirilmiş Sistem İhtimali	37
3.18. Logların Bütünlüğü	38

3.19. IP → FAIL ZİNCİRİNİ PARÇALAMAK	38
3.20. UYGULAMALI VAKA I — SOSYAL MEDYA HAKARETİ.....	39
3.21. UYGULAMALI VAKA II — CGNAT KAYDI	40
3.22. UYGULAMALI VAKA III — BİLİRKİŞİ RAPORU	41
3.23. İTİRAZ DİLİ NASIL OLMALI?	41
3.24. BİLİRKİŞİYE SORULABİLECEK SORULAR	42
3.25. AYM KARARLARINDAN ÇIKAN ÖNEMLİ DERS.....	43
3.26. MÜDAFİ İÇİN IP-CGNAT KONTROL KARTI.....	43
3.27. BÖLÜM SONU	44

BÖLÜM 4

HTS, BAZ İSTASYONU VE KONUM VERİLERİNE İTİRAZ

4.1. HTS Kayıtlarının Ceza Muhakemesindeki Önemi	45
4.2. HTS Kaydı ile Görüşme İçeriği Aynı Şey Değildir.....	45
4.3. Telefon Hattı ile Kişi Arasındaki Ayrım	46
4.4. IMEI Nedir ve Neyi Gösterir?	47
4.5. Baz İstasyonu Kaydı Neyi Gösterir?	48
4.6. Baz İstasyonu = GPS Değildir.....	48
4.7. Baz İstasyonunun Kapsama Alanı Sabit Bir Daire Değildir	49
4.8. En Yakın Baz İstasyonu Yanılgısı	50
4.9. Baz İstasyonu Verisinden Kesin Adres Çıkarılabilir mi?	50
4.10. HTS Kaydındaki Baz Bilgisi Hangi Ana Aittir?	51
4.11. Telefonun Konumu ile Kişinin Konumu	51
4.12. Aynı Baz İstasyonundan Sinyal Almak Ne Anlama Gelir?.....	52
4.13. Ardışık Baz Değişimleri ve Hareket Analizi	53
4.14. HTS Analizinde Zaman Sorunu	53
4.15. HTS Verilerinde Korelasyon	54
4.16. HTS Verilerinin Hukuka Uygun Elde Edilmesi	55
4.17. HTS Raporunun Denetlenebilirliği.....	55
4.18. Kişiselleştirilmiş HTS Analizi.....	56
4.19. UYGULAMALI VAKA I — “SANIK OLAY YERİNDEYDİ”	56
4.20. UYGULAMALI VAKA II — İKİ TELEFON AYNI BAZDA	57

4.21. UYGULAMALI VAKA III — HTS VE KAMERA ÇELİŞKİSİ.....	58
4.22. UYGULAMALI VAKA IV — ARDIŞIK ARAMA	58
4.23. HTS RAPORUNA İTİRAZDA ZAYIF VE GÜÇLÜ DİL	59
4.24. BİLİRKİŞİYE YÖNELTİLEBİLECEK SORULAR	60
4.25. MÜDAFİ İÇİN HTS–BAZ KONTROL KARTI	61
4.26. YÜKSEK YARGI UYGULAMASINDAN ÇIKAN DERS	61
4.27. BÖLÜM SONU	62

BÖLÜM 5

TELEFON VE BİLGİSAYAR İNCELEME RAPORLARINA İTİRAZ

5.1. Dijital Cihaz İncelemesinin Ceza Muhakemesindeki Önemi	63
5.2. İlk Soru: Hangi Cihaz İncelendi?	63
5.3. Cihaz Kimin?	64
5.4. Cihazın Ele Geçirildiği Durum	65
5.5. Telefon “İncelendi” Demek Yeterli Değildir	66
5.6. Mantıksal Edinim	67
5.7. Dosya Sistemi ve Fiziksel Edinim	67
5.8. Acquisition Yöntemi Neden Savunmayı Etkiler?	68
5.9. Silinmiş Veri Nedir?	68
5.10. Silinmiş Veri = Sanık Sildi mi?	69
5.11. Cache Nedir ve Neden Önemlidir?	70
5.12. Thumbnail Nedir?	70
5.13. WhatsApp ve Benzeri Uygulamalarda Otomatik Medya	71
5.14. “Dosya Cihazda Bulundu” İfadesini Parçalamak	71
5.15. Kullanıcı Tarafından Oluşturulan Veri ile Sistem Tarafından Oluşturulan Veri	72
5.16. Metadata'nın Sınırları	73
5.17. EXIF Verileri	73
5.18. Recent Files ve Kullanıcı Etkileşimi	74
5.19. Tarayıcı Geçmişi	74
5.20. Malware İhtimali	75
5.21. Uzaktan Erişim Programları	76

5.22. Bulut Senkronizasyonu.....	77
5.23. Kullanılan Adli Bilişim Yazılımı	77
5.24. NIST'in Araç Test Yaklaşımından Çıkan Ders.....	78
5.25. CMK m.134 ve Dijital Materyal İncelemesi	78
5.26. GÜNCEL HUKUKİ DURUM: AYM'NİN 2026 TARİHLİ CMK m.134 KARARI	79
5.27. Arama Kararının Kapsamı.....	79
5.28. İmajın Sanığa veya Müdafie Verilmesi Meselesi.....	80
5.29. UYGULAMALI VAKA I – TELEFONDA FOTOĞRAF BULUNMASI	80
5.30. UYGULAMALI VAKA II – SİLİNMIŞ BELGE.....	81
5.31. UYGULAMALI VAKA III – BİLGİSAYARDA ZARARLI YAZILIM.....	82
5.32. UYGULAMALI VAKA IV – “TELEFONDA BULUNAMADI”	82
5.33. BİLİRKİŞİ RAPORUNA İTİRAZ DİLİ	83
5.34. BİLİRKİŞİYE YÖNELTİLEBİLECEK SORULAR	84
5.35. MÜDAFİ İÇİN TELEFON/BİLGİSAYAR KONTROL KARTI.....	84
5.36. BÖLÜM SONU.....	85

BÖLÜM 6

WHATSAPP, SMS, E-POSTA VE MESAJLAŞMA KAYITLARINA İTİRAZ

6.1. Mesajlaşma Kayıtlarının Ceza Muhakemesindeki Önemi	87
6.2. Ekran Görüntüsü Neyi İspatlar?	87
6.3. Ekran Görüntüsü Manipüle Edilebilir mi?	88
6.4. Ekran Görüntüsünün Orijinal Dosyası	89
6.6. Telefon Numarası Daha Güçlü Delil midir?.....	90
6.7. WhatsApp'ta Bağlı Cihazlar Problemi.....	91
6.8. Mesajın Karşı Cihazda Bulunması	91
6.9. Tek Taraflı Mesaj Kaydı	92
6.10. WhatsApp Sohbet Dışa Aktarma Dosyaları	92

6.11. Mesaj Veritabanları	93
6.12. Silinmiş Mesaj	93
6.13. “Herkesten Sil” İşlemi	94
6.14. Mesajın Tarih ve Saati	94
6.15. Mesajın Düzenlenmesi	95
6.16. Bağlamdan Koparılmış Mesajlar	95
6.17. Sesli Mesajlar	96
6.18. Fotoğraf ve Video Mesajları	96
6.19. SMS Kayıtları	97
6.20. E-Posta Delilleri	97
6.21. “From” Alanı Tek Başına Yeterli midir?	98
6.22. E-Posta Hesabı = Gönderen Kişi midir?	99
6.23. Hesabın Ele Geçirilmesi Savunması	99
6.24. Mesajlaşma Delilinde Beş Aşamalı İspat Modeli	100
6.25. UYGULAMALI VAKA I — WHATSAPP EKRAN GÖRÜNTÜSÜ	100
6.26. UYGULAMALI VAKA II — SAHTE HESAP	101
6.27. UYGULAMALI VAKA III — E-POSTA İLE TEHDİT	101
6.28. UYGULAMALI VAKA IV — SİLİNİMİŞ WHATSAPP MESAJI	102
6.29. UYGULAMALI VAKA V — MESAJIN BAĞLAMİ	103
6.30. İTİRAZ DİLİ	103
6.31. BİLİRKİŞİYE YÖNELTİLEBİLECEK SORULAR	104
6.32. MÜDAFİ İÇİN MESAJLAŞMA DELİLİ KONTROL KARTI	104
6.33. BÖLÜM SONU	105

BÖLÜM 7

SOSYAL MEDYA DELİLLERİNE İTİRAZ

7.1. Sosyal Medya Delillerinin Ceza Muhakemesindeki Yeri	107
7.2. Kullanıcı Adı Kişi Değildir	107
7.3. Görünen Ad ile Kullanıcı Adı Ayrımı	108
7.4. Kullanıcı Adı Değişebilir	108
7.5. Profil URL'sinin Önemi	109

7.6. Ekran Görüntüsü Sorunu	109
7.7. Ekran Kaydı Daha Güçlü müdür?	110
7.8. Sahte Hesap Problemi.....	110
7.9. Hesap Sahipliğinin Teknik Olarak Araştırılması.....	111
7.10. IP Adresi ve Sosyal Medya Hesabı	111
7.11. Tek IP Yeterli midir?	112
7.12. Hesabın Sanığın Telefonunda Açık Olması	113
7.13. Hesabın Ele Geçirildiği Savunması	113
7.14. Paylaşımın Silinmiş Olması	114
7.15. Paylaşım Zamanı	114
7.16. Paylaşım ile Yeniden Paylaşım Ayrımı.....	115
7.17. Beğeni Delil midir?	115
7.18. Takip Etmek veya Takipçi Olmak.....	116
7.19. Hashtag, Etiket ve Mention	116
7.20. Otomatik Paylaşım ve API Kullanımı	116
7.21. Kurumsal Hesaplarda Çoklu Kullanıcı.....	117
7.22. Sosyal Medya Mesajlarında Bağlam	118
7.23. Kesilmiş Sosyal Medya Görüntüleri.....	118
7.24. Sahte Profil ile Kimlik Taklidi	119
7.25. Deepfake Profil ve Sentetik İçerik.....	119
7.26. Platform Verisi ile Kullanıcı Tarafından Sunulan Veri Arasındaki Fark	119
7.27. Platformdan Veri Gelmemesi	120
7.28. Açık Kaynak Verileri ve OSINT	121
7.29. Sosyal Medya Delilinde Arşivleme.....	121
7.30. UYGULAMALI VAKA I — INSTAGRAM HAKARETİ	122
7.31. UYGULAMALI VAKA II — X ÜZERİNDEN TEHDİT	122
7.32. UYGULAMALI VAKA III — “HESABIM ÇALINDI”	123
7.33. UYGULAMALI VAKA IV — KURUMSAL HESAP	123
7.34. UYGULAMALI VAKA V — SİLİNİMİŞ PAYLAŞIM	124
7.35. SOSYAL MEDYA ATTRIBUTION MODELİ.....	125
7.36. İTİRAZ DİLİ	125

7.37. BİLİRKİŞİYE YÖNELTİLEBİLECEK SORULAR	126
7.38. MÜDAFİ İÇİN SOSYAL MEDYA DELİLİ KONTROL KARTI.....	127
7.39. BÖLÜM SONU	127

BÖLÜM 8

FOTOĞRAF, VİDEO, SES KAYITLARI VE DEEFAKE DELİLLERİNE İTİRAZ

8.1. Görsel ve İşitsel Dijital Deliller.....	129
8.2. Orijinal Dosya Neden Önemlidir?	129
8.3. Dosyanın Kaynağı	130
8.4. EXIF ve Metadata.....	130
8.5. EXIF Bulunmaması Ne Anlama Gelir?.....	131
8.6. GPS Metadata'sı Kesin Konum mudur?	131
8.7. Dosya Zamanları	132
8.8. Görüntünün Düzenlenmiş Olması	132
8.9. Manipülasyon ile Normal İşleme Arasındaki Fark.....	133
8.10. Yeniden Kodlama	133
8.11. Video Kayıtlarında Kesinti.....	134
8.12. Güvenlik Kamerası Kayıtları.....	135
8.13. Kamera Görüntüsü ile HTS'nin Karşılaştırılması	135
8.14. Görüntüdeki Kişinin Kimliği.....	135
8.15. Yüz Tanıma Sistemleri	136
8.16. Yüz Benzerliği ile Kimlik Aynılığı	137
8.17. Ses Kayıtlarının İncelenmesi	137
8.18. Ses Kaydının Orijinali	138
8.19. Ses Kaydının Kesilmiş Olması	138
8.20. Konuşmacı Kimliği	139
8.21. Karşılaştırma Ses Örneği	139
8.22. Arka Plan Sesleri	139
8.23. Deepfake Nedir?	140
8.24. Ses Klonlama.....	140
8.26. Deepfake Nasıl Araştırılır?	141

8.27. Deepfake Detector Sonucu Kesin Delil midir?	142
8.28. Detector ile Delil Arasındaki Temel Ayrım	142
8.29. Provenance: İçeriğin Nereden Geldiğini Sormak	143
8.30. Sentetik İçerikte Negatif İspat Problemi	143
8.31. Sayısal Zekâ ile Üretilen İçeriğin Tespiti Zamanla Değişebilir	144
8.32. Sayısal Zekâ ile Üretilmiş İçerik Her Zaman Suç Delilini Geçersiz Kılar mı?.....	144
8.33. UYGULAMALI VAKA I — WHATSAPP'TAN GELEN FOTOĞRAF.....	145
8.34. UYGULAMALI VAKA II — GÜVENLİK KAMERASI	145
8.35. UYGULAMALI VAKA III — SESLİ TEHDİT.....	146
8.36. UYGULAMALI VAKA IV — DEEPFAKE VIDEO.....	146
8.37. UYGULAMALI VAKA V — “%94 DEEPFAKE”	147
8.38. İTİRAZ DİLİ.....	148
8.39. BİLİRKİŞİYE YÖNELTİLEBİLECEK SORULAR	148
8.40. MÜDAFİ İÇİN GÖRÜNTÜ–SES–DEEPFAKE KONTROL KARTI.....	149
8.41. BÖLÜM SONU	150

BÖLÜM 9

BİLİRKİŞİ RAPORUNA İTİRAZ VE DİJİTAL DELİL SAVUNMA STRATEJİSİ

9.1. Bilirkişi Raporu Neden Bu Kadar Önemlidir?	153
9.2. Bilirkişi Raporu Delilin Kendisi Değildir	153
9.3. Bilirkişi Raporu Mutlak Gerçek Değildir	154
9.4. İlk Kontrol: Bilirkişinin Uzmanlık Alanı	154
9.5. Tek Bilirkişi Her Şeyi İnceleyebilir mi?.....	155
9.6. Bilirkişi Hangi Materyali İnceledi?	155
9.7. Ham Veri ile İşlenmiş Veri.....	156
9.8. İncelenen Materyalin Bütünlüğü	156
9.9. Kullanılan Yöntem Açıklanmış mı?	157
9.10. Kullanılan Yazılım ve Sürüm	157
9.11. Yazılım Çıktısı ile Bilirkişi Kanaati	158

9.12. Bilirkişinin Hukuki Değerlendirme Yapması.....	158
9.13. Kesinlik Dili	159
9.14. Bilirkişi Alternatif Hipotezleri Değerlendirmiş mi?	159
9.15. Doğrulama Yanlılığı	160
9.16. Negatif Bulgular da Raporda Yer Almalı mı?	160
9.17. Yeniden Üretilebilirlik.....	161
9.18. Tek Araçla Elde Edilen Kritik Bulgular	161
9.19. Bilirkişi Raporunda Olması Beklenen Temel Unsurlar.....	162
9.20. ÖRNEK: ZAYIF BİLİRKİŞİ RAPORU	162
9.21. “Şüpheliden Ele Geçirilen Samsung Marka Cep Telefonu”	163
9.22. “Adli Bilişim Programıyla Yapılan İnceleme”	163
9.23. “47 Adet Fotoğraf Tespit Edilmiştir”	163
9.24. “Fotoğrafların Bir Kısımının Silindiği Görülmüştür”	164
9.25. “Delilleri Yok Etmeye Çalıştığı Değerlendirilmiştir”	164
9.26. “Dijital Materyallerin Şüpheli Tarafından Kullanıldığı Kanaati”	165
9.27. AYNI RAPOR NASIL DAHA İYİ YAZILABİLİRDİ?	165
9.28. MÜDAFİ RAPORU NASIL OKUMALI?	166
9.29. DOSYA ÖNÜNÜZE GELDİĞİNDE İLK 30 DAKİKA	166
9.30. DİJİTAL DELİLE İTİRAZIN BEŞ AŞAMALI MODELİ	167
9.31. KAYNAK TESTİ	168
9.32. BÜTÜNLÜK TESTİ	168
9.33. TEKNİK ANLAM TESTİ.....	169
9.34. ATTRIBUTION TESTİ	169
9.35. HUKUKİ SONUÇ TESTİ	169
9.36. HUKUKA AYKIRI ELDE EDİLEN DİJİTAL DELİL	170
9.37. CMK m.134 İŞLEMLERİNDE SAVUNMA KONTROLÜ	171
9.38. Hukuka Aykırılık ile Teknik Eksiklik Aynı Şey Değildir	171
9.39. Ek Bilirkişi Raporu Ne Zaman Talep Edilebilir?	172
9.40. Yeni Bilirkişi veya Bilirkişi Heyeti Ne Zaman Talep Edilebilir?	172
9.41. Bilirkişiye Hukuki Soru Sormayın	172
9.42. “Delil Geçersizdir” Demeden Önce	173
9.43. İtirazın Formülü	173

9.44. ÖRNEK İTİRAZ FORMÜLÜ	174
9.45. DOSYA ANALİZİ I — IP ADRESİ.....	174
9.46. DOSYA ANALİZİ II — BAZ İSTASYONU	175
9.47. DOSYA ANALİZİ III — TELEFONDA DOSYA	175
9.48. DOSYA ANALİZİ IV — INSTAGRAM EKРАН GÖRÜNTÜSÜ	175
9.49. DOSYA ANALİZİ V — DEEPFAKE SES	176
9.50. DOSYA ANALİZİ VI — HASH OLMAYAN İMAJ	176
9.51. LEHE DİJİTAL DELİLİ UNUTMAMAK	176
9.52. Alternatif Zaman Çizelgesi Oluşturmak.....	177
9.53. Dijital Delil Matrisi	178
9.54. Mahkemeye Teknik Konuyu Anlatmak	178
9.55. Müdafî Teknik Uzman Olmak Zorunda mı?	179
9.56. UZMANLA ÇALIŞIRKEN MÜDAFİİN ROLÜ.....	179
9.57. DİJİTAL DELİL SAVUNMASININ ON ALTIN KURALI	179
9.58. SON KONTROL — BİR DİJİTAL DELİL DOSYASINDA SORULACAK 20 SORU.....	180
9.59. SONUÇ: DİJİTAL DELİLE İTİRAZ BİR REDDETME SANATI DEĞİLDİR	181
EKLER	183