Fırat Üniversitesi Müh. Bil. Dergisi
36(2), 717-724, 2024

Araştırma Makalesi
https://doi.org/10.35234/fumbd.1430113

Yeni Adli Bilişim İnceleme Süreci (YABİS)

Ramazan OĞUZ[1*], Recep ERYİĞİT[2]
[1] Adli Tıp ve Adli Bilimler Enstitüsü, İstanbul Üniversitesi-Cerrahpaşa, İstanbul, Türkiye
[2] Bilgisayar Mühendisliği, Ankara Üniversitesi, Ankara, Türkiye
[*1] ramazan.oguz@ogr.iuc.edu.tr, [2] reryigit@eng.ankara.edu.tr

(Geliş/Received: 01/02/2024; Kabul/Accepted: 13/07/2024)

Öz: Bu çalışmanın amacı, adli bilişim incelemelerinin giderek artan karmaşıklığına çözüm sunmak amacıyla "Yeni Adli Bilişim İnceleme Süreci (YABİS)" geliştirmeyi hedeflemektedir. Ulusal ve uluslararası düzeyde mevcut adli bilişim süreçlerinin karşılaştırmalı analizi yapılarak, hukuki gerekliliklere uygun, eksiksiz ve kapsamlı bir süreç tasarlanmıştır. YABİS, hazırlık ve delillerin iadesi gibi genellikle göz ardı edilen kritik aşamaları içerecek şekilde kapsamlı bir yaklaşım sunmaktadır. Bu süreç, adli bilişim incelemelerinin etkinliğini artırma, delillerin bütünlüğünü koruma ve dijital kanıtların adli süreçlerde daha güvenilir bir şekilde kullanılmasını sağlama potansiyeline sahiptir. Araştırma, adli bilişim uzmanları, kolluk kuvvetleri ve ilgili diğer tarafların sürecin her aşamasını dikkatlice uygulaması ve sürekli olarak geliştirilmesinin önemini vurgulamaktadır. Bu yaklaşım sayesinde, dijital suçlarla mücadelede daha başarılı ve etkili stratejiler geliştirilebilir.

Anahtar kelimeler: Adli bilişim, birebir kopya, inceleme süreci.

New Digital Forensics Investigation Process (NDFIP)

Abstract: This study aims to develop the New Digital Forensics Investigation Process (YABIS) in response to the increasing complexity of digital forensics investigations. A comparative analysis of existing digital forensics processes at both national and international levels has been conducted to design a comprehensive and legally compliant process. YABIS offers an extensive approach that includes critical stages such as preparation and the return of evidence, which are often overlooked. This process has the potential to enhance the efficiency of digital forensic investigations, preserve the integrity of evidence, and ensure the reliable use of digital evidence in legal proceedings. The research emphasizes the importance of digital forensics experts, law enforcement, and other relevant parties meticulously implementing each stage of the process and continuously improving it. Through this approach, more successful and effective strategies can be developed in the fight against digital crimes.

Key words: Computer forensic, image, examination process.

1. Giriş

Gelişen teknoloji ile birlikte, dijital medyanın suç oluşturan eylemler ile birlikte kullanılmasıyla, suçu aydınlatmakla görevli kolluk kuvvetleri de dijital materyali dikkate almaya başladılar. İlk dijital verilerin suçu aydınlatmada kullanılması 1984 yılına kadar dayanmaktadır [1]. 1984 yılında FBI (Federal Bureau of Investigation- Federal Soruşturma Bürosu) laboratuvarı ve diğer kolluk kuvvetleri tarafından bilgisayar kalıntılarını incelemek için bir program geliştirmeye başlandı ve bilgisayar incelemeleri için Computer Analysis Response Team (CART) kuruldu [2]. 1991 yılının başlarında altı (6) uluslararası kolluk kuvvetinden oluşan bir grup, Amerika Birleşik Devletlerinde birleşerek adli bilişimi ve incelemede standart bir yaklaşımı belirleme konularını tartıştı. 1993 yılında, FBI'ın ev sahipliğinde düzenlenen Uluslararası Kolluk Kuvvetleri Konferansı'na adli bilişim konusunda ulusal ve uluslararası düzeyde 70 temsilci katıldı. Konferans sonunda katılımcılarca adli bilişim standartlarının eksikliği ve bu konuda bir standartlara ihtiyaç olduğunu kabul edildi.

1995 yılında Amerika Birleşik Devletleri Gizli Servisi tarafından yürütülen bir araştırma, kolluk kuvvetlerinin yaklaşık %48'inin adli bilişim laboratuvarına sahip olduğu ve bilgisayar kanıtlarının %68'inin bu laboratuvarlara gönderildiği belirlendi. Yine bu araştırma laboratuvarlarının %70 inde yazılı bir prosedürünün olmadığını gösterdi [1]. 1995 yılından itibaren tespit edilen bu eksikliğin giderilmesine yönelik "adli bilişim inceleme süreçleri" tasarlanmaya başlandı.

[*] Sorumlu yazar: ramazan.oguz@ogr.iuc.edu.tr. Yazarların ORCID Numarası: [1] 0000-0002-7297-4141, [2] 0000-0002-4282-6340

2. Adli Bilişimde İnceleme Süreçleri

Literatürde, suç soruşturmalarında olayların yeniden inşasını kolaylaştırmak veya ilerletmek amacıyla dijital kaynaklardan elde edilen kanıtları bilimsel bir yol izleyerek gerçeğe uygun değerlendirilmesi için adli bilişim süreçleri ile ilgili birçok süreç geliştirilmiştir [3]. Uluslararası alanda geliştirilen bu süreçlerden 19'u bu çalışmada incelenmiştir. İncelenen süreçlere ve süreçlerin aşamalarına ait bilgiler Tablo 1'de gösterilmiştir.

Tablo 1. Uluslararası alanda tasarlanan adli bilişim inceleme süreçleri.

Adli Bilişim İnceleme Süreçleri	Aşamaları
Bilgisayar Adli İnceleme Süreci (Computer Forensic Investigative Process)[4]	Acquisition - Identification - Evaluation - Admission as evidence
Dijital Adli Bilişim Araştırma Çalıştayı (Digital Forensics Research Workshop (DFRWS)) [5]	Identification- Preservation - Collection - Examination - Analysis - Presentation - Decision
Bilimsel Olay Yeri İnceleme Modeli (Scientific Crime Scene Investigation Model) [6]	Recognition - Identification - Individualization - Reconstruction
Soyut Dijital Adli Bilişim Modeli (Abstract Digital Forensics Model (ADFM)) [7]	Identification - Preparation - Approach Strategy- Preservation - Collection - Examination - Analysis - Presentation - Returning Evidence
Entegre Dijital İnceleme Süreci (Integrated Digital Investigation Process (IDIP)) [8]	Readiness - Deployment - Physical Crime Investigation/ Digital Crime Investigation - Review
Uçtan Uca Dijital İnceleme (End to End Digital Investigation) [9]	Collecting evidence - Analysis of Individual Events - Preliminary Correlation - Event Normaization - Event Deconfliction - Second Level Correlation - Timeline Analysis - Chain of evidence Construction - Corroboration
Siber Suç İncelemeleri Genişletilmiş Modeli (Extended Model of Cybercrime Investigations) [10]	Awareness - Authorization - Planning - Notification - Search and Identify - Collection - Transport - Storage - Examination Hypotheses - Presentation - Proof/Defance - Dissemination
Olaya Dayalı Dijital Adli Bilişim İnceleme Çerçevesi (Event-based Digital Forensic Investigation Framework) [11]	Preservation - Search - Reconstruction
Gelişmiş Dijital İnceleme Süreci Modeli (Enhanced Digital Investigation Process Model) [12]	Readiness - Deployment - Traceback - Dynamite - Review
Dijital İncelemeler Süreci için Hiyerarşik, Amaç Tabanlı Çerçeve (Hierarchical, Objective-Based Framework for the Digital Investigations Process) [13]	Preparation - Incident Response - Data Collection - Data Analysis - Presentation of Findings - Incident Closure
Dijital Adli Bilişim İncelemesi için Çerçeve (Framework for a Digital Forensic Investigation) [14]	Preparation - Investigation - Presentation
Bilgisayar Adli Bilişim Alan Triyaj Süreci Modeli (The Computer Forensic Field Triage Process Model (CFFTPM)) [15]	Planning - Triage - Usage/User Profiles - Chronology/Timeline - Internet Activity - Case specific evidence
Adli İşlem (NIST) (Ulusal Standartlar ve Teknoloji Enstitüsü) (Forensic Process (NIST) (National Institute of Standards and Technology)) [16]	Collection - Examination- Analysis - Reporting
Olay ve Bilgisayar Adli Bilişimi için Ortak Süreç Modeli (Common Process Model for Incident and Computer Forensics) [17]	Pre Analysis Phase - Analysis Phase - Post Analysis Phase
Çift Veri Analiz Süreci (Dual Data Analysis Process) [18]	Access - Acquire - Analyse - Report
Malezya İnceleme Sürecine Dayalı Dijital Adli Bilişim Modeli (DFMMIP) (Digital Forensics Model based on Malaysian Investigation Process (DFMMIP)) [19]	Planning - Identification - Reconnaissance - Transport & Storage - Analysis Proof & Defense - Archive Storage
European Network of Forensic Science Institutes (ENFSI)- Best Practice Manual for the Forensic Examination of Digital Technology - Avrupa Adli Bilim Enstitüleri Ağı (ENFSI)- Dijital Teknolojinin Adli İncelemesi için En İyi Uygulama Kılavuzu [20]	Identify - Acquire - Analysis - Report
SWGDE Best Practices for Computer Forensic Examination [21]	Preparation - Considerations - Triage - Acquisition - Examination – Report - Preservation
Digital Forensics and Incident Response (DFIR) Framework for Operational Technology (OT)(NIST) [22]	Collection - Examination - Analysis - Reporting

Ulusal alanda tasarlanan adli bilişim süreçleri incelendiğinde, 2004 yılında 5271 sayılı Ceza Muhakemesi Kanunun (CMK) yürürlüğe girmesi ile birlikte, 134. maddesinde bilgisayar ve kütüklerinde yapılacak aramaların

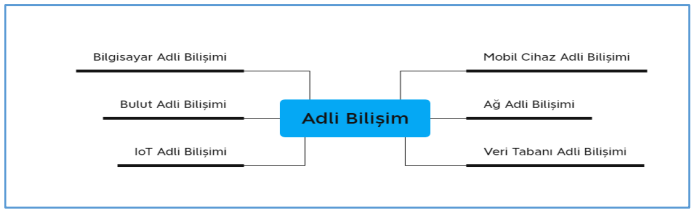
ve incelemelerin tanımlanması yapılmıştır. Müteakibinde hukuk sistemimize uygun adli bilişim süreçleri tasarlanmaya başlanmıştır. Tasarlanan bu süreçlerden altı (6)'sı bu çalışma kapsamında incelenmiştir. İncelenen süreçlere ve süreçlerin aşamalarına ait bilgiler Tablo 2'de gösterilmiştir.

Tablo 2. Ulusal alanda tasarlanan adli bilişim inceleme süreçleri.

Adli Bilişim İnceleme Süreçleri	Aşamaları
Doç.Dr. Leyla Berber Keser'e göre [23]	Toplama - İnceleme - Analiz Etme - Belge Hazırlama - Raporlama
Doç.Dr. Ahmet Koltuksuz'a göre [24]	Tanımlama - Elde Etme - Saklanması - İnceleme – Mahkemeye Sunum
Jandarma Kriminal Daire Başkanlığına göre [25]	Elde Etme - Tanımlama - Değerlendirme - Sunum
Yrd.Doç.Dr. Türkay HENKOĞLU'na göre [26]	Delillerin tespit edilmesi, toplanması ve muhafazası -Delilleri açığa çıkartma, inceleme ve analiz yapılması - Delillerin raporlanması
Yrd.Doç.Dr. Hüseyin ÇAKIR'a göre [27]	İlk Müdahale - Delil Toplama - Analiz - Rapor
Doç.Dr. Harun ARTUNER'e göre [28]	Elde Etme - Tanımlama - Değerlendirme - Sunum

3. Adli Bilişim İnceleme Süreçlerinin Analizi

Adli bilişim terimi başlangıçta adli bilişim ile ilgili olarak kullanılırken, bugün dijital verileri üreten ve depolayan tüm cihazların araştırılmasını sağlamak için birçok alt dala bölünerek genişlemiştir [29]. Adli bilişim, dijital cihazların ve verilerin türü ile ilgili olarak çeşitli alt dallara ayrılmıştır; bu dallar başlıca Şekil 1'de gösterildiği gibi bilgisayar adli bilişimi, bulut adli bilişimi, IoT (nesnelerin interneti) adli bilişimi, mobil cihaz adli bilişimi, ağ adli bilişimi ve veri tabanı adli bilişimidir [30].



Şekil 1. Adli bilişimin alt dalları.

Uluslararası alanda tasarlanmış olan adli bilişim inceleme süreçlerine ait aşamalar Şekil 2 ve Şekil 3'te, ulusal alanda tasarlanmış adli bilişim inceleme süreçlerine ait aşamalar ise Şekil 4'te gösterilmiştir. Tüm bu süreçler analiz edildiğinde,

- Aynı aşamanın farklı isimlerde (Readiness, Preparation, Authorization, Approach Strategy, Deployment; Acquisition, Acquire, Collecting Evidence, Collection, Data Collection) tanımlanmış olduğu,
- Bazı süreçlerin [4, 6, 11, 14, 16, 18, 20, 21, 22] konuyu genel çerçevede değerlendirirken, bazı süreçlerin [5, 7, 8, 10, 13, 15, 19] ise ayrıntılı bir şekilde tanımlandığı,
- [9, 16, 22] numaralı çalışmalarda, toplama aşaması ile süreçlerin başladığı,
- [8, 12, 13, 15, 19, 21] numaralı çalışmalarda, hazırlık aşaması ile süreçlerin başladığı, [10] numaralı çalışmada ise hazırlık aşamasına önem verildiği ve 3 alt aşamada tanımlandığı,
- Bazı süreçlerin [9, 15] inceleme/analiz aşamasına önem verdiği ve detaylandırdığı, [17] numaralı çalışmanın ise süreçlerini analiz aşamasına göre (analiz öncesi, analiz ve analiz sonrası) şekillendirdiği
- [7, 13] numaralı çalışmalarda delillerin iadesi aşamasına yer verildiği,
- [8] numaralı çalışmada, birçok aşamayı genel bir alt aşamada (fiziksel suç incelemesi, dijital suç incelemesi şeklinde) tanımladığı,
- [7, 13] numaralı çalışmalarda delillerin iadesi aşamasına yer verildiği,
- [23-28] numaralı süreçlerde hazırlık aşaması ve delillerin iadesi aşamasının bulunmadığı anlaşılmıştır. Görüldüğü üzere adli bilişim geniş kapsamlı bir disiplin olduğundan tasarlanan adli bilişim inceleme süreçleri de çoğunlukla alt adli bilişim dallarına göre şekillenmektedir.

4. Yeni Adli Bilişim İnceleme Süreci (YABİS)

Adli bilişimin alt dalları kapsamlı olduğundan tasarlanan adli bilişim inceleme sürecinin de tüm dalları kapsar nitelikte olması gerekmektedir. Eksiksiz bir inceleme sürecinin delil teslim zinciri (Chain of Custody) bakış açısıyla gerçekleşebilmesi için, sürecin hazırlık aşaması ile başlayıp delillerin iadesi aşaması ile son bulması gerektiği değerlendirilmektedir [31].

Bu çalışma kapsamında incelenen adli bilişim süreçlerinden [7, 13] numaralı süreçler dışında tüm aşamaları kapsayan başkaca bir sürecin bulunmadığı anlaşılmıştır. [7, 13] numaralı süreçlerin hazırlık aşaması ile başlayıp delillerin iadesi aşaması ile son bulduğu görülmektedir. Fakat iade aşamasının delillerin sahiplerine iadesi olarak açıklanmıştır.

Bu çalışma kapsamında tasarlanan adli bilişim inceleme süreci de [7, 13] numaralarda belirtilen çalışmalar gibi kapsamlı bir şekilde tanımlanmış ve olay yeri inceleme safhaları [32] çerçevesinde değerlendirilmiştir. Tasarlanan adli bilişim inceleme sürecinin dört (4) aşamadan oluşması gerektiği değerlendirilmiştir. Bunlar, Hazırlık Aşaması, Delillerin Tespit Edilmesi, Toplanması, Muhafazası ve Laboratuvara Gönderilmesi Aşaması, Deliller Üzerinde Gerekli İnceleme ve Analiz Faaliyetleri Aşaması ve İnceleme Sonucu Raporlama ve Delillerin İadesi Aşamasıdır.

4.1. Hazırlık aşaması

Çalışmada ulusal düzeyde tasarlanan süreçler içerisinde belirtilmeyen hazırlık ve delillerin iadesi aşaması bulunmaktadır. Hazırlık aşaması iki (2) yönlü olarak değerlendirilmiştir. Birincisi, hukuki hazırlıktır. Biraz açmak gerekirse, öncelikle olay yerinde bilişim delillerinin toplanması için gerekli olan yasal izinlerin [33] alınması gerekmektedir. Gerekli yasal izni olmayan bir delile teknik açıdan doğru müdahale edilse bile, hukuka aykırı olarak elde edilmiş olan deliller mahkeme tarafından bir vakanın ispatında dikkate alınmaz hükmü uyarınca mahkeme tarafından delil olarak kabul edilmeyecektir [34]. Bir diğeri ise gerekli teknik alt yapının hazır halde olması gerekliliğidir. Yeterli ve gerekli teknik bilgisi olmayan veya gerekli teknik donanımı yetersiz olan bir kolluk görevlisinin delile müdahalesi geriye döndürülemeyecek hatalara yol açacak ve bir sonraki aşamada inceleme yapan uzman/bilirkişilerin incelemelerine olumsuz bir etki yapacaktır.

4.2. Delillerin tespit edilmesi, toplanması, muhafazası ve laboratuvara gönderilmesi aşaması

Adli bilişimin başladığı nokta, el koymanın başladığı noktadır. Dolayısıyla, sürecin başladığı yer olan olay yerinde (içinde delillerin bulunduğu alan) yapılan incelemede yapılan hatalar, delillerin gerçekliğine ve güvenirliliğine gölge düşüreceği için tüm süreci sekteye uğratabilir [21]. Bu nedenle deliller, öncelikli olarak tespit edildikten sonra usulüne uygun bir şekilde toplanır ve muhafaza altına alınır. Müteakip aşamada gerekli incelemelerin yapılabilmesi amacıyla laboratuvara gönderilir. Delilin olay yerinde tespitinden laboratuvara gönderilme aşamasına kadar olan süreç ardışık ve genellikle de aynı kişiler tarafından gerçekleştirildiğinden sürecin tamamı bir bütün olarak değerlendirilmiştir.

4.3. Deliller üzerinde gerekli inceleme ve analiz faaliyetleri aşaması

İncelenmek üzere gelen delillerin bir dizi kontrol işlemleri gerçekleştirildikten sonra eksik bulunmaması durumunda (talep yazısı, mahkeme kararı, delil torbalarının mühürlü ve sağlam olması vb.) inceleme ve analiz faaliyetlerine geçilir. Gelen delilin öncelikli olarak alınabiliyorsa kopyası (imajı) alınır (Şekil 5) ve talep edilen tüm incelemeler kopya üzerinden gerçekleştirilir.

AŞAMALAR/ ALT AŞAMALAR	1	2				3	4	
	Hazırlık Aşaması	Delillerin Tespit Edilmesi,	Toplanması,	Muhafazası	ve Laboratuvara Gönderilmesi Aşaması	Deliller Üzerinde Gerekli İnceleme ve Analiz Faaliyetleri Aşaması	İnceleme Sonucu Raporlama	ve Delillerin İadesi Aşaması
Kazanım/edinme/imaj alma (Acquisition)			X					
Kazanım/edinme/imaj alma (Acquire)			X					
Erişim (Access)		X						
Kabul (Admission)							X	
Analiz (Analyse)						X		
Analiz (Analysis)						X		
Bireysel Olayların Analizi (Analysis of Individual events)						X		
Analiz Aşaması (Analysis Phase)						X		
Yaklaşım Stratejisi (Approach Strategy)	X							
Arşiv Depolama (Archive Storage)				X				
Yetkilendirme (Authorization)	X							
Farkındalık (Awareness)	X							
Özel Vaka Kanıtları (case specific evidence)						X		
Kanıt Zinciri Oluşturma (Chain of evidence Construction)	X							
Kronoloji/Zaman Çizelgesi (chronology/timeline)						X		
Kanıt Toplama (Collecting Evidence)			X					
Toplama (Collection)			X					
Değerlendirme (Consideration)						X		
Doğrulama (Corroboration)						X		
Veri Analizi (Data Analysis)						X		
Veri Toplama (Data Collection)			X					
Karar (Decision)							X	
Görevlendirme (Deployment)	X							
Dijital suç incelemesi (Digital Crime Investigation)		X						
Dağıtım (Dissemination)							X	
Fiziksel Suç Mahalli İnceleme Aşaması (Dynamite)		X						
Değerlendirme (Evaluation)						X		
Olayın Uyuşmazlığını Giderme (Event Deconfliction)						X		
Olay Normalleştirme (Event Normaization)						X		
İnceleme (Examination)						X		
Hipotezler (Hypotheses)							X	
Tanımlama (Identification)	X							
Tanımlama (Identify)	X							
Olayın Kapanışı (Incident Closure)								X
Olaya Müdahale (Incident Response)		X						
Kişiselleştirme (Individualization)						X		
Araştırma (Investigation)						X		
İnternet Aktivitesi (Internet activity)						X		
Bildirim, her iki tarafada bilgi verme (Notification)	X							
Fiziksel Suç Araştırması (Physical Crime Investigation		X						
Planlama (Planning)	X							
Analiz Sonrası Aşama (Post-Analysis Phase)							X	
Analiz Öncesi Aşama (Pre-Analysis Phase)		X						
İlk İlişkilendirme (Preliminary Correlation)							X	
Hazırlık (Preparation)	X							
Sunum (Presentation)							X	

Şekil 2. Uluslararası adli bilişim inceleme süreçleri.

AŞAMALAR/ALT AŞAMALAR	1	2				3	4	
	Hazırlık Aşaması	Delillerin Tespit Edilmesi,	Toplanması,	Muhafazası	ve Laboratuvara Gönderilmesi Aşaması	Deliller Üzerinde Gerekli İnceleme ve Analiz Faaliyetleri Aşaması	İnceleme Sonucu Raporlama	ve Delillerin İadesi Aşaması
Bulguların Sunumu (Presentation of Findings)							X	
Koruma(Preservation)				X				
Ispat&Savunma (Proof&Defance)							X	
Hazırlık(Readiness)	X							
Tanıma(Recognition)		X						
Arama/Keşif(Reconnaissance)		X						
Yeniden Yapılandırma (Reconstruction)						X		
Rapor(Report)							X	
Raporlama(Reporting)							X	
Kanıtların İadesi (Returning Evidence)								X
Gözden Geçirme(Review)							X	
Araştırma(Search)						X		
Arama ve Tanımlama (Search and Identify)		X						
Ikinci Seviye İlişkilendirme (Second Level Correlation)						X		
Depolama (Storage)				X				
Zaman Çizelgesi Analizi (Timeline Analysis)						X		
Geri İzleme(Traceback)				X				
Taşıma(Transport)					X			
Taşıma&Depolama (Transport&Storage)				X				
Ön Değerlendirme(Triage)				X				
Kullanım/Kullanıcı Profilleri (Usage/User Profiles)						X		

Şekil 3. Uluslararası adli bilişim inceleme süreçlerinin devamı.

AŞAMALAR/ALT AŞAMALAR	1	2				3	4	
	Hazırlık Aşaması	Delillerin Tespit Edilmesi,	Toplanması,	Muhafazası	ve Laboratuvara Gönderilmesi Aşaması	Deliller Üzerinde Gerekli İnceleme ve Analiz Faaliyetleri Aşaması	İnceleme Sonucu Raporlama	ve Delillerin İadesi Aşaması
Analiz						X		
Analiz Etme						X		
Belge Hazırlama							X	
Değerlendirme						X		
Delilleri açığa çıkarma, inceleme ve analiz yapılması						X		
Delillerin tespit edilmesi, toplanması ve muhafazası		X	X	X				
Delil toplama			X					
Delillerin raporlanması							X	
Elde Etme		X						
İlk müdahale		X						
İnceleme						X		
Mahkemeye Sunum							X	
Rapor							X	
Raporlama							X	
Saklanması				X				
Sunum							X	
Tanımlama		X						
Toplama			X					

Şekil 4. Ulusal adli bilişim inceleme süreçleri.

Şekil 5. Birebir kopya alma işlemleri.

4.4. İnceleme sonucu raporlama ve delillerin iadesi aşaması

İncelemeler sonucunda tespit edilen bilgiler ışığında bir rapor tanzim edilir. Rapor içeriğinin anlaşılır bir dille yazılmasına ve talep edilen isteklere cevap verir nitelikte olmasına özen gösterilir. Rapor tanzim işlemleri de tamamlandıktan sonra delillerin iadesi aşamasına geçilir. Tasarlanan bu sürecinin diğer yeni aşaması ise delillerin iadesi aşamasıdır. Delillerin iadesi konusunun çok önemli bir aşama olduğu değerlendirilmektedir. Çünkü adli bir incelemenin tamamlanması ve raporunun düzenlenmesi ile birlikte ihtimal dahilinde, incelemeyi yapan kişi/kurum tarafından inceleme son bulmuş olabilir; diğer taraftan, bir incelemenin sonu başka bir incelemenin başlangıcı olabilecektir. Sağlıklı bir incelemenin yapılabilmesi için en başta delilin sağlam (incelenebilir) olması gerekmektedir. Delilin süreç içerisinde hasar görmesi durumunda üzerinde herhangi bir inceleme yapılamayacaktır. Bu nedenle inceleme süreçleri tasarlanırken kesinlikle delilin iadesi (delilleri gönderen makama), sürecin bir aşaması olarak değerlendirilmesi gerekmektedir.

5. Tartışma ve Sonuç

Bu çalışma, dijital suçların artan oranına ve adli bilişim incelemelerinin karmaşıklığına yanıt olarak Yeni Adli Bilişim İnceleme Süreci (YABİS)'nin geliştirilmesi ve uygulanması gerekliliğini vurgulamaktadır. Ulusal ve uluslararası alandaki mevcut adli bilişim süreçlerinin karşılaştırmalı analizi, YABİS'in kapsamlı ve çok yönlü bir yaklaşım sunarak adli bilişim incelemelerini daha etkin bir şekilde yönlendirebileceğini göstermektedir. YABİS, adli bilişim süreçlerinde sıklıkla göz ardı edilen hazırlık ve delillerin iadesi gibi kritik aşamaları içerecek şekilde tasarlanmıştır.

Tartışma bölümünde, YABİS'in diğer süreçlerden farklılaşan yönleri ve bu yeni sürecin adli bilişim incelemelerine sağlayabileceği potansiyel avantajlar ele alınmıştır. Sürecin, adli bilişim alt dallarını geniş bir şekilde kapsayarak daha kapsamlı bir inceleme imkanı sunması, delillerin daha sistemli bir şekilde toplanması, muhafaza edilmesi ve analiz edilmesini sağlaması beklenmektedir.

Sonuç olarak, YABİS, adli bilişim alanında karşılaşılan zorluklara ve ihtiyaçlara yönelik olarak tasarlanmış bir süreçtir. Geliştirilen bu yeni süreç, adli bilişim incelemelerinin etkinliğini artırma, delillerin bütünlüğünü koruma ve adli süreçlerde dijital kanıtların daha güvenilir bir şekilde kullanılmasını sağlama potansiyeline sahiptir. YABİS'in başarılı bir şekilde uygulanabilmesi için, adli bilişim uzmanları, kolluk kuvvetleri ve ilgili diğer tarafların sürecin her aşamasını dikkatlice uygulaması ve sürekli geliştirilmesi önemlidir. Bu sayede, dijital suçlarla mücadelede daha etkili ve verimli bir yol izlenebilir.

Kaynaklar

[1] Noblett MG, Pollitt MM, Presley LA. Recovering and Examining Computer Forensic Evidence, Forensic Science Communications. 2000; 2(4): pp. 1-13.
[2] Digital Forensics. https://www.open.edu/openlearn/science-maths-technology/digital-forensics/content-section-4.2. Erişim Tarihi: 30.03.2024.
[3] Peasah KO, Quayson E, Agyei O, Ansong ED. Survey of Digital Forensic Models and Proposed Thematic Scheme. Int J Comput Appl Technol, 2017;169(11): pp. 41–45.
[4] Pollitt MM. Computer Forensics: An Approach to Evidence in Cyberspace. Proc Natl Inf Syst Secur Conf, 1995; pp. 487-491.
[5] Palmer G. A Road Map for Digital Forensic Research. DFRWS; Aug 7th – 8th 2001; Utica, NY.
[6] Sachowski J. Implementing Digital Forensic Readiness: From Reactive to Proactive Process. England: Taylor & Francis Group, 2021.
[7] Reith M, Carr C, Gunsch G. An Examination of Digital Forensics Models. Int J Digit Evid, 2002; 1(3).
[8] Carrier BD, Spafford E. Getting Physical with the Digital Investigation Process. Int J Digit Evid, 2003; 2(2), pp. 1-20.
[9] Stephenson PA. Comprehensive Approach to Digital Incident Investigation. Inf Secur Tech Rep, 2003; 8(2), pp. 42-52.
[10] Ciardhuain S. An Extended Model of Cybercrime Investigation. Int J Digit Evid,2004; 3(1): pp. 1-22.
[11] Carrier B, Spafford EH. An Event-based Digital Forensic Investigation Framework. Conf DFRWS; Aug 11th – 13th 2004; Baltimore, MD.
[12] Baryamereeba V, Tushabe F. The Enhanced Digital Investigation Process Model. Conf. DFRWS; Aug 11th – 13th 2004; Baltimore, MD.
[13] Beebe NL, Clark JG. A Hierarchical, Objective-Based Framework for the Digital Investigations Process. Proc. DFRWS, 2005; 2(2): pp. 147-167.
[14] Kohn M, Olivier MS, Eloff JHP. Framework for a Digital Forensic Investigation. Proceedings of the ISSA 2006 from Insight to Foresight Conference; 5-7 July 2006; Balalaika Hotel, Sandton, South Africa.
[15] Rogers MK, Goldman J, Mislan R, Wedge T, Debrota S. Computer Forensic Field Triage Process Model. Journal of Digital Forensics, Security and Law. 2006; Vol. 1(2): pp. 27-40.
[16] Kent K, Chevalier S, Grance T, Dang H. Guide to Integrating Forensic Techniques into Incident Response. NIST Spec Publ 2006; 800-86: pp. 3-1.
[17] Freiling FC, Schwittay B. A Common Process Model for Incident and Computer Forensics. Conf IT Incident Mgmt IT Forensics IMF 2007; Sep 11th – 13th 2007; Stuttgart, Germany.
[18] Bem D, Huebner E. Computer Forensic Analysis in a Virtual Environment. Int J Digit Evid, 2007; 6(2):pp. 1-13.
[19] Sundresan P. Digital Forensic Model Based on Malaysian Investigation Process, Int J Comput Sci Netw Secur, 2009; 9(8).
[20] ENFSI, Best Practice Manual for the Forensic Examination of Digital Technology. ENFSI-BPM-FIT, Version 01, 2015;17.
[21] Scientific Working Group on Digital Evidence (SWGDE), Best Practices for Computer Forensic Examination. 2018; pp. 1-11.
[22] Salfati E, Pease M. Digital Forensics and Incident Response (DFIR) Framework for Operational Technology (OT). NIST. 2022; pp. 1-58
[23] Berber LK. Adli Bilişim (Computer Forensic), Ankara: Yetkin Yayınları, 2004.
[24] Koltuksuz A. Adli Bilişime Giriş. Adli Bilişim Günü, Yaşar Üniversitesi, İzmir, 2010.
[25] Jandarma Kriminal Daire Başkanlığı, Adli Bilimler II, 2011;217,218.
[26] Henkoğlu T. Adli Bilişim: Dijital Delillerin Elde Edilmesi ve Analizi, Ankara: Pusula Yayıncılık, 2014.
[27] Çakır H, Kılıç MS. Adli Bilişim ve Elektronik Deliller, Ankara: Seçkin Yayıncılık, 2014.
[28] Artuner H. Adli Bilişim Alanında Dijital Delil, Delil Karartma, Delil Toplama, 2015.
[29] Reith M, Carr C, Gunsch G. An examination of digital forensic models. Int J Digit Evid, 2002; pp. 1-12.
[30] Uysal Z, Forensic Analysis of Social Network Application on Smartphones. Master's Thesis, Ankara Yıldırım Beyazıt University, 2021.
[31] Oğuz R, Adli Bilişimde İnceleme Süreçleri. Yüksek Lisans Tezi, Ankara Üniversitesi, Sağlık Bilimleri Enstitüsü, Fiziki İncelemeler ve Kriminalistik Yüksek Lisans Programı, 2018.
[32] Hancı İH, Vural O. Adli Bilimler ve Kriminalistik Ansiklopedisi, Adli Mühendislik ve Adli Bilişim -1- 2023; 4903.
[33] 5271 Sayılı Ceza Muhakemesi Kanunu (CMK), madde:127, 134.
[34] 6100 Sayılı Hukuk Muhakemeleri Kanunu (HMK), madde: 189/2.