T.C.

HALİÇ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİMDALI

YÖNETİM BİLİŞİM SİSTEMLERİ

ÜLKEMİZDE ADLİ BİLİŞİM LABORATUARI KURULUMU ve BİLİŞİM SUÇLARIYLA MÜCADELEYE KATKILARI

YÜKSEK LİSANS TEZİ

Hazırlayan

İLKER ÇİÇEK

Tez Danışmanı

Prof.Dr. ALİ OKATAN

Haziran 2008
İSTANBUL

T.C.

HALİÇ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Yönetim bilişim sistemleri Programı Yüksek Lisans öğrencisi İlker ÇİÇEK tarafından hazırlanan **" Ülkemizde Adli Bilişim Laboratuarı Kurulumu Ve Bilişim Suçlarıyla Mücadeleye Katkıları "** adlı bu çalışma jürimizce Yüksek Lisans Tezi olarak kabul edilmiştir.

Tez Savunma Tarihi : 17.06.2008

(Jüri Üyesinin Ünvanı , Adı , Soyadı ve Kurumu) :	İmzası :
Jüri Üyesi: Prof.Dr.Ali OKATAN (Danışman-H.Ü. Öğr.Üyesi)	.....
Jüri Üyesi :Yrd.Doç Dr.Yüksel BAL (HÜ.Öğr.Üyesi)	.....
Jüri Üyesi :Yr.Doç.Dr.Murat BEKEN (H.Ü.Uygulamalı Mat. Öğr.Üyesi)	.....

ÖNSÖZ

Bilişim teknolojilerindeki gelişime paralel olarak suç ve suçlu kavramları da değişmektedir. Suç kavramı çeşitlenmiş, karmaşıklaşmış ve etkinliğini artırmıştır. Ayrıca tehdit kapsamı kolayca ve hızla genişlemiş, sadece bireyler değil kurumlar ve devletler de hedef haline gelmeye başlamıştır.

Gelişen bilişim teknolojileri, adli süreçle ilgili kavram ve görevleri de değiştirmiştir. Delil sayısallaşmış, özgürlükler cenneti olan internetin sanal dünyası bir olay yeri haline gelmiştir.

Geleceğin dünyasının bireysel ve kurumsal açıdan en önemli ihtiyacının güvenlik ve adalet olması nedeniyle, siber çağın yöntemleriyle gerçekleştirilen suçların tespiti ve kanıtlanması sürecinde; yasal düzenlemeler ile uyumlu, standartları belirlenmiş, akredite uzman personeli olan, uluslararası sertifikalara sahip ve üniversitelerle işbirliği içerisindeki adli bilişim laboratuarlarının kurulması önem arz etmektedir.

Sayısal delil, sayısal delillerin tespiti ve değerlendirilmesi gibi adli sürece yeni dâhil olan kavramların bu laboratuarlar sayesinde ticari kaygılardan arınmış, uygulanabilir genel esaslara kavuşturulmasının, kolluk birimlerinin görev etkinliğinin artırılmasının ve adalete, kişisel hak ve özgürlükleri koruyarak uluslararası geçerliliği olan desteğin verilmesinin sağlanacağı değerlendirilmektedir. Ayrıca çalışmalar, ulusal ağ ve bilgi güvenliği konularına ilgiyi arttıracak, hızla gelişen bilişim teknolojilerinin araştırılarak adli bilişim yeteneğine katkıda bulunmasını sağlayacaktır.

Yapmış olduğum tez çalışmasında, bilgi ve zamanını benden esirgemeyen, çalışmamın her aşamasında bana yol gösteren, kendisinden çok şey öğrendiğim değerli danışmanım Sayın Prof. Dr. Ali OKATAN'a teşekkürlerimi sunarım.

Birlikte çalışmaya başladığım andan itibaren kendisinden çok şey öğrendiğim, mesleğime sevgimi ve bağlılığımı arttıran, yoğun görev tempomuzda çalışabilmem için benden desteğini eksik etmeyen, değerli komutanım Nedim ÜNAL'a sonsuz teşekkür ederim.

Bilimsel çalışmada yolda kalmamı önleyen, her fırsatta elimde notlarla kendisine koştuğum ve hiçbir zaman beni reddetmeyen değerli komutanım Halil ÇELİK'e saygı ve minnetlerimi sunarım.

Tezimin araştırma safhasında bana çok değerli bilgileri veren, yoğun temposuna rağmen istediğim an ulaşabildiğim ve sürekli motive olmamı sağlayan Sayın Citigroup Güvenlik ve Araştırma Servisi Müdürü Mesut DEMİRBİLEK'e ve kendisiyle tanışmamı sağlayan Sayın E.Korg.Mehmet ÇAVDAROĞLU ve Sayın Tümg.Osman EKER'e özel saygı ve minnetlerimi sunarım.

Ayrıca çalışmamda sürekli desteklerini gördüğüm, Hakan ORTABAĞ'a, Yrd.Doç.Dr.Leyla KESER'e ve Bülent CANSU'ya teşekkür ederim.

Bu süreci benimle birlikte yasayan, varlıklarını her zaman yanımda hissettiğim fedakâr anneme, babama ve kardeşlerime tüm kalbimle teşekkür ederim.

İÇİNDEKİLER

KISALTMALAR LİSTESİ

AG KRITIS	:Interministerielle Arbeitsgruppe Kritische Infrastrukturen (Germany)
AKSIS	:Arbeitskreis Schutz Kritischer Infrastrukturen/Working Group on Infrastructure Protection (Germany)
BBK	:Bundesamt für Bevölkerungsschutz und Katastrophenhilfe/Federal Office for Civil Protection and Disaster Response (Germany)
BCS	:British Computer Society (United Kingdom)
BfV	:Bundesamt für Verfassungsschutz/Federal Office for the Protection of the Constitution (Germany)
BITKOM	:Bundesverband für Informationswirtschaft, Telekommunikation und Neue Medien (Germany)
BKA	:Bundeskriminalamt/Federal Office of Criminal Investigation (Germany)
BMBF	:Bundesministerium für Bildung und Forschung/Federal Ministry for Education and Research (Germany)
BMI	:Bundesministerium des Inneren/Federal Ministry of the Interior (Austria;Germany)
BMJ	:Bundesministerium der Justiz/Federal Ministry of Justice (Germany)
BMVg	:Bundesministerium der Verteidigung/Federal Ministry of Defense (Germany)
BMVIT	:Ministry for Traffic, Infrastructure and Technology (Austria)
BMWA	:Bundesministerium für Wirtschaft und Arbeit/Federal Ministry of Economics and Labour (Germany)
BMWi	:Bundesministerium für Wirtschaft and Technologie/Federal Ministry of Economics and Technology (Germany)
BND	:Bundesnachrichtendienst/Federal Intelligence Service (Germany)
BPOL	: Federal Police (Germany)
BSI	: Bundesamt für Sicherheit in der Informationstechnik/ Federal Office for Information Security (Germany)
BVA	:Bundesverwaltungsamt/Federal Office of Administration (Germany)
CART	:Computer Analysis and Response Team (United States)
CCIPS	:Computer Crime and Intellectual Property Section (United States)
CCS	: Civil Contingencies Secretariat (United Kingdom)
CEN	: European Committee for Standardization
CERT/CC	: Computer Emergency Response Team Coordination Center
CERT	: Computer Emergency Response Team
CERT-Bund	: German Computer Emergency Response Team for Federal Authorities (Germany)
CESG	:Communications-Electronics Security Group (United Kingdom)
CFAA	: Computer Fraud and Abuse Act (United States)

CISA	:(Certified Information Systems Auditor) Sertifikalı Bilgi Sistemleri Denetçisi
CISM	:(Certified Information Security Manager) Sertifikalı Bilgi Güvenliği Yöneticisi
CI	: Critical Infrastructure
CIAO	: Critical Infrastructure Assurance Office (United States)
CIDDAC	: Cyber Incident Detection Analysis Centre (United States)
CII	: Critical Information Infrastructure
CIIP	: Critical Information Infrastructure Protection
CIO	: Chief Information Officer
CIP	: Critical Infrastructure Protection
CIRT	: Computer Incident Response Team
CIWG	: Critical Infrastructure Working Group (United States)
CMA	: Communications and Multimedia Act (Malaysia)
CMK	:Ceza Muhakemesi Kanunu
CNI	: Critical National Infrastructure
Computer Forensic	:Adli Bilişim
COBIT	:(Control Objectives for Information and related Technology) Bilgi Teknolojileri için Hedeflerin Kontrol Edilmesi.
CRS	: Congressional Research Service (United States)
CSD	: Computer Security Division at NIST (United States)
CSIA	:Central Sponsor for Information Assurance (United Kingdom)
CSIRT	: Computer Security Incident Response Team
CSTARC	:Cyber Security Tracking, Analysis and Response Center (United States)
CT	: Counter-terrorism
CYTEX	: Cyber Terror Exercise (Germany)
DdoS	: Distributed Denial of Service
deNIS	:German Emergency Preparedness Information System (Germany)
DHS	: Department of Homeland Security (United States)
DIA	: Defense Intelligence Agency (United States)
DoD	: Department of Defense (United States)
DoE	: Department of Energy (United States)
DSTL	: Defence Research Centre (United Kingdom)
DTI	: Department of Trade and Industry (United Kingdom)
EC-Council	:(International Council of Electronic Commerce Consultants) Uluslar arası elektronik ticaret danışmanları topluluğu
EDS	: Electronic Digital Signature (Russia)
EIA	: Electronic Industries Alliance (United States)
EMP	: Electromagnetic Pulse
EnCase	:A.B.D merkezli Guidance yazılım şirketi tarafından Adli Bilişim Analizi için yapılan ünlü delil bulma programı.
EO	: Executive Order (United States)
ETH	:Eidgenössische Technische Hochschule/Swiss Federal Institute of Technology,
EU	: European Union
FACA	: Federal Advisory Committee Act (United States)
FAPSI	:Federal Agency for Government Communications and Information (Russia)

FBI	: Federal Bureau of Investigation (United States)
FCCU	:Belçika Polis teşkilatı tarafından bilişim suçlarının Adli Analizi için açık kaynak kodlu yazılımlardan oluşan CD'den çalışan program.
FedCIRC	: Federal Computer Incident Response Center (United States)
FERC	: Federal Energy Regulatory Commission (United States)
FOIA	: Freedom of Information Act (United States)
FS/ISAC	: Financial Services Information Sharing and Analysis Center (United States)
FSB	: Federal Security Service of the Russian Federation (Russia)
G8	: Group of Eight
GAO	: General Accounting Office (United States)
GCERT	:Government Computer Emergency Response Team (Malaysia)
GCSG	:Communications-Electronics Security Group (United Kingdom)
HSPD	: Homeland Security Presidential Directive (United States)
I3P	:Institute for Information Infrastructure Protection (United States)
IA	: Information Assurance
IAAC	:The Information Assurance Advisory Council (United Kingdom)
IABG	: Industrieanlagen-Betriebsgesellschaft (Germany)
IAG	: Infrastructure Analysis Group
IAIP	:Directorate for Information Analysis and Infrastructure Protection (United States)
ICCP	:Committee for Information, Computer, and Communications Policy(OECD)
ICD	: Infrastructure Coordination Division (United States)
ICT	: Information and Communication Technologies
IETF	:(The Internet Engineering Task Force) İnternet Mühendisliğiyle Görevli Kuvvetler
IO	: Information Operations
ISACA	:(Information Systems Audit and Control Association) Bilgi Sistemleri Denetim ve Kontrol Birliği
ISF	: Information Sharing Forum (Malaysia)
ISIT	: Inter-Ministerial Board for Security (Germany)
ISP	: Internet Service Provider
IT	: Information Technology
ITIL	:(Information Technologies Infrastructure Library) Bilgi Teknolojileri Yapısal Kütüphanesi
ITAA	: Information Technology Association of America (United States)
MAMPU	:Malaysian Administrative Modernization and Management Planning Unit (Malaysia)
MCMC	:Malaysian Communications and Multimedia Commission (Malaysia)
MEWC	: Ministry of Energy, Water and Communications (Malaysia)
MoD	: Ministry of Defense
MOSTI	: Ministry of Science, Technology and Innovation (Malaysia)

MyCERT	: Malaysian Computer Emergency Response Team (Malaysia)
MyMIS	:Malaysian Public Sector Management of Information and Communications Technology Security Handbook (Malaysia)
NCI	: National Critical Infrastructures
NCS	National Communications System (United States)
NCSA	: National Cyber Security Alliance (United States)
NCSD	: National Cyber Security Division (United States)
NCSP	: National Cyber Security Partnership (United States)
NERC	: North American Electricity Reliability Council (United States)
NGO	: Non-Governmental Organizations
NHTCU	: National Hi-Tech Crime Unit (United Kingdom)
NIAC	: National Infrastructure Advisory Council (United States)
NIPC	: National Infrastructure Protection Center (United States)
NIPP	: National Infrastructure Protection Plan (United States)
NISCC	:National Infrastructure Security Co-ordination Centre (United Kingdom)
NISER	:National ICT Security and Emergency Response Centre (Malaysia)
NIST	:National Institute of Standards and Technology (United States)
NITA	: National IT Agenda (Malaysia)
NITC	: National Information Technology Council (Malaysia)
NOC	: Network Operation Centre (Russia)
NPSI	:National Plan for Information Infrastructure Protection (Germany)
NSA	: National Security Agency (United States)
NSAC	: National Security Advice Centre (United Kingdom)
NSSC	: National Strategy to Secure Cyberspace (United States)
OASD/NII	:Office of the Assistant Secretary of Defense for Networks and Information Integration (United States)
OCIIP	:Office of Computer Investigations and Infrastructure Protection (United States)
OEA	: Office of Energy Assurance (United States)
OECD	: Organisation for Economic Co-operation and Development
PARDUS	: Ulusal Açık Kaynaklı Linux İşletim Sistemi Projesi
PCCIP	: Presidential Commission on Critical Infrastructure Protection (United States)
PCII	:Protected Critical Information Infrastructure Programm (United States)
PCIS	: Partnership for Critical Infrastructure Security (United States)
PDD	: Presidential Decision Directives (United States)
PKI	: Public Key Infrastructure
PSD	: Protective Services Divison (United States)
PSYOP	: Psychological Operations
RANS:	Russian Association of Networks and Services (Russia)
RegTP:	Regulatory Authority for Telecommunications and Posts (Germany)
RIPN	: Russian Institute of Public Networks
RU-CERT	: Computer Emergency Response Team of Russia (Russia)

SEI	: Software Engineering Institute (United States)
S&T	:Science and Technology (United States)
TCK	: Türk Ceza Kanunu
TÜBİTAK- UEKAE	: Türkiye Bilimsel ve Teknik Araştırmalar Kurumu, Ulusal Elektronik Kriptoloji Araştırma Enstitüsü.
UNIRAS	:Unified Incident Reporting and Alert Scheme (United Kingdom)
USA PATRIOT	:(Act) Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (United States)
US-CERT	:United States Computer Emergency Response Team (United States)
WARP	: Warning, Advice, and Reporting Point (United Kingdom)

TABLOLAR LİSTESİ

Sayfa No.

ŞEKİLLER LİSTESİ

Sayfa No.

T.C.
HALİÇ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
YÖNETİM BİLİŞİM SİSTEMLERİ
YÜKSEK LİSANS TEZİ

ÜLKEMİZDE ADLİ BİLİŞİM LABORATUARLARININ KURULUMU ve BİLİŞİM SUÇLARIYLA MÜCADELEYE KATKISI

Hazırlayan
İlker ÇİÇEK

Tez Danışmanı
Prof.Dr.Ali OKATAN

İstanbul, Haziran 2008

ÖZET

Bilgi teknolojilerinin kaçınılmaz bir şekilde tüm hayatımızı etkilemesi, beraberinde suçlular için daha az bilgi ve tecrübe ile faydalanabilecekleri fırsatların doğmasına sebep olmuş, mahkemelerde dijital delil dönemi başlamıştır. Bu yeni dönemle birlikte suçla daha etkin mücadele edebilmek için ülkemizde standardize edilmiş ve sertifikalı bir adli bilişim laboratuarının kurulumu büyük önem arz etmektedir. Bu kapsamda bu çalışmada bilişim suçları konusunda ülkemizdeki kanuni, teknik ve uygulama alanındaki problemler incelenmiştir. Gelişmiş ülkelerin bu suç tipleriyle mücadelede uyguladıkları yöntemlere kıyasla, Türkiye Adli Bilişim'de henüz ilk basamaklarındadır. Ülkemizde akredite adli bilişim sürecine, laboratuarlarına ve uzmanlarına ihtiyaç vardır. Sadece yasal düzenlemelerle bilişim suçları konusunda yeteri başarı elde edilemeyecektir. Bundan dolayı, bu çalışma adli bilişim yeteneklerinin geliştirilmesine, akredite adli bilişim laboratuarının kurulumuna ve uluslar arası geçerliliği olan bilişim suçları mekanizmasına katkı sağlayacaktır. Ayrıca laboratuar ülkemizdeki adli bilişim uzmanların kabiliyetlerini yükseltecek ve mahkemelerde daha inandırıcı delillerin sunulmasını sağlayacaktır. Bunların yanında ulusal bilgi güvenliği sistemleri ve e-devlet çalışmalarını güçlendirecektir.

Key words: adli bilişim, bilişim suçları, adli bilişim laboratuarı

T.C.
GOLDENHORN UNIVERSITY
INSTITUDE OF SCIENCE
MANAGEMENT INFORMATION SYSTEMS
MASTER OF SCIENCE THESIS

BUILDING A COMPUTER FORENSIC LABORATORY IN OUR COUNTRY AND IT'S CONTRIBUTIONS ON STRUGGLE AGAINST COMPUTER CRIME

MASTER OF SCIENCE THESIS

Prepared By
İlker ÇİÇEK

Supervisor
Prof.Dr.Ali OKATAN

İstanbul, Haziran 2008

ABSTRACT

This thesis is a call for building a standardized and certificated computer forensics laboratory that has become vital with the rapid development of information technology which affects the whole part of our lives and provide crime opportunities even the ones that have only basic knowledge about computers. In this scope our country's legislations and the technical problems on the application side against the computer crime is examined. In comparison with developed countries' application method in the fight against computer crime committed towards individual and government, computer forensics is still in its early stages in Turkey. Certified computer forensics mechanism and certified specialists are needed. The struggle against computer crime can't be enough if it is only used in legal side. Hence, this study can be the basis to improve computer forensic capabilities, building a certificated laboratory, and establishing an internationally valid computer crime mechanism in our country. In this way, law enforcement will get more help from our laboratory. Also the laboratory enhances the ability of Turkey's computer forensic professionals and provides more convincing digital evidence in court. Furthermore, it can fortify national information security systems and the e- government environment.

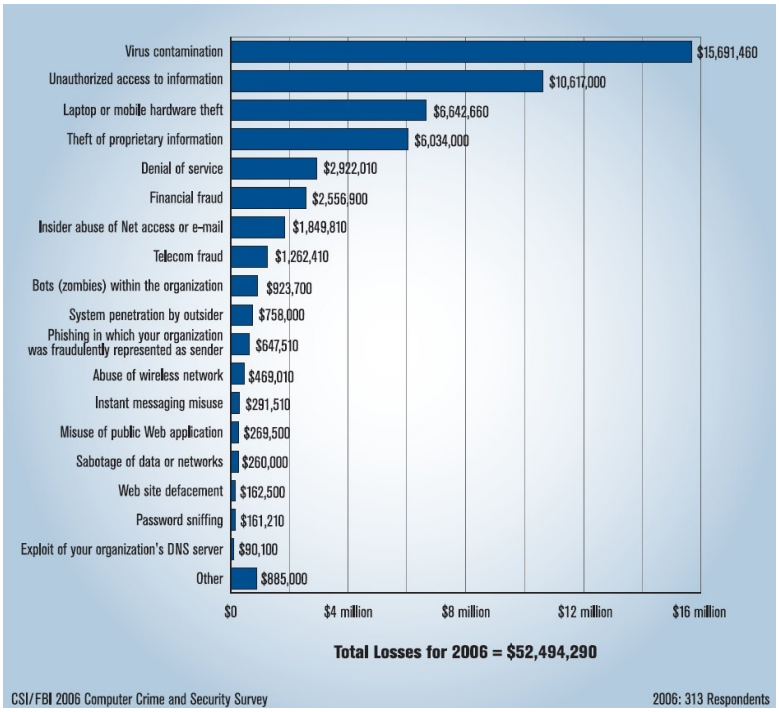
Key words: computer forensic, cyber laboratory, computer crime

1. GİRİŞ

Modern hayatın kritik sektörleri olan enerji, ulaşım, iletişim, bankacılık, sağlık hizmetleri ve benzeri kamu hizmetlerinde, verimlilik ve etkinliğin arttırılması amacıyla bilgi sistemleri teknolojilerine olan bağımlılık gün geçtikçe artmaktadır. Ancak gelişen teknolojinin suçlular tarafından da kullanılmasıyla, söz konusu sektörler risk altına girmiştir.

Amerika'da Bilgisayar Güvenliği Enstitüsü (Computer Security Institude, CSI) tarafından, FBI ile ortak olarak, her yıl güvenlik yöneticileri, CEO'lar ve direktörlerin katılımıyla hazırlanan anket tabanlı araştırmanın sonucunda; Tablo-1 ve Tablo-2'de görüleceği gibi bilişim suçları nedeniyle 2007 yılında 2006 yılına

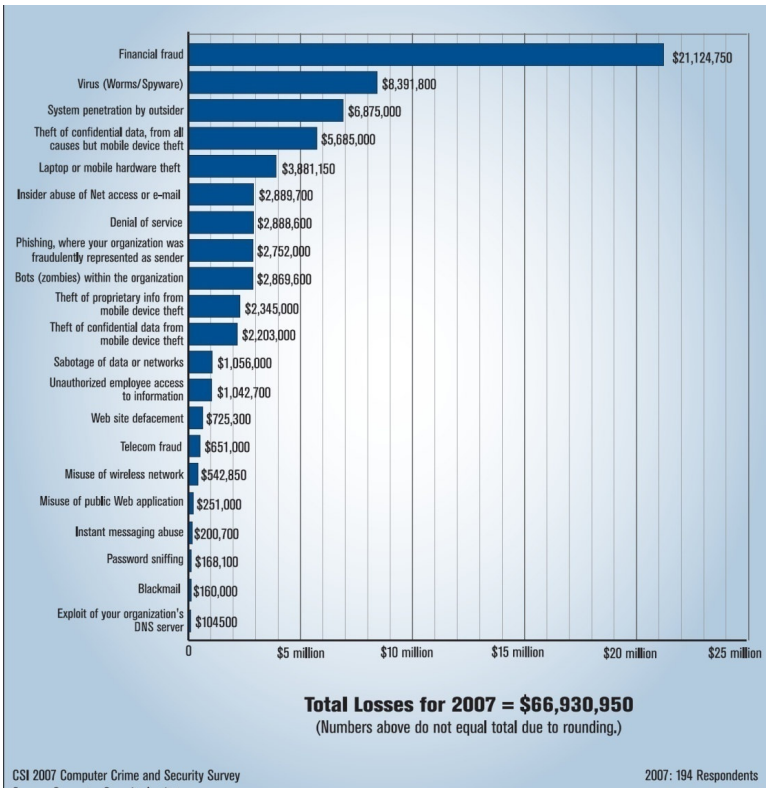
Tablo 1A- 2006 yılı Bilişim Suçu Tiplerine Göre Finansal Kayıp Miktarı



Kaynak: CSI/FBI 2006 Computer Crime Security Survey,s:15

göre finansal kayıplarda yaklaşık %28'lik bir artış olduğu görülmektedir. Ponemon Institute tarafından yapılan bir çalışmada ise, 2007 yılında şirketlerin bilgi kaybından dolayı zararının 6,3 milyar dolar (Ponemon Institude's 2007 Cost Of Data Breach Study)olduğu belirtilmiştir.

Tablo 1B 2007 yılı Bilişim Suçu Tiplerine Göre Finansal Kayıp Miktarı



Kaynak: CSI/FBI 2007 Computer Crime Security Survey,s:15

Kurumlar, finansal kayıpların yanında imajın zarar görmesi, müşteri güven kaybı gibi çok ciddi sonuçlarla karşılaşmaya başlamıştır. Bu etkenler uzun vadede bilişim suçu nedeniyle meydana gelecek zararın hesaplanmasını zorlaştırmaktadır.

Bunlara ek olarak bilişim suçlarının fail ve mağdur yelpazesi genişlemekte, mağduriyet seviyeleri çeşitlenmektedir. Kişisel tatmin, suç isleme, siyasi çıkar sağlama, ekonomik çıkar sağlama, bilgi toplama, savunma, terörizm veya psikolojik harekât maksadıyla; kişiler, devletler, hükümetler, şirketler, yöneticiler, suç örgütleri, muhalifler, teröristler ve casuslar fail veya mağdur olabilmektedir (Öztürk,2007,s.:9).

Tüm bu veriler ışığında, dünyada güvenlik güçleri enerjilerini, klasik suçlardan çok bu konulara yönlendirmiş, kamu güvenliği ve ulusal güvenlikte öncelikli tehdit olarak bilişim suçları kavramı yer almaya başlamıştır(Yen ve Chen,2006,s.:1). Bu doğrultuda mahkemelerde dijital delil dönemi başlamıştır.

Son yıllarda ülkemizde de çok sık gündeme gelmeye başlayan bilişim suçları konusunda yasal mevzuatta güncellenme çalışmalarına rağmen, hukuki süreci

destekleyecek teknik altyapı konusunda yeterli çalışma eş zamanlı olarak yapılamamıştır.

Ayrıca bilişim suçları ile mücadele, sadece kolluk kuvvetiyle değil; kamu kurumları ile özel kurumlar ve üniversitelerle işbirliği içerisinde yapılması gereken kapsamlı bir çalışmadır.

Bu noktada, siber çağın yöntemleriyle gerçekleştirilen suçların tespiti ve kanıtlanması sürecinde; yasal düzenlemeler ile uyumlu, standartları belirlenmiş, akredite uzman personeli olan, uluslararası sertifikalara sahip ve üniversitelerle işbirliği içerisindeki adli bilişim laboratuarlarının kurulması önem arz etmektedir.

Bu amaçla, bu çalışmada, bilişim suçları sürecinin hukuki, uygulama ve teknik alanındaki sorunları ortaya konmuş; konuyla ilgili literatürdeki uluslararası çalışmalar incelenerek, adli bilişim laboratuarlarının kurulumu için çeşitli öneriler getirilmiştir.

2. BİLİŞİM SUÇU, ADLİ BİLİŞİM ve DİJİTAL DELİL KAVRAMI

2.1.Bilişim Suçu

Bilginin, programların, servislerin, ekipmanların veya haberleşme ağlarının yıkımı, hırsızlığı, yasadışı kullanımı, değiştirilmesi veya kopyalanması, "Bilişim suçları" olarak tanımlanmaktadır(Perry,1986).

Avustralya, Sydney Üniversitesi, Bilişim Sistemleri Fakültesi öğretim üyesi, Dr. Jim Underwood, bilişim suçunu; "Geleneksel suçlardan olan, hırsızlık, dolandırıcılık, sahtecilik ve cinsel istismar gibi suçların, bilgisayar veya bilgisayar ağı kullanılarak işlenmesi" olarak tanımlasa da uygulamada bu tip suçlara "Bilişim Sistemleri Aracılığıyla İşlenen Suçlar" da denmektedir.

Birleşik Devletler, Adalet bakanlığı bilişim suçunu; Bilişim teknolojisi kullanılarak yapılan her türlü yasadışı eylem (USDOJ, 2004)olarak tanımlamış ve bilişim suçlarını yukarıdaki tanımlardan daha geniş kapsamlı ele almıştır.

Ülkemizde yeni Türk Ceza Kanunu kapsamında bu tip suçlar Bilişim Suçları ve Bilişim Sistemleri Aracılığıyla İşlenen Suçlar olarak görülmektedir. Bu kavramlar üçüncü bölümde detaylı olarak incelenmiştir.

2.2.Adli Bilişim

Günümüzde kriminal araştırmalar yürütülürken birçok bilişim sistemi ile karşılaşılmaktadır. Ancak bunlar, delil toplama prosedürlerine uygun olarak toplanırsa araştırmanın gidişatını değiştirebilir(Ashcroft, 2001, s.:9). Dolayısıyla adli bilimlerin içerisinde adli bilişim teknolojiye paralel olarak gelişen, karmaşıklaşan ve ihtiyacı artan bir bilim olarak ortaya çıkmaktadır.

Adli Bilişim (Computer Forensics) bilimi; suçun aydınlatılabilmesi için bilimsel metodolojiler kullanılarak, çeşitli varyasyonlardaki dijital medyalar üzerinde bulunan, suçla ilgili dijital delillerin bozulmadan ve zarar görmeden anlaşılabilir bir şekilde adalet önüne sunulmaya hazır hale getirilmesini sağlayan ve başlı başına bilimsel teknik prensiplerin uygulandığı bir delil inceleme sürecinin bütünüdür.(Ekizer,2007,s.:1)

2.3.Dijital Delil

Günümüzde bilişim suçu kapsamına girmeyen suçlarda da suçluların bilişim cihazları kullanmaktadır. Dolayısıyla, unutulmamalıdır ki her bilişim suçu bir sayısal delil kaynağıdır, ancak sayısal delil kaynağı olabilecek tek suç türü değildir(Öztürk,2007,s.:7).

Bu tip suçlarda olay yerinin incelenmesi ise başlı başlına uzmanlık gerektiren bir konudur. Adli Önleme ve Aramaları Yönetmeliği'ne dayanarak olay yeri incelemesi; suçun aydınlatılması amacıyla olay yerlerinde her türlü iz, eser, emare ve delil niteliği taşıyabilecek bulguların uzmanlaşmış personelce, çeşitli bilimsel, teknik yöntem ve metot kullanarak araştırılması, elde edilen bulguların tespit edilmesi ve kayıt altına alınması (belgelenmesi), toplanması, muhafazası ve incelenmek üzere ilgili yerlere gönderilmesini sağlayan özel amaçlı bir araştırma işlemi olarak tanımlanabilir. Olay yeri incelemesinde amaç;

- Meydana gelen bir olayın adli bir suç olup olmadığını tespit etmek,
- Olayın öngörülen şekil ve şartlarda meydana gelip gelmediğini belirlemek,
- Olay yeri-fail-mağdur (veya maktul) arasındaki ilişkiyi kuracak maddi suç delillerini bulmak,
- İşlenen suçun aydınlatılması ve adli mercilerin doğru karar vermesini sağlamak amacıyla olay yerini belgelemek,

• Olay soruşturmasında ve çözümünde olay yeri-fail-mağdur ilişkisinin ortaya çıkarılmasıdır. (Bayer ve Kaygısız, 2002, s.:10)

Bu amaçlara ulaşmak için olay yerinde bulunan delillerin ne oldukları ve nerelerde aranması gerektiği bilinmelidir. Dijital deliller genel olarak;

• Sabit diskler, CD, DVD ve disketler
• Harici diskler(USB Hardisk ve USB Flash disklerde)
• ZIP, DAT, DLT gibi teyp veri yedekleme birimleri
• Hafıza kartları (SD, MMS, CF, Memory Stick vs)
• Dijital kameralar ve fotoğraf makineleri, MP3 çalarlar
• El bilgisayarları (PDA, PALM, PocketPC vs)
• Cep Telefonları
• Oyun konsolları
• Bazı yazıcı ve faks cihazları
• Network cihazları
• İnternet ve network ortamlarında (canlı akışkan delil) vb. olarak sıralanabilir.

Bunlara ek olarak veri depolama yetisine sahip her türlü cihaz dijital delil içerme potansiyeline sahiptir(Ekizer,2007). Örneğin GPRS, GPS gibi sistemler, araçların nerede olduğunun tespiti için kullanıldığı gibi, araçların üzerine yüklenecek gömülü bilgisayar sistemine sahip modüller sayesinde aracın hızı, frenlerin durumu, olaydan önceki 5 saniye içerisindeki işlevler gibi bir kaza esnasında oldukça yararlı ve kazayı aydınlatıcı bilgilere ulaşılabilmektedir. Günümüzde, gömülü bilgisayar sistemlerine sahip mikro dalga fırınlar, internet üzerinden bilgi alışverişi yapabilmekte ve bazı ev aygıtları, kablosuz ağ veya internet kullanılarak uzaktan kumanda edilebilmektedir. Teknolojinin bu seviyede olduğu bir ortamda, mikro dalga üzerinden elde edilecek veriler, bir kundakçılık olayında fırının belirli bir zamanda yangın çıkarmak için programlandığını ortaya çıkarabilmektedir. (Uzunay,2005,s.:3)

Yukarıda bahsedilen sistemlerden elde edilebilecek sayısal delillerin muhtevasında genel olarak aranması gerekenler şunlardır:

• Marka/model/seri numarası: Bu özellikleri aranacak olan cihaz, bilgisayarın kendisi veya içerisindeki donanımlar (anakart, işlemci, ses, grafik, yedekleme birimi

vb.), internete çıkmak için kullandığı donanımlar, yazıcı, tarayıcı vb. olabileceği gibi işletim sistemi ve delil niteliği olabilecek dijital herhangi bir cihazdır.

- O andaki mevcut durumu(çalışır halde, arızalı, belirli bir işlemi gerçekleştiriyor vb.)
- O an bağlı olan yada boşta duran bağlantı kabloları, portları vb. teknik özellikleri
- Yedekleme birimi teknik özellikleri
- Yazılımlarda/veritabanlarında ürünün versiyonu, lisanslama özelliği, yüklü olan yamalar
- Yazılımların amacı
- Yazılımların mevcut durumu (çalışır halde, hatalı, son yaptığı işlem vb.)
- Yazılımların kurulumu için gerekli ön şartlar
- Yazılımların kurulum bilgileri ve yapılandırma ayar dosyaları
- İşletim sistemi veya yazılım tarafından tutulan geçici, kalıcı veya silinen Tüm kütüphane/dosya/kayıt/verilerin içerikleri ve kimlikleri (metadata)
- Eylemin işletim sistemine, yazılıma, donanıma etkileri
- Ticari olmayan kurumsal veya kişisel amaçla hazırlanmış olan yazılım/yazılımların kaynak kodları
- Yazılımlarda tanımlı bulunan kullanıcı kimlikleri
- Yazılımların yetkilendirme politikası
- Yazılımların erişim politikası
- Yazılımların güvenlik politikası ve şifreler
- Silinen dosyalar ve tarih saat bilgileri
- Dökümanlar, Kelime işlemci dosyaları, resimler, ses ve video dosyaları
- Veri tabanı dosyaları, veri tabanı erişim kayıtları
- E-Mail veya chat kayıtları, internet geçmişi.
- Erişim şifreleri ve kullanıcı adları.
- Şifrelenmiş veya kriptolanmış dosyalar
- Dosya yetkileri ve tarihleri (oluşturma, erişim, silme vs)
- Sistem Kayıt bilgileri (Registery, Event Log vs)
- Sistem tarafından verilen hizmetler
- Virus, Trojan, SpyWare vs gibi zararlı yazılımlar.
- Sanal Disk alanları ve RAM bilgileri

- EPROM ‘dan elde edilen veriler ve ağ üzerinde uzaktan erişim özellikleri
- İşletim sisteminin dosya sistemi türü (FAT, NTFS, EXT2, EXT3, vb.) ve disk bölümlemeleri
- İşletim sisteminin yapılandırma ayar dosyaları (config, registry vb.)
- İşletim sisteminde tanımlı olan harici donanım birimleri
- İşletim sisteminde tanımlı yetkilendirme politikası
- İşletim sisteminde tanımlı erişim politikası ve açık olan portlar
- Kullanıcı tarafından çalıştırılan işletim sistemi seçenekleri (virüs kontrolü, ateş duvarı, vb.)
- Görev yöneticisi vasıtasıyla tespit edilebilen uygulamalar ve işlemler
- İşletim sistemi açılış ve kapanış politikası
- İşletim sistemi açılırken ve kapanırken çalışan yazılımlar
- Bir yazılım marifetiyle ağ üzerindeki başka bilgisayar ve/veya cihazın her türlü veri trafiği dinlenerek elde edilen veriler
- Bilişim sistemine veri girişi ve çıkışı amacıyla kullanılan yazıcı, tarayıcı, çizici, kesintisiz güç kaynağı, web kamerası, mikrofon, klavye, barkot okuyucuları, küresel konum belirleme (GPS) cihazları
- Sabit disk, taşınabilir disk, disket, CD, DVD, bellek çubukları, bellek kartları, harici sürücüler, ZIP, DAT, DLT gibi Teyp/Kaset/Kartuş yedekleme ünitelerinde veri tabanı dosyaları yedekleri, e-posta sunucu dosyaları yedekleri sistem kayıtlarının yedekleri, yedekleme biriminin dosya kayıt sistemi (NTFS, FAT, EXT2,EXT3 vb.) ve bölümlemeleri, yedekleme biriminin paylaşım/erişim özellikleri dijital delil olarak incelenir ancak bu tür yedekleme ünitelerinin genellikle sunucular tarafından kullanılır. Verileri uzun süre saklama ve büyük miktarlarda veri saklama kapasitesine sahip bu tarz yedekleme ünitelerinde genellikle sistemler üzerinde bulunan dosyaların veya kayıtların yedekleri bulunmakla birlikte, çoğunlukla yedekler özel yazılımlarla farklı formatlarda sıkıştırılmış halde bulundukları göz önünde bulundurulmalıdır.
- Ağ iletişim cihazının türü (Modem, yönlendirici, hub, switch, vb.)
- Ağın konfigürasyon yapısı
- Erişim ve yönlendirme bilgileri

- Erişim denetim listeleri
- Donanım tabanlı cihaz listeleri (MAC adresi)
- Ağ üzerinde oluşmuş bazı arıza bilgileri
- Ağın performans ve kullanım bilgileri
- Ağ üzerindeki yetkisiz erişim bilgileri

- Teknik dinleme sonucu bilişim ağı üzerinden akan sayısal verinin elde edilmesi ve çözümlenmesi ile elde edilen veriler

- Cep telefonu, çağrı cihazı, sayısal kamera ve fotoğraf makinesi, özel amaçlı kameralar (ısıya hassas, kızıl ötesi, vb.), fotokopi makinesi, ATM cihazı, elektronik ajanda, faks makinesi, elektronik veri bankası, akıllı kart, POS makinesi gibi entegre cihazlardaki sayısal deliller

Bu sayılanlara ilave olarak verilerin sürekli olarak akışkanlık gösterdiği internet ve ağ ortamlarında da dijital delil elde etmek mümkündür. Bilgisayar ortamlarında bulunması muhtemel birçok dijital veri, delil olarak Stallabrass'ın[1] özgürlükler cenneti olarak bahsettiği internetten de elde edilebilir.

İnternet ortamından elde edilebilecek sayısal delil muhtevası aşağıdaki başlıklardan oluşabilir:

- İnternete bağlantı sekli (kurumsal ağ, ADSL, kablosuz, vb.)
- İnternet bağlantısı için kullanılan şifreler
- Üzerinden bağlantı sağlanan internet servis sağlayıcısı bilgileri
- Tespit edilebilen son bağlantı yaptığı site adresleri
- Söz konusu sitelerin türleri (haber, eğlence, forum, vb.)
- Bağlanılan sitelerin özellikleri (üyelik sistemi, başka bir adrese yönlendirmeli, bağlantı sonrası bir program yüklemeli, vb.)

[1] "İnternet bir özgürlükler cennetidir. Özgürleşme ifadede baslar ve giderek zamana ve mekâna, vücut ve görüntü gibi fiziki bütün özelliklere ve hatta kimliğe kadar uzanır. Kullanıcılar dünyanın neresinde olurlarsa olsunlar internete girdikleri anda zaman ve mekân anlamını yitirir. İnsanın görüntüsü ve vücudu ile ilgili özellikler de bu sanal dünyada ağırlıklarını kaybetmektedir. İnternet üzerinden haberleşenler istedikleri kişiliği, rolü, cinsiyeti ve varlık biçimini denemek sansına sahiptirler" (Stallabrass, 1995).

- Söz konusu sitelerin tespit edilen sayısal kimlikleri (IP adresi, etki alanı (domain), sahibi, hizmetin verildiği ülke, vb.) bağlantı için kullanılan internet tarayıcısının marka ve sürümü
- Kullanılan internet tarayıcısının aktif olan özellikleri
- İnternete bağlantı sonucu oluşan tüm geçici ve kalıcı kayıtlar
- İnternet ortamında iletişim ve sohbet için kullanılan yazılımlar (MSN Messenger, ICQ, Skype, vb.)
- İletişim veya sohbet yazılımlarının ürettiği geçici veya kalıcı kayıtlar
- Kullanılan elektronik posta hizmet programları (Outlook Express, Thunderbird, The Bat, Windows Live Mail Desktop vb.)
- Elektronik posta hizmet programlarının kullandığı ve ürettiği kalıcı, geçici ve silinen kayıtlar
- Gelen ve giden elektronik posta sahipleri ve alıcıları
- İnternet ortamında kullandığı takma isim/isimler (nickname)
- Şifre ile girilen sitelerde kullanılmakta olan "Beni hatırla" seçeneğinin işaretlenmiş olması ihtimali göz önünde bulundurularak bu tür sitelerde kullanılan şifre dosya/kayıtları
- Forum, sohbet (chat) veya arkadaşlık gibi internet siteleri sıklıkla olmak üzere kullanıcının girdiği veriler ve kullanımla ilgili günlük ve tarihçeler
- Kullanımı yaygınlaşmaya başlanan IP tabanlı telefon sistemlerinin tuttuğu kayıtlar
- Web kamerası tarafından kaydedilen görüntüler
- İnternet bağlantılarının denetlenmesi maksadıyla kullanılan içerik filtreleme yazılımları, ateş duvarı yazılımları veya saldırı önleme yazılımları tarafından tutulan kayıtlar ve günlük ve tarihçeler
- İnternet servis sağlayıcıları tarafından internet bağlantıları ile ilgili tuttuğu veriler
- Ağ kaynaklarını kullanan yazılım/yazılımlar ve kullandıkları portlar
- Teknik dinleme sonucu internet üzerinden akan sayısal verinin elde edilmesi ve çözümlenmesi ile elde edilen veriler

Bu sıralanan delil türleri teknolojideki gelişmeye paralel olarak sürekli çeşitlenmektedir. Ancak delillerin elde edilmesi (Acquisition), tanımlama (Identification), değerlendirme(evaluation) ve sunum(presentation) aşamalarında dijital delillerin özellikleri ve sahip olduğu hassasiyetlerini göz önünde bulunduran

bilimsel temellere dayanan metodolojiler kullanıldığı sürece adalete ihityacı olan destek verilebilecektir.

2.3.1.Dijital Delillerin Özellikleri

Yukarıda bahsedilen sayısal delillerin davada etkinlik sağlayabilmesi için, mahkeme önüne getirilmeden önce diğer maddi delillerin sahip olması gereken özelliklere de sahip olması gerekir(Keser Berber, 2004). Bu özellikler:

- Kabul olunabilir: Yasal yollardan elde edilmemiş olması
- Gerçeklik: İddiamızı doğrulayan gerçeklikte olması
- Tamlık: Tek bir bakış açısından değil tüm açılardan bakıldığında aynı sonucu göstermesi
- Güvenilirlik: Delilin elde edilmesi konusunda herhangi bir kuşkuya yer vermemesi
- İnanılırlık: Mahkeme tarafından kolaylıkla inanılabilir ve anlaşılabilir olmalısı olarak sıralanmaktadır.(Anderson ve Mohay, 2003, s.:35)

Hosmer ise sayısal delillerin, normal delillere göre yapı itibariyle barındırdığı hassasiyetleri şöyle sıralamaktadır:

1. Sayısal Delilin Bütünlüğü İlkesi: Sayısal delillerin doğası gereği kolaylıkla kasti veya yanlışlıkla silinmesi, değiştirilmesi veya bozulması mümkündür. Bu nedenle öncelikle sayısal verilerin bütünlüğüne bir zarar gelmemesi önem taşımaktadır.

2. Sayısal Delilin Doğrulanması İlkesi: Sayısal delil ele geçtikten sonra adli süreç içinde söz konusu verilerin gerçekten o olaya veya şüpheliye ait olduğunun ispatı gerekmektedir. Fakat delil olarak ele geçirilen verilerin aynısı her hangi bir kişi tarafından da oluşturulabilir. Hatta şüpheli tarafından bu verilerin daha sonra, kolluk kuvveti tarafından oluşturulduğu bile iddia edilebilir. Soruşturma sürecinde sayısal verilerin olay veya şüpheliyle ilişkisi teyit edilmelidir.

3. Sayısal Delilin Doğruluğu İlkesi: Sayısal delillendirme işlemindeki sayısal delilin kişisel veya kurumsal sahibi, onu ele geçiren kolluk birimi, delilin alındığı elektronik ortam, delilin ele geçirildiği zaman, delilin içeriği gibi bütün unsurların doğruluğunun daha sonradan inkâr edilemeyecek şekilde belgelenmesi gereklidir.

4. Sayısal Delilin İnkâr Edilemezliği İlkesi: Sayısal delillerin ele geçirilmesi esnasında kullanılan teknikler ve kullanılan bilgilerin doğruluğunun gerektiğinde tüm adli süreç boyunca bütününde ispatı gereklidir.

5. Sayısal Delilin Yeniden Ele Alınabilirliği İlkesi: Sayısal deliller oluşturulduktan sonra, bu delilleri istendiğinde üçüncü bir şahıs inceleyebilmeli ve yeniden oluşturabilmelidir.(Hosmer,2002,s.:4)

Bir bilişim suçunda sorun ne kadar karmaşık olursa olsun kolluğun her soruşturmada kabul ettiği en temel kural; "Her Temas Bir İz Bırakır" dır. Bir suçlu arkasında işlediği suçla ilgili yukarıda belirtilen delil, iz ve emareleri yada teknolojinin gelişimine paralel olarak bunlara eklenecek yeni emareleri bırakmaması neredeyse imkansızdır. Ancak kolluk, suç işlenirken kullanıldığı değerlendirilen teknolojik cihazlara nasıl müdahale etmesi gerektiğini, muhtemel delillerin nasıl toplanacağını, topladığı delilleri nasıl nakletmesi gerektiğini iyi bilmediği ve kurallara uymadığı takdirde, suçun ispatı için kullanılması muhtemel delilleri farkında olmadan karartmak veya eksik araştırma yapmak suretiyle çözümü çok zor problemler ile mücadele etmek zorunda kalmış olacaktır(Ortabağ,2008).

3. ÜLKEMİZDE BİLİŞİM SUÇLARI YLA İLGİLİ MEVZUAT İLE ADLİ BİLİŞİMİN İLİŞKİSİ

Bilişim teknolojisinin gelişmesiyle bilginin ekonomik, sosyal, siyasal değerinin artması, bu güce sahip olmak isteyen kişileri bilişim teknolojileri kullanarak suç işler hale getirmiştir. Bununla birlikte bilişim suçları diğer geleneksel suçlardan farklı olarak yeni kanunlar ve yeni araştırma teknikleri gerektiren bir alandır (Brenner, 2001). Ülkemizde, başta yeni TCK olmak üzere konu üzerinde çalışmalara başlanmıştır.

26 Eylül 2004 tarihinde kabul edilen, 5237 sayılı Türk Ceza Kanunu kapsamında, Bilişim Suçları;

TCK Md.158/1-f – Nitelikli Dolandırıcılık,

TCK Md.243/1, 243/2, 243/3– Bilişim Sistemine Girme,

TCK Md.244/1, 244/2, 244/3, 244/4 – Sistemi Engelleme, bozma, verileri yok etme veya değiştirme,

TCK Md.245/1, 245/2 – Banka ve Kredi kartlarının kötüye kullanılması,

TCK Md.239/1, Md.239/2, Md.239/3 – Ticari sır, bankacılık sırrı veya müşteri sırrı niteliğindeki bilgi veya belgelerin açıklanması,

TCK Md. 327, Md. 328, Md. 329, Md. - Devletin güvenliği veya iç veya dış siyasal yararları bakımından, niteliği itibarıyla, gizli kalması gereken bilgiler,

TCK Md. 135 - Verilerin kaydedilmesi,

TCK Md. 138 - Verilerin yok edilmesi,

TCK Md. 132 - Haberleşmenin gizliliğini ihlal,

TCK Md. 124 - Haberleşmenin engellenmesi maddelerinde yer alan hususlardır.

Bilişim Sistemleri aracı kılınarak işlenen suçlar ise:

TCK Md. 125 - Hakaret,

TCK Md. 142 - Bilişim sisteminin kullanılması yoluyla hırsızlık,

TCK Md. 158 - Bilişim sistemi yoluyla dolandırıcılık,

TCK Md. 226 - Müstehcenlik,

TCK Md. 228 – Kumar,

TCK Md. 107 – Şantaj,

TCK Md. 28 - Cebir şiddet, korkutma ve tehdit,

TCK Md. 103 - Çocukların cinsel istismarı,

TCK Md. 191 - Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma maddeleri ile Fikir ve Sanat eserleri kanununda belirtilen hususlardır.

Bilişim suçları ile mücadeledeki zorlukları aşmak amacıyla yeni TCK sonrasında ve 2007 yılı içerisinde de düzenlemeler yapılmıştır. Örneğin 01 Haziran 2005 tarihli Resmi Gazete'de yayınlanan Suç Eşyası Yönetmeliği Madde 9'da, el konulan bilgisayar malzemelerinin nasıl saklanması gerektiği anlatılmaktadır. Ayrıca;

- 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun (23 Mayıs 2007),

- İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik(1 Kasım 2007),

- İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul Ve Esaslar Hakkında Yönetmelik(30 Kasım 2007) yürürlülüğe giren diğer düzenlemelerdir.

Burada bahsedilen yasal düzenlemeler ve yaygınlaşan e-devlet uygulamalarının beraberinde getirdiği riskler nedeniyle, yargı organlarının; bilişim suçlarının tespit edilmesi, incelenmesi, araştırılması ve mahkemede delil olabilecek şekilde hazırlanmasını konu edinen bir bilim dalı olan Adli Bilişime ilgi ve ihtiyacı zorunlu olarak artmıştır.

Ancak mevzuattaki yasal düzenlemeler, artan ihtiyacı karşılamakta yetersiz kalmaktadır.

Örneğin, CMK Madde 134'de bilgisayarlarda, bilgisayar programlarında ve kütüklerinde arama, kopyalama ve el koyma işlemleri ile ilgili aşağıdaki düzenlemeler getirilmiştir:

(1) Bir suç dolayısıyla yapılan soruşturmada, başka surette delil elde etme imkânının bulunmaması halinde, Cumhuriyet savcısının istemi üzerine şüphelinin kullandığı bilgisayar ve bilgisayar programları ile bilgisayar kütüklerinde arama yapılmasına, bilgisayar kayıtlarından kopya çıkarılmasına, bu kayıtların çözülerek metin hâline getirilmesine hâkim tarafından karar verilir.

(2) Bilgisayar, bilgisayar programları ve bilgisayar kütüklerine şifrenin çözülememesinden dolayı girilememesi veya gizlenmiş bilgilere ulaşılamaması halinde çözümün yapılabilmesi ve gerekli kopyaların alınabilmesi için, bu araç ve gereçlere elkonulabilir. Şifrenin çözümünün yapılması ve gerekli kopyaların alınması halinde, elkonulan cihazlar gecikme olmaksızın iade edilir.

(3) Bilgisayar veya bilgisayar kütüklerine elkoyma işlemi sırasında, sistemdeki bütün verilerin yedeklemesi yapılır.

(4) İstenmesi halinde, bu yedekten bir kopya çıkarılarak şüpheliye veya vekiline verilir ve bu husus tutanağa geçirilerek imza altına alınır.

(5) Bilgisayar veya bilgisayar kütüklerine elkoymaksızın da, sistemdeki verilerin tamamının veya bir kısmının kopyası alınabilir. Kopyası alınan veriler kâğıda yazdırılarak, bu husus tutanağa kaydedilir ve ilgililer tarafından imza altına alınır.

Bu son madde kapsamında kopyası alınan verilerin yazdırılması uygulanabilirliği tartışmalıdır.

Adli ve Önleme Aramaları Yönetmeliği Madde 17'de, el koyma işlemini bilgisayar ağları, uzaktaki bilgisayarlar ve çıkarılabilir donanımlar için de geçerli kılmaktaysa da ancak bu maddelere ek olarak, inceleme yapan şahıs ya da birimin uygulayacağı teknikler veya sunacağı rapor konusunda standartları belirleyen düzenlemelere de ihtiyaç vardır.

Savcılar veya mahkemeler, CMK Üçüncü Kısım İkinci Bölümde yer alan maddelere göre bilirkişi atamakta ve cihazlarda delil aranması işlemini; polis, jandarma adli bilişim laboratuarları, "İl Adlî Yargı Adalet Komisyonları bilirkişi Listeleri" nde yer alan kişi ya da kurumlara veya CMK madde 64 2. Fıkrasında verilen yetkiyle, o konuda uzman bir başkasına yaptırabilmektedirler.

Kısacası adli bilişim laboratuarları ve bilirkişi tayininde savcı veya mahkemeler geniş yetkilere sahiptir. Ancak bu yetkiyle birlikte bilirkişi ya da kurumlarda ulusal veya uluslararası sertifika aranması zorunluluğu da getirilmelidir.

Yukarıda bahsedilen konular nedeniyle, uygulamanın delil incelemesi aşamasında birçok problemle karşılaşılmaktadır.

4. ADLİ BİLİŞİM SÜRECİNDE KARŞILAŞILAN PROBLEMLER

a) Bir suçlunun arkasında işlenilen suçla ilgili delil, iz ve emare bırakmaması insanoğlunun elinde olmadığından, bilişim sistemleri ile işlenilen suçlarda suç ile ilgili deliller farklı şekil ve formatlarda suç sonrasında dijital delil olarak bulunabilmektedir.

Ancak bilişim suçları konusunda dikkat edilmesi gereken özel konular vardır(Uzunay,2005,s.:1).

Ülkemizde delillere el koyma sürecinde işlemler yapılırken nelere dikkat edileceği hususu ile standartlar ve sorumluluklar henüz herhangi bir mevzuatta net olarak belirtilmemiştir. Sonuç olarak uygulamada birçok delil, daha en başta geri dönülmeyecek şekilde kaybolabilmektedir.

Son zamanlarda mevcut problemlerin çözümü için kolluk kuvvetlerinde çeşitli çalışmalar yapılmaktadır. Örneğin, kolluk kuvvetleri çalışmada standartlaşma sağlamak için EK-1'de görüleceği gibi kendi akış şemalarını oluşturmaktadır. Emniyet Genel Müdürlüğünde, bilişim suçlarıyla ilgili delil tespitleri ve kovuşturma,

İstanbul[2], Ankara ve İzmir'de Bilişim Suçları ve Sistemleri Şube Müdürlükleri tarafından yürütülmektedir. Jandarma Genel Komutanlığı'nda ise; şuan ülkemizdeki uluslararası standartlara en yakın laboratuar, Kriminal Daire Başkanlığı bünyesinde Bilişim Teknolojileri İnceleme Şube Müdürlüğü adı altında açılarak, 15 Eylül 2007 tarihinden itibaren aktif olarak, cep telefonu, sabit disk, SIM kart, multimedya kart ve çeşitli veri kartlarını inceleme konularında hizmet vermektedir. Ayrıca birimde görevli bilişim uzmanları tarafından, Olay Yeri İnceleme Timlerine, bilişim suçlarında olay yeri incelenmesi, delillere el konulması ve muhafazası konusunda eğitim verilmektedir.

b) Bilgisayar veya ağ sistemlerinin incelenmesinde hâkim ya da savcıların geniş yetkilere sahip olmasına rağmen, teknik anlamda yeterli bilgiye sahip olmamaları ve onları bu konuda yönlendirecek standartların bulunmaması nedeniyle, zaman zaman ehliyet sahibi olmayan kişileri bilirkişi olarak atadıkları görülmektedir(Özel ve Ahi,2005,s.:2).

c) Adli Tıp Kurumundaki Fizik İhtisas Dairesi Başkanlığı aslında adalet teşkilatı içinde adli bilişim konusunda resmi bilirkişilik yapmak üzere 2004 yılında kurulan bir birimdir. EK-2'de yer alan Delil türlerine göre kurumsal önem kıyaslaması tablosunda görüleceği gibi halen kurulumu tamamlanamayan birim olarak yeterli hizmeti verememektedir.

d) Ülkemizde bilişim suçları konusunda BT(bilişim teknolojileri) uzmanlarına danışılmaktadır. Ancak dijital delillerin, mahkeme esnasında gerçek delil özelliği gösterebilmesi için delillerin bütünlüğünün, doğrulanmasının, inkâr edilememesinin, doğruluğunun ve daha sonradan ele alınabilirliğinin sağlanması gereklidir(Hosmer,2002). Dolayısıyla bilişim suçları soruşturmacısı ve adli bilişim uzmanı olabilmek, bu alanda yetkin sayılabilmek için sadece bilişim sistemleri konusunda ileri seviyede bilgi sahibi olmak yeterli olmayacak kriminalistik bilimindeki gibi özel uygulamaların nasıl yürütüleceğinin bilinmesi ve bununda bilirkişi olabilecek şekilde yetki belgesiyle belgelendirilmesi gerekmektedir. Örneğin kimyager olmak farklı bir şeydir, uyuşturucu maddeler konusunda kimyasal kriminalistik uzmanı olmak farklı bir şeydir. Bu yüzden her bilişim sistemleri uzmanı

[2] Bilişim Suçları ve Sistemleri Şube Müdürlüğü 03.09.2007 tarihinde Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığına bağlı olarak, İstanbul Emniyet Müdürlüğü bünyesinde faaliyete geçirilmiştir. http://bilisimsuclari.iem.gov.tr/

bilişim suçları yada adli bilişim uzmanı olarak değerlendirilmemeli, bu aldaki almış olduğu özel eğitimler ve yetki belgelendirilmelerine bakılmalıdır.(Ekizer,2007)

e) Uygulamada kamu bilişim laboratuarları olayların çok az bir kısmında inceleme yapmaktadır(Demirbilek, 2008). Bu oranın düşük olmasının nedeni, yeterli laboratuar olmaması ve bilirkişi seçiminde savcı veya hâkimlerin bilirkişileri atarken tercihlerini o doğrultuda kullanmamasıdır.

f) Dava ile ilgilenen hâkim/savcı, raporun sonuç bölümüne bakarak karar vermektedir. Mahkemede davacı ve hükümlülerin rapora bir itirazı olduğunda yeniden inceleme için bilirkişi ya da kriminal laboratuarlarına gönderilmektedir. Bu raporu düzenleyen şahıs ya da kurumlarda, ulusal ya da uluslararası herhangi bir standart aranmaması veya tescilli kurumsal bir yapılaşmaya gidilmemesi nedeniyle yeterli inceleme yapılıp yapılmadığı ve delil bütünlüğünün bozulup bozulmadığı konusu net değildir.

g) Bilirkişiler siber suç ile ilgili delilleri tespit ederken herhangi bir standart izlememekte ve lisanssız program kullanabilmektedirler. Ortaya konulan raporda da yine standart bir format yoktur. Mevcut uygulama uluslararası mahkemelerde tazminat ödenmesine yol açabilir. Her ne kadar rapor hazırlanırken lisanssız program kullanmanın, ülkemizdeki hukukçular tarafından başka bir suç oluşturduğuna kanaat edilmiş olsa da; teknik olarak lisanssız programın incelenen sistem üzerinde delil niteliğini bozacak işlemler yapması mümkündür. Uluslararası mahkemeler rapor hazırlanırken uygulanan süreçteki standartları ve programın lisansını da göz önünde bulundurmaktadır(Demirbilek,2008).

h) Amerika'da bilişim suçları konusunda kimi özel programların kullanımı için belirli kişilere akreditasyon verilmiştir. Dolayısıyla sadece lisanslı program kullanmak değil; o programı kullanabilecek ehliyete sahip personeli yetiştirmek de gereklidir.

i) Cihazlar öncelikle yerinde incelenir ve bunun yeterli olmadığı durumlarda özel aparatlar ile yedeği alınarak bu yedekler üzerinde inceleme yapılır. Bunun ilk sebebi çalışma esnasında gerek delillerde, gerekse kişisel bilgilerde bir bozulmaya yol açmamaktır. İkincisi ise, bir itiraz gerçekleştiği zaman o dönemdeki imajdan yeniden değerlendirme yapılmasıdır. Mevzuatımızda bazı eksikliklerle birlikte konu

ile ilgili hükümler bulunmasına rağmen, bunların kimi zaman uygulanmadığı görülmüştür.

j) Bilişim suçları konusunda toplum yeteri kadar bilgilendirilmediği ve mevzuattaki hükümler, bu noktada da tam olarak uygulanmadığı için, bilişim suçuyla karşılaşan birçok firma, özel bilgilerini korumak amacıyla şikâyetçi olmamaktadır.

5. ADLİ BİLİŞİM LABORATUARLARININ KURULUMU

Bilişim suçları konusundaki problemler süreçteki; hukuki, uygulama ve teknik boyut arasındaki koordinasyon eksikliğinden kaynaklanmaktadır. Suçla, günümüzde ve gelecekte daha etkin mücadele edebilmek için daha iyi teşkilatlanma ve teknik altyapı gereklidir. Delillendirmeyi, faile ulaşmayı, diğer bir ifadeyle fiil ile fail arasındaki bağlantıyı sağlayacak standartlara sahip, Adli Bilişim laboratuarları kurulmadığı sürece, sadece yasalar ile sonuca ulaşmanın mümkün olamayacağı bilinen bir gerçektir(Özel ve Ahi, 2005).

5.1. Adli Bilişim Laboratuarı Kurulum Basamakları

5.1.1.Adli bilişim laboratuarının temel yeteneklerinin tespiti

a. Adli bilişim laboratuarının yapısı, fonksiyonları ve her birimin kullandığı özel teknikler ile ilgili bilgiler elde edilmeli, ülkemizdeki ve yurtdışındaki birimlerin incelenmesi ve buralarda eğitim alınması ile adli bilişim esaslarının kavranması sağlanmalıdır.

b. Adli bilişim sadece teknik açıdan düşünülmemeli, yönetim, planlama ve finansal açıdan da gerekli çalışmalar yapılmalıdır. Adli bilişim laboratuarlarının ülke çapında nerelerde kurulması gerektiğine ait etüt yapılmalı, bölgedeki gelişmişlik oranı, siber suçların işlenme oranı ve ivmesi hesaplanarak laboratuarın gerekliliği ve teçhizatı belirlenmelidir. Örneğin pahalı olan elektron mikroskobu sadece Ankara'daki merkez laboratuar için temin edilirken, adli bilişimi ilgilendiren, yılda 3-4 olayla karşılaşıldığı birkaç ilden oluşan bir bölgeye sadece bir adet mobil adli bilişim dijital veri platformu temin edilerek gerekli destek verilebilir.

Şekil 5.1. Mobil Adli Bilişim Veri İnceleme Platformu

c. Öncelikle lisanslı adli bilişim programlarının temin edilip eğitimleri alınmalı, uzmanların farklı adli bilişim programlarına hâkim olması sağlanmalıdır.

d. Çalışma ortamı standartları belirlenerek birime uygun donanım temin edilmelidir.

e. Bu konudaki bir diğer önemli nokta dijital delile uygun prosedürlerin oluşturulmasıdır. Delil kabulden inceleme ve rapor formatına kadar, detaylı talimat ve formlar hazırlanarak tutarlılık sağlanmalıdır.

5.1.2.Bilişim Suçlarının Tespiti Konusundaki Mekanizmanın Güçlendirilmesi

a. Bilgi güvenliği konularında tepki mekanizması ve acil durum yönetimi oluşturulmalıdır. Bu konuda bir problem meydana geldiğinde, problemi çözüp bilgiyi kullanılabilir halde tutacak temel ve uygulanabilir planlar yapılmalıdır.

b. Bilişim suçlarının tespitini desteklemek amacıyla, ağ yönetimi, analizi ve paket incelenmesi konularında çalışılmalı, suç aktiviteleri kayıt altına alınmalıdır.

c. Veri güvenliği amacıyla veri savunma mekanizmaları oluşturulmalıdır.

d. Endüstri, akademi, araştırma merkezleri, konuyla ilgili askeri birimler arasında koordinasyon sağlanarak ağ teknolojilerindeki gelişmeler ve etkilerinin anlaşılması, bu konudaki yeni teknoloji ve donanımların tespiti ve ulusal adli bilişim teknolojilerinin geliştirilmesi alanındaki çalışılmalar hızlandırılmalıdır.

e. Adli Bilişim laboratuarının akredite edilmesi; kaliteli raporların hazırlanmasını ve bunların kamu tarafından onaylanmasını sağlayacaktır. Ülkemizde

mevcut bilirkişilik yasası özel kurumlarında bilirkişi olarak hizmet vermesine imkân sağlamaktadır. Örneğin Alman Hastanesi adli tıp alanında bilirkişi olarak hizmet vermektedir. Ülkemizde adli bilişim alanında da bu tarz örnekler zamanla çoğalacaktır. Ancak amacı kar etme olan özel bir şirketin bilim üretme ya da kamu hizmeti anlamında çalışması Dünya'da tartışma konusudur. Bu noktada adli bilişim konusunda bu laboratuarı ulusal yada uluslararası akreditasyonlarla kontrol etmek bu girişimlerden faydalanmayı sağlayacaktır.

Akreditasyonda faydalanılabilecek standartlar;

i.ISO/IEC Rehber 46 (Tüketim Mallarının ve Bunlarla İlgili Hizmetlerin Karşılaştırmalı Olarak Denenmesi- Genel Presipler)

ii.TS EN ISO/IEC 17025:2005(Deney ve Kalibrasyon Laboratuarlarının Yeterliliği İçin Genel Şartlar)

iii.ISO/IEC Rehber 58(Kalibrasyon ve Test Laboratuarları Akreditasyon Sistemleri)

iv.TS ISO/IEC 15408 (Bilgi Teknolojisi-Güvenlik Teknikleri-Bilgi Teknolojisi (BT) Güvenliği için Değerlendirme Kriterleri),

v. RFC3227 2002 (Delil Toplama ve Arşivleme Kılavuzu) olarak sıralanabilir(Patrick ve Chen,2005,s.:6,7).

Örneğin Adli bilişim laboratuarlarının ISO17025 adaptasyonu olmadığı takdirde dijital delil inceleme gibi çok kritik bir alanda merkezi otorite oluşturulana kadar minimum rehberlik ile ve muhtemelen yavaş işleyiş riskleriyle karşı karşıya kalınacaktır(Wilsdon ve Slay,2005,s.:7).

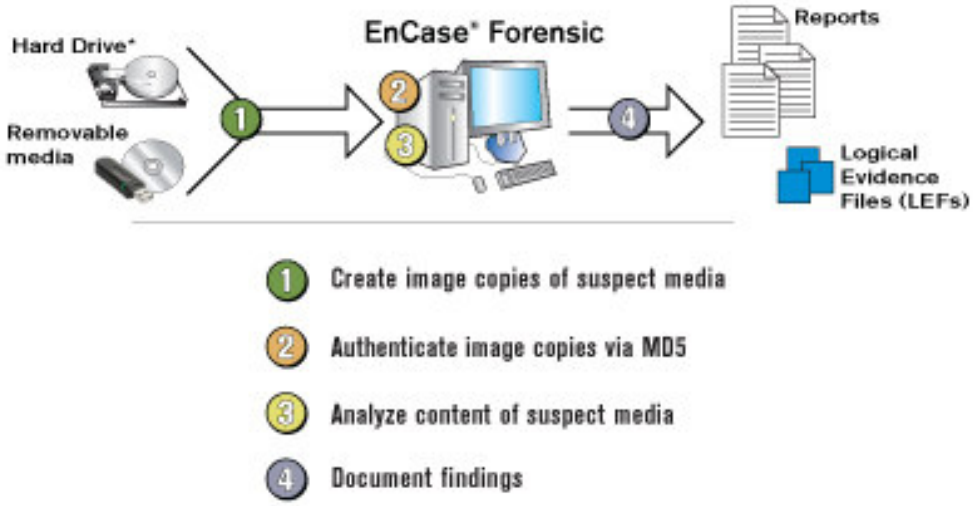
Bilişim Suçları ve Adli Bilişim alanında bilirkişilik yapacak ve laboratuarda görev yapacak personelin de akreditasyonu önemli bir husustur. Bu konuda uluslararası alanda en çok kabul görmüş sertifikasyonlardan bazıları şunlardır:

EnCase Certified Examiner (ENCE)[3]

Guidance Software'in EnCase yazılımı tüm dünyaca kabul görmüş ve kanun uygulayıcılar tarafından en çok tercih edilen dijital delil inceleme yazılımlarından bir tanesidir. Yazılımsal tabanlı delil imajı alabilme ve her türlü alınmış delil imajını

[3] http://www.guidancesoftware.com

inceleyebilme özelliğine sahip olan EnCase[4]; kendi içerisinde barındırdığı özel scripting dili ile birlikte adli bilişim uzmanına menüleri olan bir araçtan çok, incelemelerde mükemmel seviyede esneklik sağlayan bir yazılımdır.



Şekil 5.1.2 EnCase Yazılımı Delil İşleme Süreci[3]

Gudaince Software Computer Forensic(Adli Bilişim) konularında sadece EnCase yazılımının kullanımı eğitimini vermemekte bunun yanında da Adli Bilişim prensiplerinden detaylarıyla bahseden bir eğitim içeriği sağlamaktadır.

Bu sertifikaya sahip olabilmek için öncelikle Guidance Software'in EnCase yazılımının yasal/lisanslı bir sürümünün kullanıcısı olmak ve sonrasında Guidance Software'in yetkili bir eğitim merkezinden en az bir eğitim almış olmak gerekmektedir. Bu, kendi kendine çalışma yaparak sertifikasyon almayı zorlaştırmaktadır.

Certified Computer Examiner (CCE)[5]

CCE sertifikasyonu Adli Bilişim uzmanlığı için profesyonel bir şekilde hazırlanmış değerlendirme aşamalarından sonra verilen bu alandaki en başarılı sertifikasyonlardandır. Bu sertifikasyon Uluslararası Bilgisayar Kiriminalistiği (Adli Bilişim) Birliği "International Society of Forensic Computer Examiners", Kennesaw Eyalet Üniversitesi Güneydoğu Siber Suç Enstitüsü (The Southeast Cybercrime

[4] EnCase tarafından desteklenen dosya sistemleri: FAT12/16/32, NTFS, EXT2/3 (Linux), Reiser (Linux), UFS (Sun Solaris), AIX Journaling File System (JFS and jfs) LVM8, FFS (OpenBSD, NetBSD and FreeBSD), Palm, HFS, HFS+ (Macintosh), CDFS, ISO 9660, UDF, DVD, ad TiVo® 1 ve TiVo 2 dosya sistemleri.
[5] http://www.certified-computer-examiner.com/

Institute at Kennesaw State University), Tri Country Teknik Koleji (The Tri County Technical College, Pendleton, South Carolina) ve Sir Sanford Fleming Koleji (Sir Sanford Fleming College, Ontario, Canada) tarafından ortaklaşa olarak düzenlenen bir sertifikasyondur.

CCE sertifikasyonu gerek sivil kuruluşlarda veri kurtarma ve olay müdahaleleri için çalışan bilişim sistemleri uzmanları gerekse de kanun uygulayıcılar için Adli Bilişim uzmanlığı yönünde verilmektedir. Yazılı ve uygulamalı olarak yapılan sınav sonucunda bu sertifikasyonu almaya hak kazanılmaktadır. Her iki aşamadan da %80 başarı sağlanması halinde sertifikasyon sahibi olunabilmektedir. CCE ile yetkilendirilmiş bir Adli Bilişim uzmanı ABD'de oldukça rağbet görmektedir.

Certified Computer Crime Investigator (CCCI)[6]

Sertifikalı Bilgisayar Suçları Araştırmacısı (CCCI) sertifikasyonu iki aşamalı sertifikasyonlandırmadan oluşmaktadır. Basic ve Advanced (Başlangıç/Basit ve İleri/Uzman) olmak üzere iki seviyedir. Bu sertifikasyon sadece kanun uygulayıcılar yani kolluk kuvvetleri çalışanlarına verilmektedir. Uluslararası alanda geçerliliği mevcuttur ve her ülkeden başvuru yapılarak gereksinimleri karşılamak şartıyla sınav hakkı elde edinilebilir.

CCCI Basic: Başlangıç seviyedeki CCCI sertifikasyonu için; En az 2 yıl kanun uygulayıcı bir alanda çalışmış olmak yada üniversitelerin bu alandaki bölümlerinde çalışıyor olmak(Polis Akademisi, Harp okulu ve Adli Bilimler Enstitüsü gibi), en az üniversite mezunu olmak, en az 18 ay bilişim suçları veya bilişim güvenliği gibi teknik bir alanda kamuda çalışmış olmak ve kendi düzenledikleri kurslardan en az bilişim suçları alanında olan 40 saatlik bir kursu tamamlamış olmak gerekmektedir. 10 farklı alanda yapılan yazılı ve uygulamalı sınav neticesinde bu sertifikasyonun hak edilmesi söz konusu olmaktadır.

CCCI Advanced: İleri düzey olan CCCI sertifikasyonu için; en az 3 yıl kanun uygulayıcı bir alanda çalışmış olmak yada üniversitelerin bu alandaki bölümlerinde en az 2 yıldır çalışıyor olmak (Polis Akademisi,Harp okulu ve Adli Bilimler Enst gibi), üniversite mezunu olmak, en az 4 yıl bilişim suçları veya bilişim güvenliği gibi teknik bir alanda kamuda çalışmış olmak, Basic CCCI sertifikasyonuna sahip olmak

[6] http://www.htcn.org/

ve kendi düzenledikleri kurslardan en az bilişim suçları alanında olan 80 saatlik bir kursu tamamlamış olmak gerekmektedir. 20 özel ve 40 genel amaçlı test ve uygulama sonrasında bu sertifikasyon elde edilebilmektedir. ABD'de mahkemelerde bilirkişilik yapabilmek ve FBI, CIA ve USSS gibi yerlerde bu alanlarda profesyonel olarak çalışabilmek için CCCI sertifikasyonuna ihtiyaç vardır.

Computer Forensic Computer Examiner (CFCE)[7]

Bu sertifikasyon sadece kanun uygulayıcı kolluk kuvvetleri mensupları, bunların eğitici alanlarında çalışan kişiler ve Uluslararası Bilgisayar Araştırmaları Uzmanları Birliği'ne(International Association of Computer Investigative Specialists (IACIS)) girmeye hak kazanmış kişiler için olup IACIS tarafından organize edilmektedir. CFCE sınavı bu alandaki sertifikasyon sınavlarından en zor olanlarındandır. Özel olarak hazırlanmış 6 aşamalı disk incelemelerinden sonra sınava giren aday son olarak da yine özel olarak hazırlanmış tam bir hard disk incelemesi testinden geçirilir. Bu disklerdeki tüm detaylar incelenmeli, deliller saptanmalı, problemler giderilmeli, bulunan deliller bulunma yöntemlerine göre detaylarıyla raporlanmalıdır.

CFCE sertifikasyonunda inceleme aşamasında baştan sona kadar uyulması gereken tüm Adli Bilişim prensipleri kontrol edilmekte ve buna göre de bir puanlama yapılmaktadır. Aday en son olarak da yazılı bir sınavdan geçirilmekte ve bilgi seviyesi yazılı olarak da ölçülmektedir. Bu sertifikasyonda disk incelemeleri için sınava giren adaya toplam da 5 ay gibi bir zaman verilmekte ve adayın 5 ay içerisinde ilgili raporlarını IACIS'e sunması gerekmektedir.

Certified Information Forensics Investigator (CIFI)[8]

CIFI sertifikasyonu kazanımı için Bilişim Suçları ve Adli Bilişim alanında birçok farklı konudaki bilgi birikimleri test edilmektedir. Yazılı, pratik inceleme, raporlama ve demo sunumu sınavın başlıca aşamalarıdır. Aynı zamanda Adli Bilişim prensipleri de sertifikasyon sınavında test edilmektedir. Sınav Uluslararası Bilişim Sistemleri Kriminalistiği Birliği (International Information Systems Forensics Association (IISFA)) tarafından düzenlenmekte ve uygulanmaktadır.

[7] http://www.iacis.com/
[8] http://www.infoforensics.org/

CIFI sertifikasyon sınavı bilişim kiriminalistiği üzerine aşağıdaki 6 alanı içeren bir sınavdır.

- Auditing (Delilleri, problemleri ve olayı saptama bilgisi)
- Incident Response (Olay müdahalesi)
- Law and Investigation (Hukuk ve inceleme süreci)
- Tools and Techniques (Kullanılan araçlar ve Teknikler)
- Traceback (Geriye doğru bilgi çıkarımı)
- Reporting (Raporlama)

Professional Certified Investigator (PCI)[9]

Bilişim Suçları ve Adli Bilişim uzmanlığı alanındaki en zorlu sertifikasyonlardan bir taneside PCI sertifikasıdır. Bu sertifikaya sahip olabilmek için en az 9 yıl Bilişim Suçları ve Adli Bilişim alanlarında çalışmış olmak, üniversite mezunu olmak, 9 yılın en az 3 yılını direk olarak inceleme aşamalarında geçirmiş olmak gerekmektedir. Bu sertifikasyon sınavı çok aşamalı olup adayın bilişim güvenliği, bilişim suçları ve adli bilişim bilgisini her alanda ölçen en zor sınavdır denebilir. Yukarıda listelenen birçok sertifikayı kazanmış bir insanın bile bu sertifikasyon sınavından başarısız olduğu görülmüştür. Tamamen bilgi birikimi ve tecrübeye endeksli bir sınavdır.

Yukarıda sayılan 6 adet sertifikasyon Bilişim Suçları ile mücadelede Adli Bilişim Uzmanlığı konusunda en çok değer arz eden sertifikasyonlardır. Bunların dışında aşağıda yer alan sertifikasyonlar da mevcuttur. Unutulmamalıdır ki bilgiyi sistemli bir şekilde öğrenmek kadar önemli başka bir şeyde bilginin derecelendirilmesi ve yetkilendirilmesidir.

Diğer Serfikasyonlar:

- Certified Cyber-Crime Expert(C3E): http://www.trcglobal.com/
- Advanced Information Security (AIS): http://www.securityuniversity.net/certification.php

[9] http://www.asisonline.org/certification/pci/pciabout.xml

- Certified Computer Forensic Technician (CCFT): http://www.htcn.org/
- Certified Information Systems Auditor (CISA): http://www.isaca.org/
- GIAC Certified Forensic Analyst (GCFA): http://www.giac.org/subject_certs.php

5.1.3.Suçu önleme amaçlı yapılması gerekenler

Bir kolluk kuvvetinin başarısı; tespit ettiği suç miktarıyla değil, meydana gelmeden önledikleri ile ölçülür. Bu bağlamda siber suçlarla mücadelede özel birimler oluşturulmalıdır.

Örneğin Almanya'da kritik bilgi sistemlerine toplumun artan bağımlığına bağlı olarak, Alt Yapı Çalışma Grubu(AKSIS) ve erken uyarı amaçlı bilgisayar güvenliği olay müdahale birimleri[10] gibi özel birimler kurulmuştur. (Şehitoğlu,2005,s.:156).

Gelişmiş ülkelerde Tablo 5.1 ve Tablo 5.2 'de görüleceği gibi kamu kurum ve kuruluşları, kamu özel sektör işbirliği ve erken uyarı yaklaşımları olarak üç grupta güçlü ve aktif birimlerin görev yaptığı görülmektedir.

Bu noktada Almanya örneği çeken ve emsal teşkil etmesi gereken bir ülkedir. 2002 yılı itibariyle mevcut sistemlerini Linux altyapısına oturtmuştur. Yapıyı ve açıkları en iyi kendisi bilmektedir, dolayısıyla e-devlet yapılanmasıyla kritik bilgilerin akacağı sistemlerdeki yazılım güvenliğini üst seviyeye çıkarmıştır.

Bu konuda yapılması gerekenler şu şekilde sıralanabilir:

Tablo 5.1A Bilişim Suçları Konusunda Çeşitli Ülkelerde Görev Yapan Kamu Kurum ve Kuruluşları

	ALMANYA	İNGİLTERE	RUSYA	MALEZYA	AMERİKA
KAMU KURUM VE KURULUŞLARI	Federal Ministry of the Interior (BMI)	National Infrastructure Security Co-ordination Centre (NISCC)	Security Council of the Russian Federation	Communications and Multimedia Commission (MCMC)	Homeland Security Council

[10] CERT-Bw-Silahlı Kuvvetlere, RUSCERT-Araştırma Geliştirmeye, mCERT ufak çaplı işyerlerine yönelik, Almanya'da hizmet veren olay yeri müdahale birimlerdir.

	Th e Federal Offi ce for Information Security (BSI)	Communications Electronics Security Group (CESG)	Ministry of Information Technologies and Communications	Administrative Modernization and Management Planning Unit (MAMPU)	Directorate for Information Analysis and Infrastructure Protection (IAIP)
	Federal Offi ce for Civil Protection and Disaster Response (BBK)	Civil Contingencies Secretariat (CCS)	Federal Technical and Export Control Service	Government Computer Emergency Response Team (GCERT)	Critical Infrastructure Assurance Offi ce (CIAO)
	German Emergency Preparedness Information System (deNIS)	Central Sponsor for Information Assurance (CSIA)	Federal Agency for Government Communications and Information (FAPSI)	ICT Strategic Plan	National Infrastructure Protection Center (NIPC)
	Th e Federal Criminal Police Agency (BKA)	Cabinet Office	Special Communication and Information Service	Forensic Computer Laboratory	Critical Infrastructure Assurance Offi ce (CIAO)
	Federal Ministry of Economics and Technology (BMWi)	Government Communications Headquarters (GCHQ)	Computer and Information Security Directorate Federal Guard Service	Technology Crime Investigation Unit	US Department of State
	Federal Network Agency	Department of Trade and Industry (DTI)	Federal Security Service of the Russian Federation (FSB)	Ministry of Science, Technology and Innovation (MOSTI)	International CIP Interagency Working Group
	Other ministries involved	National High Tech Crime Unit (NHTCU),		Ministry of Energy, Water and Communications (MECM)	House Subcommittee on Economic Security, Infrastructure Protection and Cybersecurity
		Ministry of Defence (MoD)			Offi ce of the Assistant Secretary of Defense for Networks and Information Integration (OASD/NII)
		Security Service's National Security Advice Centre (NSAC)			Computer Crime and Intellectual Property Section (CCIPS)
		Other ministries involved (CSIA,CCS)			Other ministries involved

Kaynak: ABELE I, DUNN W. And G., International CIIP Handbook 2006 Vol.1, An Inventory of 20 National and 6 International Critical Information Infrastructure Protection Policies

Tablo 5.1B Bilişim Suçları Konusunda Çeşitli Ülkelerde Görev Yapan Kamu Özel Sektör İş Birliği Kurumları ve Erken Uyarı Yaklaşımları

	ALMANYA	RUSYA	İNGİLTERE	MALEZYA	AMERİKA
KAMU-ÖZEL SEKTÖR İŞ BİRLİĞİ	Initiative D21	Russian Association of Networks and Services (RANS)	National Infrastructure Security Co-ordination Centre (NISCC)	Information Sharing Forum (ISF)	Offi ce of Private Sector, Department of Homeland Security
	Working Group on Infrastructure Protection (AKSIS)	Russian Development Gateway	Communications Electronics Security Group (CESG)		Information Sharing and Analysis Centers (ISACs)
		PRIOR	Civil Contingencies Secretariat (CCS)		InfraGard
			Central Sponsor for Information Assurance (CSIA)		National Cyber Security Alliance (NCSA)
			Cabinet Office		Partnership for Critical Infrastructure Security Cyber Incident Detection Analysis Centre (CIDDAC)
			GCHQ, DTI,MoD, NHTCU, NSAC		National Cyber Security Partnership (NCSP)
ERKEN UYARI YAKLAŞIMLARI	CERTBUND	Russian Computer Emergency Response Team (RU-CERT)	Unified Incident Reporting and Alert Scheme (UNIRAS)	National ICT Security and Emergency Response Center (NISER)	Federal Bureau of Investigation (FBI)
	Mcert	Russian Institute of Public Networks (RIPN)	Ministry of Defence Computer Emergency Response Team (MODCERT)	Malaysian Computer Emergency Response Team (MyCERT)	Directorate for Information Analysis and Infrastructure Protection (IAIP)
	CERT Network	Russian Backbone Network (RBNet)	ITsafe: IT Security Awareness for Everyone		National Cyber Security Division (NCSD)
	IT Crisis Response Center		GetSafeOnline		National Cyber Alert System
					Federal Computer Incident Response Center (FedCIRC)
					CERT Coordination Center (CERT/CC)

					Other ministries involved

Kaynak: ABELE I, DUNN W. And G., International CIIP Handbook 2006 Vol.1, An Inventory of 20 National and 6 International Critical Information Infrastructure Protection Policies

a. Tatbikatlar ile saldırı meydana geldiğinde yapılacak işlemler simule edilmelidir. Örneğin Almanya'da 2001 yılının Kasım ayında AKSIS, Münih yakınlarındaki Ottobrunn'da Siber Terör Uygulaması (CYTEX) gerçekleştirmiştir. Çeşitli federal bakanlıklardan gelen temsilciler ile endüstri ve kamu yönetimi alanında çalışanların da iştirakiyle gerçekleştirilen bu uygulamayla, Berlin'deki çeşitli kamu ve özel sektör bilişim sistemlerine yönelik şantaj maksatlı yapılan çeşitli saldırı senaryoları oluşturulmuştur(Bruno,2002,s.:49).

b. Bilgi güvenliği ve adli bilişim eğitimi verilebilecek birim oluşturulmalıdır. Bilgi güvenliği konusunda kamu ve özel kurumalar dikkati çekilmeli, bilişim suçlarında tepki mekanizmalarının yetenekleri dolayısıyla bilgi güvenliği seviyesi arttırılmalıdır.

c. Adli bilişim sempozyumları düzenlenmeli; adli bilişim alanında uzman personel eğitilmelidir. Bu uzmanlar, uluslararası koordinasyon sağlanarak uluslararası anti terörist ağ araştırmalarına katılmalıdır(Yen ve Chen,2006,s.:6).

d. Tüm yönleriyle mevcut hacker aktiviteleri, birbirleriyle ilişkileri ve alakalı oldukları organizasyonlar tespit edilmelidir. Böylece hem onların karakteristikleri ve teknikleri hem de hedeflerine ait kanun uygulayıcılarının soruşturmalarda faydalanabileceği bir veritabanı oluşturulmalıdır.

e. Suç önleme amacıyla internet, düzensiz bir şekilde taranmalıdır.

f.Bilişim suçları ile daha etkili mücadele edebilmek için şüpheli ve zaman kaybı yaratacak bilgi kanallarının da tespiti yapılmalıdır.

g. Sistemin en iyi testi ona saldırmakla mümkündür. Çeşitli bankaların güvenlik birimlerinin yaptığı gibi Türkiye'deki kamu, askeri ve istek dâhilinde özel kurumların güvenlik sistemlerine saldırarak açıkları tespit edilmelidir. Bu sayede bilgi güvenliği seviyesi arttırılarak, suçludan önce kullanacağı teknik belirlenmeli, uygun savunma teknikleri geliştirilmelidir.

5.2. Üniversitelerin Sürece Katkıları

a. Her geçen gün hızla gelişen bilgi sistemleri teknolojilerinde, bilişim suçları başlı başına uzmanlık gerektiren bir konu olmuştur. Dolayısıyla ülkemizin gelecekte bu ihtiyacını karşılamaya yönelik enstitü açılmalıdır.

Yapılacak çalışmalarda yeni gelişen sistem ve tekniklere uygun esnek yapıda örgüt ve çalışma sistemlerine ihtiyaç vardır. Amerika uygulamasında olduğu gibi artık bilişim sektöründe teknik ve bilgi üretenler her alandaki hakimiyeti sağlayacaklardır. Bu yüzden oluşturulacak sistemlerde eğitim, proje üretme ve uygulama iç içe olmalı Amerika'ya göre daha çok devletçi olan yapımızda tüm kamu kuruluşlarının ve gerekli ise bu konuda esnek olarak özel sektörün katılımının da sağlandığı birliktelikler oluşturulmalıdır. Bu konuda Amerika'da var olan ve Federal birimler ile birlikte çalışan Bilgisayar Güvenlik Enstitüsü (CSI) birimi bize bu konuda örnek olacaktır(Şeker,2002).

Bununla beraber bu tarz bir enstitüde eğitim görecek öğrenciler konusunda ön koşullar tespit edilmelidir. Aksi takdirde eğitimli korsanlar da yetiştirilebilir.

b. Adli Bilişim Laboratuarları için Ulusal Standartlar tespit edilmelidir.

c. Daha verimli çalışma sağlamak amacıyla farklı tipteki dijital delile uygun, farklı inceleme süreçleri modellenmeli, her basamakta görevli olan kişi ya da birimlerin yetenekleri ve sorumlulukları belirlenmelidir.

d. Dijital delil arama sürecinde yasal yöntemler tespit edilmelidir. Böylece gelecekte hem yurt içindeki hem de uluslar arası davalarda ülkemizi tazminat ödemeye zorlayacak ya da şahısları mağdur edecek uygulamalar engellenecektir.

e. Ulusal Mobil adli bilişim dijital delil platformları tasarlanmalıdır. Amerika'da da örneğini görebileceğimiz, bir çanta büyüklüğündeki bu cihaz üzerindeki yazılım ve donanım ile farklı platformlara adapte olabilmeli, veri bütünlüğünü sağlamalı ayrıca, dijital delillere kaynak teşkil edebilmesi nedeniyle mobil telefonlar, PDA cihazları, akıllı kartlar gibi gömülü bilgisayar sistemlerine de uyumlu olmalıdır(Uzunay ve Koçak,2005).

f. Şifrelenmiş veriler üzerinde dijital delilleri yakalamaya yönelik algoritmalar geliştirilmeye çalışılmalıdır. Mevcut kriptografik çözümler veya daha değişik yöntemler kullanılarak dijital delillerin mahkeme esnasında geçerliliklerinin sağlanması için entegre çözümler, sistemler üretilebilir(Uzunay ve Koçak,2005).

g. ABD(Carnivore,EnCase,Autopsy , The Sleuth Kit), İtalya, Belçika (FCCU), Hollanda[11] gibi ülkeler, artan bilişim suçları ve suçlunun tespiti için çoğu açık kaynak kodlu ulusal adli bilişim analizi araçları ve yazılımları geliştirmektedirler.

Adli Bilişim Analizi için ulusal standartları belirlemek ve yazılım-donanım geliştirmek, doğal olarak beraberin de bir bilişim eko-sistemini doğuracaktır. Elektronik imzadan, mobil imzaya, şifreleme ve kripto algoritmalarına kadar olan süreç günlük kullanıma geçtiğinde e-devlet projeleri için güven ve tespite dayalı bir standardı beraberinde getirmiş olacaktır.(Ceylan,2007)

h. Ağ üzerinde tarama yapan sniffer (ağ yoklayıcısı) cihazları araştırılmalıdır. Özellikle büyük verileri yakalayabilmeli ve ağda eş zamanlı olarak çalışmalıdır.

i. Pasif ağ kayıt sistemleri ile suç incelemelerinde kullanılmak üzere, ticari ve finansal işlemler ile ilgili kayıtlar tutulmalıdır.

j. Dijital delillerin şifrelenmiş olabileceği göz önünde bulundurularak, dağıtık bilgisayar sistemleri ile şifre kırma teknikleri üzerine araştırmalar yapılmalıdır.

k. Süreci daha verimli hale getirmek amacıyla, veri madenciliği ve etkili mücadele için yapay zekâ uygulama çalışmaları yapılmalıdır.

l. Suçları önleme amacıyla, yeni nesil kullanıcı ve öğreticilerinin bilişim suçları konusunda daha bilinçli olması sağlanmalıdır. Özellikle geleceğin nesillerini yetiştirecek eğitim fakülteleri olmak üzere, tüm fakültelerin müfredatında yer alan bilgisayar dersi içeriğine bilgi güvenliği konusu eklenmelidir.

m. Hukuk fakültelerinde konu ile ilgili çalışmalar yapılmalıdır[12]. Bilmesi gereken prensibine göre bilişim suçları konusunda gelecekte karar verecek personelin, teknik anlamda da bilgi sahibi olması sağlanmalıdır.

5.3. Koordinasyon

E-devlet uygulamalarının yaygınlaşmasıyla; resmi, özel tüm kurumları tehdit eden bilgi güvenliği riski de artmaktadır. Örneğin, e-devlet uygulamalarının yaygın

---

[11] www.forensix.org :Hollanda merkezli olup, adli bilişim analizi konusunda gerekli program ve kitapların tanıtıldığı bir web sitesidir.

[12] İstanbul Bilgi Üniversitesi Bilişim Teknolojisi Hukuku Uygulama ve Araştırma Merkezi 06.01.2004'de kurularak bu konuda faaliyet gösteren ilk ve tek enstitü olmuştur.

olduğu ABD'den sonra sekizinci devlet konumunda olan Estonya, 2007 Nisan sonunda Ülkeye 50 ayrı yönden ve ülke üzerinden saatte 2 binden fazla saldırı gerçekleşmiş ve saldırı nedeniyle birçok devlet dairesi ve finans grubu kapatılmış ve ülkede hayat durmuştur.

E-devlet uygulamaların hızla tüm kamusal alanda yaygınlaştığı ülkemizde de bilgi güvenliği açısından gerekli çalışmalar yapılmalıdır. Saldırıya maruz kalabilecek birimler, önleyici birimler, suçu takip edecek birimler, teknik desteği sağlayacak birimler ile ARGE faaliyetleri yürütecek birimlerin nitelik ve sorumlulukları belirlenmelidir. Bu noktada standartları belirleyecek ve aradaki koordinasyonu sağlayacak üst düzey bir birim oluşturmalıdır.

Koordinasyon, internetin sınırlarına bağlı olarak uluslararası boyutta da yürütülmelidir. Bilişim suçları olgusu teknolojiyi kullanan ve kullanacak bütün ülkelerin ortak problemi haline gelmiştir. Bu nedenle ulusal düzenlemeler ve ulusal hukuklar bilişim suçları ile mücadelede yetersiz kalmaktadır. Bilişim suçları ile ideal bir mücadele, teknolojik gelişmeler ile globalleşen dünyada bu tip suçlara karşı dünya çapında bir işbirliği ile mümkündür. Dijital ortamın getirmiş olduğu bütün imkanları dünya devletleri suçla mücadelede kullanmadıkça bu alandaki suç tipleri ile mücadelede başarılı olmak mümkün değildir(Özdemir,2007,S.:1)

Adli bilişim laboratuarlarının kurulumu, yukarıdaki birimler ile koordinasyon sağlandığı takdirde ihtiyaçları en iyi şekilde karşılayacak yapıya kavuşacaktır.

6. SONUÇ ve ÖNERİLER

Adli Bilişim laboratuarının kurulumu ile adalete, kişisel hak ve özgürlükleri koruyarak uluslararası geçerliliği olan desteğin verilmesi amaçlanmaktır. Ancak bu alandaki çalışmaların etki ve sonuçları sadece bununla sınırlı değildir.

Çalışmalar, ulusal ağ ve bilgi güvenliği konularına ilgiyi arttıracak, hızla gelişen bilişim teknolojilerinin araştırılarak adli bilişim yeteneğine katkıda bulunmasını sağlayacaktır. Bununla beraber, adli bilişim teknolojisinin geliştirilmesi amacıyla üniversite, kamu kurum ve kuruluşları, BT sektörü ile konuyla ilgili uluslararası kuruluşlar arasında işbirliği, bilgi ve tecrübe paylaşımı sağlanacaktır.

Bu iş birliği kapsamında, resmi ve özel kurumları, bilgi ve ağ güvenliği konusunda destekleyecek, eksiklikleri tespit edecek ve sürekli olarak önlemlerin alınmasını sağlayacak bir birim meydana getirilmiş olacaktır.

Bilişim konusunda gerek akreditasyon, gerekse donanım veya yazılım açısından yapılan harcalamalar ithalata dayanmaktadır. Bir sonraki adımda, adli bilişim sürecinde, ulusal donanım ve yazılımların geliştirilmesine yönelik çalışmalar hızlandırılarak, bilişim güvenliği ürünlerinin ihracatta payı arttırılarak maddi kazanç elde edilmesinin yanında, kazanılan tecrübeler yabancı değil yerli sistemlerin geliştirilmesinde kullanılacak, harcanan kaynaklar ülkemize geri dönecektir.

Ayrıca gelişmiş ülkelerde olduğu gibi, ülkemizde de adli bilişim ihtiyacının akredite özel laboratuarlar tarafından karşılanması teşvik edilecektir.

Ülkemizde yukarıda bahsedilen özelliklere sahip uluslararası standartlarda kurulacak özel ve resmi Adli Bilişim laboratuarları ülkemizdeki ihtiyacı karşılamanın yanında, gelişmekte olan ülkelerdeki kamu ve finans alanında da birçok kuruma hizmet verebilecektir.

Üniversitelerde Adli Tıp Enstitüleri şeklinde hizmet veren fakültelerin "Adli Bilimler Enstitülerine" ve Adalet Bakanlığına bağlı bulunan Adli Tıp Kurumunun kapsamı değişerek Adli Bilimler Kurumu gibi bir yapıya dönüştürülmesi adli bilişim konusunda bilirkişi ihtiyacını karşılamaya yönelik önemli gelişmeler olacaktır. Bu enstitülerde laboratuarlarının akreditasyonuna ilave olarak adli bilişim uzmanlarının da hukuki açıdan yeterli işlemleri yapabilmesi için bilirkişilik yapabilecek seviyede olup olmadığının belgelenmesine yönelik çalışmalar da yapılacaktır.

.

KAYNAKLAR

ABELE I, DUNN W. And G., International CIIP Handbook 2006 Vol.1, An Inventory of 20 National and 6 International Critical Information Infrastructure Protection Policies

ANDERSON, A., MOHAY, G. (2003). Computer and Intrusion Forensics. Boston:Artech House.

ASHCROFT, J. (2001). Electronic Crime Scene Investigation: A Guide for First Responders. Washington: U.S. Department of Justice, National Institute of Justice.

BAYER, M., KAYGISIZ, M., Olay Yeri İnceleme, Emniyet Genel Müdürlüğü,Ankara,2002

BRENNER, Susan W.(2001), "Is There Such a Thing as "Virtual Crime"?", California Criminal Law Journal, s.1.

BRUNO, Stefano. "CIIP Country Surveys", WENGER, A.ve J. METZGER (Ed.), CIIP Handbook An Inventory of in Eight Countries Critical Information Infrastructure Protection, 2002.

CEYLAN,C., Adli Bilişim Analizi İçin Ulusal Çözüm Ve Ekonomiye Etkisi,18.03.2008, http://www.caginpolisi.com.tr/76/20-21-22.htm

ÇİÇEK İ. ve OKATAN A., Ülkemizde Adli Bilişim Laboratuarlarının Kurulumu ve Bilişim Suçlarıyla Mücadeleye Katkıları, Ağ ve Bilgi Güvenliği Sempozyumu 2008, Girne/KKTC, Mayıs 2008

DEMİRBİLEK Mesut, Emekli Emniyet Md., Citigroup Güvenlik ve Araştırma Servisi Müdürü, Görüşme 10.01.2008

EKİZER, Ahmet, 2007, Adli Bilişim Uzmanlığı Sertifikasyonları, Erişim: http://www.ekizer.net/content/view/20/1/ (20.05.2008)

EKİZER, Ahmet, 2007, Adli Bilişim (Computer Forensics – Bilgisayar Kriminalistiği.), Erişim: http://www.ekizer.net/content/view/20/1/ (20.05.2008)

HOSMER Chet, "Proving the Integrity of Digital Evidence with Time", International Journal of Digital Evidence, Spring 2002

KESER BERBER, L.(2004). Adli Bilişim. Ankara, Yetkin Yayınları, s.:39-44.

MEYERS M. and ROGERS M., The Need for Standardization and Certification, International Journal of Digital Evidence, Fall 2004

ORTABAĞ H.,Kolluğun Adli Bilişim delillerine müdahale yöntemleri, Jandarma Dergisi, Sayı 117,Mart 2007

ÖZDEMİR M., Bilişim Suçları Ve Mücadelede Taşra Teşkilatında Karşılaşılan Problemler Ve Çözüm Önerileri,10.01.2008,http://www.caginpolisi.com.tr/24/43-44-45-46.htm

ÖZEL C.,AHİ M.G.,Bilişim Suçları'nda Usul Ve Sorumluluk Sistemi Üzerine Öneriler 2005.7.4, 15.01.2008 http: //www.turkhukuksitesi .com

PATRICK S.Chen,Ying-Chieh Chen,Standardizing the Construction of a Digital Forensics Laboratory,IEEE 2005

PERRY, R.L. 1986. Computer Crime. New York: Franklin Watts.

ŞEHİTOĞLU, Onur, Bilgisayar ve ağ üzerinden işlenen siber suçlarla mücadelenin hukuksal ve güvenlik boyutu, Kara Harp Okulu Komutanlığı, Savunma Bilimleri Enstitüsü, 2005, Ankara

ŞEKER, Güven(2002), "Bilişim Suçlarının Delillendirilmesinde Amerikan Uygulaması ve Ülkemizdeki Durum", İnsan Bilimleri Dergisi (ISSN: 1303-5134), Salı Ekim 01, Erişim: http ://www.egm.gov.tr/egitim/ dergi/eskisayi /37/web/makaleler/Guven_SEKER.htm#_ftn1

USDOJ, 2004 U.S Department of Justice, FBI Law Enforcement Bulletin, August 2004

UZUNAY Y.,2. Dijital Delil Araştırma Süreci, Polis Bilişim Sempozyumu, Nisan 2005, Ankara

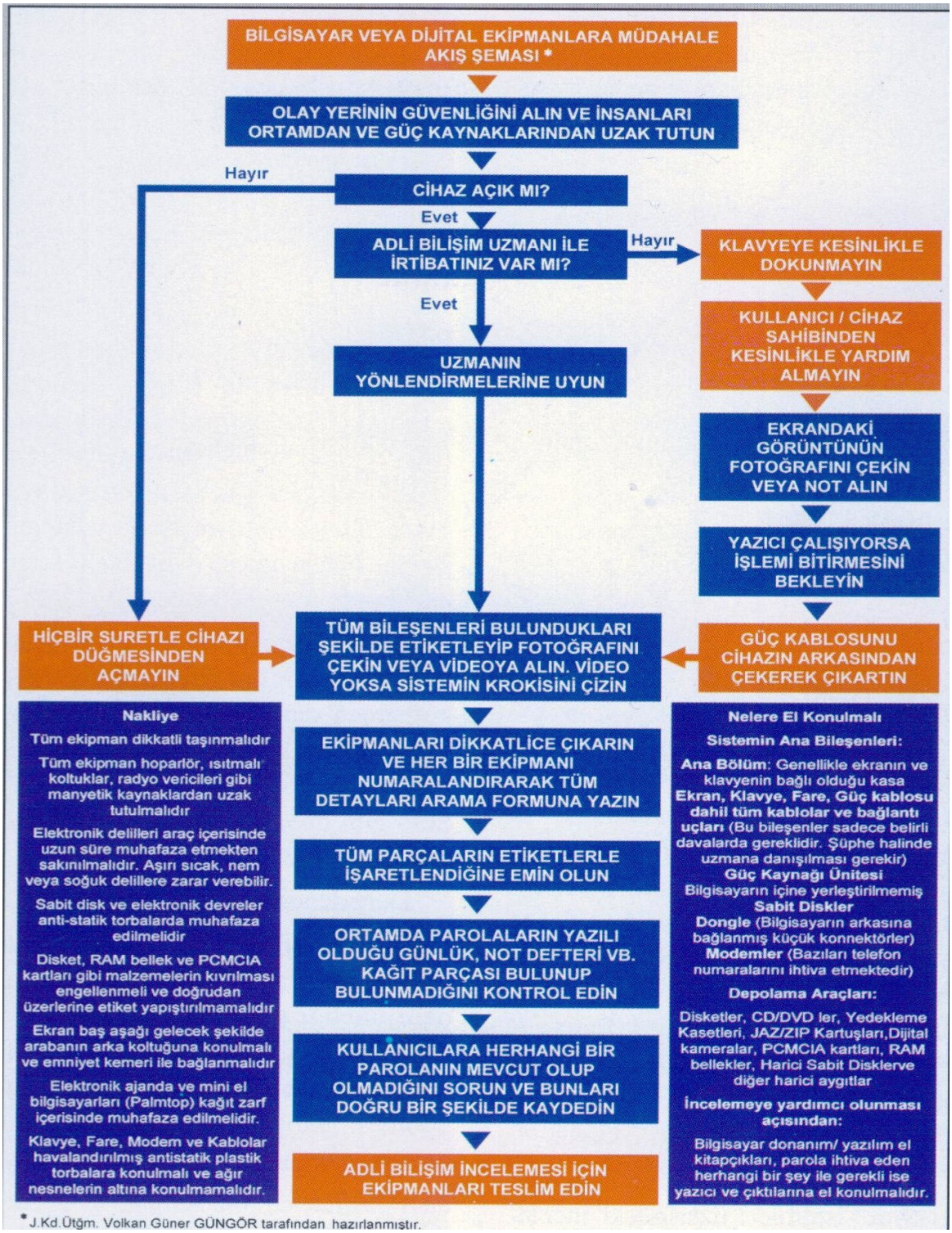
UZUNAY Y., KOÇAK M., "Bilişim Suçları Kapsamında Dijital Deliller", AB'05 Akademik Bilişim Konferansı, Gaziantep, Şubat 2005

WILSDON T., SLAY J., Digital Forensics: Exploring Validation, Verification & Certification, Enterprise Security Management Laboratory School of Computer & Information Science University of South Australia, 2005, Australia

YEN So-Lin, CHEN Sou-Chan,The Study on Planning and Building a Cyber Forensic Laboratory in MJIB, Taiwan, IEEE 2006

EK-1

Şekil A.1. Bilgisayar Veya Dijital Delil Ekipmanlarına Müdahale Akış Şeması



Kaynak: Ortabağ H.,Kolluğun Adli Bilişim delillerine müdahale yöntemleri, Jandarma Dergisi, Sayı 117,Mart 2007,s.:19

EK-2 Tablo A1. Delil Türlerine Göre Kurumsal Önem Kıyaslaması

			Adli Süreç içinde				
Delil Türü	Bilinme Düzeyi	Geçtiği yönetmelikler	Sertifikalı Uzman Personel Eğitimi	Standart İş Akışı	Standart Raporlama	Standart örnek alma ve delil koruma yöntemleri	Disipline Özel Laboratuvar
Otopsi	Yüksek	Adlî Tıp Kurumu Kanunu Uygulama Yönetmeliği	Var	Var	Var	Var	Var
Biyolojik Deliller	Yüksek	Adlî Tıp Kurumu Kanunu Uygulama Yönetmeliği Emniyet Genel Müdürlüğü Kriminal Polis Laboratuarları Dairesi Başkanlığı ve Kriminal Polis Laboratuvarı Müdürlükleri Kuruluş, Görev ve Çalışma Yönetmeliği Jandarma Genel Komutanlığı Kriminal Daire Başkanlığı ve Bölge Kriminal Laboratuar Şube Müdürlükleri Görev ve Yetkileri Yönetmeliği	Var	Var	Var	Var	Var
Kimyasal Deliller	Yüksek	Adlî Tıp Kurumu Kanunu Uygulama Yönetmeliği Emniyet Genel Müdürlüğü Kriminal Polis Laboratuarları Dairesi Başkanlığı ve Kriminal Polis Laboratuvarı Müdürlükleri Kuruluş, Görev ve Çalışma Yönetmeliği Jandarma Genel Komutanlığı Kriminal Daire Başkanlığı ve Bölge Kriminal Laboratuar Şube Müdürlükleri Görev ve Yetkileri Yönetmeliği	Var	Var	Var	Var	Var
Fiziksel Deliller	Yüksek	Adlî Tıp Kurumu Kanunu Uygulama Yönetmeliği Emniyet Genel Müdürlüğü Kriminal Polis Laboratuarları Dairesi Başkanlığı ve Kriminal Polis Laboratuvarı Müdürlükleri Kuruluş, Görev ve Çalışma Yönetmeliği Jandarma Genel Komutanlığı Kriminal Daire Başkanlığı ve Bölge Kriminal Laboratuar Şube Müdürlükleri Görev ve Yetkileri Yönetmeliği	Var	Var	Var	Var	Var
Sayısal Deliller	Düşük	Adlî Tıp Kurumu Kanunu Uygulama Yönetmeliği	Yok	Yok	Yok	Yok	Kuruluş Aşamasında
İzler	Yüksek	Adlî Tıp Kurumu Kanunu Uygulama Yönetmeliği Emniyet Genel Müdürlüğü Kriminal Polis Laboratuarları Dairesi Başkanlığı ve Kriminal Polis Laboratuvarı Müdürlükleri Kuruluş, Görev ve Çalışma Yönetmeliği Jandarma Genel Komutanlığı Kriminal Daire Başkanlığı ve Bölge Kriminal Laboratuar Şube Müdürlükleri Görev ve Yetkileri Yönetmeliği	Var	Var	Var	Var	Var
Diğer Deliller (Böcek, Polen, vb.)	Orta	Adlî Tıp Kurumu Kanunu Uygulama Yönetmeliği Emniyet Genel Müdürlüğü Kriminal Polis Laboratuarları Dairesi Başkanlığı ve Kriminal Polis Laboratuvarı Müdürlükleri Kuruluş, Görev ve Çalışma Yönetmeliği Jandarma Genel Komutanlığı Kriminal Daire Başkanlığı ve Bölge Kriminal Laboratuar Şube Müdürlükleri Görev ve Yetkileri Yönetmeliği	Var	Var	Var	Var	Var

Kaynak: Öztürk,2007,s.:92

EK-3 Tablo A2. Adli Bilişim İncelemelerinde Kullanılan Bazı Yazılımsal Ürünler

ÜRÜN	AÇIKLAMA
EnCase Boot Disk/CD EnCase www.guidancesoftware.com	Yazılımsal yazma koruma, imaj alma ve dijital delil inceleme yazılımı. FBI dahil bir çok polis teşkilat tarafından tercih edilen ve sıklıkla kullanılan bilgisayar kriminalistiği yazlımıdır.
FTK Imager Forensic Toolkit®(FTK™) www.accessdata.com	FTK komple bir bilgisayar kriminalistiği yazılımıdır. Oldukça güçlü özellikleri ile EnCase yazılımını aratmamaktadır. FTK Imager sayesinde yazma koruma tedbiri alınarak Imaj alma işlemi gerçekleştirilebilir.
IXimager ILook Investigator www.ilook-forensics.org	ILook IXimager yazılımı vasıtası ile yazılımsal yazma koruma tedbiri alınarak imaj alma işlemi gerekleştirilebilir. IXImager Linux tabanlı yazılımsal bir çözümdür. ILook Investigator yazılımı ise çok kuvvetli bir bilgisayar kriminalistiği yazılımıdır. ILook bedava bir yazılım olmakla birlikte sadece belirli şartlar ispat edildiği müddetçe kamusal kurum çalışanlarına (polis, asker, adli görevli) dağıtılmaktadır.
Forensic Replicator Paraben Forensic Tools www.paraben-forensics.com	Forensic Replicator Paraben Forensics Software tarafından sunulan yazılımsal bir imaj alma çözümüdür. Paraben firmasının dijital delil incelemeye yönelik yazılımları ve yazma koruma donanımları mevcuttur.
Linux – dd ve diğerleri www.opensourceforensics.org	Linux işletim sistemi (özellikle live dist) üzerindeki dd aracı kullanılarak da bir veri depolama biriminin raw imajı alınabilir. dd aracının aldığı imajı EnCase, ILook ve FTK dahil bir çok dijital delil inceleme yazılımı okuyabilmektedir. Linux doğası itibariyle mount (bağlanmayan) edilmeyen hiçbir veri depolama biriminde yazma bağlamında erişmemektedir. Dolayısıyla imaj alma ve işlemi yazma korumalı olarak gerçekleştirilebilir. Hali hazırda Linux işletim sistemi üzerinde bulunan bir çok yazılımla bilgisayar kriminalistiği araştırmaları gerçekleştirilebilir.

Kaynak: Erişim http://www.ekizer.net/content/view/16/1/ 16.05.2008

EK-4 Tablo A3. Adli Bilişim İncelemelerinde Kullanılan Bazı Donanımsal Ürünler

ÜRÜN	AÇIKLAMA
Digital Intelligence Tools ULTRABLOCK FORENSIC CARD READERS ULTRABLOCK USB WRITE BLOCKER ULTRABLOCK IDE, SATA AND SCSI HARDCOPY www.digitalintelligence.com	Digital Intelligence firması bilgisayar kiriminalistiği alanında dijital delil inceleme ve elde etme cihazları üreten en büyük ve en eski firmalardan bir tanesidir. Burada bir çok farklı kullanım amacıyla donanımsal yazma koruma çözümü bulunabileceği gibi, başlı başına bilgisayar kriminalistiği için özel olarak tasarlanmış bilgisayar sistemleri de bunmaktadır. Her türlü veri depolama birimi için özel olarak üretilmiş inceleme ve imaj alma donanımları Digital İntelligence firması bünyesinde mevcuttur.
Image Master Solo Drive Lock Disk Jockey IT www.ics-iq.com	Image Master Solo cihazı o kadar mükemmel bir imaj alma donanımıdır ki üzerinde hiçbir imaj alma donanımını taşımadığı özellikleri taşımaktadır. (Hash alma, bire bir kopyalamanın haricinde çeşitli sıkıştırma algoritmaları kullanma vs.) Firmanın daha bir çok çeşit ürünü mevcut. Drive Lock ise sadece yazma koruması için olan bir ürün olmakla birlikte Disk Jocket IT nin kullanışlılığına sitesinden bakılabilir.
Forensic Computers Write Blockers Imagers Forensic Workstations Forensic Air Lite Series Tableu T335 www.forensic-computers.com	Forensic Computers firması Virginya'da bulunan ve Türk Emniyet teşkilatına ilk olarak bilgisayar kriminalistiği cihazlarının temin edildiği kaliteli bir firmadır. Digital Intelligence firması bu firmadan kopmuş ancak US Hava kuvvetlerinin ve FBI'ın desteğini almasıyla birlikte pazar payında en büyük pastayı kapmıştır. Sitesini ve üretim yaptığı donanımları özenle incelemek yararlı olacaktır.
LCTECHNOLOGY Drag 2000 Drag 1500 Mini Drag P-Drag www.lc-tech.com	Genellikle hazır dijital delil inceleme sistemleri üreten firmanın ürünleri oldukça kullanışlıdır. Dijital Delil inceleme alanında Avrupa birliğinde en çok kullanılan ancak bu alanda ABD'deki sistemleri örnek alan firmanın ürünleri bazı durumlarda yetersiz kalabilmektedir

Kaynak: Erişim http://www.ekizer.net/content/view/16/1/ 16.05.2008

ÖZGEÇMİŞ

23 Eylül 1982 yılında Ankara'da doğdu. 1993 yılında Sakarya İlköğretim Okulu'ndan,1997'de Nallıhan Şehit Vural Arıcı Anadolu Lisesi'nden, 2000 yılında Eskişehir Anadolu Teknik Lisesi'nden mezun oldu. Lisans eğitimini Marmara Üniversitesi Teknik Eğitim Fakültesi Elektronik ve Haberleşme Öğretmenliği bölümünde 2004 yılında tamamladı.

2005 Ağustos ayı itibariyle Jandarma Genel Komutanlığında Muvazzaf Muhabere Astsubayı olarak göreve başladı. Halen İstanbul Jandarma Bölge Komutanlığı'nda görev yapmaktadır.