Master's Degree in

DIGITAL FORENSICS

Overview of a Graduate Program

Begin: Oct. 2010

Digital Forensics

As a science that involves the identification, preservation, extraction, documentation,

and interpretation of digital media for evidentiary purposes

Need for an academic offer

- Better-educated digital forensics professionals will help to gain further trust of and respect for the field of digital forensics
- lack of educated personnel has negative effects upon our nation's safety, security, competitiveness, economic stability, and sense of due process
- general growing demand for students with expertise in computer forensics

Initiators

- interdisciplinary team
- The degree is a collaborative effort between various academic partners:

- Eberhard Karls University Tübingen, Faculty of Law
- University of Mannheim, Laboratory for Dependable Distributed Systems
- University of Education Thurgau, Centre of Instructional Design
- University of Applied Sciences Albstadt-Sigmaringen, Centre of Continuing Education

Philosophy of the curriculum

to provide each student with:

1. Technical computer skills, including detailed knowledge on computers and networks;
2. Digital forensics knowledge and skills covering all aspects of the field, including all procedures to be used in the identification, collection, and examination/analysis of digital evidence from a myriad of digital devices;
3. Criminal and civil legal issues so that the student understands the legal implications that may occur as a result of his/her actions;
4. Numerous practical experiences to reduce the transition time from student to working professional (lab periods)

Student Outcome Objectives

1. Preparation for becoming a digital forensics professional
2. Opportunities to establish a network of digital forensics contacts
3. An educational background directly linked to the work in a digital forensics laboratory
4. Exposure to the breadth of forensic science disciplines
5. Acculturation into the digital forensics and justice communities
6. Provision of a foundation for professional certification

Target Populations for the Degree

- graduate or advanced undergraduate students from computer science, engineering technology, information technology, or similar technical programs.
- security and IT workers from business and industry.
- local, state, and national law enforcement

Curriculum Overview

1. Semester
Basics in Computing and Networking
Basics in System Programming and Script Programming
Internet-Basics
Basics in Web-Programming
Corporate Computer Network

2. Semester
Operating Systems
Computer Networks
Informationsrecht

3. Semester
IT-Security
Grundlagen digitaler Forensik
Cyberkriminalität und Computerstrafrecht

4. Semester
Datenträgerforensik
Live Response
Cyberkriminalität und Computerstrafprozessrecht

5. Semester
Reverse Engineering
Browser- und Anwendungsforensik
Wirtschaftskriminalität

6. Semester
Master-Thesis

General Conditions

Masters Degree

- is composed of 17 required modules + thesis (120 ECTS) delivered within 6 semesters
- costs EUR 15,000 (recognition of academic credentials possible, reduces costs)
- appropriate undergraduate degree and relevant professional experience of at least 1 year required

Delivery

courses will be delivered through a hybrid format (75% online / 25% on-campus program)

- provides the ability to reach non-traditional, working and mature students
- allows to reach a geographically dispersed student population

Teaching Professionals

- prominent non-tenure track professionals with real-world experience in law enforcement and digital forensics
- Professors and Ph.D. students

Curriculum

Inhalt	Dauer (Wochen)
Modul 6: Operating Systems	
Zweck, Funktionsweise und Komponenten eines Betriebssystems Prinzipien, Ansätze, Grundsätzliche Mechanismen	1
Prozesse: Prozesse, Threads, Scheduling, Prozesskommunikation, Implemen-tierungen bei Unix und MS Windows	3
Speicherverwaltung: Memory Management, Virtueller Speicher, Paging, Im-plementierungen bei Unix und MS Windows	1
Eingabe und Ausgabe (IO): Geräte, Konzepte und Architektur für IO, Geräte-treiber	1
Sicherheit: Schutzziele, Autorisierung und Zugriffskontrolle, Hochsichere Betriebssysteme, Sicherheitskonzepte unter Unix und Windows	2
Systemprogrammierung am Beispiel LINUX und MS Windows; Ergänzungen mit MAC und Solaris	2
Praktische Aspekte I: Systemprogrammierung an Beispielen	2
Summe	12
Modul 7: Computer Networks	
ISO/OSI Referenzmodell. Grundlagen lokaler Netzwerke LAN und externer Netzwerke WAN. IP Adressing und Subneting	2
Netzwerk-Komponenten: Repeater, Hubs, Bridges, Switches, Router, Gateways	1
Topologien und Protokolle (Übersicht): Ethernet (10,100,1000), WLAN, UMTS, HSCDA, DHCP, DNS, TCP, IP, UDP, http, https, ftp, sftp, ssh usw.	1
VLAN; Routing und Routing Protokolle; Probleme in Netzwerken lokalisiern	1
Praktische Aspekte I: Netzwerke analysiern mit Sniffer und Analysator	1
Client Server Programming mit Socket API	2
Praktische Aspekte II: Implementierung einer Client-Server-Anwendung: einfacher http-Server	2
Schwächen der TCP/IP Protokollfamilie und mögliche Angriffsszenarien	1
Praktische Aspekte III: Übungen zu Angriffen und Abwehrmechanismen auf Basis der TCP/IP-Protokolle	1
Summe	12
Modul 8: Informationsrecht	
Überblick, Einordnung in das Rechtssystem, Zusammenhänge, arbeitsrechtliche Fragestellungen (u.a. persönliche Haftung von verantwortlichen Funktionsträgern eines Unternehmens), Mängelhaftung (auch Produkthaftung), Verfahrensrecht (Durchsetzung zivilrechtlicher Ansprüche)	4
Vertragsschluss: Kaufverträge im Internet, Beweiswert digitaler Dokumente	1
Immaterialgüterrecht: Urheberrecht (Schutz von „geistigem Eigentum", Rechtsschutz und Verwertung von Computerprogrammen, Rechtsschutz für Informationssysteme / Datenbanken, das Recht am eigenen Bilde), Recht der Open-Source-Software, Patentrecht, Markenrecht	3
Wettbewerbsrecht, Abmahnung, Schadenersatz, prozessuale Fragen	1
Datenschutzrecht: EU-Datenschutzrichtlinie, BDSG u.a.	1
Sonstige Rechtsfragen des Internetrechts: u.a. Aufbewahrungsfristen für elektronische Daten, Domainrecht, Web und Impressum, Pfändung	1
Rechtsentwicklungen im IT-Recht (Elektronische Signatur, Vorratsdatenspeicherung, Kryptographie) und Normen (IuKDG, TKG, TMG), internationale Fragestellungen	1
Summe	12

Inhalt	Dauer (Wochen)
Modul 9: IT-Sicherheit	
Die Ziele der IT-Sicherhiet: Vertrauen, Integrität, Verfügbarkeit; die Gefahren, die IT-Systeme bedrohen; Risiko und Methoden es zu meiden bzw. zu minimieren	1
Angriffsstrategie: die Ziele, die Voraussetzungen, die Methoden, die Tools	1
Angriff-Gegenstrategien im Überblick: Die Infrastruktur- und Die Informationssicherheit (darunter Datenschutz, Firewalls, Authentication und Verschlüsselung)	1
Die Algorithmen der symmetrischen und der asymmetrischen Verschlüsselung, die Elemente der Kryptoanalyse	2
Digitale Signatur, Digitale Zertifizierung, Public Key Infrastructure	2
Beispiele von Technologien und Systemen für die digitale Datenverschlüsselung und Signierung (u.a. Protokolle für Datenaustausch, Authentifizierungssysteme, Sicherheit Mobiler Anwendungen)	1
Praktische Aspekte I: Authentifizierung in Web Anwendungen	2
Praktische Aspekte II: Entwicklung eines selbst-signierten Zertifikates und seine Anwendung in einem Web-Server	2
Summe	12
Modul 10: Grundlagen digitaler Forensik	
Begriff „Forensik", Forensische Wissenschaften, Beispiele, Geschichte, Forensische Prinzipien: divisibility, transfer (Inman und Rudin, etc)	2
Definitionen und Abgrenzungen: Digitale vs. analoge Forensik, digitale vs. analoge Beweismittel, Digitale Beweismittel und Abstraktion (Dissertation Carrier), Klassifikation digitaler Beweismittel nach Flüchtigkeit (persistent = Festplatte, semi-persistent = RAM, flüchtig = Kabel)	2
Theoretische Forensik: Vergangenheitsinformationen in Algorithmen und Datenstrukturen (Dissertation Carrier) wissenschaftliches Arbeiten, hypothesenbasiertes Vorgehen, Beweistechniken (Über-Kreuz-Beweise)	1
forensischer Prozess, Vorgehensmodelle	2
Dokumentation forensischer Untersuchungen, Aufbau & Inhalt von forensischen Berichten	2
Praktische Aspekte: Durchführung (großer) digitaler Ermittlungen (z.B. Beschlagnahme ganzer IT-Infrastrukturen), Organisation und Analyse großer Datenmengen, Aufgabentypen und Aufgabenverteilung, Datenschutz Überblick über Automatisierung forensischer Prozesse	3
Summe	12
Modul 11: Computerkriminalität und Computerstrafrecht	
Cyberkriminalität und deren Bekämpfung: Aktualität, Entwicklungslinien, Herausforderungen	1
Grundlagen, Grundbegriffe und Grenzen des Strafrechts Voraussetzungen strafrechtlicher Verantwortlichkeit, Sanktionen	4
Systematik der Computer- und Internetdelikte, Informationstechnische Systeme als Werkzeug zur Deliktsbegehung, Informationstechnische Systeme und Netzwerke als Schutzgegenstand	5
Alternative Methoden zur Bekämpfung von (Cyber-)Kriminalität, Polizei- und Ordnungsrecht, Compliance, Störerhaftung, Unterlassungsansprüche, Filterung	2
Summe	12

Inhalt	Dauer (Wochen)
Modul 12: Datenträgerforensik	
Übersicht Speichermedien: Festplatten, Flashspeicher, Magnetbänder	1
Festplattentechnik: Aufbau, Arten von Festplatten, Standards, Schnittstellen	1
AKlassifikation von Datenträgerdaten nach Carrier, Arten von Slack Space, DOS-Partitionssystem: Partitionstabelle, primäre Partitionen, erweiterte Partitionen. Prinzipielle Analysemöglichkeiten	2
Praktische Aspekte I: Einfache Analyse von Datenträgern (z. B. mit Hex-Editor – Dateisystem betrachten, Positionen , MBR analysieren,)	1
Sicherung von Festplatten (Imaging): Lesen des Originals, Schreiben der Kopie, Integrität der Kopie, Verwenden von Hardware und Software-Write-Blockern	2
Aufbau und Analyse von Standarddateisystemen: FAT, NTFS, ext2/3/4, MAC, Solaris, Verschlüsselung von Dateien; Entsperren von gesperrten Bereichen, Arbeiten mit Passwortknacker	3
Praktische Aspekte II: Festplattenanalyse mit Standardwerkzeugen: Sleuthkit, file, foremost (file carver), Rekonstruktion gelöschter Dateien; Arbeiten mit Kommerziellen Tools (z. B. FTK, Encase, X-Ways,)	2
Summe	12
Modul 13: Live Response	
Sichern flüchtiger Daten (sniffing, kurz)	1
Rootkit-Erkennung, Live Response, Dokumentation	2
Umgang mit verschlüsselten Festplatten (z.B. TrueCrypt), Password/Key, Recovery, Cold Boot, Umgehung von Zugangssicherungen, Sichern von Hauptspeicher (z.B. über Firewire), dazu Übungen	2
Analyse von Logdateien (Betriebssystem, Firewall, Antivirus, IDS)	2
Internet-Infrastruktur-Abfrage (whois, DNS, traceroute)	2
Zugriff auf persistente Daten übers Netz (Google cache, Web Archiv, Geolocation)	2
Umgang mit Netzwerkfestplatten	1
Summe	12
Modul 14: Cyberkriminalität und Computerstrafprozessrecht	
Grundlagen, Grundbegriffe und Grenzen des Strafprozessrechts	1
Offene und verdeckte Ermittlungsmethoden, Mitwirkungspflichten Dritter	4
Beweisführung im Strafverfahren, Beweisverwertungsverbote und Datenschutz	2
Strafrechtliche und sonstige Verantwortlichkeit von ermittelnden Akteuren	1
Anwendungs- und Wirkbereich deutscher Normen	1
Internationale und europäische Zusammenarbeit	3
Summe	12

Inhalt	Dauer (Wochen)
Modul 15: Reverse Engineering	
Reverse Engineering Theorie	1
Reverse Engineering von (bösartiger) Software (Vorgehen, Tools), Fokus auf Kontrollfluss in Binärdateien, obfuscation Techniken	1
Fallstudien bekannter und unbekannter Malware	2
Reverse Engineering von Dateisystemen (Vorgehen, Experimente, Tools)	4
Fallbeispiele: Analyse von nicht-standard Dateisystemen (z.B. Serverdateisysteme, Mobiltelefone)	4
Summe	12
Modul 16: Browser- und Anwendungsforensik	
Browser Cache, History, Cookies, Zertifikate	3
Analyse von E-Mail-Clients (Outlook, Thunderbird) und Mailservern (Exchange, IMAP)	3
Blackbox-Analyse von unbekannten Anwendungen (I/O-Flow), Virtualisierung, Experimente	2
Projekte und Fallstudien mit anderen Anwendungen (VOIP, Chat/IRC, Browser Plugins, Instant Messaging)	4
Summe	12
Modul 17: Wirtschaftskriminalität	
Wirtschaftskriminalität und deren Bekämpfung: Aktualität, Entwicklungslinien, Herausforderungen	1
Wirtschaftsstrafrechtliche Besonderheiten der Tatbestands-, Rechtfertigungs- und Irrtumslehre	2
Kernstrafrecht, insbesondere Betrug, Computerbetrug und Untreue	2
Nebenstrafrecht, insbesondere Wettbewerbsdelikte, Finanzwirtschaftsdelikte, Delikte gegen das geistige Eigentum	3
Strafrechtliche Verantwortlichkeit von juristischen Personen?	2
Strafprozessrechtliche Besonderheiten bei Wirtschaftskriminalität	3
Summe	12

6. Semester

Inhalt	Dauer (Wochen)
Modul 18: Master-Thesis	
Anfertigen einer wissenschaftlichen Abschlussarbeit	1
Summe	12