

**Modulhandbuch**

**Wb Stud.-pr. Sachbearbeiter:in Digitale Forensik  
(ohne angestrebte Abschlussprüfung)**

# Inhaltsverzeichnis

<i>MNR</i>	<i>MC</i>	<i>Modulbezeichnung</i>	<i>Seite</i>
0001	03-WSES	<u>Einführung in das Studium</u>	4
0002	03-WSRGA	<u>Rechtsgrundlagen Allgemein</u>	5
0003	03-WSRGC	<u>Rechtsgrundlagen Cybercrime</u>	6
0004	03-WSDF	<u>Digitale Forensik Grundlagen</u>	7
0005	03-WSBS	<u>Betriebssysteme</u>	8
0006	03-WSNCF	<u>Netzwerke und Cloudforensik</u>	10
0007	03-WSFS	<u>Filesysteme</u>	11
0008	03-WSWZ	<u>Werkzeuge</u>	12

**Hinweis zur Bestellung der Prüfer:**

Die in dem Modulhandbuch genannten Verantwortlichen werden für die jeweilige Modulprüfung zum Prüfer bestellt.

**Formen für Prüfungsvorleistungen und Prüfungsleistungen:**

PVL-Formen: Te = Testat, s = schriftlich, m = mündlich, Prüfungsformen: M = Modulprüfung, PI = Prüfungsleistung, s = schriftlich, m = mündlich, a = alternativ, sn = sonstige

**Sonstige Abkürzungen:**

V = Vorlesung (SWS), S = Seminar/Übung (SWS), P = Praktikum (SWS), T = Tutorium (SWS), PVL = Prüfungsvorleistung, PL = Prüfungsleistung, CP = Credit Points, SWS = Semesterwochenstunden, MNR = Modulnummer, MC = Modulcode

# 0001 Einführung in das Studium

<i>Modulname:</i>	<b>Einführung in das Studium</b>	<i>Unterrichtssprache:</i>	deutsch					
<i>Modulnummer:</i>	0001	<i>Abschluss:</i>	ohne angestrebte Abschlussprüfung					
<i>Modulcode:</i>	03-WSES	<i>Häufigkeit:</i>	Sommersemester					
<i>Pflicht/Wahl:</i>	Pflicht	<i>Dauer:</i>	1					
<i>Studiengang:</i>	Wb Stud.-pr. Sachbearbeiter:in Digitale Forensik	<i>Regelsemester:</i>	1					
<i>Ausbildungsziele:</i>	Die Studierenden verstehen den Ablauf, Inhalte und Prüfungsformen des Studiums und kennen die Kommunikationsmöglichkeiten mit den Dozenten							
<i>Lehrinhalte:</i>	Vorstellung der Hochschule Kommunikationswege mit Dozenten und der Verwaltung Vorstellung der Module mit dessen Inhalte, Ziele und Prüfungsformen Semesterpläne							
<i>Lernmethoden:</i>								
<i>Literatur:</i>								
<i>Arbeitslast:</i>	<b>15</b> Stunden Lehrveranstaltungen <b>0</b> Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung							
<i>Anbieter:</i>	<u>03 Fakultät Angewandte Computer- und Biowissenschaften</u>							
<i>Dozententeam (Rollen):</i>	Prof. Dr. rer. nat. Dirk Labudde (Dozent)							
<i>Lerneinheitenformen und Prüfungen:</i>	<i>Modulstruktur</i>	<i>V</i>	<i>S</i>	<i>P</i>	<i>T</i>	<i>PVL</i>	<i>PL</i>	<i>CP</i>
	<u>Einführung in das Studium</u>	0	1	0	0			0

# 0002 Rechtsgrundlagen Allgemein

<i>Modulname:</i>	<b>Rechtsgrundlagen Allgemein</b>	<i>Unterrichtssprache:</i>	deutsch					
<i>Modulnummer:</i>	0002	<i>Abschluss:</i>	ohne angestrebte Abschlussprüfung					
<i>Modulcode:</i>	03-WSRGA	<i>Häufigkeit:</i>	Sommersemester					
<i>Pflicht/Wahl:</i>	Pflicht	<i>Dauer:</i>	1					
<i>Studiengang:</i>	Wb Stud.-pr. Sachbearbeiter:in Digitale Forensik	<i>Regelsemester:</i>	1					
<i>Ausbildungsziele:</i>	Lernziele in diesem Modul sind Kenntnisse im Ablauf von Hauptverhandlungen (Gericht, Instanzen und Spruchkörper) und die Rolle der Beteiligten, mit dem Schwerpunkt auf den Sachverständigen im Strafprozess.							
<i>Lehrinhalte:</i>	Hauptverhandlung und Rolle der Beteiligten Prozessablauf Sachverständigen Rolle							
<i>Lernmethoden:</i>								
<i>Literatur:</i>								
<i>Arbeitslast:</i>	<b>15</b> Stunden Lehrveranstaltungen <b>75</b> Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung							
<i>Anbieter:</i>	03 Fakultät Angewandte Computer- und Biowissenschaften							
<i>Dozententeam (Rollen):</i>	Prof. Dr. rer. nat. Dirk Labudde (Dozent)							
<i>Lerneinheitsformen und Prüfungen:</i>	<i>Modulstruktur</i>	<i>V</i>	<i>S</i>	<i>P</i>	<i>T</i>	<i>PVL</i>	<i>PL</i>	<i>CP</i>
	<u>Rechtsgrundlagen Allgemein</u>	1	0	0	0		Ms/60	3

# 0003 Rechtsgrundlagen Cybercrime

<i>Modulname:</i>	<b>Rechtsgrundlagen Cybercrime</b>	<i>Unterrichtssprache:</i>	deutsch					
<i>Modulnummer:</i>	0003	<i>Abschluss:</i>	ohne angestrebte Abschlussprüfung					
<i>Modulcode:</i>	03-WSRGC	<i>Häufigkeit:</i>	Sommersemester					
<i>Pflicht/Wahl:</i>	Pflicht	<i>Dauer:</i>	1					
<i>Studiengang:</i>	Wb Stud.-pr. Sachbearbeiter:in Digitale Forensik	<i>Regelsemester:</i>	1					
<i>Ausbildungsziele:</i>	Die Studierenden machen sich mit dem Begriff Cybercrime vertraut und sind in der Lage Cybercrime im engeren und weiteren Sinne auf aktuelle Straftatbestände und Straftatbestandsmerkmale anzuwenden.							
<i>Lehrinhalte:</i>	Cybercrime Ausgewählte Gesetzestexte Tatmittel Internet Phänomene im Bereich Cybercrime Objektive und subjektive Straftatbestandsmerkmale an aktuellen Phänomenen							
<i>Lernmethoden:</i>								
<i>Literatur:</i>								
<i>Arbeitslast:</i>	<b>15</b> Stunden Lehrveranstaltungen <b>75</b> Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung							
<i>Anbieter:</i>	<u>03 Fakultät Angewandte Computer- und Biowissenschaften</u>							
<i>Dozententeam (Rollen):</i>	Prof. Dr. rer. nat. Dirk Labudde (Dozent)							
<i>Lerneinheitsformen und Prüfungen:</i>	<i>Modulstruktur</i>	<i>V</i>	<i>S</i>	<i>P</i>	<i>T</i>	<i>PVL</i>	<i>PL</i>	<i>CP</i>
	<u>Rechtsgrundlagen Cybercrime</u>	1	0	0	0		Ms/60	3

# 0004 Digitale Forensik Grundlagen

<i>Modulname:</i>	<b>Digitale Forensik Grundlagen</b>	<i>Unterrichtssprache:</i>	deutsch					
<i>Modulnummer:</i>	0004	<i>Abschluss:</i>	ohne angestrebte Abschlussprüfung					
<i>Modulcode:</i>	03-WSDF	<i>Häufigkeit:</i>	Sommersemester					
<i>Pflicht/Wahl:</i>	Pflicht	<i>Dauer:</i>	1					
<i>Studiengang:</i>	Wb Stud.-pr. Sachbearbeiter:in Digitale Forensik	<i>Regelsemester:</i>	1					
<i>Ausbildungsziele:</i>	Gewinnung eines Überblicks über Aufgaben und Anforderungen der digitalen Forensik. Kennenlernen der wichtigsten Methoden und Vorgehensweisen zur Sicherung und Untersuchung digitaler Spuren sowie Vermittlung von Grundlegendem Wissen über Hard- und Software im Zusammenhang mit dem Arbeitsumfeld der digitalen Forensik.							
<i>Lehrinhalte:</i>	Einordnung der Digitalen Forensik Digitale Spuren und deren Eigenschaften Vorgehensmodelle in der Digitalen Forensik Sicherung digitaler Spuren und Anforderungen Ausgewählte Gebiete der Digitalen Forensik							
<i>Lernmethoden:</i>								
<i>Literatur:</i>								
<i>Arbeitslast:</i>	<b>30</b> Stunden Lehrveranstaltungen <b>120</b> Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung							
<i>Anbieter:</i>	03 Fakultät Angewandte Computer- und Biowissenschaften							
<i>Dozententeam (Rollen):</i>	Prof. Dr. rer. nat. Dirk Labudde (Dozent)							
<i>Lerneinheitsformen und Prüfungen:</i>	<i>Modulstruktur</i>	<i>V</i>	<i>S</i>	<i>P</i>	<i>T</i>	<i>PVL</i>	<i>PL</i>	<i>CP</i>
	<u>Digitale Forensik Grundlagen</u>	2	0	0	0		Ms/90	5

# 0005 Betriebssysteme

<i>Modulname:</i>	<b>Betriebssysteme</b>	<i>Unterrichtssprache:</i>	deutsch
<i>Modulnummer:</i>	0005	<i>Abschluss:</i>	ohne angestrebte Abschlussprüfung
<i>Modulcode:</i>	03-WSBS	<i>Häufigkeit:</i>	Sommersemester
<i>Pflicht/Wahl:</i>	Pflicht	<i>Dauer:</i>	1
<i>Studiengang:</i>	Wb Stud.-pr. Sachbearbeiter:in Digitale Forensik	<i>Regelsemester:</i>	1
<i>Ausbildungsziele:</i>	Nach diesem Modul verstehen die Studierenden den klassischen Aufbau der von Neumann Architektur mit den wichtigsten Ebenen für die Funktion eines Betriebssystems. Die Teilnehmenden kennen die verschiedenen Klassifikationen von Betriebssystemen und können gängige aktuelle Windows-, Linux und macOS-Systeme installieren, administrieren und verstehen Hintergrundprozesse, welche bedeutsam für die forensische Auswertung sind.		
<i>Lehrinhalte:</i>	<p>Betriebssystemarchitektur:</p> <ul style="list-style-type: none"> <li>• Ebenen eines Rechnersystems</li> <li>• Definition, schematischer Aufbau und Aufgabe von Betriebssystemen</li> <li>• Ressourcenverwaltung durch Betriebssysteme</li> <li>• Betriebssystemarchitekturen</li> <li>• Zugriffsverwaltung</li> <li>• Prozesse, Tasks und Threads</li> <li>• Speicherverwaltung und Speicherzugriffe</li> <li>• Datenträgeranbindung</li> </ul> <p>Windows:</p> <ul style="list-style-type: none"> <li>• Einrichtung und Administration aktueller Betriebssysteme</li> <li>• Systeminterne Spuren und forensische Aspekte (Speicherstrukturen, Event-Logging, Registrierungsdatenbank, Betriebssystemartefakte, Benutzerkonten und Gruppen)</li> <li>• Verwendung von Netzwerken und Schutzmechanismen</li> <li>• Virtualisierung und Subsysteme in Windows</li> </ul> <p>Linux:</p> <ul style="list-style-type: none"> <li>• Historie und aktuelle Distributionen</li> <li>• Filesystem Hierarchy Standard</li> <li>• Paket- und Dienstmanager</li> <li>• Sicherheitsmechanismen in Linux</li> <li>• Systeminterne Spuren und forensische Aspekte (Speicherstrukturen, Logging, Konfiguration, Betriebssystemartefakte, Benutzerkonten und Gruppen)</li> </ul> <p>macOS:</p> <ul style="list-style-type: none"> <li>• Speicherstrukturen</li> <li>• SQLite und Plist verstehen und anwenden</li> <li>• Systeminterne Spuren und forensische Aspekte (zuletzt verwendete Dokumente, Kommunikationsapps, Spotlight und</li> </ul> <p>Browser-Artefakte)</p> <ul style="list-style-type: none"> <li>• Logdateien</li> <li>• Umgang mit Diskimages und Backupmöglichkeiten (iOS und Time-Machine)</li> <li>• Grundlagen und Integration von iCloud</li> </ul>		
<i>Lernmethoden:</i>	Vorlesung online Einzel- und Gruppenübungen während der Online-Phase praktischen Aufgaben Hochschule Mittweida / BKA Wiesbaden		
<i>Literatur:</i>	Mandel, P.: Grundkurs Betriebssysteme. Wiesbaden: Vieweg, 4. Aufl. 2014 Schneider, U. (Hrsg.): Taschenbuch der Informatik. München: Hanser (Leipzig: Fachbuchverlag), 7. Auflage, 2012 Tanenbaum, A.S.: Moderne Betriebssysteme, 3. Aufl., Pearson Studium, 2009		
<i>Arbeitslast:</i>	<b>90</b> Stunden Lehrveranstaltungen <b>120</b> Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung		
<i>Anbieter:</i>	<u>03 Fakultät Angewandte Computer- und Biowissenschaften</u>		
<i>Dozententeam (Rollen):</i>	<u>Prof. Ronny Bodach</u> (Dozent)		

Lerneinheitenformen und Prüfungen:	Modulstruktur	V	S	P	T	PVL	PL	CP
		Betriebssysteme	4	0	2	0		Ms/90

# 0006 Netzwerke und Cloudforensik

<i>Modulname:</i>	<b>Netzwerke und Cloudforensik</b>	<i>Unterrichtssprache:</i>	deutsch					
<i>Modulnummer:</i>	0006	<i>Abschluss:</i>	ohne angestrebte Abschlussprüfung					
<i>Modulcode:</i>	03-WSNCF	<i>Häufigkeit:</i>	Sommersemester					
<i>Pflicht/Wahl:</i>	Pflicht	<i>Dauer:</i>	1					
<i>Studiengang:</i>	Wb Stud.-pr. Sachbearbeiter:in Digitale Forensik	<i>Regelsemester:</i>	1					
<i>Ausbildungsziele:</i>	Das Modul Netzwerke bietet eine Einführung in das Themengebiet Netzwerktechnik und Cloudforensik. Ziel ist es, Grundlagenwissen aus diesem Gebiet zu vermitteln. Nach Besuch des Moduls sind die Studierenden mit der Funktionsweise unterschiedlicher Netzwerkdienste vertraut und kennen Besonderheiten und Herausforderungen bei der forensischen Analyse von Clouddaten.							
<i>Lehrinhalte:</i>	<p>Entwicklung und Struktur weltweiter Netzwerke</p> <p>Cloud-Computing Architekturen</p> <p>Virtualisierung (Speicher- und Netzwerkvirtualisierung)</p> <p>OSI Schichtenmodell</p> <p>Protokolle (IP, ICMP, TCP, TPC, UDP, Mac, ARP)</p> <p>IPv4 vs. IPv6</p> <p>DNS und URL</p> <p>Möglichkeiten der Verbindungshardware</p> <p>Technische Grundlagen (Hardware und Software)</p> <p>Funktionsweise E-Mail, FTP, Peer to Peer</p> <p>Anonymisierungsdienste</p> <p>TOR-Netzwerk</p> <p>Herausforderungen Cloudforensik im Bereich SaaS und PaaS</p>							
<i>Lernmethoden:</i>	<p>Vorlesung online</p> <p>Einzel- und Gruppenübungen während der Online-Phase</p>							
<i>Literatur:</i>	<p>Michael Gregg: Hack the Stack. Syngress, 2006.</p> <p>Ryan Trost: Practical Intrusion Analysis. Addison-Wesley, 2009</p> <p>Michael S Collins: Network Security Through Data Analysis: Building Situational Awareness. O'Reilly, 2014.</p> <p>Michael Messner: Metasploit. dpunkt, 2012</p> <p>Eric Amberg: Linux-Server mit Debian 8 GNU/Linux. Mitp, 2015.</p> <p>Limoncelli, T.A., Hogan, C.J. et al: The Practice of System and Network Administration. Addison-Wesley Longman 2007.</p> <p>Klaus M. Rodewig: Webserver einrichten und administrieren. Galileo Computing, 2011.</p> <p>Brian Carrier: File System Forensic Analysis. Addison-Wesley, 2005.</p>							
<i>Arbeitslast:</i>	<p><b>30</b> Stunden Lehrveranstaltungen</p> <p><b>120</b> Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung</p>							
<i>Anbieter:</i>	03 Fakultät Angewandte Computer- und Biowissenschaften							
<i>Dozententeam (Rollen):</i>	<p><u>Prof. Dr. rer. pol. Dirk Pawlaszczyk</u> (Dozent)</p> <p><u>Philipp Engler</u> (Dozent)</p>							
<i>Lerneinheitenformen und Prüfungen:</i>	<i>Modulstruktur</i>	<i>V</i>	<i>S</i>	<i>P</i>	<i>T</i>	<i>PVL</i>	<i>PL</i>	<i>CP</i>
	<u>Netzwerke und Cloudforensik</u>	2	0	0	0		Ms/90	5

# 0007 Filesysteme

<i>Modulname:</i>	<b>Filesysteme</b>	<i>Unterrichtssprache:</i>	deutsch					
<i>Modulnummer:</i>	0007	<i>Abschluss:</i>	ohne angestrebte Abschlussprüfung					
<i>Modulcode:</i>	03-WSFS	<i>Häufigkeit:</i>	semesterweise					
<i>Pflicht/Wahl:</i>	Pflicht	<i>Dauer:</i>	1					
<i>Studiengang:</i>	Wb Stud.-pr. Sachbearbeiter:in Digitale Forensik	<i>Regelsemester:</i>	2					
<i>Ausbildungsziele:</i>	Das Module Filesysteme erläutert, was ein Dateisystem ist und wozu diese entwickelt wurden. Gleichzeitig werden Grundlegende Begriffe wie Sektoren und Cluster und deren Bedeutung erklärt. Nach erfolgreicher Teilnahme am Modul sind die Studierenden befähigt, gängige Dateisysteme zu verstehen und forensische Analysen manuell durchzuführen.							
<i>Lehrinhalte:</i>	<p>Einführung:</p> <ul style="list-style-type: none"> <li>• Grundbegriffe und Bedeutung von Dateisystemen</li> <li>• Festplattenpartitionierung (Master Boot Record und GPT Partitionierung)</li> <li>• Besonderheiten in Dateisystemen (Zeitstempel, Slackspeicher, Disabling Last Access Timestamp)</li> </ul> <p>Windows Dateisysteme:</p> <ul style="list-style-type: none"> <li>• FAT-Dateisysteme (Aufbau FAT-Partition, Strukturen im FAT Dateisystem, Löschung und Wiederherstellung von Daten in FAT)</li> <li>• NTFS-Dateisystem (Historie, Aufbau von NTFS, Strukturen im NTFS, Speichern und Löschen von Daten in NTFS)</li> <li>• ExFAT Dateisystem (Aufbau ExFAT-Partition, Strukturen im ExFAT Dateisystem, Löschung und Wiederherstellung von Daten in ExFAT)</li> <li>• LDM, WSS und ReFS Dateisystem</li> </ul> <p>Linux Dateisysteme:</p> <ul style="list-style-type: none"> <li>• Ext-Dateisystem (Klassifikation von Linux Dateisysteme, Grundlegendes und Komptabilität von Extx, Besonderheiten von Ext3 und Ext4, Journaling in Ext, Sparse, Flex und Meta Blockgroups)</li> <li>• F2FS Dateisystem (Aufbau Log Structured Dateisysteme, Aufbau von F2FS, Strukturen im F2FS, Speichern und Löschen von Daten in F2FS)</li> <li>• Logical Volume Manager / Device Mapping</li> </ul> <p>macOS Dateisysteme:</p> <ul style="list-style-type: none"> <li>• HFS+ (Historie, Aufbau von HFS, Strukturen im HFS, Besonderheiten der B-Tree Strukturen, Speichern und Löschen von Daten in HFS)</li> <li>• APFS (Neuerungen und Features von APFS, Aufbau von APFS Partitionen, Forensische Untersuchung von APFS Container)</li> </ul>							
<i>Lernmethoden:</i>	Vorlesung online Einzel- und Gruppenübungen während der Online-Phase praktischen Aufgaben							
<i>Literatur:</i>								
<i>Arbeitslast:</i>	<b>90</b> Stunden Lehrveranstaltungen <b>120</b> Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung							
<i>Anbieter:</i>	03 Fakultät Angewandte Computer- und Biowissenschaften							
<i>Dozententeam (Rollen):</i>	Prof. Ronny Bodach (Dozent)							
<i>Lerneinheitsformen und Prüfungen:</i>	<i>Modulstruktur</i>	<i>V</i>	<i>S</i>	<i>P</i>	<i>T</i>	<i>PVL</i>	<i>PL</i>	<i>CP</i>
	Filesysteme	3	0	2	1		Ms/90	7

# 0008 Werkzeuge

<i>Modulname:</i>	<b>Werkzeuge</b>	<i>Unterrichtssprache:</i>	deutsch					
<i>Modulnummer:</i>	0008	<i>Abschluss:</i>	ohne angestrebte Abschlussprüfung					
<i>Modulcode:</i>	03-WSWZ	<i>Häufigkeit:</i>	jahresweise					
<i>Pflicht/Wahl:</i>	Pflicht	<i>Dauer:</i>	1					
<i>Studiengang:</i>	Wb Stud.-pr. Sachbearbeiter:in Digitale Forensik	<i>Regelsemester:</i>	2					
<i>Ausbildungsziele:</i>	In diesem Modul werden Teilnehmende dazu befähigt, Werkzeuge zur forensischen Auswertung digitaler Systeme zu verwenden und eigenständig forensische Analysen an Datenträgern und IT-Systemen durchzuführen. Die Teilnehmenden können unter anderem X-Ways, Autopsy, Dumpl, LiME und Volatility anwenden und kennen weitere Werkzeuge zur forensischen Analyse von Datenträgern.							
<i>Lehrinhalte:</i>	<p>spezielle Werkzeuge</p> <ul style="list-style-type: none"> <li>• Tools zur Datensicherung (GUI, CLI, Datensicherungsformate, etc.)</li> <li>• Tools zur Analyse und Aufbereitung (xmount, scalpel, etc.)</li> </ul> <p>spezielle Methoden der digitalen Forensik</p> <ul style="list-style-type: none"> <li>• Sicherung defekter Datenträger</li> <li>• RAID Sicherung</li> <li>• RAM Sicherung</li> <li>• Carving</li> <li>• GdPDU/GoBD</li> </ul> <p>Datenuntersuchung mit Forensik Frameworks</p> <ul style="list-style-type: none"> <li>• X-Ways</li> <li>• Sleuthkit/Autopsy</li> </ul> <p>Virtualisierung</p> <ul style="list-style-type: none"> <li>• Grundlagen der Virtualisierung</li> <li>• Datensicherung innerhalb Virtualisierungsumgebungen (Docker, QEMU, ESxi, Hyper V, OpenVZ, etc.)</li> <li>• Virtualisierung von Beweismitteln (Grundlagen, Einrichtung, Rücksetzen von Benutzerkennungen, etc.)</li> </ul>							
<i>Lernmethoden:</i>	Vorlesung online Einzel- und Gruppenübungen während der Online-Phase praktischen Aufgaben							
<i>Literatur:</i>								
<i>Arbeitslast:</i>	<b>90</b> Stunden Lehrveranstaltungen <b>120</b> Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung							
<i>Anbieter:</i>	03 Fakultät Angewandte Computer- und Biowissenschaften							
<i>Dozententeam (Rollen):</i>	Martin Klöden (Dozent)							
<i>Lerneinheitenformen und Prüfungen:</i>	<i>Modulstruktur</i>	<i>V</i>	<i>S</i>	<i>P</i>	<i>T</i>	<i>PVL</i>	<i>PL</i>	<i>CP</i>
	<u>Werkzeuge</u>	3	0	2	1		Ms/90	7