

# Zur Aktualisierung von Studienbriefen am Beispiel der Mobilfunkforensik

Björn Roos, Harald Baier

da/sec - Biometrics and Internet Security Research Group

Hochschule Darmstadt, Darmstadt, Germany

Email: {bjoern.roos, harald.baier}@{h-da, cased}.de

## Zusammenfassung

Die sich sehr schnell wandelnde Technologielandschaft erfordert von den Mitarbeitern, wie Studierenden, sich dynamisch wandelnde Inhalte und Kompetenzen anzueignen. Lebenslanges Lernen ist daher heute eine Selbstverständlichkeit, um das benötigte Know-how im (späteren) Berufsleben auf dem aktuellen Stand zu halten. Neue Themengebiete implizieren aber den dynamischen Wandel von Studien- und Weiterbildungsinhalten, eine große Herausforderung für Hochschulen und Weiterbildungsträger. Bei der Erstellung und Überarbeitung von Studien- und Weiterbildungsinhalten ist wichtig zu entscheiden, welche der Inhalte aktuell sind und welche gestrichen werden können. Im nächsten Schritt muss eine geeignete Möglichkeit zur Integration der Neuerungen gefunden werden. Allerdings kann die Umsetzung dieser Schritte zu unerwünschten Ergebnissen führen, wie z. B. die Überschreitung des Umfangs. Ein Ansatz zur Lösung dieser Herausforderungen liefert die Didaktik mithilfe eines mesodidaktischen Konzepts.

Die vorliegende Publikation leistet einen Beitrag zu der Frage, wie sich Neuerungen in Studieninhalte am Besten integrieren lassen. Dies ist Teil des Ausbildungskonzepts des OPEN C3S Projektes. Grundlage hierfür ist vor allem die didaktische Konzeption der Module. Wir zeigen und erläutern anhand eines Fallbeispiels die Wirksamkeit der mesodidaktischen Konzeption eines Lehrmoduls an Hand des Weiterbildungsmoduls „Einführung in die Computerforensik“. Dieses wurde für das OPEN C3S Projekt entwickelt und enthält Lehrinhalte im Bereich Mobilfunkforensik. Gerade in diesem Bereich müssen die Inhalte aufgrund des technischen Fortschrittes oftmals angepasst werden. Das mesodidaktische Konzept beinhaltet mehrere Maßnahmen, damit Neuerungen auf diesem Gebiet schnell und effektiv integriert werden können.

## 1 Einleitung

In naher Zukunft werden auf dem deutschen Arbeitsmarkt vermehrt Fachkräfte benötigt. Vor allem im Bereich Informatik mit dem Schwerpunkt IT-Sicherheit wird es einen großen Bedarf geben. Laut dem Verband Bitkom existierten Ende Oktober 2012 43000 offene Stellen im IT-Sektor [Pfis13]. Die vermehrte Nachfrage zeigt, dass der IT-Bereich ein sehr stark wachsender Markt ist, der der wandelnden Technologielandschaft unterworfen ist. Allerdings benötigen neue Technologien auch neue Kompetenzen, die die Fachkräfte mitbringen müssen. Diese können durch Fort- und Weiterbildungen erlangt werden. Ein lebenslanges Lernen ist daher heute eine Selbstverständlichkeit, um das benötigte Know-how im Berufsleben auf dem aktuellen Stand zu halten. Denn das erlangte Wissen und die gewonnenen Fähigkeiten der Berufsausbildung, sowie die Erfahrungen von einigen Berufsjahren reichen nicht mehr für eine gesamte berufliche Laufbahn aus, um diese erfolgreich zu bewältigen. Das lebenslange Lernen

ist somit eine komplexe Herausforderung und ist für den Einzelnen und für die Gesellschaft unverzichtbar geworden. Es soll den Menschen das ganze Leben lang begleiten und in erster Linie zu einem bewusstem, zweckorientiertem, zielorientiertem und systematischem Lernen befähigen, das von der vorschulischen Bildung bis zur Altenbildung reicht [BuLe13].

Das zu vermittelnde Wissen ist ebenso dem technologischen Wandel unterworfen und führt dazu, dass die Lehrinhalte ständigen Veränderungen unterworfen sind, um das benötigte Know-how zu vermitteln. Die dynamischen Lehr- und Weiterbildungsinhalte sind aber für Hochschulen und Weiterbildungsträger eine große Herausforderung. Es muss entschieden werden, welche Inhalte aktuell sind und welche gestrichen werden können. Dies ist aber nur ein Teil der Herausforderung, denn die Neuerungen müssen auch in die Lehrinhalte integriert werden können, ohne dass es zu unerwünschten Ergebnissen, wie z. B. der Überschreitung des Umfangs kommt. Ein Ansatz zur Lösung dieser Herausforderung liefert die Didaktik mithilfe eines mesodidaktischen Konzepts, wie es beim Modellprojekt „effekt“ angewandt wurde [SaSc11]. Dieses Konzept wurde an einem Fernstudiummodul des OPEN C3S (Open Competence Center for Cyber Security) Projektes, anhand eines Fallbeispiels getestet.

Das OPEN C3S Projekt [Open13] ist ein hochschuloffenes Verbundvorhaben von Hochschulen und Universitäten für ein transdisziplinäres Programm wissenschaftlicher Weiterbildung im Sektor Cyber Security, das durch das Bildungsministerium für Bildung und Forschung gefördert wird. Ziel des Verbundes ist es, dem Bedürfnis der Wirtschaft für eine akademische Begleitung des lebenslangen Lernens in einer modernen Informations- Wissenschaftsgesellschaft gerecht zu werden. Die Kernziele des Projektes sind zum einen die Verfügbarkeit von Fachkräften und zum anderen die Bildungsgerechtigkeit zu verbessern. Hierbei werden die Hochschulen für nicht-traditionell Studierende geöffnet [Open13]. Das OPEN C3S Projekt umfasst einige Aus- und Weiterbildungsangebote, die durch ein Fernstudium, neben Zertifikaten, einen Bachelor und Master of Science Abschluss ermöglichen.

Für den Bachelorstudiengang IT-Sicherheit in OPEN C3S sind Themen, wie die Mobilfunkforensik sehr relevant, da immer mehr Menschen, ob im Privat- oder Berufsleben die Mobiltelefone als Ersatz für Netbooks oder Notebooks verwenden. Diese Geräte bieten aus diesem Grund für die Polizei, wie auch für Kriminelle ein umfangreiches Informationspotential. Das Gebiet der Mobilfunkforensik unterliegt dabei einem starken technologischen Wandel. Die Lehrinhalte in diesem Bereich müssen deshalb sehr oft aktualisiert werden, um die benötigten Kompetenzen zu vermitteln.

Der zentrale Beitrag des vorliegenden Papers ist daher die Übertragung des mesodidaktischen Konzepts auf den Cluster Cybersecurity. Nach einer Analyse des Konzepts zeigen wir exemplarisch an dem Fernstudiummodul 'Einführung in die Computerforensik' des OPEN C3S (Open Competence Center for Cyber Security) Projektes, wie Mesodidaktik die Problemstellung der Aktualisierung dynamischer Inhalte ermöglicht.

Der Rest des Beitrages ist wie folgt aufgebaut: Innerhalb des Abschnitts 2 erläutern wir das Problem der Konzeption von Studieninhalten, die dem technologischen Wandel unterworfen sind und erläutern weiter unsere Klassifizierung von Lehrinhalten. Im Abschnitt 3 erläutern wir unser Lösungskonzept zur Integration neuer Inhalte, das auf der didaktischen Konzeption von Lernaufgaben basiert, welches im Modellprojekt „effekt“ verwendet wurde, anhand eines Fallbeispiels. Abschließend fassen wir unser Ergebniss im Abschnitt 4 zusammen.

## 2 Problemstellung

Es gibt Lehrinhalte in Studiengängen, die aufgrund ihrer Art ständig Veränderungen bzw. Neuerungen unterworfen sind und solche, die kaum Veränderungen erfahren. Als Beispiel hierzu können Inhalte der Mathematik und Informatik herangezogen werden. Im Bereich der Mathematik gibt es bei den Lehrinhalten gar keine oder sehr wenig Neuerungen. Anders hingegen bei der Informatik. Hier gibt es sehr viele Änderungen in kurzer Zeit. Dabei sind ältere Inhalte teilweise noch gültig, wobei andere Inhalte aufgrund der technologischen Entwicklung an Bedeutung verlieren und somit in der Lehre keine Relevanz mehr haben.

Die Mobilfunkforensik, als Teilbereich der Informatik, ist solch ein Bereich der großen Wandlungen unterworfen ist, da die Inhalte sehr schnelllebig sind. Die Aktualität der Inhalte und deren Aktualisierung kann zu einem Overhad führen. Weiter besteht das Problem zu entscheiden, auf welche Inhalte verzichtet werden kann und welche Neuerungen in welcher Form aufgenommen werden.

Um zu entscheiden, welche Inhalte aktualisiert bzw. gestrichen werden sollen, müssen diese zunächst klassifiziert werden. Als Klassifikationsfaktor lässt sich die Art des Inhaltes heranziehen.

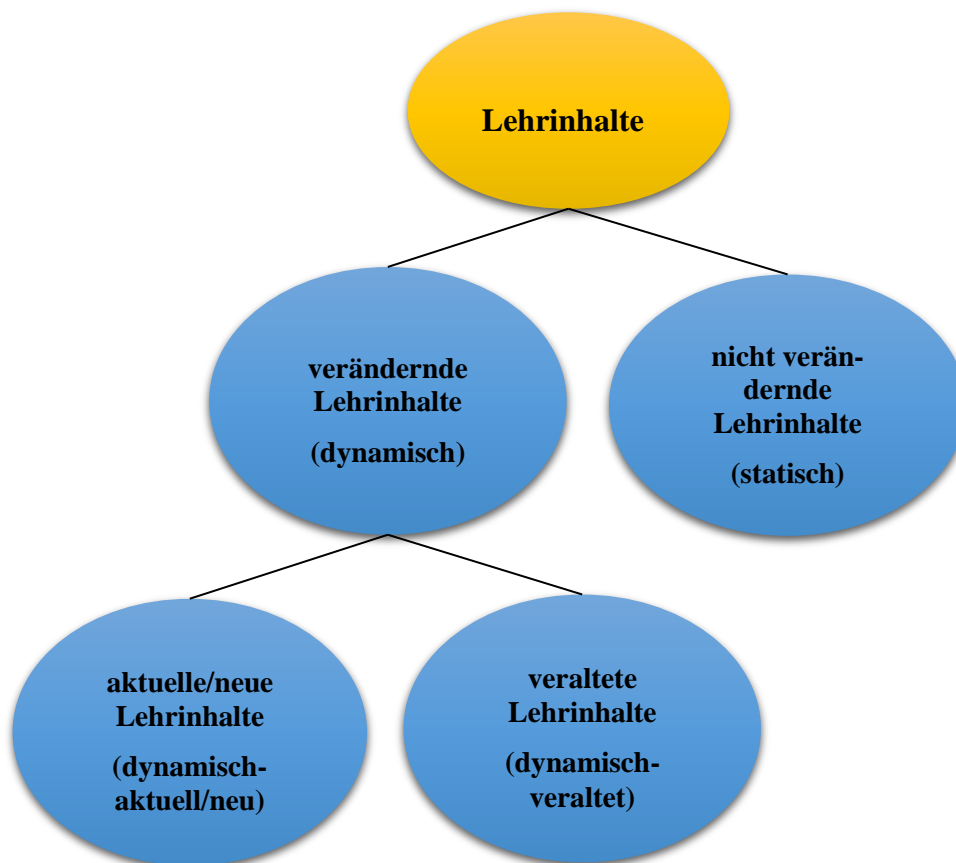


Abbildung 1: Taxonomie der Lehrinhalte<sup>1</sup>.

<sup>1</sup> Die Taxonomie wurde selbst erstellt.

Die Inhalte können nach dynamisch-aktuell/neu, dynamisch-veraltet und statischen Lehrinhalten unterschieden werden. Statische Lehrinhalte sind Inhalte, die sich nicht verändern. Dynamisch-aktuelle Inhalte sind zum jetzigen Zeitpunkt aktuell. Es ist aber abzusehen, dass diese in absehbarer Zeit veraltet sein werden und erneuert bzw. aktualisiert werden müssen. Dynamisch-neue Lehrinhalte sind Inhalte, die aufgrund ihrer Aktualität neu als Lehrinhalte aufgenommen worden sind. Es ist aber abzusehen, dass auch sie in absehbarer Zeit veraltet sein werden. Dynamisch-veraltete Inhalte sind Lehrinhalte, die zum jetzigen Zeitpunkt nicht mehr aktuell sind und aktualisiert werden müssen.

Die Klassifikation hilft zu entscheiden, welche Inhalte aktualisiert werden sollen. Sie wirft aber auch gleichzeitig die Frage auf, zu entscheiden, wann etwas veraltet ist. Dies ist abhängig vom vermittelnden Lehrinhalt und lässt sich leicht beantworten, wenn der Entwickler auf dem neuesten Stand ist.

Als Beispiel werden Inhalte des Moduls „Einführung in die Computerforensik“ anhand der Klassifizierung unterschieden. Die Inhalte beziehen sich nur auf das Android OS, da es das derzeit am weitesten verbreitete Betriebssystem für Smartphones ist. Rund 40 Prozent aller Endgeräte nutzen das Google-OS [Bitk12]. Folgende Inhalte wurden klassifiziert:

- Die allgemeinen forensischen Grundprinzipien werden sich nicht oder wenig ändern (statisch).
- Das YAFFS-Dateisystem. Dieses Dateisystem wird bis zur Android Version 2.2 in vielen Geräten verwendet. Ab 2.3 wird das Dateisystem EXT4 verwendet. Im Moment verwenden noch 5,8 % aller Android Geräte eine Android Version, die kleiner ist als die Version 2.3 [Stat12]. Das YAFFS-Dateisystem ist somit noch verbreitet und spielt im Mobilfunkforensikbereich für eine gewisse Zeit noch eine Rolle. Die Inhalte sind noch aktuell, aber in absehbarer Zeit werden sie veraltet sein (dynamisch-aktuell).
- Die Android 1.6 Struktur und Inhalte haben sich gegenüber den neueren Android Versionen geändert. Das wäre kein Problem, wenn Android 1.6 noch eine große Verbreitung hätte. Aber nur noch 0.10% aller Android Geräte verwenden diese Version. Deswegen sind diese Inhalte veraltet (dynamisch-veraltet).

Um die Aktualität des zu vermittelnden Stoffes zu gewährleisten und die einhergehenden Probleme, wie der übermäßige Lehraufwand entgegen zu wirken, müssen diese anhand eines Konzeptes gelöst werden.

## 3 Lösungskonzept

Das Lösungskonzept basiert auf der didaktischen Konzeption von Lernaufgaben, das im Modellprojekt „effekt“ verwendet wurde [SaSc11]. Für die Entwicklung der Module wurde auf die verwendete mesodidaktische Konzeption zurückgegriffen und den Bedürfnissen für die eigene Modulentwicklung angepasst. Die Konzeption der Module gehört zur Mesodidaktik, die ein Teil der Didaktik ist. Aus diesem Grund erfolgt zunächst eine kurze Einführung in die Didaktik.

### 3.1 Einführung in die Didaktik

Das Wort „Didaktik“ kommt aus dem altgriechischen und bedeutet „Lehrkunst“. Sie wurde erstmals von Johann Amos Comenius in seinem Werk „Didactics Magna“ als „Lehrkunst“, der vollständigen Kunst einem Menschen alles beizubringen, beschrieben. Die Didaktik beschäf-

tigt sich heute im engeren Sinn mit der Theorie des Unterrichts und im weiteren Sinne mit der Theorie und Praxis des Lehrens und Lernens [Dude13]. Die Didaktik stellt keine eigene autonome Wissenschaft dar. Sie ist wie viele andere Wissenschaften auch, auf die Integration des Wissens aus verschiedenen Partnerwissenschaften angewiesen und stellt eben gerade dadurch ihre wissenschaftliche Eigenständigkeit dar. Neben den allgemeinen Didaktiken, die theoretisch umfassend und praktisch folgenreich die Voraussetzungen, Möglichkeiten, Folgen und Grenzen des Lernens und Lehrens erforschen und strukturieren [Dida13a], gibt es Fachdidaktiken und Spezialdidaktiken, die zur Anwendung kommen, wenn der Unterricht nur einem bestimmten Fächerkanon zum Gegenstand hat [Dida13b]. Die allgemeinen Didaktiken wurden in den 60er und -70er Jahren rege diskutiert und in diesem Zeitraum wurden viele allgemeindidaktische Modelle entwickelt und angewandt. Allerdings sind bis heute nur wenige Ansätze entstanden und die Entwicklung neuer Modelle verläuft zurückhaltend [Dida13a]. Die didaktischen Theorien und Modelle können nach Bildung, Lernen und Interaktion eingeteilt werden.



Abbildung 2: Didaktische Theorien und Modelle [Dida13a].

Grundsätzlich beschäftigt sich die Didaktik mit den Fragen der Analyse und Deskription sowie der Planung und Präskription des Unterrichts. Hierbei treten zwei didaktische Probleme auf. Problematisch ist zum einen die Auswahl des Unterrichtsinhalts aus dem Bereich aller möglichen Inhalte (didaktische Reduktion) und die Aufbereitung der ausgewählten Inhalte hinsichtlich der Intention und der Adressaten (didaktische Transformation). Nach der didaktischen Reduktion und Transformation wird der Inhalt zum Lehrgegenstand [Wiki13b].

Die Didaktik läßt sich weiter in drei Ebenen klassifizieren, der Makrodidaktik, der Mesodidaktik und die Mikrodidaktik. Die Makrodidaktik beschäftigt sich allgemein mit Unterrichtskonzepten oder Lernbereichen. Die Mikrodidaktik beschäftigt sich mit der Gestaltung von Unterricht. Die Mesodidaktik ist als Ebene dazwischen geschaltet und beschreibt die Unterrichtseinheiten [Eloq13].

### **3.2 Übersicht auf die mesodidaktische Konzeption der Lernmaterialien des Modellprojektes „effekt“**

Das Modellprojekt „effekt“ ist ein vom Bundesministerium für Bildung und Forschung gefördertes Forschungsvorhaben im Rahmen des Förderprogramms „Neue Medien in der Bildung“.

Die didaktische Konzeption der Lehr-Lernmaterialien hat als Basis das Prinzip der Arbeitsprozessorientierung und der Handlungsorientierung. Die Ausbildungsmaterialien wurden hierbei adaptiv gehalten, um sie langfristig an sich verändernde Lerninhalte und Rahmenbedingungen anpassen zu können [SaSc11].

Die mesodidaktische Konzeption der Lernaufgaben beinhaltet einen modularen Aufbau der Lernaufgaben. Diese sind untergliedert in Kern- und darin enthaltene Teilaufträge. Sie erlaubt eine flexible Anpassung an sich verändernde Rahmenbedingungen. Dadurch können technologische Neuerungen und betriebliche Anforderungen sehr gut eingebunden werden [SaSc11].

Die Konzeption erläutert nur wie Neuerungen eingebunden werden können. Sie gibt allerdings keine Antwort auf die Frage, was Neuerungen sind oder welche veraltete Inhalte herausgestrichen werden können. Dies wird weiter unten näher erläutert.

### **3.3 Mesodidaktische Konzeption des OPEN C3S Projekt Moduls Einführung in die Computerforensik**

Als Basis für die didaktische Konzeption des OPEN C3S Projektes dient das Prinzip der Handlungsorientierung. Handlungsorientierung bedeutet eine Verknüpfung von Lernen und Handeln. Der handlungsorientierte Unterricht ist ein ganzheitliches Modell. Der Schüler bzw. Student wird hierbei zunehmend in problemorientierte Situationen versetzt, die er durch große Eigenaktivität lösen muß. Dieser Ansatz ist weit bei Fernkursen in der beruflichen Aus- und Weiterbildung verbreitet [Fern13].

Beim Modul „Einführung in die Computerforensik“ wurde, wie auch beim Projekt „effekt“ die Lernaufgaben, modular aufgebaut. Jedes Modul besteht aus verschiedenen Studienbriefen (beim „effekt“ Projekt werden diese als Kernaufträge bezeichnet), die jeweils ein eigenständiges Themengebiet abhandeln.

## Modul 1

### Einführung in die Computer Forensik

---

Studienbrief 1: Einführung

Studienbrief 2: Klassische forensische Wissenschaften

Studienbrief 3: Digitale Forensik

Studienbrief 4: Einführung Dateisystemanalyse

Studienbrief 5: Tools

Studienbrief 6: Anwendungsforensik

Studienbrief 7: Mobilfunkforensik

Abbildung 3: Modularer Aufbau des Moduls Einführung in die Computerforensik.

Jeder Studienbrief selbst ist wieder unterteilt in verschiedene Unterthemengebiete (beim „effekt“ Projekt werden diese als Teilaufträge bezeichnet). Das ganze Modul mit seinen Studienbriefen und die darin enthaltenen Unterthemen können allein durch den Aufbau schon flexibel an Neuerungen angepasst werden.

Die flexible Anpassung wird zusätzlich noch vereinfacht, wenn eine entsprechende Umgebung verwendet wird. Durch die Verwendung eines Latex-Templates ist es im Gegensatz zu einem Word-Template einfacher neue Inhalte einzubinden. Ganze Themengebiete in Studienbriefen, sogar ganze Studienbriefe selbst können einfach mithilfe des Latex-Befehls „include“ eingebunden werden.

```
%%% Hauptteil
\include{studienbrief_1} % Einführung

\include{studienbrief_2} % Klassische forensische Wissenschaften

\include{studienbrief_3} % Digitale Forensik

\include{studienbrief_4} % Einführung Dateisystemanalyse

\include{studienbrief_5} % Tools

\include{studienbrief_6} % Anwendungsforensik

\include{studienbrief_7} % Mobilfunkforensik
```

Abbildung 4: Einbindung der Inhalte mittels des Latex Befehls include.

### 3.4 Was sind neue bzw. alte Inhalte?

Im Abschnitt 3.3 haben wir gezeigt, wie neue Inhalte eingebunden und alte Inhalte herausgestrichen werden können. Allerdings stellt sich nun die Frage, was Neuerungen sind bzw. was ist veraltet?

Um diese Frage beantworten zu können, ist es notwendig, die Bedeutung des Wortes Neuerung zu kennen. Der Begriff Neuerung hängt sehr eng mit dem Wort Innovation zusammen. Dieses leitet sich aus dem lateinischen Wort „innovare“ ab, welches „erneuern“ bedeutet und bedeutet in seinem ursprünglichen Wortsinn „(Er-)Neuerung“ [Röpk13]. Der Begriff ist nicht allgemeingültig definiert, sodass nur Umschreibungen dafür existieren. Allgemein bedeutet Innovation eine Neuerung, die aus technischem, sozialem und wirtschaftlichem Wandel einhergeht [Röpk13]. Betrachtet man dies im engeren Sinne, so resultieren Innovationen bzw. Neuerungen erst dann aus Ideen, wenn diese in neue Produkte, Dienstleistungen oder Verfahren umgesetzt werden, die tatsächlich eine erfolgreiche Anwendung finden und den Markt durchdringen [Wiki13a]. Kehrt man den Begriff Neuerung nach dem engeren Sinn um, so erhält man die Definition für veraltete Inhalte. Dementsprechend sind veraltete Inhalte, Produkte, Dienstleistungen oder Verfahren, die keine erfolgreiche Anwendung mehr finden und den Markt nicht mehr durchdringen.

Wendet man diese Definition von Innovation bzw. Neuerung auf die Mobilfunkforensik und hier im Speziellen, auf das Android OS an, so läßt, sich aus Abbildung 4 erkennen, dass Android in der Version 1.6 nur noch einen Marktanteil von 0,10% hat und somit veraltet ist, da es den Markt nicht mehr durchdringt.

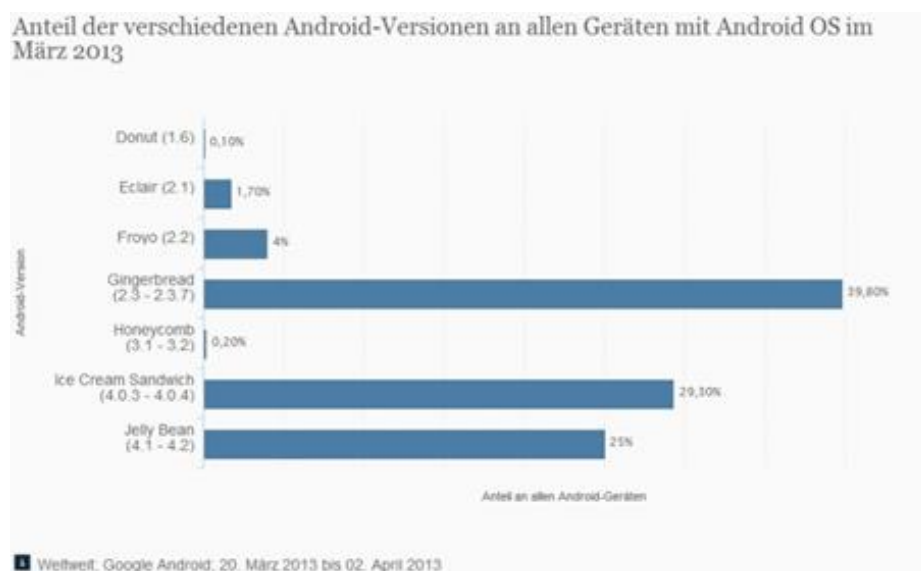


Abbildung 5: Verbreitung der Android OS Versionen vom 20.März bis 02. April 2013 [Stat12].

Weiter lässt sich erkennen, dass das Android OS in der Version 2.3.x den größten Marktanteil in Höhe von 39,80% besitzt und somit zum jetzigen Zeitpunkt, die größte Verbreitung am Markt erfährt. Das Android OS 2.3.x (Gingerbread) hat sich somit als Neuerung gegenüber dem Android OS 1.6 durchgesetzt. Die Android Version ab 4.1- 4.2 (Jelly Bean) als Neuheit gegenüber vorherigen Android Versionen besitzt schon jetzt einen Marktanteil von 25% und wird sich gegenüber allen vorherigen Versionen durchsetzen.

Nimmt man nun Bezug zu der in Kapitel 1 definierten Klassifizierung von Inhalten, so lässt sich nun Folgendes in Bezug auf Neuerungen im Bereich des Mobilfunks ableiten:

- Inhalte, die das Android OS 1.6 betreffen, sind als veraltet anzusehen. (dynamisch-veraltet)



- Inhalte, die die Android Version 2.3.x betreffen, sind zum jetzigen Zeitpunkt noch aktuell. Sie werden allerdings in absehbarer Zeit veraltet sein (dynamisch-aktuell).
- Alle Inhalte, die die Android Version 4.x betreffen sind als Neuerungen anzusehen (dynamisch-neu).

Hierzu mehrere Klassifizierungsbeispiele aus dem Modul „Einführung in die Computerforensik“:

**Beispiel 1:** Das Modul beinhaltet Lehrinhalte, die das YAFFS2-Dateisystem betreffen. Dieses wurde bis zur Android Version 2.2 in vielen Geräten verwendet. Ab Android 2.3 wird nun das Linuxdateisystem EXT4 verwendet.

**Beispiel 2:** Bis Android 2.3.7 kann die Sicherung einzelner Prozesse des RAM Speichers mithilfe des kill-Befehls erfolgen. Die Sicherung erfolgt für jede Applikation separat. Es wird hierbei eine eingebaute Methode im Android OS verwendet. Zu diesem Zweck wird die PID der Applikation benötigt. Mittels der PID und einem SIGUSR1 Signal wird ein RAM Dump eines Prozesses des Speichers der Applikation erzeugt. Dieser wird auf dem internen Flash-Speicher im Verzeichnis `/data/misc` gespeichert. Mit dem Befehl `kill -10 <PID>` in der adb shell lässt sich ein Dump der gewünschten Applikation erzeugen. Der Dump wird gespeichert mit der Namenskonvention `heap-dump-tm<timestamp>-pid<PID>.hprof`. Bei späteren Android Versionen wird kein RAM Dump mehr abgespeichert. In diesem Fall oder falls der gesamte RAM Speicher gesichert werden soll, muss auf eine andere Methode zurückgegriffen werden. Hierbei hilft das Tool LiME. Das Tool ermöglicht eine Sicherung des gesamten RAM Speichers [Cann12].

**Beispiel 3:** Das Android OS bis einschließlich Version 2.x „Gingerbread“ speichert im internen Gerätespeicher bis zu 50 Mobilfunkzellen und bis zu 200 WLAN-Access-Points in den Dateien `cache.cell` und `cache.wifi`. Diese Dateien befinden sich im Verzeichnis: `/data/data/com.google.android.location/files`. Die Speicherung der Daten erfolgt nur, wenn der Benutzer dem Google-Standortservice zugestimmt hat. Der Sinn hinter diesem Service ist die Möglichkeit der Ortung ohne GPS-Empfänger, nur mithilfe durch WLAN-Netze. Nach einer Zeitspanne von 12 Stunden für Mobilfunkzellen und 48 Stunden für WLAN-Access-Points werden die Daten durch eine neue Anfrage von Google erneuert. Die Aufzeichnung und das Senden der Daten an Google werden unterbunden, wenn die Option Wireless nutzen unter *Einstellungen/Orte* deaktiviert ist. Die Zustimmung kann jederzeit widerrufen werden. Für jede Mobilfunkzelle sendet das Gerät die Informationen an Google und erhält dafür ein Set von Koordinaten. Anhand der Cache Dateien lässt sich ein Bewegungsprofil des Nutzers erstellen.

**Beispiel 4:** Im Bereich Forensik herrscht das Prinzip der Unverändertheit der Daten. Dies dient dazu zu gewährleisten, dass Beweismaterial nicht verfälscht oder gelöscht wird. Forschungen im Bereich der Mobilfunkforensik haben nun ergeben, dass dies im Bereich der Mobilfunkforensik nicht zwingend gelten muss, falls nachgewiesen werden kann, dass durch Veränderungen am Beweismaterial, keine Veränderung der eigentlichen Beweise erfolgt, da oftmals der Forensiker vor dem Dilemma steht, entweder verändere ich minimal den Gerätespeicher, um an Daten zu gelangen oder ich erhalte gar keine [RoBa12].

Das Beispiel 1 zeigt einen Inhalt, der bis vor kurzem noch aktuell war, aber sehr bald veraltet sein wird, da die Verbreitung von Android OS 2.2 Anfang Januar 2012 noch bei über 20% lag. Die Beispiele 2-3 zeigen Inhalte, die noch aktuell sind, aber in absehbarer Zeit veraltet sein werden. Dies ist abhängig von der Android OS Version. Forensische Inhalte, die das An-

droid OS Version 1.6 direkt betreffen, sind im Modul nicht vorhanden. Das Beispiel 4 zeigt eine Neuerung, die durch Forschung im Bereich der Mobilfunkforensik gewonnen werden konnte und als Neuheit in dem Modul diskutiert worden ist.

## 4 Ergebnis

Um Neuerungen im Bereich der Mobilfunkforensik in Lehrmodule am Besten einzubinden, hängt von mehreren Faktoren ab. Grundsätzlich für die Integration von Neuerungen ist die mesodidaktische Konzeption der Module. Diese müssen modular und adaptiv aufgebaut sein. Dies erlaubt eine flexible Anpassung an sich verändernde Ausbildungsbedingungen. Es erlaubt auch eine einfache Einbindung neuer Inhalte und es können auch alte Inhalte herausgenommen werden. Weiter zeigen auch die Beispiele, dass die Frage, was nun neue bzw. alte Inhalte sind, nur durch einen Modulentwickler beantwortet werden kann, der in diesem Bereich entsprechende Kenntnisse hat. Er muss sich zu jedem Zeitpunkt fortbilden und mindestens auf dem Stand der Wissenschaft und Technik' sein. Am Besten betreibt er in diesem Bereich Forschung, um neueste Inhalte sofort weitergeben zu können. Nur wenn der Entwickler technologisch auf dem neuesten Stand ist, kann er entscheiden, in welche Kategorien vorhandene Inhalte einzugruppiert sind und weiter entscheiden, was Neuerungen und was veraltete Inhalte sind und diese in die Module aufnehmen oder herausnehmen.

## Literatur

- [BuLe13] O. Bun LEE: Erwachsenenbildung: Lebenslanges Lernen und dessen Bedeutung für die Entwicklung moderner Gesellschaften, Url: [http://kaad.de/fileadmin/kaad/pdf/Vortrag\\_Lee.pdf](http://kaad.de/fileadmin/kaad/pdf/Vortrag_Lee.pdf), zuletzt aufgerufen am 27.04.2013.
- [Bitk12] BitKom: Wettkampf der Smartphone-Plattformen, Url: [http://www.bitkom.org/de/presse/74534\\_72316.aspx](http://www.bitkom.org/de/presse/74534_72316.aspx), zuletzt aufgerufen am: 27.04.2013.
- [Cann12] Thomas Cannon: Android Reverse Engineering, Url: <http://thomascannon.net/projects/android-reversing>, zuletzt aufgerufen am: 31.07.2012.
- [Dude13] Duden-Didactica: Didaktik und Methodik, Url: [http://www.duden-didactica.de/index.php?option=com\\_content&view=article&id=54&Itemid=76](http://www.duden-didactica.de/index.php?option=com_content&view=article&id=54&Itemid=76), zuletzt aufgerufen am: 19.04.2013.
- [Dida13a] Duden-Didactica: Didaktik, Url: [http://glossar.didagma.de/index\\_print.php?sid=&sc=&p=glossar&x=12](http://glossar.didagma.de/index_print.php?sid=&sc=&p=glossar&x=12), zuletzt aufgerufen am: 18.04.2013.
- [Dida13b] Duden-Didactica: Allgemeine Didaktik, Url: [http://glossar.didagma.de/index\\_print.php?sid=3052&sc=56fda80520c64714ae38eccdb8bcfe66&p=glossar&x=210](http://glossar.didagma.de/index_print.php?sid=3052&sc=56fda80520c64714ae38eccdb8bcfe66&p=glossar&x=210), zuletzt aufgerufen am: 18.04.2013.
- [Eloq13] Duden-Didactica: Makro-, Meso- und Mikrodidaktik, Url: <http://www.projekt-eloq.de/didaktische-szenarien/didaktische-szenarien/makro-meso-und-mikrodidaktik/alle>, zuletzt aufgerufen am: 18.04.2013.

- [EBZB13] EBZ Business School: Was sie wissen sollten, Url: <http://www.fernstudium-immobilien.de/was-sie-wissen-sollten.html>, zuletzt aufgerufen am 17.04.2013.
- [Open13] OPEN C3S: [http://open-c3s.de/startseite\\_open-c3s.html](http://open-c3s.de/startseite_open-c3s.html), zuletzt aufgerufen am : 25.04.2013.
- [Pfis13] S, Pfisterer: Fachkräfte, Url: [http://www.bitkom.org/files/documents/bitkom\\_policy\\_paper\\_fachkraefte\\_2013%281%29.pdf](http://www.bitkom.org/files/documents/bitkom_policy_paper_fachkraefte_2013%281%29.pdf), zuletzt aufgerufen am : 25.04.2013.
- [Röpk13] J. Röpke: Nanotechnologie als Basisinnovation und Kondratieffdynamik, Url: [www.staff.uni-marburg.de/~roepke/Documents/nano2a.doc](http://www.staff.uni-marburg.de/~roepke/Documents/nano2a.doc), zuletzt aufgerufen am: 17.04.2013.
- [RoBa12] B. Roos, H. Baier: IT-Forensik im Wandel – Die Aufweichung des Paradigmas der Unveränderbarkeit bei Smartphones, D-A-CH Security 2012, Konstanz, ISBN 978-3-00-039221-4, September 2012.
- [SaSc11] S. Salzer, A. Schulz (2011): Ein mediendidaktischer Ansatz zur verknüpfenden Vermittlung von Fach- und Medienkompetenz in der betrieblichen Ausbildung - Forschungsergebnisse des Modellprojektes "effekt". In: *bwp@ Spezial 5 – Hochschultage Berufliche Bildung 2011*, Fachtagung 13, hrsg. v. KNUTZEN, S./ HEINEN, U./ EDER, A., 1-15. Online: [http://www.bwpat.de/ht2011/ft13/salzer\\_schulz\\_ft13-ht2011.pdf](http://www.bwpat.de/ht2011/ft13/salzer_schulz_ft13-ht2011.pdf) (26-09-2011).
- [Stat13] Statista: Anteil der verschiedenen Android-Versionen an allen Geräten mit Android OS im März 2013, Url: <http://de.statista.com/statistik/daten/studie/180113/umfrage/anteil-der-verschiedenen-android-versionen-auf-geraeten-mit-android-os/>, zuletzt aufgerufen am 17.04.2013.
- [Wiki13a] Wikipedia: Innovation, Url: <http://de.wikipedia.org/wiki/Innovation>, zuletzt aufgerufen am: 17.04.2013.
- [Wiki13b] Wikipedia: Diaktik, Url: <https://de.wikipedia.org/wiki/Didaktik>, zuletzt aufgerufen am: 17.04.2013.