

# AKTENZEICHEN UNGELÖST

## ÜBER DIE WACHSENDE BEDEUTUNG DER DIGITALEN FORENSIK



*Prof. Bodach (li) und Prof. Dr. Labudde (re) von der Hochschule Mittweida*

Am 23. September wird Prof. Bodach auf dem 9. JUG Saxony Day die Keynote „Aktenzeichen ungelöst – die herausragende Bedeutung der digitalen Forensik zur Tataufklärung“ präsentieren. Wir wollten genauer wissen, was sich hinter dem spannenden Titel versteckt und haben die Gelegenheit genutzt, ihn und seinen Kollegen Prof. Dr. Labudde vor Ort an ihrer Wirkungsstätte, der Hochschule Mittweida, zu interviewen.

### **Prof. Bodach, Prof. Dr. Labudde, wie war Ihr jeweiliger Hergang, der Sie zum Lehrstuhl bzw. zum Studiengang gebracht hat?**

**Labudde:** Wir haben es 2014 mit vielen Querverbindungen geschafft, einen Bachelor-Studiengang zu gründen: Die Allgemeine und Digitale Forensik. Wie der Name schon sagt, brauchen wir sowohl die allgemeine als auch die digitale Forensik, um die gesellschaftlichen Herausforderungen zu bewältigen. Zu Beginn stand die Frage, welches Lehrpersonal wir für den Studiengang benötigen. Zum Glück konnten wir Herrn Prof. Bodach akquirieren, der direkt aus der Praxis stammte und definieren konnte, was ein Absolvent der Forensik am Ende können muss. Wir ermöglichen den Studierenden den Einstieg über

die allgemeine Forensik, sodass sie verstehen: Was bedeutet Forensik im wissenschaftlichen Sinn, was ist übertragbar auf die digitale Welt und was sind meine Werkzeuge? Was ist eine Spur und wie kann ich sie analysieren? So können sie sowohl im analogen als auch im digitalen Raum Forensik betreiben.

**Bodach:** Mein Kollege hat es schon angesprochen: Ich bin direkt von der Polizei Sachsen zur Hochschule Mittweida gestoßen und brachte über 15 Jahre Erfahrung in der Kriminaltechnik, der Spurensicherung an unterschiedlichen Tatorten u. a. bei Kapitaldelikten mit. Mit der Suche der Hochschule Mittweida nach Lehrpersonal im Bereich der Forensik bot sich mir die Möglichkeit, mein Wissen, das ich mir über die Jahre angeeignet habe, praktisch weiterzugeben.

Es gibt im wissenschaftlichen Bereich noch andere Herangehensweisen als in der angewandten Forensik. Und das Wissen über beide Bereiche ist unser Mehrwert, zum einen natürlich für die Hochschule und zum anderen auch für die Studierenden.



**Was man sich vorstellen und was man akzeptieren muss: Es gibt eigentlich keinen reinen analogen Tatort mehr.**

**Prof. Dr. Labudde**

### **Und was ist das eigentlich: Digitale Forensik? Gibt es da große Unterschiede zur klassischen?**

**Labudde:** Was man sich vorstellen und was man akzeptieren muss: Es gibt eigentlich keinen reinen analogen Tatort mehr. Das heißt also, man beginnt damit, dass man das Smartphone etc. auswertet und erhält dadurch auch Informationen für die reale Welt. So ist also eine Trennung zwischen allgemeiner und digitaler Forensik überhaupt nicht mehr sinnvoll. So unsere Grundphilosophie. Wenn man das wissenschaftlich betrachtet, dann gibt es eigentlich gar keinen Unterschied. Man erweitert den analogen um den Begriff des digitalen Tatorts.

Bei den Werkzeugen gibt es ebensowenig einen Unterschied. Es geht immer darum, Spuren zu suchen, zu sichern und zu analysieren, um dann Informationen weiterzugeben. Das ist die Grundidee und deswegen wollen wir keine Trennung, keinen Studiengang nur für digitale und keinen nur für allgemeine bzw. naturwissenschaftliche Forensik. Nur wer ganzheitlich denkt, kann auch ganzheitlich ein Verbrechen aufklären.

**Bodach:** Die digitalen Spuren bringen immer Hinweise auf die reale Welt und müssen dann auch in der realen Welt überprüft werden. Stellen Sie sich vor, irgendjemand hat sich per Smartphone verabredet – das ist eine digitale Spur. Dann haben sie sich irgendwo getroffen und irgendetwas ist dort vor Ort passiert. Hier haben wir natürlich wieder andere Spuren und einen anderen Sachverhalt. Man kann also nicht trennen.

### **Es gibt ja bestimmte Beweissicherungs-Verfahren, die sich leicht auf einen physischen Gegenstand anwenden lassen. Wie sieht es hier in der digitalen Welt aus?**

**Labudde:** Was in der realen Welt galt und noch gilt, gilt natürlich auch in der digitalen Welt. Die lückenlose Zurückverfolgbarkeit aller Schritte mit einem digitalen Datum, die dann irgendwann zu einer digitalen Spur werden. Die sogenannte Chain of Custody gilt also auch im digitalen Raum. Wenn man bspw. Bilder hat, dann dürfen sie nicht verändert werden und man muss nachweisen, dass das Bild, das man gesichert hat, auch das Bild ist, welches in die Akte der Staatsanwaltschaft überführt wird. Meiner Meinung nach ist es sogar leichter, die Chain of Custody im digitalen Bereich zu erfüllen, als im analogen Bereich.

**Bodach:** Es gibt z. B. Hardware, um sicherzustellen, dass keine Veränderungen an den Spuren durchgeführt werden können. Das ist das A und O und ist nicht anders als im analogen, klassischen Bereich. Hier gibt es mittlerweile ausreichend Mittel und auch Standards.

### **Sie sagen, es ist leichter, die Kette im digitalen Bereich zu erhalten. Aber gibt es da nicht auch mehr Manipulations-Möglichkeiten?**

**Labudde:** Ja, das ist richtig. Man sagt, die Manipulierbarkeit im digitalen Bereich ist größer. Dagegen gibt es die Freiheitsgrade im realen Bereich. Im realen Bereich kann man etwas nehmen und von allen Seiten begutachten. Im digita-

len Bereich braucht man allerdings das Werkzeug für diese Spur. Aber ja, natürlich kann man sehr schnell bewusst oder unbewusst, gezielt oder nicht gezielt digitale Spuren verändern. Und deswegen liegt das Augenmerk hier noch stärker darauf, die Chain of Custody nachzuweisen.

### **Sie arbeiten mit vielen verschiedenen Programmen, u. a. auch Open-Source. Welche gibt es und wie können Sie ausschließen, dass diese Programme fehlerhaft sind? Oder kann man das nicht ausschließen?**

**Labudde:** Um Fehler besser ausschließen zu können, sollte man mit zwei Tools arbeiten und die jeweiligen Ergebnisse gegenprüfen. Und gerade um den Studierenden auch etwas an die Hand geben zu können, entscheiden wir uns oft für Open-Source-Tools. Aber wir setzen natürlich auch auf kommerzielle Software, damit sie das Handling mit diesen in Behörden gängigen Programmen ebenfalls beherrschen.

**Bodach:** Der Einsatz von Open-Source-Tools gehört einfach mit dazu. Ich versuche, den Studierenden einen Weg aufzuzeigen, wie sie die Spuren durchaus auch von Hand untersuchen können. Um die Menge an Spuren zu untersuchen, benötigt man natürlich entsprechende Software. Aber fürs Grundverständnis ist es sehr wichtig, dass die Studierenden den Aufbau von Spuren verstehen und selbst überprüfen können, wie die zur Verfügung stehenden Tools funktionieren. Es gibt sehr viele kommerzielle Anbieter, die sagen, dass man nach fünf Klicks das Ergebnis hat. Aber wie das Tool zum Ergebnis kommt, kann keiner sagen. Wenn das Tool

mal zu keinem Ergebnis kommt, kann man das hinnehmen und sagen, dass entweder nichts war oder das Tool es einfach nicht gefunden hat. Und an der Stelle geht die eigentliche Forensik los. Wir entwickeln auch unsere eigene Software, falls es sie auf dem Markt noch nicht gibt. Denn generell funktioniert die Forensik ohne Tools nicht, da die Datenmenge einfach zu groß ist.

### **Wie wird das große Ganze aus den verschiedenen Bereichen – medizinisch, analog, digital – am Ende sinnvoll zusammengeführt?**

**Labudde:** Wer sonntags 20:15 Uhr Tatort schaut, sieht immer diese kleinen gelben Zettel, die mit Strichen miteinander verbunden sind... Nein, da gibt es natürlich auch Möglichkeiten der Digitalisierung, wie z. B. Graphdatenbanken, die ein Personennetzwerk zusammen mit den Spuren übereinanderlegen. Man muss sich einfach vorstellen, dass jeder Fall ein Fall ist, also ein eigenständiges System. Jeder Fall hat etwas Spezifisches. So ein generelles Schema zu schaffen, ist relativ schwer. Es ist tatsächlich immer noch so, dass Mord- bzw. Sonderkommissionen sehr viel auf Papier festhalten. Irgendwann muss natürlich auch die reale Welt digitalisiert werden. Deswegen ist es auch so schön, dass die Forensik in Deutschland Einzug in die Wissenschaft hält.

### **Wie schätzen Sie die Akzeptanz und Vermittelbarkeit komplexer Methoden der digitalen Forensik in der Gesellschaft ein?**

**Labudde:** Na ja, man muss definitiv zeigen, wie die Methoden funktionieren. Und das ist auch



**Der Einsatz von Open-Source-Software gehört einfach dazu.**

**Wir entwickeln auch unsere eigene Software, falls es sie auf dem Markt noch nicht gibt.**

**Prof. Bodach**

der Grundansatz der Ausbildung. Die Studierenden lernen, wie sie etwas formulieren müssen, um wissenschaftlich exakt und gleichzeitig allgemein verständlich zu sein. Es ist leider so, dass eine Hauptverhandlung nicht so schön ist wie eine wissenschaftliche Konferenz, bei der man auf Fachexperten trifft. Man muss also zweifelsfrei und allgemeingültig formulieren können.

**Bodach:** Das kenne ich aus meiner Arbeit bei der Polizei zur Genüge. Nicht jeder ist dafür geeignet und kann komplexe Sachverhalte so erklären, dass es auch vor Gericht verstanden wird. Hier haben wir entsprechende Studienfächer, die diese Kompetenz vermitteln sollen.

### Die Hochschule Mittweida bietet zahlreiche Studiengänge auf diesem Gebiet an. Welche Inhalte lehren Sie beispielsweise?

**Labudde:** Wir sind die Einzigen in Deutschland, die allgemeine und digitale Forensik wirklich miteinander verbinden. Wir bilden Forensiker aus, die in jedem Gebiet eingesetzt werden können. Wir haben fünf Module der allgemeinen Forensik und zusätzliche Module, die sich mit den digitalen Inhalten beschäftigen, von der Programmierung über Datenbanken und Bildverarbeitung sowie Bildbearbeitung bis hin zu Rechner- und Netzwerkarchitektur. Und dann gibt es die Spezialfächer, in denen gelehrt wird, wie digitale Spuren gefunden werden können.

**Bodach:** Ein Forensiker sucht digitale Spuren und benötigt daher eine entsprechende Denkweise. Er muss sich Wege überlegen, wie er bestimmte Dinge nachweisen kann. Er muss kriminalistisch denken und die digitale mit der realen Welt in einen Kontext bringen können. Und das ist etwas Anderes als das Verstehen der reinen Informatik.

#### Impressum:

JUG Saxony e. V., Leipziger Straße 93, 01127 Dresden, Telefon: +49 351 418868710, E-Mail: team@jugsaxony.org, Web: jugsaxony.org, Vorstand: Dr. Falk Hartmann, Bernd Fischer, Torsten Busch, Bildernachweis: Alle Fotos © JUG Saxony e. V. Copyright 2022 Alle Rechte vorbehalten. Kein Teil dieses Dokumentes darf ohne schriftliche Genehmigung des Verfassers vervielfältigt oder verbreitet werden. Unter dieses Verbot fällt insbesondere die gewerbliche Vervielfältigung per Kopie, die Aufnahme in elektronische Datenbanken und die Vervielfältigung auf elektronischen Datenträgern. Aus Gründen der besseren Lesbarkeit wird bei Personenbezeichnungen und personenbezogenen Hauptwörtern in diesem Dokument die männliche Form verwendet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter. Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

### Welches Feedback bekommen Sie denn von Ihren Absolventen über die Qualität der Ausbildung in Ihrem Studiengang und umgekehrt von den Arbeitgebern über Ihre Absolventen?

**Labudde:** Mittlerweile arbeiten viele unserer Absolventen erfolgreich als Spezialisten in den verschiedenen LKAs und BKAs. Man sieht, wenn man seinen Abschluss hier in Mittweida macht, kann man danach definitiv in diesem Feld arbeiten, egal ob Industrie, Behörde, Forschung oder angrenzende Institutionen.

**Bodach:** Wir erhalten von den verschiedensten Behörden Anfragen, ob wir passende Absolventen haben, da bekannt ist, was bei uns gelehrt wird. Der Markt gibt einfach noch nicht so viel her in dem Bereich.

### Wo sehen Sie denn die Entwicklungsmöglichkeiten und das Potenzial dieses Bereichs?

**Labudde:** Wir haben den Vorteil, dass wir aktiv mit den Behörden zusammenarbeiten und sehen, in welche Richtungen die Trends gehen, z. B. das Thema IoT. Das nehmen wir direkt in die Forschung mit und geben es wiederum in die Lehre zurück. Das macht uns aus. Wir sind praxiserfahren. Wir erkennen, wo es hingehet und haben ein riesiges Netzwerk.

### Das Gespräch führten Dr. Falk Hartmann und Torsten Busch mit Prof. Bodach und Prof. Dr. Labudde am 30. Juni 2022. Wir bedanken uns für das freundliche Interview und die Zeit.

Wir hoffen, dass das Interview Lust gemacht hat, den 9. JUG Saxony Day am 23. September 2022 in Radebeul bei Dresden zu besuchen und freuen uns auf die Keynote von Prof. Bodach zum Thema „Digitale Forensik“.