IT Forensik
FH Aachen

FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

IT First Responder App

für Android Version 1

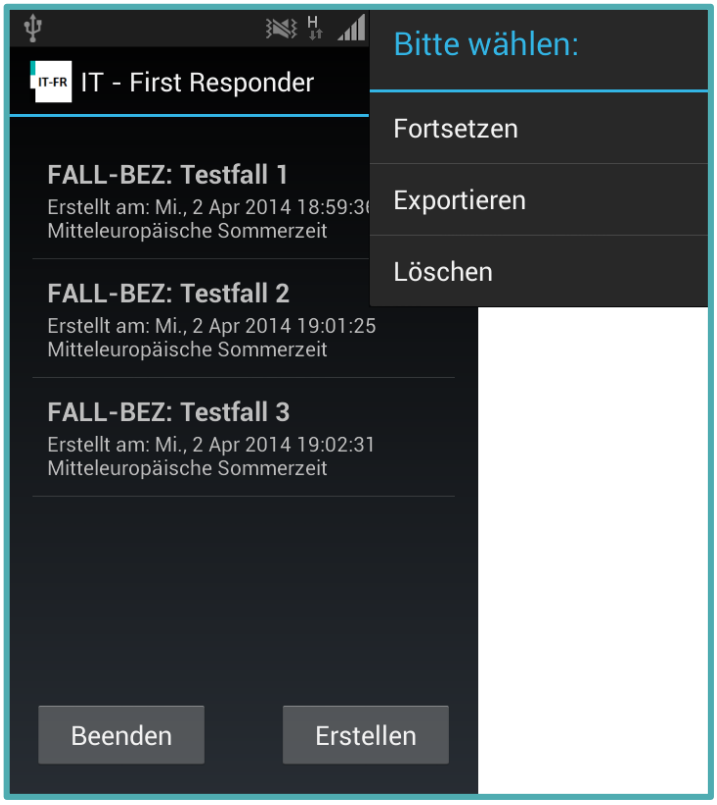
Installationsanleitung:

Um die Apk auf dem Smartphone zu installieren, muss zuerst in den Einstellungen unter *Anwendungen* ein Haken bei *Unbekannte Quellen* gesetzt werden.

Anschließend kann die Apk mit einem File Manager auf dem Smartphone ausgeführt werden.

Bedienungsanleitung:

Hauptmenü:



Das Hauptmenü dient zur Verwaltung aller bereits erstellten Fälle und zum Erstellen neuer Fälle.

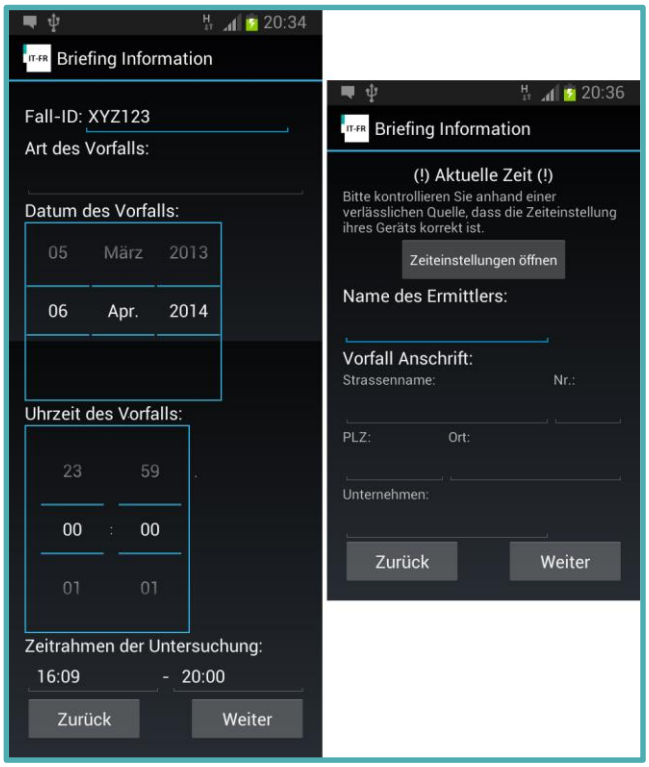
- **Erstellen-Button** Mithilfe des Erstellen-Buttons kann ein weiterer Fall hinzugefügt werden.
- **Beenden-Button** Die Applikation wird geschlossen.

Wenn Sie einen Fall aus der Liste anwählen, kann dieser weiter bearbeitet werden. Es erscheint ein Popup mit den folgenden Auswahlmöglichkeiten:

- **Fortsetzen** Der Fall wird am letzten bearbeiteten Dialog fortgesetzt. Wurde er bereits abgeschlossen, wird er in der *Collection/Acquisition*-Phase neu aufgerufen.
- **Exportieren** Der Export des Falls wird gestartet. Hier kann automatisch ein Abschlussbericht erstellt werden. Weitere Informationen im Kapitel *Export*.
- **Löschen** Der Fall wird komplett aus der Datenbank gelöscht. Außerdem werden alle zu dem Fall erstellten Fotos vom Smartphone gelöscht. Zip-Archive des Falls, die beim Exportieren erstellt wurden, werden nicht gelöscht. Diese Löschung ist nicht umkehrbar.

Durch das Anwählen des *Settings* Buttons  des Smartphones kann auf jeder Seite die zugehörige Hilfe angezeigt werden. Im Hauptmenü kann auch die Ermittler-Einstellung aufgerufen werden. Hier kann ein Standardname für den Ermittler eingegeben werden. Dieser wird dann anschließend bei jedem Fall automatisch eingetragen.

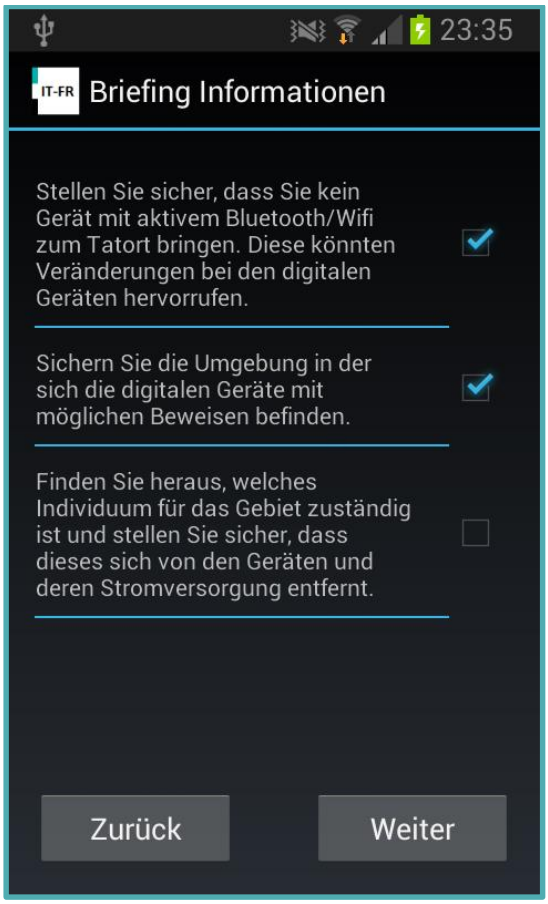
Neuer Vorfall:



Sobald ein neuer Fall erstellt wurde, werden zuerst die *Briefing Informationen* abgefragt. Diese sollten so genau wie möglich eingetragen werden, um einen ausführlichen Abschlussbericht zu ermöglichen.

- **Fall-ID** Hier kann eine ID für den Fall eingegeben werden. Diese Eingabe ist verpflichtend da sie im Hauptmenü zum Identifizieren des Falls genutzt wird.
- **Art des Vorfalls** Hier kann die Art des Vorfalls dokumentiert werden. (Bsp. Hacker Angriff..)
- **Datum des Vorfalls** Mit dem Date Picker kann das Datum ausgewählt werden, an dem der Vorfall stattgefunden hat. Hierbei kann kein Datum in der Zukunft ausgewählt werden.
- **Uhrzeit des Vorfalls** Mit dem Time Picker kann die Uhrzeit dokumentiert werden, an der der Vorfall stattgefunden hat.
- **Zeitrahmen** In diesem Punkt kann der wahrscheinliche Zeitrahmen der Untersuchung festgehalten werden. Als Startwert wird hier die aktuelle Uhrzeit eingetragen. Bitte nutzen Sie dasselbe Format bei der Eingabe der Zeit.
- **Aktuelle Zeit** Bitte vergleichen Sie die Systemzeit ihres Smartphones mit einer verlässlichen Quelle. Über den Button *Zeiteinstellung öffnen* können Sie die Einstellungen ihres Geräts starten und die Systemzeit verändern. Bitte kontrollieren Sie die Zeit auch, wenn Sie die automatische Aktualisierung aktiviert haben, da alle Dokumentationen mit Zeitstempeln des Geräts versehen werden.
- **Name des Ermittlers** Die Eingabe des Namens ermöglicht eine Personalisierung des Abschlussberichts. Wenn Sie im Hauptmenü einen Standardwert gesetzt haben wird dieser automatisch eingetragen.
- **Vorfall Anschrift** Hier können Sie die Anschrift des Vorfalls und, falls vorhanden, das betroffene Unternehmen dokumentieren.

Richtlinien:



Auf dieser Seite werden alle Richtlinien angezeigt, die bei der Arbeit als First Responder am Ort des Vorfalls zu beachten sind. Sobald eine Richtlinie als gelesen makiert wurde, wird die nächste angezeigt. Die nächste Seite kann erst angezeigt werden, nachdem alle Richtlinien gelesen und bestätigt wurden. Falls ihr Gerät einen kleinen Bildschirm hat, scrollen Sie bitte nach unten um sicherzustellen, dass keine Richtlinie übersehen wurde.

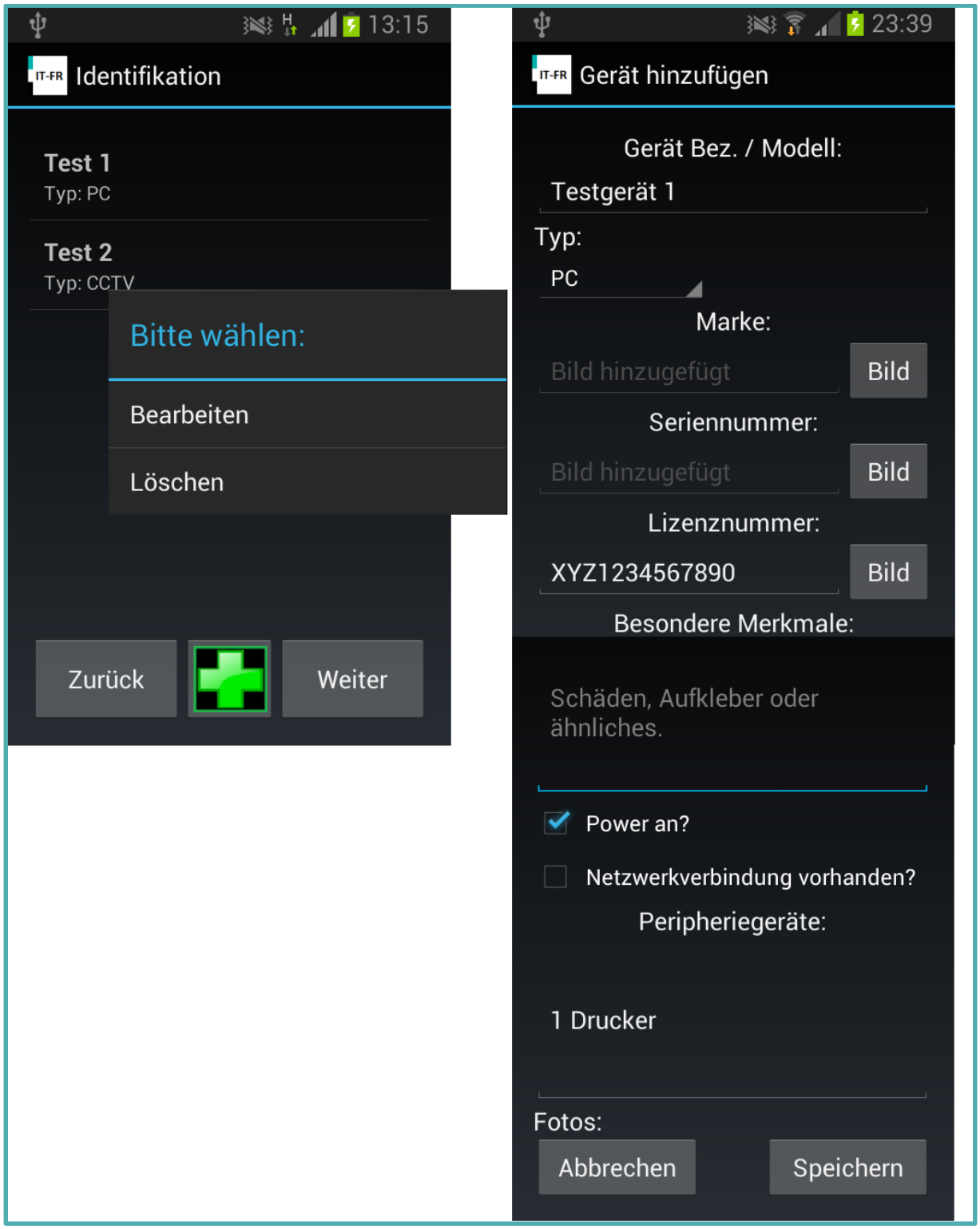
Generelle Informationen:

Auf dieser Seite kann dokumentiert werden, welche Personen mit dem Tatort in Kontakt gekommen sind. Außerdem kann mithilfe der Kamera der Tatort dokumentiert werden um eine spätere Rekonstruktion zu ermöglichen.

- **Zuständiger** Hier können Sie die zuständige Person für den Tatort eintragen. Dies kann zum Beispiel ein Systemadministrator sein der weitere Informationen wie Passwörter besitzen kann.
- **Personen** Dokumentieren Sie alle Personen, die mit dem Tatort und den Geräten in Kontakt gekommen sind. So kann später rekonstruiert werden wer mit dem Vorfall in Verbindung steht. Mit dem Button *Hinzufügen* wird der aktuell eingegebene Name der Liste hinzugefügt. Bitte stellen Sie sicher, dass der Name korrekt ist, da aktuell ein Löschen der Eingabe nicht möglich ist. Mit dem Button *Anzeigen* kann die gesamte Personenliste angezeigt werden. Diese wird nach dem Abspeichern automatisch alphabetisch sortiert.
- **Fotos** Bitte dokumentieren Sie den Tatort mithilfe der Smartphonekamera, um eine spätere Rekonstruktion zu ermöglichen. Wenn Sie lange auf ein Vorschaubild drücken, können Sie dieses durch ein neues Bild ersetzen. Wählen Sie das Vorschaubild nur kurz an, wird das Bild vergrößert angezeigt.

Aus Speichergründen kann leider nur eine geringe Auflösung dargestellt werden.

Identifikation:



Dieser Abschnitt listet alle bereits am Ort des Vorfalls identifizierten Geräte auf. Mit dem Anwählen des Buttons *Hinzufügen* (Grünes Plus) können beliebig viele weitere

Geräte hinzugefügt werden und durch Anwählen eines eingetragenen Geräts kann dieses bearbeitet oder gelöscht werden.

Bei neuen Geräten können alle benötigten Informationen eingegeben werden. Bitte tragen Sie alle Daten so genau wie möglich ein:

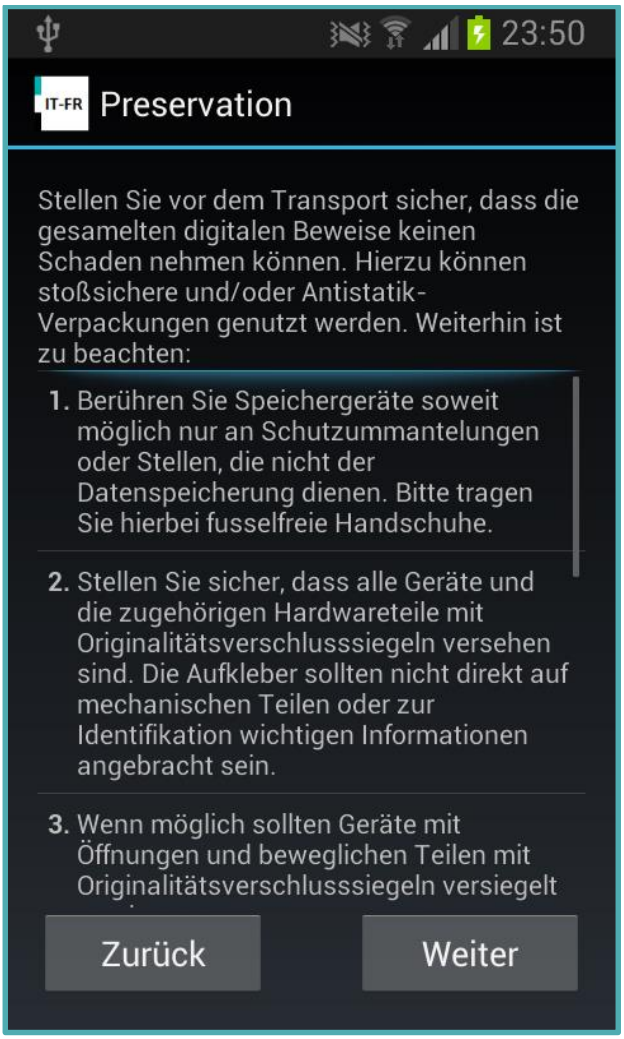
- **Typ** In diesem Drop-down Menu sind alle möglichen Typen für das Gerät zu finden. Der Typ *CCTV* führt dabei zu einer anderen Bearbeitung in der *Collection/Acquistion*.
- **Marke/Lizenz-/Seriennummer** Diese Daten können per Hand eingegeben werden. Sie können Sie aber auch mithilfe der Buttons *Bild* durch Fotos dokumentieren. Dies vermeidet Eingabefehler.
- **Merkmale** In dieser Textbox können alle besonderen Merkmale des Geräts dokumentiert werden, die für eine spätere Identifizierung wichtig sein könnten.
- **Power-/Netzwerkstatus** Bitte stellen Sie unbedingt sicher, dass diese beiden Punkte korrekt dokumentiert sind, da Sie über die weiteren Bearbeitungs-schritte in der *Collection/Acquistion* entscheiden.
- **Peripheriegeräte** Falls an das Gerät weitere Geräte angeschlossen waren dokumentieren Sie diese bitte hier. Wenn diese Geräte Einfluss auf die weitere Bearbeitung des Falls haben könnten, sollten Sie über eine Beschlagnahmung nachdenken.
- **Fotos** Bitte dokumentieren Sie die Verkabelung/die Ports des Geräts mithilfe der Smartphonekamera um eine spätere Rekonstruktion zu ermöglichen. Wenn Sie lange auf ein Vorschaubild drücken, können Sie dieses durch ein neues Bild ersetzen. Wählen Sie das Vorschaubild nur kurz an, wird das Bild vergrößert angezeigt. Aus Speichergründen kann leider nur eine geringe Auflösung dargestellt werden.

Collection/Acquisition:

In dieser Phase werden alle Geräte aufgelistet die identifiziert wurden. Diese werden unterteilt in bereits Bearbeitete und noch Ausstehende. Wenn Sie ein ausstehendes Gerät anwählen, müssen Sie im Popup selbst entscheiden, ob Sie eine Collection oder eine Acquisition durchführen möchten. Der jeweilige Bearbeitungsdialog wird dann angezeigt. Die eingegeben Informationen, wie zum Beispiel der Status der Netzwerkverbindung, fließen in die anschließenden Bearbeitungsschritte ein. Diese werden in Form eines Entscheidungsbaums für den Benutzer dargestellt (hier ist nur ein solcher Baum teilweise als Beispiel dargestellt).

Sobald alle Geräte bearbeitet wurden, kann die nächste Phase gestartet werde.

Preservation/Transport:



In dieser Phase werden dem Benutzer die notwendigen Richtlinien aufgezeigt, die er für den Transport und die weitere Aufbewahrung der Beweise beachten muss. Mit dem Beenden dieser Phase wird die Bearbeitung eines Falls abgeschlossen.

Export:

Dieser Dialog dient zum Export eines Falls. Hier werden alle beim Fall eingegebenen Daten komprimiert dargestellt und können noch einmal überprüft werden. Anschließend können Sie einen Dateinamen am Ende der Seite eingeben. Wenn Sie einen Dateinamen angegeben haben wird ein Zip-Archiv im angegebenen Dateipfad erstellt.

Inhalt des Archivs:

- **HTML-Bericht** Ein Bericht, der alle Daten des Falls und alle Fotos enthält. Dieser Bericht kann als Abschlussbericht genutzt werden.
- **XML-Datei** Eine XML-Datei, die alle Daten des Falls und alle Dateinamen der Fotos enthält. Diese Datei kann genutzt werden, falls aus den Daten ein eigener Bericht aufgebaut werden soll.
- **Checksums** Eine HTML-Datei, die zu jedem Fotos des Falls und zu den gerade erstellten HTML/XML-Dateien einen SHA-256 Hash enthält.
- **Fotos** In dem Archiv sind alle während dem Bearbeiten des Vorfalls erstellten Bilder komprimiert, sodass eine manuelle Zusammensuche entfällt.

Features:

- Leitung durch die Durchführung einer forensischen Untersuchung mit Hilfe eines ANDROID Smartphones (nach ISO/IEC 27037:2012)
- Läuft unter ANDROID ab Version 3
- Automatische Lokalisierung Deutsch/Englisch
- Dokumentation der Entscheidungen
- Nutzen der Smartphonekamera für die Dokumentation
- Automatisches Erstellen eines Abschlussberichts
- Zu jeder Eingabemaske eigener Hilfebildschirm
- Exportieren aller erstellten Daten/Fotos zur Weiterverarbeitung auf einem PC

Kontakt: itfr@etechnik.fh-aachen.de