Zivilrechtliches Besichtigungsverfahren

Typische Aufgabenstellungen für einen Sachverständigen
Planung, Vorbereitung, Ablauf und Kosten

DGRI – Fachausschuss Softwareschutz
18.02.2016

Markus Schmidt (ö.b.u.v. IT-Sachverständiger, fast-detect GmbH)

Kontakt

Dipl.-Inf. Markus Schmidt
ö.b.u.v. IT-Sachverständiger

Fast-detect GmbH
Ehrengutstr. 1
80469 München
Tel.: 089 - 46 13 58 02
eMail: markus.schmidt@fast-detect.de

Agenda

- Typische Aufgabenstellungen
- (guter) Beweisbeschluss
- Besichtigungstermin / Sicherstellung
  - Ablauf
  - Vorbereitung
  - Durchführung
  - Forensische Grundprinzipien
- Kosten

Einige (typische) Aufgabenstellungen

1. X nutzt Software von Y ohne Lizenz.
2. X verstößt gegen Open Source-Lizenzbedingungen.
3. X nutzt und vervielfältigt Zeichnungen in eigener Software ohne Lizenz.
4. X kopiert Artikeldaten aus Software von Y via „Screen Scraping“.
5. X übernimmt Codeteile aus Softwaresystem von Y.
6. X umgeht Kopierschutz des Softwaresystems.

Der Beschluss

Wichtige Bestandteile eines (guten) Beschlusses

Beschluss

I. Der Antragsgegnerin wird aufgegeben,

1. die nachfolgend beschriebene Untersuchung ihrer sämtlichen Personalcomputer (Arbeitsplatzrechner) und derjenigen Datenbank-Server, auf denen sich die Datenbanken befinden, sowie derjenigen File-Server, auf denen das Programm „[redacted]“ installiert ist, in ihren Geschäftsräumen

durch den mit Beweisbeschluß vom [redacted] bestellten Sachverständigen Markus Schmidt zu dulden

und dem jeweils zuständigen Gerichtsvollzieher zu diesem Zweck Zutritt zu den Geschäftsräumen und, sofern sich die Datenbank- und/oder Fileserver nicht in ihren Geschäftsräumen befinden, auf diese einen Fernzugriff zu ermöglichen und zu gewähren sowie dem jeweiligen Sachverständigen eine für die Server und für die Inbetriebnahme der Personalcomputer evtl. erforderliches Passwort und Zugangskennung mitzuteilen.

1. **Fernzugriff !**
2. **Kennung/ Passwort für Inbetriebnahme !**

Wichtige Bestandteile eines (guten) Beschlusses

Sollten sich solche Server (Datenbank- und/oder Fileserver) außerhalb der Geschäftsräume der Antragsgegnerin befinden, hat die Antragsgegnerin die Untersuchungen über von ihr zu gewährenden Fernzugriff zu ermöglichen und zu dulden.

Neben dem Sachverständigen hat die Antragsgegnerin folgenden anwaltlichen Vertretern der Antragstellerin die Anwesenheit während der Begutachtung zu gestatten:

[redacted]

3. Hoheit beim GVZ !

2. Für die Dauer der nachfolgend beschriebenen Untersuchung wird die amtliche Verwahrung der vorgenannten Personalcomputer und Server durch den jeweils zuständigen Gerichtsvollzieher angeordnet. Dieser hat sicherzustellen, dass an den Gegenständen keine Veränderungen vorgenommen werden und dem jeweils Sachverständigen eine sofortige Untersuchung der nachfolgend beschriebenen Art der Personalcomputer und Server vor Ort ermöglicht wird.

Wichtige Bestandteile eines (guten) Beschlusses

3. Die zu duldenden Untersuchungen erstrecken sich insbesondere auf die Feststellung, ob auf den Festplatten der Personalcomputer die Software bzw. Teile der Software [redacted] installiert sind. Es soll dabei festgestellt werden, auf welchen PCs (Arbeitsplatzbezeichnung, Name des Nutzers) welche Client-Softwarekomponenten der Software [redacted] installiert sind, insbesondere

Die [redacted]-Hauptprogramme sind wie folgt benannt und können sowohl auf dem Server, als auch auf dem Client installiert sein und können ggf. vom Kunden auch umbenannt worden sein:

Dazu wird dem jeweiligen Sachverständigen gestattet:

- Jeden Personalcomputer in Betrieb zu nehmen und an einen Drucker anzuschließen und Ausdrucke, insbesondere Screenshots, anzufertigen,
- Einsicht in das Inhaltsverzeichnis der ausführenden Programmdateien zu nehmen,
- Die auf dem Bildschirm erscheinende Auflistung von auf der Festplatte des jeweiligen Personalcomputers gespeicherten Dateien auf einem von ihm mitgebrachten Datenträger zu übertragen und zu sichern,

4. Inbetriebnahme !

5. Durchsuchung !

6. Mitnahme von Kopien !

Wichtige Bestandteile eines (guten) Beschlusses

- evtl. aufgefundene Programme der Antragstellerin zu starten und in der Login-Maske das ggf. voreingestellte User-Kürzel und den Datenbanknamen und eine evtl. vorgefundene Seriennummer oder eine evtl. dort vermerkten Lizenznehmer zu notieren. Vorgefundene Programme sollten insbesondere, aber nicht ausschließlich, aus dem Desktop gestartet werden. Sofern mehrere Aufrufe der Software [redacted] installiert sind, sollen alle Aufrufe geprüft werden und festgestellt werden, welches User-Kürzel und welcher Datenbankname jeweils dabei genutzt wird. Der Sachverständige ist berechtigt, die Mitarbeiter der Antragstellerin nach ihrem bzw. ihren User-Kürzeln zu fragen, da Mitarbeiter bei Nutzung mehrerer Datenbanken mehrere User-Kürzel haben können.
- die für jeden Personalcomputer ermittelte Auflistung der ausführbaren Dateien auszudrucken.

7. Auskunft einholen soll gestattet sein !

Wichtige Bestandteile eines (guten) Beschlusses

4. Die Antragsgegnerin hat es zu dulden, dass der Sachverständige die zu begutachtenden Sachen in Augenschein nimmt und

von den Datenbanken

zum Zwecke der weiteren Begutachtung eine Kopie anfertigt. Diese Handlungen werden dem Sachverständigen gestattet.

Die Antragsgegnerin hat es zu ermöglichen, dass der Sachverständige Zugang zu den Datenbanken

und den vorgenannten File-Servern erhält sowie zu sämtlichen Personalcomputern. Insbesondere hat sie es zu ermöglichen, dass der Sachverständige Zugang zu dem Server erhält, auf dem die Software der Antragstellerin installiert ist und/oder abläuft und auf den Server, auf dem sich die Datenbanken befinden.

Die Antragsgegnerin hat insbesondere den Usernamen und das Passwort für die Systemadministration zur Verfügung zu stellen und den Zugang zu den oben genannten Datenbanken und Servern zu ermöglichen.

8. Anfertigung von Kopien !

9. Zugang zu Datenbanken und Servern !

10. Admin-Berechtigung !

Wichtige Bestandteile eines (guten) Beschlusses

Für den Fall, dass der Username und das Passwort oder sonstigen Zugangskennungen nicht verfügbar sein sollten und/oder von der Antragsgegnerin nicht zur Verfügung gestellt werden, wird der Sachverständige [redacted] anrufen (sofern sie bzw. er nicht anwesend ist und das Programm auf einem Datenträger übergeben kann) und die Zusendung per E-Mail eines Programms anfordern, mit dessen Hilfe er in der Lage ist, das bei der Antragsgegnerin hinterlegte Passwort zurückzusetzen und sich auf diese Weise die Administrationsrechte zu verschaffen. Dies hat die Antragsgegnerin zu dulden.

5. Die Antragsgegnerin hat dem Sachverständigen Zugang zu den zu begutachtenden Sachen zu verschaffen und ihm evt. erforderliche Benutzerkennungen und Passwörter mitzuteilen, wobei dem Sachverständigen auch die Zugangsbefugnisse des höchsten Systemadministrators einzuräumen sind.

11. Mitteilung der Zugangsdaten !

Wichtige Bestandteile eines (guten) Beschlusses

6. Auf Verlangen der Antragsgegnerin hat der Sachverständige die Begutachtung für die Dauer von maximal zwei Stunden zurückzustellen, um der Antragsgegnerin Gelegenheit zu geben, ihrerseits einen anwaltlichen Vertreter hinzuzuziehen. Der Sachverständige hat die Antragsgegnerin vor Beginn der Begutachtung auf dieses Recht hinzuweisen.

7. Der Antragsgegnerin wird – mit sofortiger Wirkung und für die Dauer der Begutachtung – untersagt, eigenmächtig Veränderungen an der zu begutachtenden Software und an ihrem die Software betreffenden Teile ihres IT-Systems vorzunehmen, insbesondere der vorgenannten Server.

12. Wartefrist von 2 Stunden !

Wichtige Bestandteile eines (guten) Beschlusses

8. Für den Fall, dass die Antragsgegnerin die oben beschriebenen Handlungen der Ziffern 1. -7. nicht vornimmt bzw. nicht duldet, wird der zuständige Gerichtsvollzieher ermächtigt, sämtliche den/die Server, auf denen sich die Software und/oder die Datenbanken der Antragstellerin befinden, sowie sämtliche Personalcomputer, die sich in ihren Geschäftsräumen, [redacted] befinden, zu beschlagnahmen und an den Sachverständigen herauszugeben. Er wird darauf hingewiesen, dass er im Rahmen des § 758 ZPO befugt ist, die verschlossenen Haustüren, Zimmertüren und Behältnisse öffnen zu lassen. Er ist, wenn er Widerstand findet, zur Anwendung von Gewalt befugt und kann zu diesem Zweck die Unterstützung der polizeilichen Vollzugsorgane nachsuchen.

9. Für jeden Fall der Zuwiderhandlung gemäß §§ 935 ff, 890 ZPO gegen die unter Ziffer 1.-7. bezeichneten Anordnungen wird der Antragsgegnerin ein vom Gericht für jeden Fall der Zuwiderhandlung festzusetzendes Ordnungsgeld von €5,- bis zu €250.000,-, an dessen Stelle im Falle der Uneinbringlichkeit eine Ordnungshaft bis zu sechs Monaten tritt, oder eine Ordnungshaft von bis zu sechs Monaten angedroht, wobei die Ordnungshaft an dem bzw. den Geschäftsführer(n) der Antragsgegnerin zu vollziehen ist.

13. Beschlagnahme-Recht des GVZ !

Üblicher Ablauf eines Besichtigungstermins

1. **Kontaktaufnahme des anwaltlichen Vertreters des AS mit dem Sachverständigen** bzgl. grundsätzlicher Bereitschaft zur Durchführung der Besichtigung (u.a. auch Termin) mit anschließender Begutachtung.

2. Gericht übersendet **Akte** an SV. Studium der Gerichtsakte und der Beschlüsse. Prüfung des **Kostenvorschusses**.

3. Anforderung **weiterer Unterlagen** (zur Durchführung der Besichtigung / Gutachtenerstattung) vom AS über den anwaltlichen Vertreter des AS.

4. **Terminvereinbarung** mit anwaltlichem Vertreter des AS und des GVZ bzgl. der Durchführung der Besichtigung. Klärung, ob Polizei notwendig ist.

5. **Vorbereitung** des Besichtigungstermins (technisch und organisatorisch).

6. **Durchführung** des Besichtigungstermins. Sicherung der Daten.

7. **Gutachtenerstattung**

8. **Abgabe** des Gutachtens. Unter Umständen verlangt Gericht Schwärzung bestimmter Stellen des Gutachtens.

Vorbereitung des Besichtigungstermins

Vorbereitung des Besichtigungstermins

Auf Basis der vorhandenen Informationen und unter Berücksichtigung der nachfolgenden Fragen sollte die Strategie erarbeitet werden:

- **Was wird gesucht?** (E-mails, Dokumente, Buchhaltungsdaten, etc.)
- **Gibt der Antragsgegner / Beschuldigte die Daten freiwillig heraus?** (*Überprüfung notwendig, ob die herausgegebenen Daten vollständig sind und der Durchsuchungsgrund hierdurch erschöpft ist?*)
- **Wo werden diese Daten vermutet?** (*mögliche Eingrenzung der zu sichernden Datenmenge*)
- **Sind gelöschte Daten zur Aufklärung notwendig?**
- **Wie groß ist die zu sichernde Datenmenge und reichen Zeit und vorhandene Ressourcen?**
  (*Hinweis: USB 2.0 = ca. 100GB/Stunde; eSATA = ca. 320GB/Stunde*)

Vorbereitung des Besichtigungstermins

Sachverständigenseitig wird für die Planung benötigt:

- möglichst detaillierte Informationen zum Durchsuchungsobjekt, zu der Art des Verfahrens und zu den Vorermittlungserkenntnissen
- je nach „Größe des Durchsuchungsobjekts“ 1 bis 5 Tage zur Vorbereitung (evtl. Beschaffung):

Micro-SD-Karte


Laptop


Serverraum


Rechenzentrum

Vorbereitung des Besichtigungstermins

Sachverständigenseitig wird außerdem für die Planung benötigt:

- Lokation / Lage des Objekts
- Anzahl der Lokationen
- Planung des Sachverständigen-Teams
- Kontaktdaten von GVZ und AS (evtl. auch Polizei und Schlosser)
- Prüfung des Kostenvorschusses
- Planung der Anreise und des Treffpunkts

Durchführung des Besichtigungstermins

Forensische Grundprinzipien

Im Rahmen der Beweissicherung sind folgende Schritte von Bedeutung:

- **Beweiskette** (Chain of Custody) einhalten (Übergaben protokollieren, Beschriften und Verbleib mittels Sicherstellungsprotokoll dokumentieren)
- **Überlegtes Vorgehen** im Rahmen definierter Prozesse (Überlegungen zu An- oder Abschalten, bzw. Netzwerkverbindungen trennen etc.)
- **Datensicherung** (forensische Werkzeuge, ggf. Signieren oder Hashwerte dokumentieren)
- Gesicherten **Transport** organisieren (Stoßsicher verpacken, ggf. noch Backups vor Ort erstellen)
- Grundsätzlich werden nur Beweismittelkopien ausgewertet (**niemals das Original**)

IT-Forensik

Beispiel Rechnerfestplatten-Auswertung

Was lässt sich evtl. feststellen?

- Hinweise auf stattgefundene Datenmanipulationen
- Zeitpunkte bzw. zeitliche Verläufe der Rechnernutzung durch bestimmte Betriebssystemnutzer (wer hat wann einen Rechner benutzt)
- Identifikation der Erstellungszeitpunkte, letzten Änderungszeitpunkte und letzten Lesezugriffe auf bestimmte Dateien oder Dokumente anhand der Dateisystemattribute
- Identifikation stattgefundener Dateiübertragungen (z.B. per E-Mail, Chat oder über Tauschbörsen)
- Zuordnung vormals angeschlossener USB-Speichergeräte und Festplatten zu einem bestimmten Rechner (und evtl. zu einem bestimmten Nutzer)
- Wiederherstellung längst gelöschter Daten und Dateien inkl. Eingrenzung oder Bestimmung des Löschzeitpunktes

IT-Forensik

Beispiel Dokumenten-Auswertung

Was lässt sich evtl. anhand der Dateiattribute feststellen?

- Name des Druckers und Zeitpunkt des letzten Ausdrucks
- Dateierstellungszeitpunkt
- Name oder Kürzel des Autors
- Datum der letzten inhaltlichen Änderung
- Bei PDF-Dokumenten : Name und Version des verwendeten Dokumentenerstellungsprogramms
- Bei E-Mails: Identifikation der Echtheit des Absenders (kommt die E-Mail tatsächlich vom angegeben E-Mailserver des Absenders oder ist sie auf eine gefälschte Identität zurückzuführen)
- Überprüfung der Echtheit von E-Mail-Nachrichten zum Nachweis stattgefundener Kommunikation einschließlich der Bestimmung von Versendezeitpunkten anhand des E-Mail-Nachrichtenkopfes

IT-Forensik

Ausstattung für die Auswertung von Handys und anderer mobiler Geräte

Zur Auswertung von Mobiltelefonen, anderen mobilen Geräten und von Navigationsgeräten benötigt man eine moderne technische Spezialausrüstung:

- UFED von Cellebrite zum physikalischen Auslesen und Auswerten unterschiedlichster Mobiltelefontypen (insb. Auch Smartphones wie iPhones oder Android-Telefone)

- Flasherboxen zum Umgehen von Sicherheitscodes und -sperren

IT-Forensik

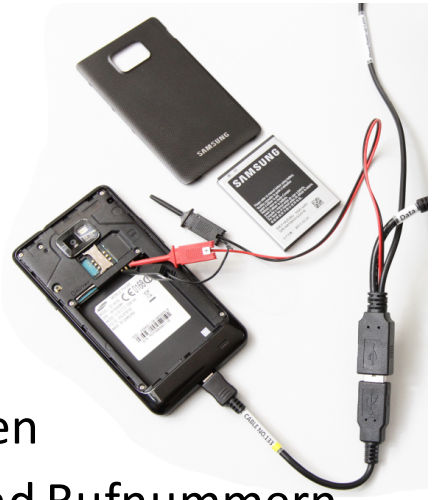
Beispiel Navigationsgeräte-Auswertung

Was lässt sich evtl. feststellen?

- Die letzten eingegeben Navigationsziele und -Strecken
- Abhängig vom Gerät vollständige Streckenverläufe mit Zeitstempel
- Vom Nutzer gespeicherte Adressen und Sonderziele
- Letzte vor dem Ausschalten erfasste GPS-Position
- Gespeicherte Informationen zum registrierten Eigentümer

IT-Forensik

Beispiel Mobiltelefon-Auswertung



Was lässt sich evtl. feststellen?

- Rufnummern der letzten Anrufer und Angerufenen
- Im Adressbuch gespeicherte Namen, Adressen und Rufnummern
- Inhalt ausgetauschter SMS- und MMS-Nachrichten
- Stattgefundene E-Mail-Kommunikation bei modernen Smartphones
- Geräteabhängig, bei einigen GPS-fähigen Smartphones, Historie der Geo-Lokalisationsdaten einschließlich Zeitstempel (wo war das Telefon, zu welchem Zeitpunkt)
- Alle mit der eingebauten Kamera angefertigten Fotos (ggfl. mit Geo-Lokalisationsdaten des Aufnahmestandortes)
- Rekonstruktion gelöschter Speicherbereiche abhängig vom jeweiligen Gerätetyp

IT-Forensik

Beispiel Digitalfoto-Auswertung

Was lässt sich evtl. anhand der Bilddaten feststellen?

- Das genaue Aufnahme- und Änderungsdatum
- Aufnahmeort anhand gespeicherter Geo-Lokalisationsdaten
- Marke und Typ der verwendeten Digitalkamera
- Ggfl. Identifikation der zur Aufnahme verwendeten Kamera anhand von gespeicherter Seriennummern oder Firmwareversionen
- Informationen über verwendete Bildbearbeitungsprogramme
- Weitere EXIF-Informationen (z.B. Besitzer, Copyrightvermerk etc.)

Auswertbare Daten der Kamera

- Seriennummer und Firmwareversion zum Abgleich mit festgestellten Bildern
- Vergleich des Datums und der Uhrzeit der eingebauten Uhr mit der aktuellen Zeit zur Berechnung von Aufnahmezeitabweichungen

Üblicher Ablauf des Besichtigungstermins

1. **Briefing** mit Gerichtsvollzieher und/oder leitendem Polizeibeamten und weiteren Unterstützungskräften (z.B. Schlosser)
   (*idealerweise ca. 60 min. vor Besichtigung / Durchsuchung*)

2. **Zustellung** des Beschlusses durch Gerichtsvollzieher

3. Schneller **Überblick vor Ort**. Auffinden des System-Admins. Trennung des System-Admins von anderen Mitarbeitern (insbes. von der GL). Positionierung von Polizeibeamten.

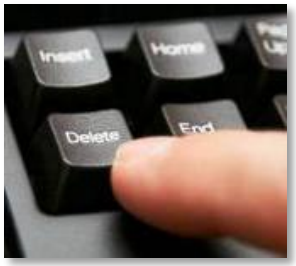
4. **Durchführung der Beweissicherung** gem. Strategie.

Wichtige Hinweise

Es muss verhindert werden, dass ...

... die Stromzufuhr unterbrochen wird!
(Steckdosen/-leisten, Sicherungskasten etc.)

... wichtige Schalter betätigt werden!
(Notausschalter, Feueralarm, Löschanlagen etc.)



... der Beschuldigte oder Dritte Zugang zu Computern oder Servern im Sachzusammenhang erlangen!

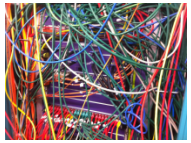
(*z.B. Abmeldungen oder Löschvorgänge evtl. auch über Netzwerk*)

Überblick vor Ort

Verschlüsselung

Rechner
(Anzahl, Art)

Datenmenge
(Komplett oder gefiltert?)



Netzwerk
(Architektur, Netzplan)

Internetdienste
(Daten beim Provider?)

WEB.DE

1&1

Kann je nach Größe ein bis zwei Stunden dauern.

Betriebssysteme
(Windows, Apple, Linux)

Buchhaltung
(Warenwirschaftssystem)

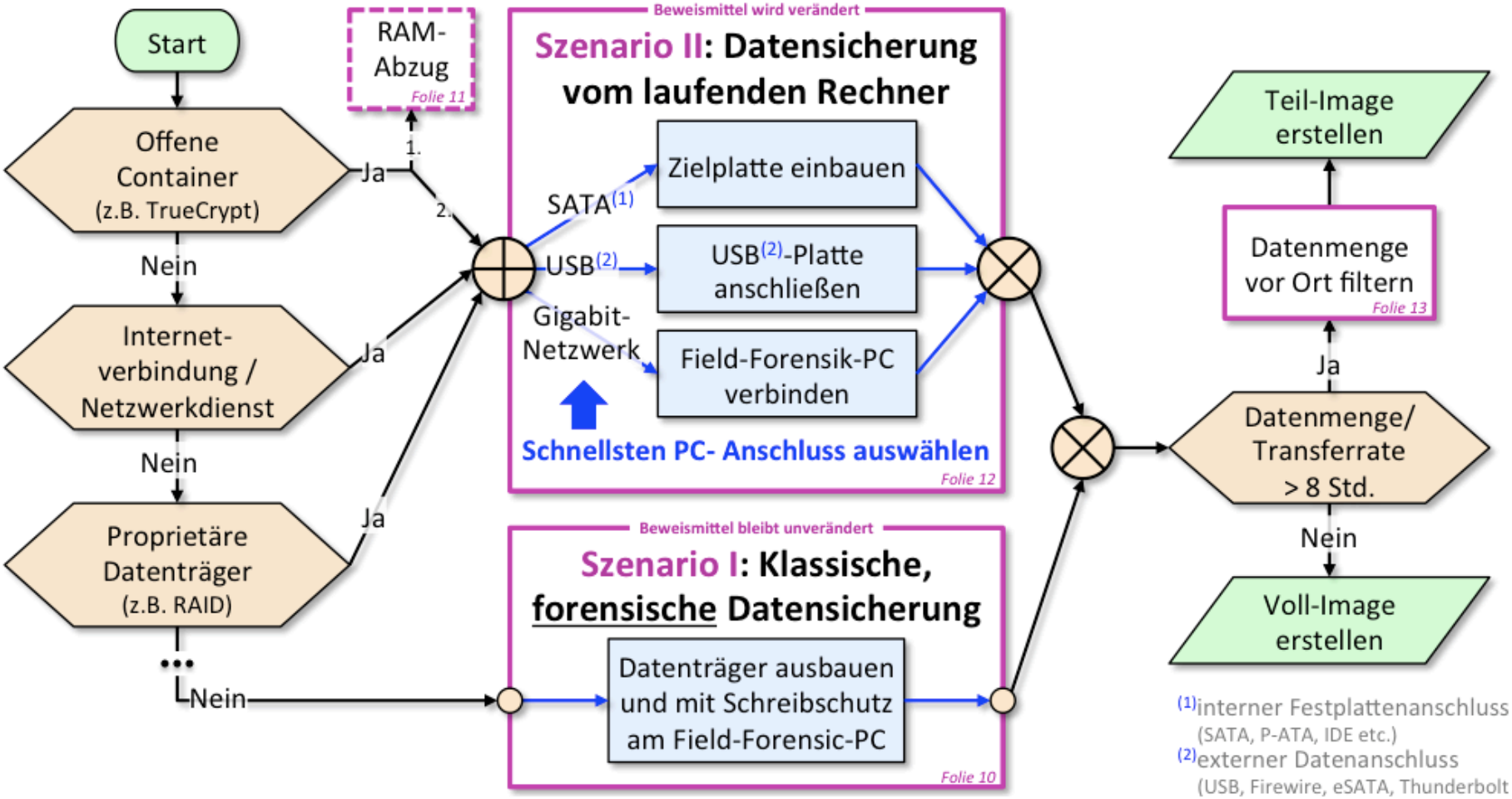
SAP

Entfernte Standorte
(Sicherung über Netzwerk?)

Verbindungen
(Internet-, Remote- u. VPN-Verbindungen)

Kommunikation
(E-mail, VoIP-Telefon)

Entscheidungsbaum - Datensicherung



(1) interner Festplattenanschluss (SATA, P-ATA, IDE etc.)
(2) externer Datenanschluss (USB, Firewire, eSATA, Thunderbolt etc.)

Datensicherung

Szenario I: Klassische, forensische Datensicherung

Vorteile:

- Schnellstmögliche Datenverbindung
- Forensische Kopie
  - mit gelöschten Bereichen möglich
  - Beweismittel bleiben unverändert

Nachteile:

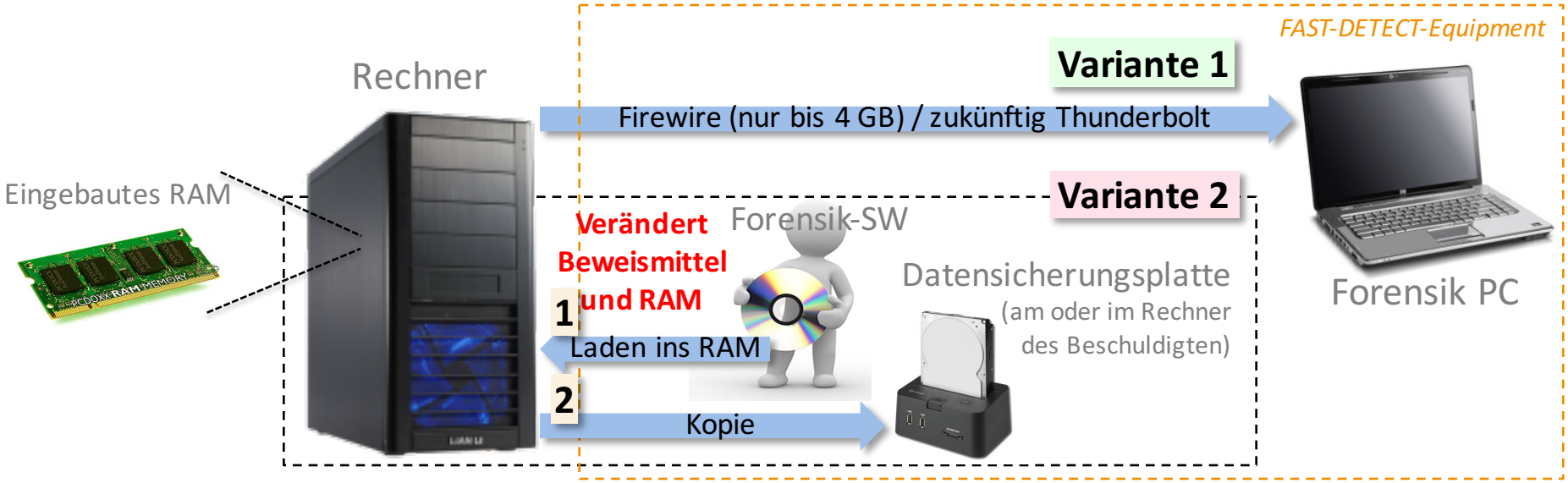
- Nur begrenzter Parallelbetrieb möglich
- Rechnerbetrieb muss unterbrochen werden; RAM-Verlust
- Sehr aufwendig bei komplexen RAID-Systemen
- Zugriffsverlust bei geöffnet vorgefundener Verschlüsselung
- Zugriffsverlust auf entfernte Server

Nicht möglich bei:

- eingelötetem Flash-Speicher (Handys, manche Notebooks)

Datensicherung

Hauptspeicher-Abzug (vor Szenario II)



Variante 1:

- Verändert weder Beweismittel noch RAM (benötigt keine Software)
- Geht nur bei FireWire-Anschluss
- Geht nur für die ersten 4 GB

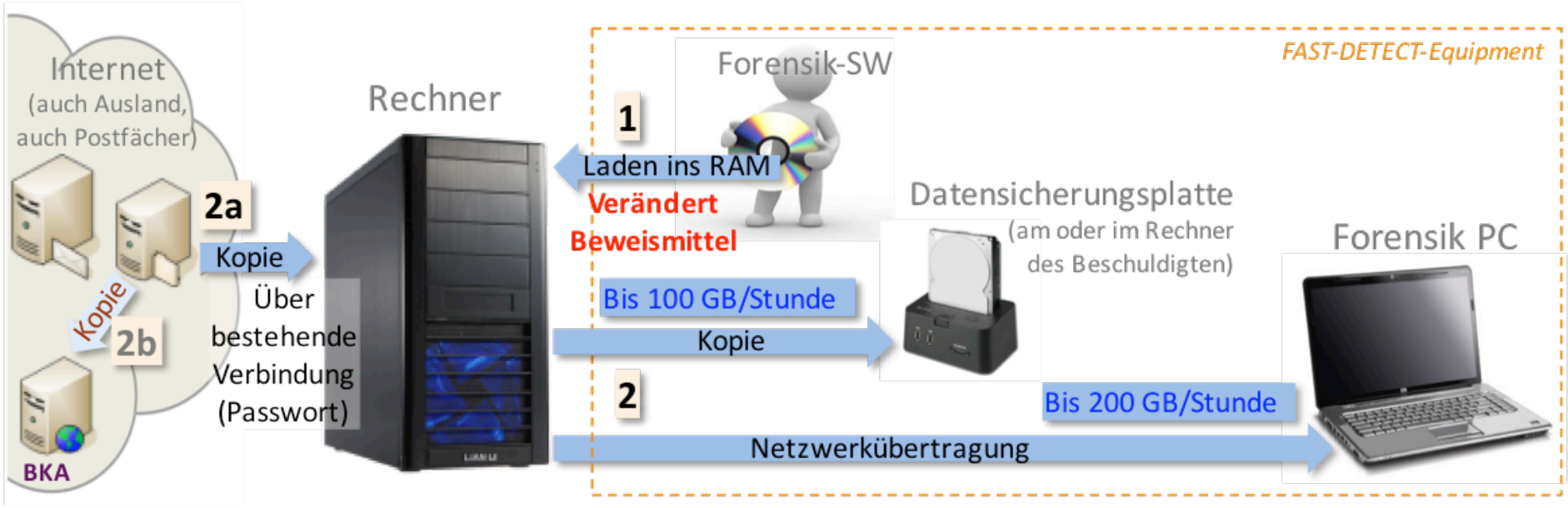
Beide Varianten sind kombinierbar!

Variante 2:

- Eignet sich für Speichergrößen > 4 GB RAM und nutzt vorhandene Ressourcen
- Verändert Beweismittel und RAM
- Geht nicht bei LOCK

Datensicherung

Szenario II: Datensicherung vom laufenden Rechner



Vorteile:

- Nutzt vorhandene Ressourcen (paralleles Kopieren)
- Eignet sich f. offene Verschlüsselungen
- Ermöglicht Serverdaten-Abzug
- Eignet sich bei eingelötetem Flash-Speicher (Handys, manche Notebooks, ...)

Nachteile:

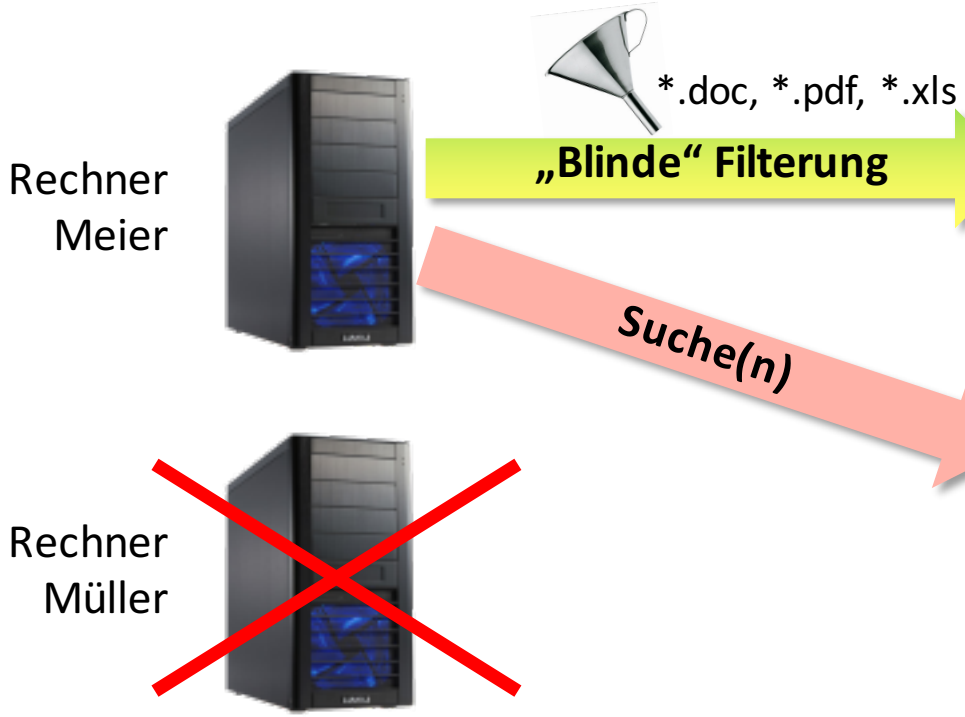
- Keine 100%ige forensische Kopie
- Evtl. zu langsam für vollständige Kopien

Variante 2b:

- Notfalls auch Zwischenspeicherung auf einen anderen, schnell angebundenen Internetserver (z.B. des BKA)

Datensicherung

Datenmenge vor Ort filtern



Einfache Filter können i.d.R. leicht angewandt werden.

Filterung nach Zeitfenstern oder bestimmten Personen sind häufig eher schwierig!

Ausgedehnte Suche nach Schlüsselwörtern oder bereits Auswertungen der Daten vor Ort, sind aufgrund des limitierenden Zeitfensters häufig nicht möglich.

Manchmal ist es einfacher und schneller, **zunächst mehr** zu sichern als man braucht. Dennoch ist eine grobe Auswahl häufig sinnvoll und/oder notwendig.
Der Datenabzug muss **verhältnismäßig** sein und er wird auch von den **technischen Möglichkeiten** bestimmt!

Sicherstellungsunterstützung an mehreren Standorten

- Bei einer Datensicherung/Auswertung an mehreren Standorten sollte ein Sachverständigenbüro mehrere **Forensik-Teams** (mindestens zwei erfahrene IT-Forensiker pro Standort) und ausreichend **Equipment** stellen können.

- Der beauftragte Sachverständige sollte bei **standortübergreifenden Sicherstellungen zusätzlich die Organisation/Koordination** übernehmen.

Sicherstellungsunterstützung - Equipment

Kosten

- Abrechnung erfolgt stundengenau nach Aufwand gem. JVEG Honorargruppe 8 (100 EUR / Stunde), zzgl. der Aufwände für Anreise, Übernachtung, etc.
- Grobe Aufwandkalkulation (durchschnittliche Komplexität, 1 Standort, 2 MA):
  - Vorbereitung: 4 – 8 Std.
  - Sicherstellung: 8 – 20 Std.
  - Auswertung: 8 – 32 Std.
  - Gutachtenerstattung: 8 – 32 Std.
  - Gesamt: 28 – 92 Std. (ohne Reisezeit)

Vielen Dank.