Dirk Schindowski

Holmes & Co
Detektei - Sicherheitsmanagement

Am Bahnhof 7
56414 Steinefrenz

Telefon: 06435 / 54 80 287
Fax: 06435 / 90 91 58
e-Mail: info@holmes-und-co.de

www.holmes-und-co.de

Eine IT-Forensische-Schnellprüfung umfasst:

1.) **Entnahme des relevanten Datenträgers aus dem zu untersuchenden Gerät, falls möglich**

2.) **Erstellung eines forensischen Images (immer notwendig, falls etwas gefunden wird)**

3.) **Kompletter X-Ways-Durchlauf des Datenbestandes mit**
- struktureller Durchsuchung des Dateisystems nach zusätzlichen Informationen
- Signatursuche nach Dateiheadern und Spuren im gelöschten Speicher (Carving)
- Überprüfung auf Manipulation von Dateityp-Endungen
- Zerlegung von E-Mail-Archiven und Dateicontainern in Einzelkomponenten
- Extraktion von E-Mail-Anhängen aus Mailarchiven zur weiteren Untersuchung
- Extraktion von eingebetteten Elementen aus anderen Dateien
- Suche nach verschlüsselten Dateien und statistische Verschlüsselungstests
- Auswertung der Windows-Registrierung(en) und Cache-Dateien
- Bei Bedarf: Erzeugung von Standbildern aus Videodateien
- Bei Bedarf: Suche nach Hashwerten (z.B. vertrauliche Dateien)
- Bei Bedarf: Stichwortsuche für alle Suchbegriffe, die der Kunde bei Auftragserteilung benennt
- Bei Bitlocker-Laufwerksverschlüsselung Entsperrung des Datenträgers für die Untersuchung (wenn der Wiederherstellungsschlüssel bekannt ist und keine zusätzliche Hardwareverschlüsselung wie z.B. OPAL vorliegt)

Mit Schnellprüfungen können beispielsweise folgende Dinge untersucht werden:

- Unzulässige Privatnutzung
- Nicht freigegebene installierte Software
- Versand von Daten per E-Mail / E-Mail-Auswertung
- Angeschlossene Geräte in einem bestimmten Zeitraum (z.B. externe Datenträger)
- Installierte Software / Nutzungsstatistiken von Software
- Verbundene Netzwerke / Netzlaufwerke / Remote-Verbindungen
- Registrierte Benutzer auf dem Gerät und nutzerspezifische Suche
- Öffnungs- und Änderungszeiten von Dateien
- Gelöschte Daten, eingeschränkt auch der Löschzeitpunkt und löschender Benutzer
- Internet- und Dateiaktivitäten
- Druckaktivitäten (eingeschränkt)
- Bild- und Videoanalyse (z.B. Suche nach pornografischem Material)
- Nutzungszeiträume der Geräte (z.B. bei Arbeitszeitbetrug)

Dirk Schindowski

Holmes & Co
Detektei - Sicherheitsmanagement

Am Bahnhof 7
56414 Steinefrenz

Telefon: 06435 / 54 80 287
Fax: 06435 / 90 91 58
e-Mail: info@holmes-und-co.de

www.holmes-und-co.de

Nicht enthalten sind:

- Abholung/Rücktransport der Geräte
- Mehrere Quelldatenträger (z.B. Computer mit mehreren Festplatten)
- Ziel-Datenträger > 1,0 TB
- Zusätzliche Suchläufe (wie bei dem letzten Fall geschehen)

4.) **Bis zu 10 Stunden Bearbeitungszeit inklusive (Ausbau, Einbau, manuelle Spurensuche, Bericht)**

5.) **Erstellung eines Untersuchungsberichtes, bei Bedarf mit Extraktion relevanter Dateien**

6.) **Archivierung des erzeugten Images und der Falldaten für 12 Monate (Standard)**

Wichtig ist auf jeden Fall, dass vor der Auftragsannahme eine Absprache stattfindet, da manche Geräte (z.B. diverse Apple-Modelle) andere forensische Auswertungsumgebungen benötigen oder nicht zerlegbar sind. Bei diesen Geräten muss die Vorgehensweise angepasst werden oder eine klassische Schnellprüfung macht so keinen Sinn.

Unser Preis beläuft sich pro Schnellcheck auf 1.800,00 € netto. Sollte von den o.g. Rahmenbedingungen abgewichen werden (z.B., wenn mehrere Datenträger verbaut sind), dann muss das einzelfallabhängig eingeschätzt werden.
Falls wir Abholungen durchführen sollen, werden diese separat abgerechnet.

(gilt jeweils pro Gerät, es sei denn, ein Computer enthält mehrere sachverhaltsrelevante Speichergeräte)