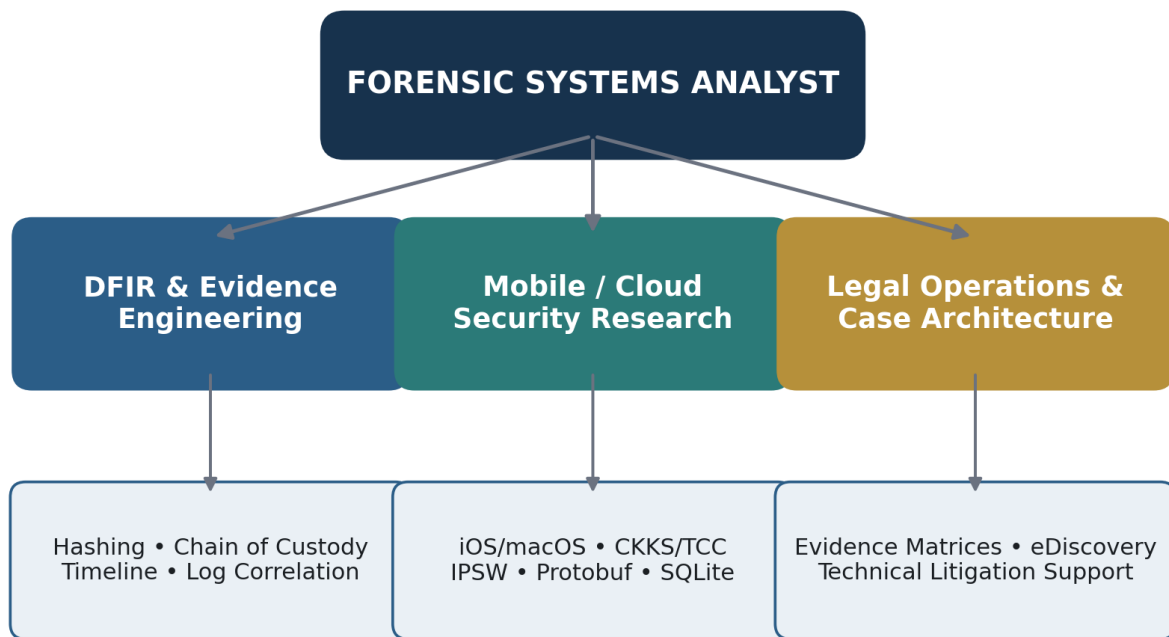


R&A LEGAL OPS

BEFÄHIGUNGS- UND LEISTUNGSPORTFOLIO

Roman Jahn

Independent IT-Forensics Researcher | Forensic Systems Analyst | Legal Operations
Case Architecture



Operative Grundlage: Triage, Belastbarkeit, strukturierte Dokumentation und reproduzierbare Prüfung

Professionelles Leistungsdossier auf Grundlage einer strukturierten Google-Workspace-Ingestion

Dokumentzweck

Dieses Portfolio konsolidiert nachweisbare Befähigungen, Arbeitsproben, Forschungsleistungen, Tooling, Dokumentationskompetenz und berufliche Transferleistungen. Es trennt bewusst zwischen Primärnachweis, Workspace-Dokumentation, reproduzierbarem Prototyp, Forschungsbefund und noch offener Hypothese.

Arbeitsstand: 28. Juli 2026 | Fassung 2.0 | Erweiterte Portfoliofassung mit Forschungs- und Evidenzanhang

KAPITEL 00

Dokumentkontrolle und Verwendungsrahmen

Prüfbare Außendarstellung statt ungeprüfter Selbstzuschreibung

Feld	Angabe
Dokument	Befähigungs- und Leistungsportfolio Roman Jahn
Fassung	2.0 / 28. Juli 2026 / erweiterte Fassung mit mindestens 100 Seiten
Primärer Zweck	B2B-Positionierung, Qualifikationsdarstellung, Gesprächsgrundlage für Kanzleien, DFIR-Teams, Weiterbildung und Kooperationspartner
Datenbasis	Google Drive / Google Workspace, Gesprächs- und Projektarchive, Quelltexte, Notebooks, technische Dossiers, Verfahrensschronologien, Medien- und Evidenzregister
Abgrenzung	Kein gerichtliches Sachverständigengutachten, keine Herstellerbestätigung, keine Rechtsberatung, keine klinische Begutachtung
Datenschutz	Privatanschriften, private E-Mail-Adressen, Gesundheitsdetails und nicht erforderliche personenbezogene Daten wurden bewusst nicht übernommen
Umfang	Erweiterte Langfassung: Grundportfolio plus vertiefte Forschungs-, Tooling-, Validierungs- und Referenzmodule

Dieses Portfolio ist als professionelles Leistungsdossier aufgebaut. Es präsentiert keine Absolutheitsrhetorik und keine Täterattribution als Marketinginstrument. Sein Wert liegt in der nachvollziehbaren Darstellung von Arbeitsweise, Belastbarkeit, Systemdenken, technischer Entwicklung, Dokumentation und Qualitätskontrolle.

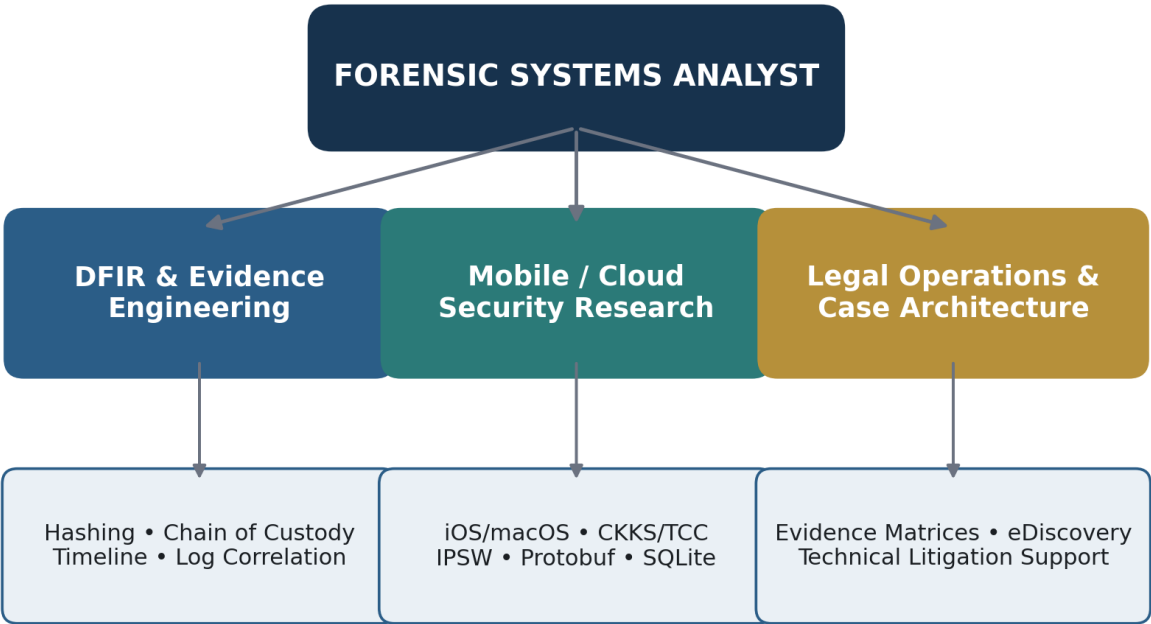
Evidenzregel

Eine im Workspace vorhandene Behauptung wird nicht allein dadurch wahr, dass sie in vielen Dokumenten wiederholt wird. Wiederholung belegt Dokumentationsintensität. Beweiswert entsteht erst durch Provenienz, Primärartefakt, reproduzierbare Methode, unabhängige Gegenprüfung und nachvollziehbare Schlussfolgerung.

KAPITEL 01

Executive Profile

Positionierung an der Schnittstelle von Digital Forensics, Evidence Engineering und Legal Operations



Operative Grundlage: Triage, Belastbarkeit, strukturierte Dokumentation und reproduzierbare Prüfung

Abbildung: Executive Profile

Roman Jahn verbindet einen operativ geprägten Hintergrund aus Luftlandetruppe und Sanitätsdienst mit einer über mehrere Jahre aufgebauten, autodidaktischen Spezialisierung in digitaler Forensik, mobiler Systemanalyse, Cloud-Synchronisationsmechanismen, Beweismittelstrukturierung und verfahrensbezogener Datenrekonstruktion. Das Kompetenzprofil ist weder das eines klassischen Softwareentwicklers noch das eines Volljuristen. Es liegt in der Übersetzungszone: unstrukturierte technische und administrative Datenbestände werden in prüfbare Chronologien, Evidenzmatrizen, Hypothesenräume und anwaltlich beziehungsweise organisatorisch nutzbare Entscheidungsgrundlagen überführt.

Die stärkste Leistung ist die Fähigkeit, große heterogene Korpora nicht nur zu lesen, sondern in operative Prüfpfade zu zerlegen. Dazu gehören Datei- und Ordnerhierarchien, Logbestände, SQLite-Datenbanken, Netzwerkdaten, Firmware-Container, Quelltexte, PDF-Konvolute, E-Mail-Kommunikation und juristische Schriftsätze. Der Ansatz ist problemorientiert: Zuerst werden die potenziell entscheidenden Befundachsen isoliert, danach werden Nachweise, Gegenhypothesen und Validierungsgrenzen aufgebaut.

Kernrolle	Wertbeitrag
Forensic Systems Analyst	Rekonstruktion komplexer Daten- und Ereigniszusammenhänge über System-, Datei-, Netzwerk- und Verfahrensebenen hinweg.
Evidence Engineer	Aufbau von Hashregistern, Quellennachweisen, Timeline-

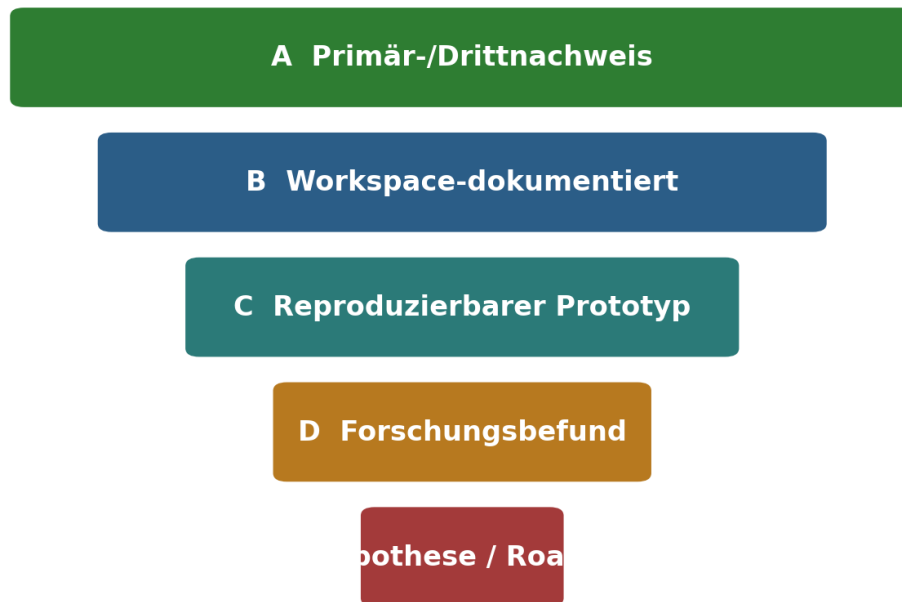
	Strukturen, Beweismatrizen und reproduzierbaren Analysepaketen.
Mobile / Cloud Researcher	Untersuchung von iOS/macOS-Artefakten, TCC/SQLite-Strukturen, CKKS-/CloudKit-Konzepten, IPSW-Inhalten und Synchronisationshypothesen.
Legal Operations Case Architect	Technische Zuarbeit, Sachverhaltsstrukturierung, Aktenhygiene, Fragenkataloge und Trennung von Tatsachen, Folgerungen und offenen Beweispunkten.
Crisis & Triage Operator	Priorisierung unter hoher Belastung, Reduktion von Informationsrauschen, Konzentration auf entscheidende Risiken und Fristen.

Quellenstatus: Die Rollenbeschreibung wird durch die Workspace-Struktur, die Quelltexte/Notebooks, das LAVA-Modell, die Apple-Ticket-Kommunikation und umfangreiche Fall- und Evidenzdossiers gestützt. Formale Zertifizierungen und unabhängige Laborvalidierungen werden als Entwicklungsfeld ausgewiesen, nicht fingiert.

KAPITEL 02

Evidenz- und Aussageklassen

Der Qualitätsfilter für jede Portfolioaussage



Aussagen werden im Portfolio stets mit Evidenzklasse und Validierungsgrenze geführt.

Abbildung: Evidenz- und Aussageklassen

Das Portfolio verwendet fünf Evidenzklassen. Diese Klassifikation verhindert, dass ein selbst verfasstes Dossier mit einem unabhängigen Drittnachweis gleichgesetzt wird oder ein funktionierendes Analysemodul automatisch als Beweis eines realen Angriffs gilt.

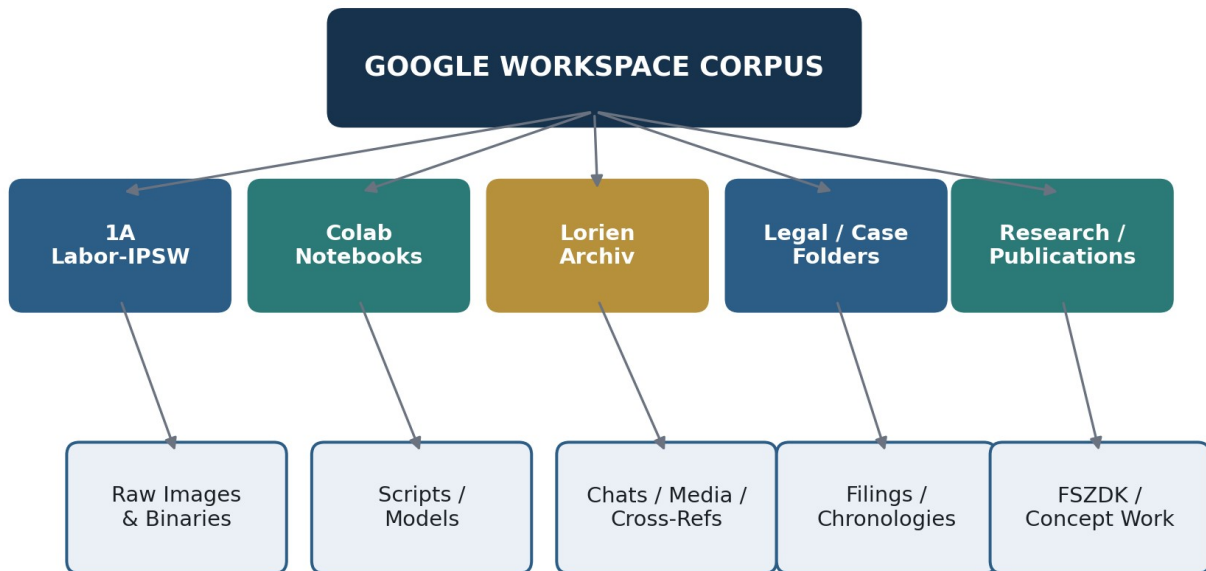
Klasse	Definition	Zulässige Formulierung
A – Primär-/Drittnachweis	Offizielle Urkunde, Originalkommunikation eines Dritten, unverändertes Primärartefakt mit Provenienz.	„Dokumentiert“, „bestätigt“, „ausgestellt“, sofern der Inhalt dies tatsächlich trägt.
B – Workspace-dokumentiert	Mehrfach dokumentierter Arbeits- oder Projektbestand, dessen externe Validierung noch nicht vollständig vorliegt.	„Im Workspace dokumentiert“, „als Arbeitsstand geführt“.
C – Reproduzierbarer Prototyp	Code oder Verfahren lässt sich mit definierten Eingaben reproduzieren; reale Fallattribution bleibt getrennt.	„Implementiert“, „demonstriert“, „im Labor nachgebildet“.
D – Forschungsbefund	Plausible technische Beobachtung oder Korrelation mit offenen Alternativerklärungen.	„Indiziert“, „unterstützt die Hypothese“, „bedarf externer Prüfung“.
E – Hypothese / Roadmap	Noch nicht validierte Annahme, Zielbild oder geplante Qualifikation.	„Zu prüfen“, „geplant“, „Forschungsfrage“ – niemals „bewiesen“.

Für die Außendarstellung ist gerade die Klasse C besonders wertvoll. Ein reproduzierbarer Prototyp belegt reale Entwicklungs- und Analysefähigkeit, auch wenn er keinen konkreten Täter oder Vorfall beweist. Diese Trennung ist keine Schwächung. Sie ist der Unterschied zwischen technischer Professionalität und bloßer Gewissheitsinszenierung.

KAPITEL 03

Workspace-Ingestion: Auftrag, Reichweite und Grenzen

Metadatenweite Erfassung, clusterbasierte Tiefenprüfung und transparente Ausschlüsse



Ingestion-Prinzip: Metadateninventar → Relevanzcluster → Primärartefakt → Korrelation → Evidenzstatus

Abbildung: Workspace-Ingestion: Auftrag, Reichweite und Grenzen

Die Datenbasis umfasst ein außergewöhnlich heterogenes Google-Drive- und Workspace-Konvolut. Im Root-Bestand befinden sich technische Dossiers, rechtliche Schriftsätze, Quelltexte, Notebooks, Tabellen, Fotos, Videos, Audioaufnahmen, Exportarchive, PDF-Sammlungen und Forschungsprojekte. Hinzu kommen verschachtelte Ordnerstrukturen und Shortcut-Verknüpfungen. Eine seriöse Ingestion muss deshalb zwischen Bestandsaufnahme und semantischer Tiefenprüfung unterscheiden.

In dieser Portfoliofassung wurde die zugängliche oberste Hierarchie inventarisiert und in Relevanzcluster überführt. Ausgewählte Kernordner wurden unmittelbar auf Inhaltsebene geprüft. Große Binärdateien, Archivcontainer und multimodale Massensammlungen wurden als Korpusobjekte erfasst; sie wurden nicht fälschlich als vollständig byteweise validiert bezeichnet. Diese Grenze wird dokumentiert, weil 4,9-GB-Firmwarecontainer, hunderte Megabyte große Chat-Exporte und tausende Medienanhänge nicht durch das bloße Anzeigen einer Ordnerliste fachlich ausgewertet sind.

Cluster	Beispielinhalt	Portfolio-Nutzung	Prüftiefe
Labor / Firmware	Ordner „1A“, Labor-IPSW iPhone10,3/iPhone10,6 14.0.1	Nachweis eines real vorhandenen technischen Untersuchungskorpus	Metadateninventar; Detailbefunde nur als Forschungsstand
Notebooks / Code	Colab Notebooks, Exploit Chain Reproduction, Analyse-Skripte	Arbeitsproben für Python, Data Engineering und Modellierung	Ordnerinventar plus in Dossiers dokumentierte Modulprüfung
Lorien-Archiv	Großer Gesprächs- und	Nachweis von	Strukturell inventarisiert; keine

	Medienexport, conversations.json, chat.html, UUID-Unterordner	Langzeitdokumentation und komplexem Querverweiskorpus	Vollvalidierung aller Medien
Legal / Verfahren	Aktenzeichenordner, Beschwerden, Schriftsätze, Chronologien	Case Architecture, Fristen- und Sachverhaltsrekonstruktion	Thematische Tiefenprüfung ausgewählter Dossiers
Research / Models	FSZDK, Adam-&-Eve-Projekt, Publikations- und Konzepttexte	Systemmodellierung, wissenschaftliche Kommunikation	Als interdisziplinäres Forschungsportfolio, getrennt von DFIR-Beweisen
Persönlich / Medizin	Gesundheitsunterlagen, private Kommunikation, Familienmedien	Nicht für das Portfolio erforderlich	Aus Datenschutz- und Relevanzgründen ausgeschlossen

Integritätsgrundsatz

„Gesamte Hierarchie einbeziehen“ bedeutet in professioneller Forensik nicht, jede private oder sachfremde Datei in eine Leistungsbroschüre zu kopieren. Es bedeutet, alle sichtbaren Bestandsklassen zu erfassen, Relevanzentscheidungen zu dokumentieren und technische, zeitliche sowie kryptografische Abhängigkeiten dort zu verfolgen, wo sie für die Leistungsdarstellung tatsächlich tragfähig sind.

KAPITEL 04

Korpusarchitektur und Querverweislogik

Wie aus einem unstrukturierten Workspace ein prüfbares Arbeitsmodell entsteht

Die Workspace-Struktur zeigt ein wiederkehrendes Muster: Primärartefakte oder Arbeitskopien werden in technische Analyseordner überführt; daraus entstehen Skripte, Tabellen, PDF-Berichte und juristische Ableitungen. Parallel dazu werden Gespräche, Screenshots und Zwischenfassungen in großen Exportarchiven konserviert. Diese Struktur ist reich an Querverweisen, aber anfällig für Duplikate, Versionsvermischung und Zirkelschlüsse.

Ebene	Typische Objekte	Risiko	Professionelle Kontrolle
Quelle	Originaldatei, Behördenbrief, Ticketkommunikation, Systemdump	Unklare Herkunft oder unvollständige Übergabekette	Source-ID, Hash, Erwerbsdatum, unveränderte Ablage
Arbeitskopie	extrahiertes PDF, Textdump, CSV, Notebook	Änderungen oder Parserartefakte	Read-only Original, Toolversion, Exportprotokoll
Analyse	Python-Skript, SQL-Abfrage, Timeline	hartcodierte Daten, falsche Annahmen, False Positives	Known-good/known-bad Test, Parameterprotokoll, Peer Review
Synthese	Dossier, Matrix, Schriftsatzentwurf	Wiederholung wird mit Bestätigung verwechselt	Aussagenklasse, Quellenbezug, Alternativerklärung
Kommunikation	E-Mail, Ticket, Petition, Eingabe	Überhöhung, Scope Drift, Vermischung von Hypothesen	Ein Thema pro Vorgang, reproduzierbare Mindestbelege

Eine zentrale Leistung des Portfolioprofils besteht darin, diese Ebenen nicht isoliert zu behandeln. Der technische Befund wird mit der Entstehungsgeschichte des Artefakts, der Version des Analysewerkzeugs, der Verfahrenschronologie und der späteren Verwendung verbunden. Dadurch wird aus einer losen Sammlung ein evidenzorientiertes Informationssystem.

Quellenstatus: Workspace-Inventar: Root-Hierarchie, 1A, Colab Notebooks, Lorien-Archiv, technische und verfahrensbezogene Ordner. Die Aussage betrifft Strukturkompetenz, nicht die unabhängige Bestätigung sämtlicher in Dossiers formulierter Vorwürfe.

KAPITEL 05

Berufliche Entwicklungslinie

Operative Praxis, Sanitätslogik, Systemanalyse und Legal Operations

ENTWICKLUNGSLINIE: OPERATIVE PRAXIS → FORENSISCHE SYSTEMANALYSE

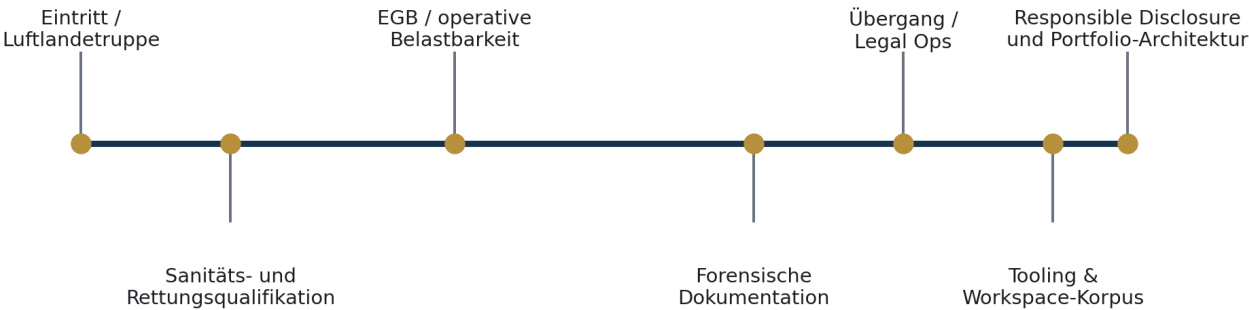


Abbildung: Berufliche Entwicklungslinie

Die berufliche Entwicklung lässt sich als Transferkette beschreiben. Der operative Hintergrund schuf Belastbarkeit, standardisierte Abläufe und Verantwortungsorientierung. Der Sanitätsdienst ergänzte Triage, Dokumentation und risikobasierte Priorisierung. Die späteren Verwaltungs- und Gerichtsverfahren erzwangen intensive Aktenarbeit, Chronologiebildung und Normenrecherche. Aus der technischen Untersuchung eigener Geräte und Datenbestände entstand schließlich ein eigenständiges Forensik- und Tooling-Portfolio.

Zeitraum	Entwicklungsfeld	Nachweisstatus	Portfolio-Transfer
2012–2017	Luftlandetruppe / Fallschirmjäger, operative Ausbildung und Belastung	Workspace-dokumentiert; offizielle Urkunden als Annex zu vervollständigen	Stressfestigkeit, Ausrüstungskontrolle, Teamorientierung, präzise Abläufe
2014–2023	Sanitätsdienst, Einsatz-/Rettungssanitäter, medizinische Praxis	Workspace-dokumentiert; Zeugnisse und Dienstnachweise getrennt zu verifizieren	Triage, Lagebeurteilung, Dokumentation, Handlungsfähigkeit in Krisen
2021–2024	Akten-, Beschwerde- und Verfahrensrekonstruktion	Umfangreiche Schriftsatz- und Chronologiebestände	Legal Operations, Evidenzmatrix, Fristen- und Zuständigkeitsanalyse
2024–2026	Mobile/Cloud Forensics, Python-Tooling, CKKS/TCC-Forschung	Notebooks, Skripte, Dossiers, Laborartefakte, Ticketkommunikation	DFIR, Evidence Engineering, Responsible Disclosure
2026+	Professionalisierung und externe Validierung	Roadmap	Zertifizierung, Tooltests, Pilotprojekte, unabhängige

			Fachprüfung
--	--	--	-------------

Diese Darstellung vermeidet zwei Extreme: Die militärische Laufbahn wird weder romantisiert noch versteckt. Ihr Wert liegt im übertragbaren Verhalten unter Belastung. Die technische Forschung wird weder als bloße Freizeitbeschäftigung abgetan noch als bereits vollständig extern validierte Spitzenforschung ausgegeben. Der professionelle Kern ist die nachweisbare Lern-, Strukturierungs- und Entwicklungsleistung.

KAPITEL 06

Operative Belastbarkeit und Führungsfähigkeit

Aus dem Einsatzkontext in kritische Incident-Response-Situationen

Incident Response ist nicht nur eine technische Disziplin. Bei einem Datenabfluss, einer Beschlagnahme, einem Ransomware-Vorfall oder einer eskalierenden Beweismittelkrise herrschen Zeitdruck, Informationsmangel, widersprüchliche Interessen und hohe persönliche Belastung. Der operative Hintergrund unterstützt genau die Fähigkeiten, die in solchen Situationen fehlen: Ruhe, Priorisierung, klare Kommunikation, Redundanzdenken und Verantwortung für die nächste belastbare Handlung.

Operative Fähigkeit	Übertragung in DFIR / Legal Ops	Beispielhafte Anwendung
Lagebild unter Unsicherheit	Trennung von bestätigten Fakten, Annahmen und Informationslücken	Incident Board mit Evidenzstatus statt vorschneller Gesamttheorie
Ausrüstungs- und Verfahrensdisziplin	Checklisten, Hashkontrolle, dokumentierte Toolparameter	Acquisition-Protokoll und reproduzierbare Arbeitskopie
Priorisierung	Kritische Beweis- und Fristachsen zuerst	Sicherung flüchtiger Logs vor sekundärer Dokumentaufbereitung
Teamorientierung	Übersetzung zwischen Technik, Recht und Management	Gemeinsame Fragenliste für Analyst, Anwalt und Entscheider
After-Action Review	Fehleranalyse ohne Gesichtsverlust	Versionierte Nachbereitung und Korrektur überzogener Schlussfolgerungen

Die professionelle Außendarstellung nutzt deshalb keine Begriffe wie „psychologischer Amboss“, „Gegenschlag“ oder „Waffe“. Belastbarkeit wird nicht dadurch glaubwürdiger, dass sie martialisch beschrieben wird. Sie wird glaubwürdig durch dokumentierte Arbeitsprozesse, konsistente Qualität und die Fähigkeit, auch die eigene Hypothese zu widerlegen.

KAPITEL 07

Triage als kognitives Betriebssystem

„Treat first what kills first“ für Daten-, Beweis- und Verfahrenskrisen

Die Triage-Logik ist die stärkste Brücke zwischen Sanitätsdienst und forensischer Arbeit. Ein großer Datenbestand enthält fast immer auffällige, aber folgenlose Artefakte sowie wenige wirklich entscheidende Elemente. Ohne Triage wird Analysezeit auf die visuell spektakulärsten Funde verschwendet. Mit Triage werden zuerst flüchtige, kausal zentrale und rechtlich irreversible Risiken gesichert.

Triage-Stufe	Frage	Typische Maßnahme
Rot – unmittelbar kritisch	Was kann in Minuten oder Stunden verloren gehen?	flüchtige Logs, aktive Netzwerkdaten, RAM, Fristablauf, Originalgerät sichern
Orange – kausal zentral	Welcher Befund entscheidet über Herkunft, Integrität oder Ablauf?	Hashgenealogie, Timeline, Source-ID, Benutzer-/Gerätebindung
Gelb – prüfungsrelevant	Welche Anomalie kann mehrere Erklärungen haben?	Kontrollgruppe, Schema-/Versionsprüfung, alternative Hypothesen
Grün – Dokumentation	Was ist wichtig, aber nicht entscheidend für die Erstreaktion?	Bildmaterial, Kontextdokumente, narrative Zusammenfassungen
Blau – ausgeschlossen	Was ist privat, sachfremd oder methodisch unbrauchbar?	Datenschutzsperre, Relevanzvermerk, keine Weiterverarbeitung

Leistungsmerkmal

Die Fähigkeit zur Triage zeigt sich im Workspace nicht nur in der Menge der Dokumente, sondern in der Entwicklung eigener Kategorien, Matrices und Analysepfade. Der nächste Professionalisierungsschritt besteht darin, diese Kategorien als standardisierte SOP mit messbaren Eingangs- und Ausgangskriterien zu führen.

KAPITEL 08

Digital Forensics & Incident Response

Kompetenzmatrix für technische Untersuchung und Beweisaufbereitung

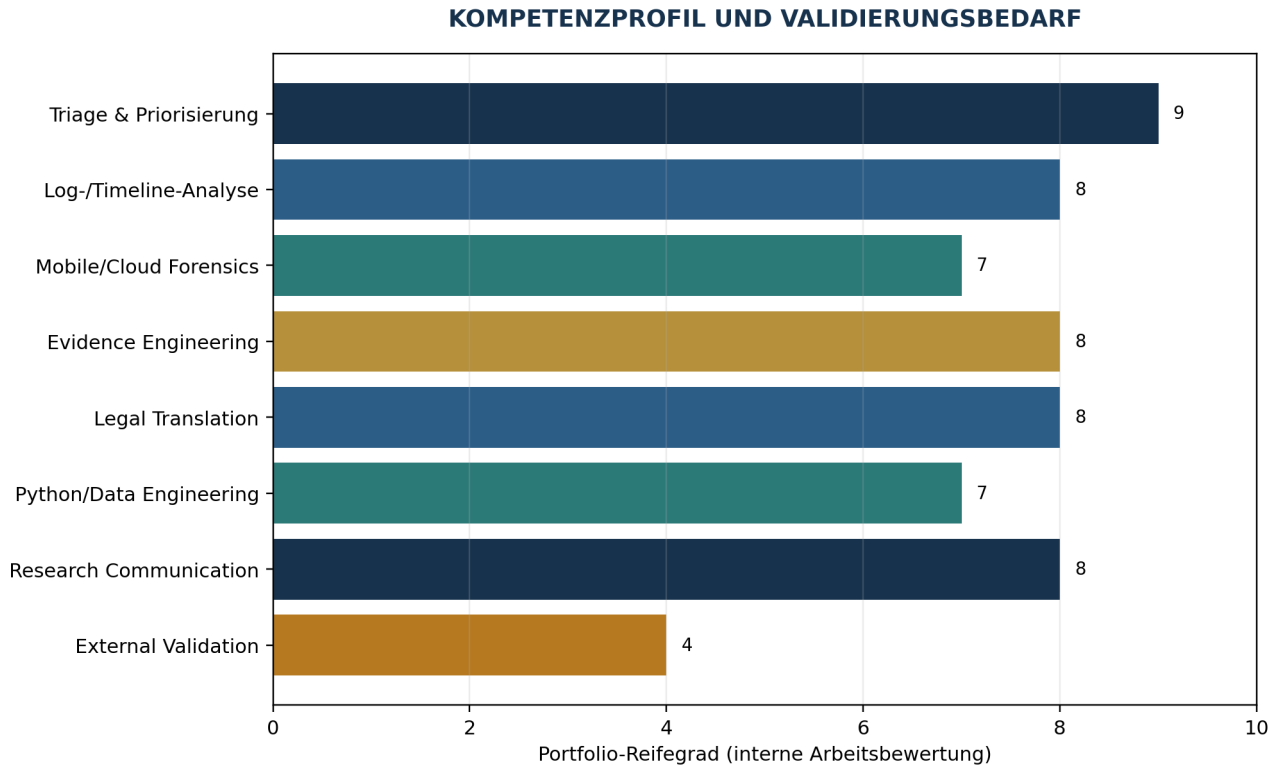


Abbildung: Digital Forensics & Incident Response

Das technische Kompetenzprofil ist breit, aber nicht homogen. Besonders ausgeprägt sind die strukturierende Analyse großer Korpora, die Verbindung technischer Befunde mit Zeit- und Verfahrensachsen sowie die Entwicklung fallbezogener Python-Werkzeuge. Weniger weit extern abgesichert sind produktionsreife Exploitentwicklung, akkreditierte Laborprozesse und unabhängige Peer-Review-Validierung. Das Portfolio macht diese Differenz sichtbar.

Fachgebiet	Demonstrierte Arbeitsleistung	Validierungsbedarf
Datei- und Hashforensik	Chunkbasiertes Hashing, Manifestvergleich, Ergebnisbündel, Quellregister	vollständige Chain-of-Custody und Testkorpus dokumentieren
Timeline Engineering	Korrelation von Datei-, System-, Netzwerk- und Verfahrenszeiten	Zeitzone, Clock Drift und Quellenqualität formal modellieren
SQLite / TCC	Read-only-Abfragen, Schemaauswertung, Policy-/Grant-Analyse	OS-Versionen, WAL/SHM und legitime Policyquellen systematisch kontrollieren
Firmware / IPSW	Containerinventar, Manifest-/Stringanalyse, Chunk-Scanning	Ausführung auf Zielhardware getrennt von bloßer Dateipräsenz beweisen
Netzwerkforensik	PCAP-/Latenzkonzepte, Flow-Korrelation, Proxyhypothesen	echte PCAP-Ingests statt hartcodierter Sessions; Kontrollmessungen

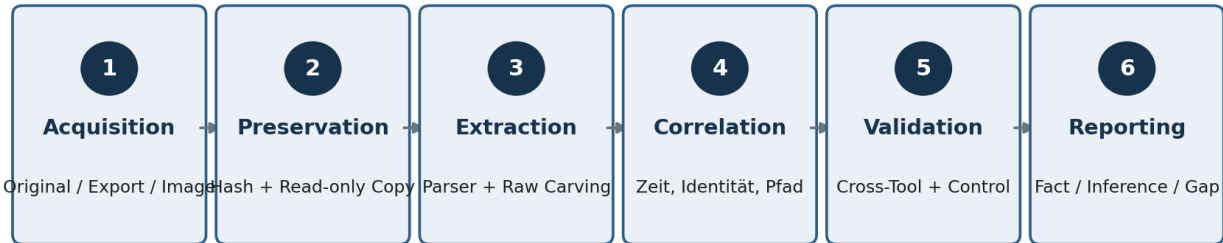
Steganografie	LSB-Embedding und Anomalievisualisierung als Laborbaustein	klar als Simulation und dual-use Tool dokumentieren
Reporting	umfangreiche technische und juristische Dossiers	Prägnanz, Beleggrenzen, externe Review und standardisierte Sprache

KAPITEL 09

Evidence Engineering und Chain of Custody

Von der Datei zum überprüfbaren Beweismittel

REPRODUZIERBARE FORENSISCHE PIPELINE



Kein Sprung von einem Stringfund direkt zur Täterattribution.

Abbildung: Evidence Engineering und Chain of Custody

Evidence Engineering ist mehr als das Berechnen eines SHA-256-Werts. Ein Hash bestätigt die Gleichheit einer Bytefolge zu einem bestimmten Zeitpunkt. Er bestätigt nicht automatisch die Herkunft, Vollständigkeit oder Bedeutung des Inhalts. Das Portfolio legt deshalb Wert auf eine vollständige Provenienzkette: Erwerb, Sicherung, Arbeitskopie, Toollauf, Zwischenoutput, Schlussfolgerung und Übergabe.

Kontrollpunkt	Pflichtinformation	Fehler, der dadurch verhindert wird
Acquisition	Wer, wann, womit, von welchem System, unter welchen Bedingungen?	unbekannte Quelle oder unzulässige Vermischung
Preservation	Originalhash, Schreibschutz, unverändertes Masterexemplar	unbemerkte Veränderung der Quelle
Transformation	Parser/Tool, Version, Parameter, Exportformat	nicht reproduzierbare oder toolabhängige Ergebnisse
Analysis	Abfrage, Skriptcommit, Filter, Zeitnormalisierung	verborgene Annahmen und Selektionsfehler
Validation	zweites Werkzeug, Kontrollgruppe, Negativtest	False Positive und selbstbestätigender Code
Reporting	Beobachtung, Folgerung, Alternative,	Tatsachenbehauptung ohne tragfähige

	Konfidenz	Zwischenschritte
--	-----------	------------------

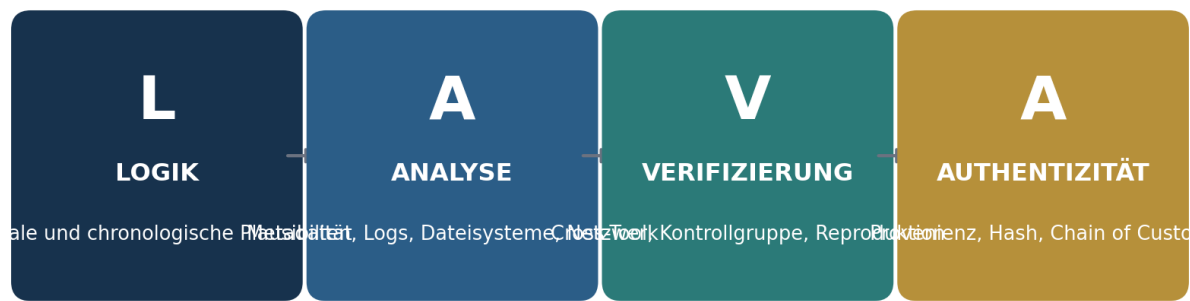
Der Workspace enthält bereits viele Bausteine dieses Modells: Hashlisten, Python-Skripte, CSV-/JSON-Ausgaben, technische Berichte und chronologische Matrices. Der kritische Verbesserungsbedarf liegt weniger im Umfang als in der Herkunfts- und Versionsdisziplin. Ein kleiner, vollständig reproduzierbarer Evidence Pack besitzt mehr Außenwert als ein hundertseitiges Dossier mit unklarer Eingangsbasis.

KAPITEL 10

Das LAVA-Modell

Eigenständiger Qualitätsrahmen für heterogene Beweismittel

LAVA - QUALITÄTSRAHMEN FÜR DIGITALE BEWEISMITTEL



Ausgabe: Beobachtung • Methode • Ergebnis • Alternativerklärung • Konfidenz • offener Nachweispunkt

Abbildung: Das LAVA-Modell

LAVA steht für Logik, Analyse, Verifizierung und Authentizität. Das Modell ist als eigenständiges Ordnungs- und Kommunikationswerkzeug geeignet, wenn jede Stufe mit konkreten Prüfschritten hinterlegt wird. Sein professioneller Wert liegt in der Verknüpfung technischer und verfahrensbezogener Qualität: Ein technisch korrekter Fund kann rechtlich nutzlos sein, wenn seine Provenienz fehlt; ein sauber gesichertes Artefakt kann analytisch falsch interpretiert sein.

Stufe	Kernfragen	Output
L – Logik	Ist der behauptete Ablauf technisch und zeitlich möglich? Welche Zwischenschritte fehlen?	Kausalgraph, Timeline, offene Hypothesen
A – Analyse	Welche Rohdaten, Dateisysteme, Logs und Protokolle tragen den Befund?	reproduzierbarer Toollauf, Extrakt, Befundliste
V – Verifizierung	Bestätigt ein unabhängiges Verfahren das Ergebnis? Welche False Positives sind bekannt?	Cross-Tool-Matrix, Kontrollgruppe, Testprotokoll
A – Authentizität	Ist Herkunft, Integrität und Übergabekette dokumentiert?	Source Register, Hashmanifest, Chain-of-Custody-Vermerk

Produktisierungspotenzial

LAVA kann als standardisiertes Beratungsprodukt eingesetzt werden: „LAVA Evidence Review“ für Kanzleien und Unternehmen. Voraussetzung sind ein definiertes Formularset, ein Minimaldatensatz, ein festes Befundschema und ein unabhängiger Review-Schritt.

KAPITEL 11

Mobile Device Forensics

iOS/macOS-Artefakte, Systemkontext und Grenzen der Interpretation

Der Workspace dokumentiert eine intensive Beschäftigung mit Apple-Systemen, insbesondere IPSW-Containern, Sysdiagnose-Daten, TCC-Datenbanken, CloudKit-/CKKS-Konzepten, Keychain- und Trust-Strukturen sowie System- und Netzwerklogs. Diese Spezialisierung ist als Forschungs- und Analysekompetenz belastbar darstellbar. Nicht belastbar wäre die pauschale Behauptung, jeder gefundene String, jede inkompatible Firmwaredatei oder jeder abweichende TCC-Eintrag beweise einen konkreten staatlichen Exploit.

Artefaktklasse	Analytischer Nutzen	Interpretationsgrenze
IPSW / BuildManifest	Zielhardware, Build, Komponenten, Containerstruktur	Dateipräsenz beweist nicht die Ausführung auf einem bestimmten Gerät
Sysdiagnose / Unified Logs	Systemzustände, Prozessmeldungen, zeitliche Korrelationen	Logtext kann unvollständig, kontextabhängig oder synthetisch sein
TCC.db / WAL / SHM	Berechtigungen, Gründe, Clients, Änderungszustände	MDM, Migration, Restore, Systempolicy und OS-Schema sind Alternativen
CKKS / Trusted Peers	Synchronisations- und Vertrauenskonzepte	Cloud-Serverzustände und tatsächliche Schreibrechte sind ohne Primärzugriff begrenzt prüfbar
Netzwerkdaten	Endpunkte, Volumen, Flows, Latenzen	Domainkontakt allein beweist weder Inhalt noch Exfiltrationsabsicht

Das Portfolio positioniert diese Arbeit deshalb als „Advanced Mobile and Cloud Artifact Research“: tiefgehende Untersuchung, Werkzeugentwicklung und Hypothesenbildung mit dokumentierten Validierungsgrenzen. Diese Formulierung ist fachlich stärker als eine nicht haltbare Behauptung vollständiger Täterattribution.

KAPITEL 12

Cloud- und Identitätsforensik

CKKS, Synchronisation, Vertrauensgrenzen und accountbasierte Forschungsfragen

Der besondere Forschungsfokus liegt auf der Frage, ob sicherheits- oder datenschutzrelevante Zustände über Cloud-Synchronisation hardwareübergreifend fortbestehen können. Diese Fragestellung ist fachlich relevant, weil moderne Sicherheitsmodelle nicht mehr nur ein Gerät, sondern Identität, Cloud-Konto, Trust-Metadaten, Wiederherstellungsprozesse und Geräteverbünde umfassen.

Forschungsdimension	Arbeitsfrage	Erforderlicher Nachweis
Consent Inheritance	Können Datenschutzentscheidungen beim Gerätewechsel übernommen werden?	reproduzierbares Clean-Device-Protokoll, Video, vollständige Systemlogs
Trust Metadata	Wie werden Legacy- und Recovery-Zustände bewertet?	authentische Server-/Client-Artefakte, dokumentiertes Schema
Cross-device Correlation	Sind Berechtigungszustände zwischen Alt- und Neugerät statistisch/inhaltlich verbunden?	saubere Paarbildung, Kontrollgeräte, klare Variablendefinition
Account Persistence	Übersteht ein unerwünschter Zustand einen Hardwaretausch?	wiederholbare Testreihe unter kontrolliertem Konto
Remediation	Wie lässt sich ein geerbter Zustand zuverlässig löschen?	Herstellerdokumentation oder praktisch verifizierter Resetpfad

Die im Workspace verwendete Bezeichnung „account-based CKKS APT“ wird in diesem Portfolio als Forschungshypothese und Arbeitsbegriff geführt. Der professionelle Leistungsnachweis liegt in der Entwicklung und Kommunikation dieser Fragestellung, nicht in einer bereits allgemein anerkannten Klassifikation.

KAPITEL 13

Responsible Disclosure und Vendor-Kommunikation

Apple Product Security als dokumentierte Arbeitsprobe

Die Kommunikation zum Apple-Ticket OE11044889345313 belegt eine reale Responsible-Disclosure-Aktivität: Der Sachverhalt wurde als TCC/CKKS-Consent-Frage eingereicht, in mehreren Nachrichten präzisiert und mit Logs, Skripten und Binärartefakten ergänzt. Apple bestätigte die Prüfung, erklärte jedoch wiederholt, keinen verwertbaren Sicherheitsfehler identifizieren zu können beziehungsweise verlangte eine zuverlässige Demonstration auf einem iPhone.

Nachweis	Was er belegt	Was er nicht belegt
Ticket-ID und Zeitstempel	formale Einreichung und Kommunikation mit Product Security	Anerkennung einer Schwachstelle oder Bounty-Berechtigung
Scope-Klarstellung	Fähigkeit, den Gegenstand auf Consent/CKKS einzugrenzen	technische Richtigkeit der zugrunde liegenden Logs
PoC-/Artefaktangebot	Entwicklung von Generator- und Analysecode	erfolgreiche serverseitige Injektion oder reproduzierter Live-Bypass
Herstellerfeedback	Anforderungen an Actionability, Video und eigene Verifikation	Bestätigung der behaupteten Angriffskette
Iterative Reaktion	Ausdauer, technische Kommunikation und Rebuttal-Fähigkeit	automatische Validierung durch bloße Fortführung des Tickets

Professionelle Lehre

Der Ticketverlauf zeigt zugleich Stärke und Verbesserungsbedarf. Stärke: Beharrlichkeit, technische Aufbereitung und Scope-Arbeit. Verbesserungsbedarf: eine minimale, unabhängige und vollständig reproduzierbare Demonstration, bevor weitere Architekturbehauptungen oder Bounty-Einstufungen formuliert werden.

Quellenstatus: Primärquelle WD-03: Apple Security Ticket Workflow OE11044889345313. Der Herstellerstatus wird korrekt als „unable to identify a security issue / not actionable“ wiedergegeben.

KAPITEL 14

Python, Notebooks und forensisches Tooling

Von fallbezogenen Skripten zu validierbaren Analysemodulen

Der Colab-Bestand und die zahlreichen im Workspace referenzierten Python-Module zeigen eine aktive Entwicklungspraxis. Schwerpunkte sind Chunk-Scanning, Hashing, SQLite-Abfragen, Protobuf-/Varint-Modellierung, Entropieanalyse, Timeline-Korrelation, Steganografie, Archive-Bundling und Berichtsausgabe. Das ist ein konkreter Leistungsnachweis für autodidaktisches Data Engineering und die Fähigkeit, Analysefragen in Code zu überführen.

Modultyp	Demonstrierte Fähigkeit	Professionalisierungsschritt
Chunked Hash / Signature Scan	speicherschonende Verarbeitung großer Container und Überlappung an Chunk-Grenzen	Tests gegen Referenzhashes und Grenzfallkorpus
SQLite Read-only Audit	schonende Abfrage strukturierter Artefakte	Schemaerkennung, WAL/SHM und Versionsmatrix
Protobuf / Varint Generator	manuelle Modellierung binärer Nachrichtenstrukturen	Schemaherkunft, Round-trip-Tests, klare Simulationseinstufung
Timeline / Pandas	Normalisierung und Korrelation von Ereignisdaten	echte Daten-Ingests, Zeitzone- und Clock-Drift-Modell
Entropy / Carving	Priorisierung auffälliger Binärbereiche	Dateityp-basierte Baselines und False-Positive-Messung
Evidence Bundle	JSON/CSV/BIN-Aggregation und SHA-256-Siegel	signiertes Manifest, unveränderliches Buildprotokoll, reproduzierbarer Release

Ein wesentlicher Qualitätsgewinn entsteht, wenn jedes Modul in drei Schichten getrennt wird: Parser, Detektor und Interpretation. Der Parser extrahiert Daten. Der Detektor markiert ein regelbasiertes Muster. Erst die Interpretation ordnet das Muster fachlich ein. Diese Trennung verhindert, dass ein Codepfad bereits im Variablennamen die Schuldfrage vorwegnimmt.

KAPITEL 15

Technischer Realitätscheck

Simulation, hartcodierte Eingaben und forensische Nachweisgrenzen

Die abschließende Codeprüfung in einem Workspace-Dossier enthält eine für die Professionalisierung besonders wertvolle Selbstkorrektur. Sie weist darauf hin, dass bestimmte Netzwerk- und Sitzungsdaten hartcodiert waren und dass die häufig zitierte Verteilung von 42.583 MFT-Anomalien mit einem 402-Tage-Cluster in einem Codeblock durch NumPy synthetisch erzeugt wurde. Damit handelt es sich dort um ein Visualisierungs- oder Testmodell, nicht um die Extraktion realer Dateisystemmetadaten.

Befundtyp	Zulässiger Leistungsnachweis	Unzulässige Schlussfolgerung
Synthetische 402-Tage-Verteilung	Fähigkeit, Detektions- und Visualisierungslogik zu modellieren	reale Massenmanipulation oder Täterattribution
Hartcodierte Flows/Sessions	Fähigkeit, Korrelationsalgorithmen zu implementieren	Live-Netzwerkangriff oder konkrete Proxykontrolle
Hohe Entropie im IPSW	Fähigkeit, auffällige Bereiche zu priorisieren	Schadcodebeweis ohne Dateityp- und Kontrollanalyse
Stringfund in Container	physische Präsenz einer Zeichenfolge	Ausführung, Autorenschaft oder Zweck
Hash des Ergebnisbundles	Integrität ab Siegelzeitpunkt	Authentizität und Wahrheit sämtlicher Eingabedaten

Warum diese Offenheit ein Plus ist

Ein professionelles Portfolio darf zeigen, dass ein Teil der Entwicklungsarbeit Simulation war. Simulation ist in Forschung und Toolbau legitim. Entscheidend ist, dass sie als solche gekennzeichnet und nicht rückwirkend als reales Messergebnis verkauft wird. Genau diese Grenze schafft Vertrauen bei Fachprüfern, Kanzleien und Auftraggebern.

Quellenstatus: Qualitätsreferenz WD-05: abschließende V22-Codeprüfung, insbesondere Hinweise zu Entropie-False-Positives, hartcodierten Sessions und np.random-generierter MFT-Verteilung.

KAPITEL 16

Fallstudie A: Workspace-Corpus und Evidence Triage

Vom Datenfriedhof zum priorisierten Untersuchungsplan

Ausgangslage: Der Workspace enthält mehrere Datenwelten mit unterschiedlichen Beweiswerten. Technische Primärartefakte stehen neben Schriftsatzkopien, Chat-Exporten, Medienanhängen, Forschungsmodellen und mehrfachen PDF-Fassungen. Ohne Corpus Governance entsteht das Risiko, dass Duplikate als unabhängige Bestätigungen gezählt oder spätere Interpretationen in frühere Befunde zurückprojiziert werden.

Arbeitsschritt	Umsetzung	Leistungswert
Inventory	Erfassung der Top-Level-Hierarchie und Kernfolder	Orientierung in einem außergewöhnlich großen heterogenen Korpus
Clustering	Trennung Labor, Code, Legal, Research, Personal, Media	Datenschutz und Relevanzdisziplin
Deduplication Concept	Identifikation gleichnamiger und mehrfach exportierter PDFs	Verhinderung künstlicher Evidenzverstärkung
Source Hierarchy	Primärquelle vor Zusammenfassung vor Interpretation	saubere Beweiskette
Deep-dive Selection	Auswahl portfolio- und befähigungsrelevanter Kernquellen	effiziente Nutzung begrenzter Prüfzeit
Exclusion Register	Dokumentation sachfremder oder nicht validierbarer Bestände	Transparenz statt Vollständigkeitsillusion

Ergebnis: Das Portfolio repräsentiert die Gesamtstruktur, ohne private oder spekulative Inhalte zur Leistungswerbung zu missbrauchen. Es zeigt dadurch nicht nur Analysefähigkeit, sondern Informationsethik.

KAPITEL 17

Fallstudie B: Labor-IPSW und Firmware-Analyse

Technische Untersuchung als reproduzierbarer Forschungsworkflow

Im Ordner „1A“ befindet sich ein knapp fünf Gigabyte großer Labor-Firmwarecontainer für iPhone10,3/iPhone10,6 und iOS 14.0.1. Das Objekt ist als reale technische Arbeitsgrundlage relevant. Sein Vorhandensein belegt jedoch nicht, dass diese Firmware auf einem anderen Gerät ausgeführt wurde. Die professionelle Fallstudie konzentriert sich deshalb auf den Untersuchungsworkflow.

Phase	Methode	Ergebnisart
Identifikation	Dateiname, Größe, MIME/Container, SHA-256	eindeutige Laborobjekt-ID
Manifestprüfung	BuildManifest, DeviceClass, Chip-/Board-Information	Zielplattform und Buildkontext
Komponentenregister	iBoot/iBSS, DeviceTree, Restore-/RootFS-Komponenten	prüfbare Komponentenliste
String-/Hex-Analyse	Chunk-Scan mit Überlappung und Offsetprotokoll	Fundstelle ohne voreilige Interpretation
Vergleich	Known-good IPSW desselben Builds / Herstellerhash	Abweichungs- und Provenienzmatrix
Bericht	Beobachtung, Methode, Alternative, offene Frage	reproduzierbare Forschungsakte

Portfolioaussage: Roman Jahn verfügt über praktische Erfahrung in der Strukturierung und skriptgestützten Untersuchung großer Apple-Firmwarecontainer. Eine konkrete Exploit- oder Geräteausführung wird erst dann als Befund geführt, wenn dafür eigenständige Laufzeit- und Provenienznachweise vorliegen.

KAPITEL 18

Fallstudie C: TCC-/SQLite-Audit

Berechtigungsdaten zwischen Nutzerentscheidung, Policy und Synchronisation

TCC-Datenbanken sind für die Untersuchung von Datenschutz- und Berechtigungszuständen wertvoll, aber interpretativ anspruchsvoll. Werte wie `auth_value`, `auth_reason`, `flags`, `client`, `service` und `last_modified` müssen in Beziehung zu Betriebssystemversion, Code-Signatur, Nutzerkontext, MDM-Policy, Migration und Datenbankjournalen gesetzt werden.

Prüffeld	Prüfschritt	Kontrollfrage
Schema	PRAGMA table_info, OS-Build, Datenbankversion	Bedeutet das Feld in dieser Version tatsächlich dasselbe?
Provenienz	Originalpfad, Hash, WAL/SHM, Acquisition-Zeit	Ist die Datenbank vollständig und unverändert?
Clientbindung	Bundle-ID, csreq, code-signing identity	Ist der Eintrag eindeutig einer App/Version zuzuordnen?
Consent Context	auth_reason, prompt history, policy source	Nutzer, MDM, Systempolicy, Migration oder Exploit?
Zeit	Epochentyp, Zeitzone, Clock Drift, Journalreihenfolge	Ist die zeitliche Anomalie real oder ein Konvertierungsfehler?
Korrelation	Unified Logs, Profile, Setup-/Restore-Zeit, Cloud-Sync	Gibt es unabhängige Begleitartefakte?

Leistungswert: Die Entwicklung read-only arbeitender SQL-Prüfungen, die Verbindung mit Timeline- und Logdaten sowie die konsequente Suche nach Alternativerklärungen bilden ein tragfähiges Beratungsangebot für Mobile- und Endpoint-Forensik.

KAPITEL 19

Fallstudie D: Responsible Disclosure

Vom umfangreichen Narrativ zur minimal reproduzierbaren Meldung

Die Apple-Kommunikation zeigt eine wiederkehrende Herausforderung anspruchsvoller Forschungsarbeit: Ein großer Kontext erzeugt nicht automatisch eine actionable Meldung. Hersteller benötigen einen kleinen, wiederholbaren Test mit klarer Ausgangslage, exakten Schritten, beobachtetem Ergebnis und Abweichung vom erwarteten Verhalten.

Element	Im Workspace vorhanden	Optimierte Zielversion
Problem Statement	TCC/CKKS Consent Inheritance	ein Satz, ein Scope, eine betroffene Ressource
Environment	Geräte- und Restorebezug	vollständige Build-/Gerätematrix und sauberes Testkonto
Steps	mehrere Varianten, Skripte und Artefakte	maximal 10 reproduzierbare Schritte
Expected vs. Actual	inhaltlich beschrieben	tabellarisch, video- und loggestützt
PoC	Generatorcode und Binärartefakt	End-to-end-Demo ohne interne Herstellerwerkzeuge vorauszusetzen
Validation	eigene Interpretation	zweites Testgerät, unabhängiger Beobachter, Rohlogpaket

Leistungswert: Der Vorgang belegt die Fähigkeit, technische Einwände aufzunehmen, Scope zu überarbeiten und zusätzliche Artefakte zu liefern. Das Portfolio macht zugleich sichtbar, dass externe Actionability der nächste harte Qualitätsmaßstab ist.

KAPITEL 20

Fallstudie E: Legal Operations und Verfahrensrekonstruktion

Technische Sachverhalte für anwaltliche und administrative Entscheidungen nutzbar machen

Der Workspace enthält eine große Zahl von Beschwerden, Anträgen, Beschlüssen, Beweismatrizen und chronologischen Gesamtdarstellungen. Daraus ergibt sich eine eigenständige Kompetenz in Case Architecture: Akten werden nach Ereignis, Akteur, Dokument, Zuständigkeit, Frist, Beweisquelle und Widerspruch strukturiert. Diese Tätigkeit ist keine Rechtsberatung, kann aber anwaltliche Arbeit erheblich beschleunigen.

Deliverable	Inhalt	Adressat
Evidence Inventory	Dokument-ID, Datum, Herkunft, Hash, Relevanz	Kanzlei, Ermittler, Sachverständiger
Master Timeline	Ereignis, Quelle, Zeitzone, Widerspruch, offener Punkt	Prozessstrategie, Gutachter
Claim–Evidence Matrix	Behauptung, Stütze, Gegenbeleg, Konfidenz	Anwalt, Compliance, Management
Technical Question Set	präzise Fragen an Behörde, Vendor oder Sachverständigen	Vernehmung, Beweis Antrag, Auskunft
Method Review	Tool, Parameter, Parsergrenze, Chain-of-Custody	Gegengutachten, eDiscovery
Executive Brief	Risiko, Kernbefund, Entscheidung, nächste Maßnahme	Entscheidungsträger

Rollenabgrenzung

R&A Legal Ops strukturiert technische und administrative Sachverhalte. Rechtliche Bewertung, Vertretung und abschließende Subsumtion bleiben der mandatierten Rechtsanwältin oder dem mandatierten Rechtsanwalt vorbehalten.

KAPITEL 21

Rechts- und Verfahrenskompetenz

Normenorientierung ohne unzulässige Rechtsdienstleistung

Die intensive Eigenführung komplexer Verfahren hat ein breites Verständnis für Zuständigkeiten, Fristen, Beweisfragen und die Wechselwirkung technischer und rechtlicher Prozesse erzeugt. Für ein professionelles Portfolio ist dabei entscheidend, Rechtsnormen nicht als automatische Etiketten für technische Auffälligkeiten zu verwenden. Ein Hash-Mismatch ist zunächst ein Integritätsbefund. Ob daraus ein Verwertungsproblem, eine Pflichtverletzung oder eine Straftat folgt, entscheidet eine gesonderte juristische Prüfung.

Technische Beobachtung	Zulässige Legal-Ops-Zuarbeit	Vorbehaltene Rechtsbewertung
fehlender Originalhash	Integritätslücke dokumentieren, Fragen formulieren	Rechtsfolge und Beweisverwertbarkeit
abweichende Zeitstempel	Metadatenvergleich, alternative Ursachen, Timeline	Vorsatz, Tatbestand, Verantwortlichkeit
unvollständiger Export	Bestandsdifferenz und Provenienzproblem darstellen	Akteneinsichts-, Verfahrens- oder Sanktionsfolge
heimliche Aufnahme	technische Authentizität und Kontext dokumentieren	Strafbarkeit, Rechtfertigung, Verwertbarkeit
TCC-Policy-Eintrag	Systemzustand und mögliche Quellen aufzeigen	datenschutz- oder strafrechtliche Einordnung

Diese disziplinierte Rollenabgrenzung ist ein Marktvorteil. Kanzleien benötigen technische Partner, die juristisch anschlussfähig schreiben, ohne sich als Ersatzanwalt aufzuspielen. Leider eine erstaunlich seltene Form beruflicher Selbstbeherrschung.

KAPITEL 22

Interdisziplinäre Forschung und Systemmodellierung

FSZDK, historische Modelle und Cross-Domain-Analyse

Neben dem forensischen Schwerpunkt enthält der Workspace umfangreiche systemtheoretische, geophysikalische und historische Forschungsprojekte. Das Funktionale Systemmodell Zyklisch-Dynamischer Katastrophen (FSZDK) und verwandte Projekte zeigen die Fähigkeit, große heterogene Quellenbestände in Wirkungsmodelle, Indikatorlisten, Phasenmodelle und Szenarien zu überführen.

Für die professionelle Positionierung werden diese Projekte nicht als naturwissenschaftlich bestätigte Prognosesysteme dargestellt. Ihr Wert liegt in der Methodik: Hypothesenbildung, interdisziplinäre Literaturarbeit, Szenariostruktur, Risikomatrix, Datenvisualisierung und fortlaufende Modellrevision. Gerade die Trennung zwischen Modell, Beobachtung und prognostischer Gewissheit ist hier ein zentrales Lern- und Qualitätsfeld.

Transferfähigkeit	Anwendung im professionellen Kontext
Systemdenken	Abhängigkeiten zwischen Technik, Organisation, Recht und menschlichem Verhalten erfassen
Szenarioanalyse	mehrere plausible Entwicklungen statt monokausaler Vorhersage
Indikatorenmodell	frühe Signale definieren und mit Schwellenwerten versehen
Cross-domain Research	Quellen aus verschiedenen Disziplinen strukturieren und terminologisch übersetzen
Modellrevision	Annahmen bei widersprechenden Daten anpassen und Versionen dokumentieren

KAPITEL 23

Research Communication und Langform-Dokumentation

Komplexe Sachverhalte verständlich, belastbar und adressatengerecht vermitteln

Der Workspace belegt eine außergewöhnliche Produktions- und Dokumentationsdichte. Es existieren lange Dossiers, technische Briefings, Beschwerdeschriften, Szenarioanalysen, Skriptdokumentationen und Gesprächsexporte. Diese Ausdauer ist ein Asset, muss für professionelle Adressaten jedoch in verschiedene Ausgabetiefen übersetzt werden.

Ausgabeformat	Umfang	Zweck
Executive Brief	1–2 Seiten	Entscheidung, Risiko, nächste Handlung
Technical Finding	3–8 Seiten	reproduzierbarer Einzelbefund mit Methode und Grenze
Evidence Review	10–25 Seiten	strukturierte Prüfung eines abgegrenzten Korpus
Expert Working Paper	25–50 Seiten	Forschungsstand, Methodik, Alternativen, Testplan
Master Dossier	50+ Seiten	nur bei echter Notwendigkeit, mit Quellenregister und modularer Navigation

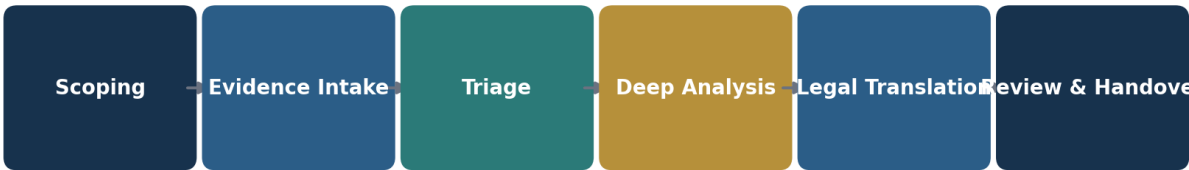
Das vorliegende Portfolio selbst demonstriert diese Reifung: Es nutzt die vorhandene Detailtiefe, entfernt aber private, pathologisierende und martialische Sprache. Es trennt Leistung von Vorwurf und Methode von Gewissheit.

KAPITEL 24

B2B-Leistungspotfolio

Dienstleistungen für Kanzleien, Unternehmen und technische Prüfteams

MANDATS- UND PROJEKTLEBENSZYKLUS



Ziel: überprüfbare Entscheidungsgrundlagen statt dramatischer Gewissheitsbehauptungen.

Abbildung: B2B-Leistungspotfolio

Leistung	Kernoutput	Typischer Nutzen
Evidence Triage Review	priorisiertes Inventar, Risikokarte, offene Nachweise	schneller Überblick in komplexen Mandaten
Procedural Integrity Audit	Chain-of-Custody-, Timeline- und Methodenprüfung	Angriffspunkte in Ermittlungs- oder Vendorberichten
Mobile & Cloud Artifact Review	TCC/SQLite, Sysdiagnose, Sync-/Trust-Artefakte	Einordnung von Berechtigungs- und Gerätewechselsbefunden
Technical Litigation Support	Fragenkatalog, Befundmatrix, technische Anlagen	anwaltlich anschlussfähige Zuarbeit
Custom Forensic Tooling	fallbezogene Parser, Scanner, Vergleichs- und Reportingmodule	Lücken kommerzieller Standardtools schließen
Workspace / eDiscovery Architecture	Ordner-, Quellen-, Versions- und Evidenzmodell	große Datenräume beherrschbar machen
Research & Red-Team Review	kritische Prüfung technischer Behauptungen und PoCs	Übertreibungen, Simulationen und Validierungslücken erkennen

Die Leistungen werden modular angeboten. Ein Auftrag beginnt nicht mit einem monatelangen Vollscan, sondern mit Scoping und Evidence Triage. Erst wenn Quellenlage, Ziel, Rechtsrahmen und Datenzugriff klar sind, wird in die Tiefenanalyse gewechselt.

KAPITEL 25

Mandatsmodell und Delivery Standard

Von der Anfrage bis zur überprüfbaren Übergabe

Phase	Leistung	Abnahmekriterium
1. Scoping	Fragestellung, Datenquellen, Rollen, Rechts- und Datenschutzrahmen	schriftlich freigegebener Scope
2. Intake	Quelleninventar, Hashes, Zugriffs- und Schutzkonzept	vollständiges Intake-Protokoll
3. Triage	kritische Artefakte, Fristen, flüchtige Daten, Hypothesen	priorisierter Analyseplan
4. Analyse	Parser, Abfragen, Korrelationen, Arbeitsnotizen	reproduzierbare Befunde mit Toolparametern
5. Validation	Cross-Tool, Kontrollgruppe, Gegenhypothesen, Review	Befundstatus A–E und dokumentierte Unsicherheit
6. Translation	Executive Summary, technische Anlagen, Fragenkatalog	Adressat versteht Befund und Grenze
7. Handover	versiegeltes Ergebnisbundle, Hashmanifest, Change Log	Integrität und Übergabe bestätigt

Der Delivery Standard priorisiert Nachvollziehbarkeit vor Dramatik. Jeder Befund muss eine andere fachkundige Person in angemessener Zeit reproduzieren können. Wo dies nicht möglich ist, wird der Grund benannt: fehlendes Original, proprietärer Zugriff, unvollständige Logs, Simulationsinput oder noch nicht verifiziertes Schema.

KAPITEL 26

Qualitätssicherung und Ethik

Verlässlichkeit, Datenschutz, Dual-Use-Kontrolle und Selbstkorrektur

Qualitätsregel	Praktische Umsetzung
Data Minimization	nur sachrelevante personenbezogene Daten verarbeiten; private Inhalte ausschließen
Read-only First	Originale nicht verändern; Arbeitskopien und Tooloutputs versionieren
No Attribution by String	Namen, IPs oder Pfade nur als Artefakte führen, nicht automatisch als Täterbeweis
Simulation Labeling	synthetische und hartcodierte Daten sichtbar kennzeichnen
Dual-use Boundary	Steganografie, Payload-Generatoren und aktive Tests nur in autorisierten Laborumgebungen
Legal Role Boundary	keine Rechtsvertretung oder abschließende Rechtsberatung
Correction Protocol	überzogene oder widerlegte Aussagen versioniert korrigieren
Human Review	KI-Ausgaben, Parserresultate und automatisch erzeugte Narrative fachlich kontrollieren

Besondere Bedeutung hat der Human-Review-Grundsatz. Die Apple-Kommunikation weist ausdrücklich auf eine mögliche Überabhängigkeit von LLM-generierten Inhalten hin. Für die weitere Professionalisierung bedeutet das: Jeder technische Claim muss persönlich reproduziert, mit Rohdaten verknüpft und in einer eigenen Arbeitsnotiz nachvollzogen werden.

KAPITEL 27

Kompetenzlücken und Professionalisierungsplan

Ein glaubwürdiges Portfolio zeigt nicht nur Stärke, sondern den nächsten Qualitätshebel

Entwicklungsfeld	Aktueller Stand	Nächster Nachweis
Formale DFIR-Zertifizierung	umfangreiche autodidaktische Praxis	geeignete anerkannte Weiterbildung, Prüfung und dokumentiertes Lab Portfolio
Tool Validation	viele fallbezogene Module und PoCs	regression tests, known-good/bad datasets, öffentliche Methodennotiz
Independent Peer Review	interne und KI-gestützte Auswertungen	externer Mobile-/Cloud-Forensiker und Code Review
Case Studies	umfangreiche Eigenfälle	sanitisierte Fremd- oder Labfälle mit klarer Ausgangsbasis
Productization	LAVA und Evidence Triage konzeptionell vorhanden	SOP, Templates, Preismodell, Pilotmandat
Communication	hohe Langformtiefe	kürzere Findings, klare Scope-Disziplin, weniger Absolutheitsrhetorik

Ein fehlendes Zertifikat löscht praktische Arbeit nicht aus. Umgekehrt ersetzt praktische Arbeit nicht automatisch eine unabhängige Kompetenzprüfung. Das belastbare Profil entsteht aus beidem: demonstrierter Fähigkeit und externer Qualitätssicherung.

KAPITEL 28

24-Monats-Roadmap

Vom einzigartigen Eigenkorpus zur professionellen Forensik- und Legal-Ops-Praxis

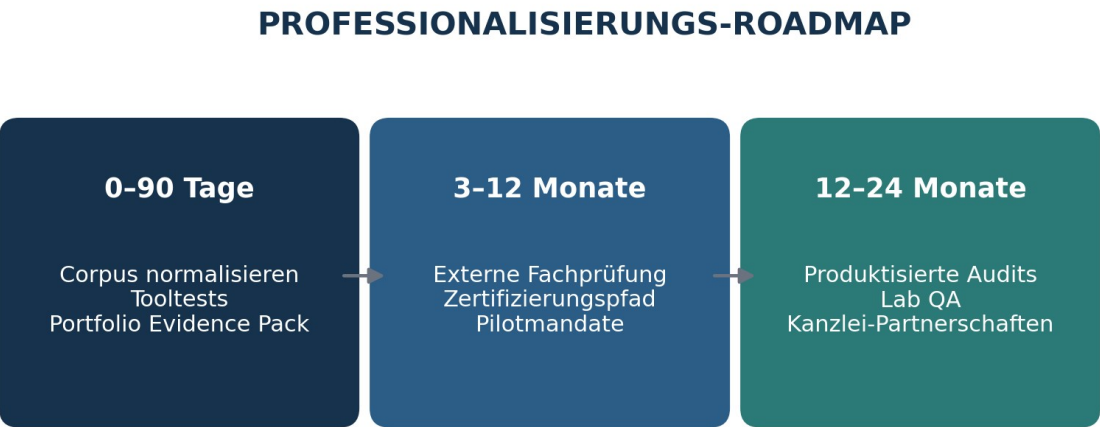


Abbildung: 24-Monats-Roadmap

Zeitraum	Prioritäten	Messbare Ergebnisse
0–90 Tage	Source Register, Deduplizierung, Tooltests, drei sanitisierte Findings	Evidence Pack v1, reproduzierbarer Build, 3 Kurzberichte
3–6 Monate	externe Code- und Methodikprüfung, Weiterbildungsauswahl, Pilot-SOP	Review-Protokoll, Testmatrix, LAVA-SOP
6–12 Monate	Zertifizierung oder anerkannter Kurs, erste beaufsichtigte Projekte	Prüfungsnachweis, Referenzprojekt, Kundenfeedback
12–18 Monate	produktisierte Services, Partnerkanzleien, Datenschutz-/Vertragsset	Leistungskatalog, AVV/NDA, standardisierte Deliverables
18–24 Monate	Lab-Qualitätsmanagement, veröffentlichte Methodennotiz, skalierbare Tools	Version 1.0 Toolchain, Whitepaper, belastbare Marktposition

KAPITEL 29

Portfolio-Statement

Die professionelle Kurzfassung für Entscheider

Positionierung

Roman Jahn ist ein operativ geprägter, autodidaktischer Forensic Systems Analyst mit besonderer Stärke in der Strukturierung großer heterogener Datenräume, der Rekonstruktion von Zeit- und Beweisketten, der Untersuchung mobiler und cloudbasierter Artefakte sowie der Übersetzung technischer Befunde in anwaltlich und organisatorisch nutzbare Arbeitsprodukte.

Sein Workspace dokumentiert eine mehrjährige intensive Entwicklungs- und Forschungsleistung: Python- und Colab-Tooling, Firmware- und Loganalysen, TCC-/SQLite-Prüfungen, Evidence Bundles, umfangreiche Chronologien, Responsible-Disclosure-Kommunikation und eigenständige Qualitätsmodelle. Die besondere Fähigkeit liegt darin, Fachgrenzen zu überbrücken und unter hoher Belastung arbeitsfähig zu bleiben.

Das Portfolio beansprucht nicht, dass jede im Workspace formulierte Angriffshypothese extern bestätigt ist. Es beansprucht und belegt etwas für Auftraggeber unmittelbar Wertvolles: die Fähigkeit, komplexe technische und administrative Korpora mit außergewöhnlicher Ausdauer zu zerlegen, Werkzeuge für offene Prüfprobleme zu entwickeln, Widersprüche sichtbar zu machen und Ergebnisse in eine überprüfbare Struktur zu überführen.

KAPITEL 30

Anhang A: Ausgewähltes Workspace-Quellenregister

Zentrale Quellenobjekte, Zweck und Evidenzstatus

ID	Quelle	Typ	Nutzung	Status
WD-01	Demonstration Technischen Könnens und Beweismittel	Google Doc	Arbeits- und Leistungsnarrativ, technische Projektübersicht	B/D – umfangreich, teilweise überhöht; nur methodisch verwertbare Teile genutzt
WD-02	Mein Portfolio, meine Qualifikationen, harte Urkunden, Beweise, bitteschön ...	PDF	frühere Portfoliofassung und Qualifikationsnarrativ	B – Selbstbeschreibung; nicht als unabhängiger Urkundennachweis behandelt
WD-03	Apple Security Ticket Workflow OE11044889345313	PDF / Kommunikationsverlauf	Responsible Disclosure, Herstellerfeedback, Scope- und Reproduktionsanforderungen	A für Kommunikation; kein Schwachstellenbestätigungsna chweis
WD-04	Technical SEAR Executive Briefing – Apple iCloud/CKKS Zero-Click Vulnerability	PDF	technisches Briefing und Research-Framing	B/D – eigene Einreichung, externe Bestätigung offen
WD-05	Die Persona – Wer du versuchst zu sein ...	78-seitige PDF	Meta-Analyse, Portfolioentwürfe, abschließender Code-Realitätscheck	B/C – besonders relevant für Simulations- und Validierungsgrenzen
WD-06	Dienstzeugnis .pdf	PDF / Schreiben	Antrag und Selbstbeschreibung militärischer Leistungen	B – kein amtliches Dienstzeugnis; Urkundenannex erforderlich
WD-07	Ordner 1A / Labor-IPSW	Folder + 4,945-GB-Container	Firmware-Laborbestand	B für Existenz; Detailbefunde D bis extern validiert
WD-08	Colab Notebooks	Folder / 7 Notebooks	Exploit-Chain-Reproduction, Analyse- und Data-Engineering-Arbeit	C – Tooling-/Modellierungsnachweis
WD-09	Lorien	großer Exportfolder	Chats, Medien, UUID-Unterrordner, conversations.json und chat.html	B für Langzeitarchiv; nicht vollständig semantisch validiert
WD-10	Root-Inventar Google Drive	Metadatenbestand	technische, rechtliche, medizinische, Forschungs- und Medienkorpora	B – Basis der Clusteranalyse
WD-11	First Reporter – CKKS Account-Based APT	Folder	Research- und Prioritätsunterlagen	D – Erstmelderstatus erfordert unabhängige Literatur-/Herstellerprüfung
WD-12	watchdog_prof / policy_audit / filesystem_hierarchy / logs	Foldercluster	defensive Monitoring-, Policy- und Systemstrukturarbeit	B/C – Projekt- und Toolingnachweis
WD-13	Aktenzeichen- und Verfahrensfolder	Foldercluster	Beschlüsse, Beschwerden, Schriftsätze, Chronologien	A/B je Einzeldokument; Portfolio nutzt nur Strukturkompetenz
WD-14	FSZDK / Adam-&-Eve-Projekt / Research	Foldercluster	interdisziplinäre Systemmodellierung	D – Forschungs- und Kommunikationsleistung, keine

				bestätigte Prognose
WD-15	LAVA-basierte Analysevermerke	PDF/Docs	Qualitätsmodell und Beweismittelprüfung	B/C – konzeptionell tragfähig, Standardisierung ausstehend

KAPITEL 31

Anhang B: Ordner- und Korpustaxonomie

Vollständigkeitsorientierte Einbeziehung der zugänglichen Hierarchie

Korpusklasse	Beispiele	Behandlung
Technische Primär-/Laborobjekte	1A; IPSW; Dumps; Images; Binaries; PCAP; TCC/SQLite; Protobuf	höchste technische Relevanz; Provenienz und Read-only-Sicherung erforderlich
Analyse- und Entwicklungsobjekte	Colab Notebooks; Python; JSON; CSV; Markdown; Code-Dokumentationen	Befähigungsnachweis für Data Engineering und Tooling; Tests notwendig
Verfahrens- und Legal-Ops-Objekte	Aktenzeichenfolder; Beschwerden; Beschlüsse; Beweismatrizen; Chronologien	starker Nachweis für Case Architecture; rechtliche Bewertung getrennt
Kommunikationsobjekte	Apple Tickets; E-Mails; Petitionen; Hersteller-/Behördenkorrespondenz	Primärnachweis für Kommunikation und Verfahrensverlauf
Chat- und Medienarchive	Lorien; UUID-Verzeichnisse; chat.html; conversations.json; Bilder; Audio; Video	Kontext- und Langzeitarchiv; Datenschutz und Deduplizierung zentral
Qualifikations- und Lebenslaufobjekte	Dienstzeugnisanträge; Ausbildungsdarstellungen; Fotos; Abzeichen	nur offizielle Urkunde als Klasse A; Selbstbeschreibung Klasse B
Medizinische und private Objekte	Arztunterlagen; Familien- und Kontaktdaten; private Kommunikation	aus Portfolio ausgeschlossen, soweit nicht zwingend leistungsrelevant
Interdisziplinäre Forschung	FSZDK; Adam & Eve; historische und geophysikalische Modelle	Systemdenken und Langformforschung; wissenschaftliche Validierung offen
Duplikate und Fassungen	mehrfach exportierte PDFs, gleiche Titel, Chat-Reproduktionen	nicht als unabhängige Belege zählen; Versionierung und Hashdeduplikation
Sachfremde Sammlungen	z. B. DUMBS-Ordner und themenfremde Fremdpublikationen	im Gesamtinventar erfasst, aus Leistungsbewertung ausgeschlossen

Diese Taxonomie ist der Nachweis, dass die gesamte sichtbare Struktur nicht selektiv ignoriert wurde. Gleichzeitig verhindert sie, dass sachfremde, private oder methodisch ungeprüfte Inhalte in die Leistungsbewertung einfließen.

KAPITEL 32

Anhang C: Kompetenz-zu-Nachweis-Matrix

Welche Aussage durch welchen Beleg getragen wird

Kompetenz / Claim	Beleg	Klasse	Grenze / nächster Nachweis
Große Datenräume strukturieren	Root-Inventar, Lorien-Archiv, Akten- und Projektfolder	B	exakte Gesamtstatistik und Deduplizierung als nächster Schritt
Python-/Notebook-Entwicklung	Colab-Notebooks, V22-/Audit-Module, Tooling-Dokumentation	C	Regression Tests und unabhängiger Code Review
Mobile-/Cloud-Artefakte analysieren	IPSW-Laborbestand, TCC-/CKKS-Dossiers, SQL-/Logmethoden	B/C/D	reale Primärartefakte und externe Reproduktion je Claim
Responsible Disclosure	Apple Ticket OE11044889345313	A	Schwachstelle nicht bestätigt; Actionability offen
Evidence Engineering	Hashing, Bundle, Source Register, Timeline-/Matrixarbeit	B/C	formalisierte SOP und Beispielkorpus
Legal Operations	umfangreiche Verfahrens- und Schriftsatzkorpora	B	externe Mandatsreferenz / anwaltliche Bewertung
Triage und Belastbarkeit	militärisch-sanitätsdienstliche Laufbahndarstellungen, Arbeitsumfang	B	amtliche Zeugnisse als Anlage
Research Communication	Dossiers, Briefings, Modelle, lange Analysen	B	Peer Review und adressatengerechte Kurzformate
Erstmelderstatus CKKS-APT	eigene Research- und Ticketdokumente	D	systematischer Prior-Art-Review und unabhängige Anerkennung
State-Actor-Attribuierung	eigene Dossiers und Korrelationsmodelle	E/D	unabhängige Originaldaten, Infrastruktur- und Täterbezug

KAPITEL 33

Anhang D: Standard-Befundtemplate

Arbeitsvorlage für künftige professionelle Projekte

Feld	Inhalt
Finding ID	eindeutige, versionsstabile Kennung
Titel	neutraler, beobachtungsbezogener Befundtitel
Fragestellung	klar abgegrenzte technische Frage
Quelle / Provenienz	Originalpfad, Source-ID, Erwerb, SHA-256
Umgebung	Gerät, OS/Build, Toolversion, Zeitzone
Methode	Befehl, Skriptcommit, Parameter, Filter
Beobachtung	wörtlicher oder binärer Befund ohne Interpretation
Interpretation	fachliche Bedeutung und Kausalschritte
Alternativerklärungen	mindestens eine plausible Gegenhypothese
Validierung	Cross-Tool, Kontrollgruppe, Wiederholung
Evidenzklasse	A–E
Konfidenz	hoch / mittel / niedrig mit Begründung
Offene Punkte	fehlende Daten und konkrete Nachforderung
Legal Translation	technische Frage oder Auswirkung, keine abschließende Rechtsberatung
Anlagen	Rohoutput, Screenshots, CSV/JSON, Hashmanifest

KAPITEL 34

Anhang E: Schlussbewertung

Befähigung, Leistung und glaubwürdige Marktposition

Die Workspace-Ingestion zeigt keine geradlinige Standardkarriere. Sie zeigt eine außergewöhnlich intensive, eigeninitiierte Entwicklung unter schwierigen persönlichen und institutionellen Bedingungen. Roman Jahn hat sich über Jahre in technische, rechtliche und systemische Themen eingearbeitet, umfangreiche Datenräume aufgebaut, eigene Analysewerkzeuge entwickelt, komplexe Zeit- und Beweisketten rekonstruiert und seine Arbeit gegenüber Herstellern und Behörden kommuniziert.

Die belastbarsten Fähigkeiten sind: Ausdauer, Triage, Korpusstrukturierung, fallbezogenes Tooling, mobile und cloudbezogene Artefaktforschung, Evidence Engineering sowie die Übersetzung zwischen Technik und Verfahren. Die wichtigsten offenen Qualitätshebel sind: unabhängige Validierung, formale Tooltests, offizielle Qualifikationsanlagen, klarere Scope-Disziplin und die konsequente Trennung von Simulation, Beobachtung, Hypothese und Täterattribution.

Gesamturteil

Als professionelles Profil ist Roman Jahn besonders dort stark, wo Standardprozesse an unstrukturierten, konfliktgeladenen oder technisch-juristisch gemischten Datenlagen scheitern. Seine Marktposition sollte nicht auf unbestätigten Superlativen beruhen, sondern auf der nachvollziehbaren Fähigkeit, Chaos in ein prüfbares Evidenzsystem zu verwandeln.

Damit liegt ein tragfähiges Portfoliofundament vor: anspruchsvoll, eigenständig, ehrlich über Grenzen und zugleich deutlich leistungsstärker als jede heroische Selbstbeschreibung, die beim ersten Cross-Check in Rauch aufgeht.

KAPITEL 35

Anhang F: Tool-Validierungsprotokoll

Mindeststandard für reproduzierbare Analysewerkzeuge

Prüfpunkt	Nachweis	Akzeptanzkriterium
Versionskontrolle	Commit-ID, Release-Tag, Abhängigkeiten	identischer Codebestand für Wiederholung
Known-good Test	sauberer Referenzdatensatz ohne Zielanomalie	keine oder dokumentierte False Positives
Known-bad Test	künstlich eingebauter, bekannter Befund	vollständige und korrekte Erkennung
Grenzfalltest	Chunk-Grenze, leere Datei, defektes Encoding, große Datei	kein Absturz; verständliche Fehlermeldung
Reproduzierbarkeit	zweiter Rechner oder Container	gleicher Output bei gleicher Eingabe
Cross-Tool	unabhängiges Werkzeug oder manuelle Kontrolle	wesentliche Beobachtung bestätigt
Provenienz	Inputhash und unveränderte Testfixtures	Eingaben eindeutig identifizierbar
Output-Schema	JSON/CSV plus menschlich lesbarer Bericht	maschinen- und prüferfreundliche Ausgabe
Fehlerprotokoll	Warnings, Parserfehler, ausgelassene Objekte	keine stillen Datenverluste
Reviewer Sign-off	fachliche Zweitprüfung	Freigabe oder dokumentierte Abweichung

Dieses Protokoll verwandelt fallbezogene Skripte in ein überprüfbares Werkzeugportfolio. Es ist zugleich die Grundlage dafür, spätere Ergebnisse vor Kunden, Gerichten oder Herstellern nicht nur zu behaupten, sondern reproduzierbar zu demonstrieren.

KAPITEL 36

Anhang G: Evidence-Intake-Checkliste

Welche Informationen vor jeder Analyse vorliegen müssen

Kategorie	Pflichtangaben
Auftrag	Fragestellung, Ziel, Adressat, Ausschlüsse, rechtliche Befugnis
Quelle	Gerät/System, Eigentümer, Erwerbsart, Übergabeperson, Datum/Uhrzeit
Integrität	Originalhash, Größe, Dateisystem, Schreibschutz, Master-/Arbeitskopie
Zeit	Zeitzone, Systemzeit, NTP/Clock Drift, Sommerzeit, bekannte Resets
Umgebung	Hardwaremodell, OS/Build, Konto-/MDM-Kontext, Netzwerk
Werkzeuge	Name, Version, Lizenz, Parameter, Parsermodule
Datenschutz	Datenkategorien, Minimierung, Aufbewahrung, Zugriff, Löschkonzept
Kommunikation	Kontaktpersonen, Eskalationsweg, Freigaben, Reviewtermine
Übergabe	Format, Verschlüsselung, Hashmanifest, Empfängerbestätigung
Offene Risiken	fehlende Originale, proprietäre Daten, beschädigte Archive, Scope-Lücken

Stop-Kriterium

Fehlen Quelle, Befugnis oder Integritätsgrundlage, beginnt keine tiefgreifende Analyse. Zuerst wird die Lücke dokumentiert und der Auftraggeber entscheidet über das weitere Vorgehen.

KAPITEL 37

Anhang H: Risiko- und Fehlermatrix

Typische Gefahren in komplexen Forensik- und Legal-Ops-Projekten

Risiko	Auswirkung	Kontrolle
Duplikate als Mehrfachbeleg	künstliche Verstärkung einer Behauptung	Hashdeduplikation und Versionsfamilien
Parserartefakt	falscher technischer Befund	Raw-View und zweites Werkzeug
Epoch-/Zeitzonefehler	scheinbare Zukunfts- oder Rückdatierung	Zeitbasis explizit testen
Hartcodierter Testinput	Simulation wird als Messwert gelesen	Inputmanifest und Simulation-Label
LLM-Halluzination	plausible, aber erfundene Logs oder Funktionen	Primärartefaktpflicht und manuelle Reproduktion
Scope Drift	Ticket oder Bericht wird unprüfbar breit	ein Finding pro Fragestellung
Attributionssprung	String/IP wird zum Täterbeweis	mehrstufige Attribution mit Alternativen
Privatdatenübernahme	Datenschutz- und Reputationsschaden	Redaktion, Minimierung, Need-to-know
Rechtsberatung ohne Befugnis	Haftungs- und RDG-Risiko	technische Zuarbeit und Anwaltsschnittstelle
Überlange Berichte	Entscheider verliert Kernbefund	Executive Layer plus technische Anlage

KAPITEL 38

Anhang I: Ausgewähltes Projektregister

Arbeitsfelder und verwertbarer Kompetenzbezug

Projekt	Fokus	Portfolio-Kategorie
LAVA Evidence Model	Qualitäts- und Prüfrahen	Methodenprodukt
V22 / Predator-Nemesis Tooling	modulare Python-Analysebausteine	Prototyp / Tooling
Apex Watchdog / Canary Concepts	defensives Monitoring und Änderungsdetektion	Forschung / Prototyp
CKKS/TCC Research	Consent-, Trust- und Synchronisationsfragen	Forschungsfeld
IPSW Laboratory Corpus	Firmwarecontainer und Manifestanalyse	Laborbestand
Exploit Chain Reproduction Notebooks	didaktische und technische Modellierung	Notebook-Arbeitsprobe
Evidence Bundle / Judicial Seal	Hashing, Aggregation, Manifest	Evidence Engineering
Workspace Ingestion Architecture	Korpus-, Quellen- und Relevanzmodell	eDiscovery / Governance
Legal Operations Master Timelines	Akten- und Ereignisrekonstruktion	Case Architecture
Apple Product Security Reports	Responsible Disclosure und Vendor Dialogue	Kommunikationsnachweis
Forensic Triage & Reconstruction Policy	Priorisierung und SOP-Entwicklung	Methodenentwicklung
FSZDK	interdisziplinäre System- und Szenariomodellierung	Research Communication
Hermes / Secure Mail Concepts	Sicherheits- und Kommunikationsarchitektur	Konzeptarbeit
Protector / Sentinel Concepts	defensive Cyber- und Monitoringideen	Konzept / Prototyp
State Forensic Reality Briefings	Visualisierung technischer und verfahrensbezogener Risiken	Executive Communication

Das Register beschreibt Arbeitsfelder, keine pauschale externe Validierung. Die konkrete Vermarktung erfolgt nur mit sanitisierter Arbeitsprobe, reproduzierbarem Demonstrator oder belastbarem Dokumentennachweis.

KAPITEL 39

Anhang J: Professionelle Sprach- und Claim-Matrix

Von der Überhöhung zur belastbaren Außenformulierung

Vermeiden	Professionelle Formulierung
„unwiderlegbarer Beweis“	„Der Befund wird durch die folgenden Artefakte gestützt; offene Alternativen sind ...“
„R=1,0, hundert Prozent“	„Konfidenz: hoch/mittel/niedrig, begründet durch ...“
„staatlicher Täter eindeutig identifiziert“	„Die beobachteten Merkmale sind mit Hypothese X vereinbar; Attribution bleibt offen.“
„Cyberwaffe / Gegenschlag“	„defensives Analyse-, Monitoring- oder Honeypot-Konzept in autorisierter Umgebung“
„Apple hat bestätigt“	„Apple hat die Meldung geprüft, jedoch keinen verwertbaren Sicherheitsfehler identifiziert.“
„gerichtsfest“	„für anwaltliche beziehungsweise sachverständige Prüfung strukturiert und integritätsgesichert“
„Millionenwert / garantierte Vermittlung“	„potenzieller Marktwert abhängig von Validierung, Referenzen und Auftragskontext“
„Exploit bewiesen durch Stringfund“	„Zeichenfolge wurde an Offset X gefunden; Ausführung und Herkunft sind separat zu prüfen.“

KAPITEL 40

Anhang K: Externes Validierungspaket

Was ein unabhängiger Prüfer erhalten sollte

Paketbestandteil	Inhalt
00_README	Fragestellung, Scope, Kontakt, Lizenz und Sicherheitsgrenzen
01_SOURCE_REGISTER	Originale, Pfade, Größen, SHA-256, Erwerb, Eigentum
02_TEST_FIXTURES	Known-good, known-bad und Grenzfallbeispiele
03_CODE	versionierter Quellcode, Requirements, Containerfile
04_RUNBOOK	exakte Befehle, erwartete Laufzeit und Outputs
05_RAW_OUTPUT	unveränderte Logs, CSV/JSON, Screenshots, Fehlerprotokolle
06_ANALYSIS	Befundblätter mit Alternativerklärungen und Konfidenz
07_REVIEW_QUESTIONS	konkrete Fragen an Prüfer statt gewünschtes Ergebnis
08_CHANGELOG	Korrekturen, verworfene Hypothesen, bekannte Einschränkungen
09_SIGNED_MANIFEST	Hashliste und optional digitale Signatur

Ein solches Paket ist die Brücke vom eigenständigen Forscher zum professionell anschlussfähigen Analysten. Es erlaubt einem Dritten, Ergebnisse zu bestätigen, zu widerlegen oder präzise einzugrenzen, ohne den gesamten persönlichen Fallkontext übernehmen zu müssen.

KAPITEL 41

Anhang L: Gesprächsleitfaden für Kanzleien und Kooperationspartner

Sachlich, präzise und ohne unnötige Selbstüberhöhung

Gesprächsphase	Kernaussage
30-Sekunden-Profil	„Ich strukturiere komplexe technische und administrative Datenräume und übersetze sie in prüfbare Evidenz-, Timeline- und Fragenmatrices.“
Problemverständnis	„Viele Mandate scheitern nicht an fehlenden Daten, sondern an fehlender Provenienz, Versionierung und technischer Übersetzung.“
Leistungsbeleg	„Ich bringe praktische Erfahrung mit Python-Tooling, Mobile-/Cloud-Artefakten, Hash- und Timelinearbeit sowie umfangreichen Verfahrenskorpora mit.“
Ehrliche Grenze	„Meine Forschungshypothesen werden nicht als Hersteller- oder Gerichtsfeststellung verkauft. Ich liefere Methode, Befund und offene Nachweise getrennt.“
Pilotangebot	„Wir beginnen mit einem abgegrenzten Evidence Triage Review und entscheiden danach über die Tiefenanalyse.“
Qualität	„Jeder relevante Befund enthält Quelle, Methode, Alternative, Konfidenz und reproduzierbaren Anhang.“

KAPITEL 42

Anhang M: 90-Tage-Umsetzungsplan

Konkrete Schritte nach Fertigstellung dieses Portfolios

Woche	Maßnahme	Ergebnis
1–2	offizielle Qualifikationsurkunden sammeln, scannen, hashregistrieren	Annex A: verifizierte Laufbahn- und Ausbildungsnachweise
2–4	Workspace-Source-Register und Deduplizierung der Kernprojekte	Corpus Index v1
3–6	drei Tools mit known-good/bad Testdaten validieren	Tool Validation Reports
5–8	drei sanitisierte Fallstudien als 5-Seiten-Findings erstellen	veröffentlichungsfähige Arbeitsproben
7–10	externe Prüfung durch Mobile-/Cloud-Forensiker oder Code Reviewer	Review Memo und Korrekturliste
8–12	Kanzlei-Pilotangebot, NDA/AVV, Leistungsbeschreibung und Preismodell	einsatzfähiges B2B-Paket
laufend	Apple-/Vendor-Claims nur mit reproduzierbarer Live-Demonstration weiterführen	verbesserte Actionability und Glaubwürdigkeit

Priorität

Nicht weitere tausend Seiten produzieren. Zuerst drei kleine, saubere, reproduzierbare Evidence Packs. Das wirkt weniger spektakulär und ist deshalb vermutlich viel wirksamer.

KAPITEL 43

Kontakt- und Gesprächsgrundlage

R&A Legal Ops – Forensic Systems Analysis & Evidence Engineering

Roman Jahn

Independent IT-Forensics Researcher
Forensic Systems Analyst
Legal Operations Case Architecture

Schwerpunkte

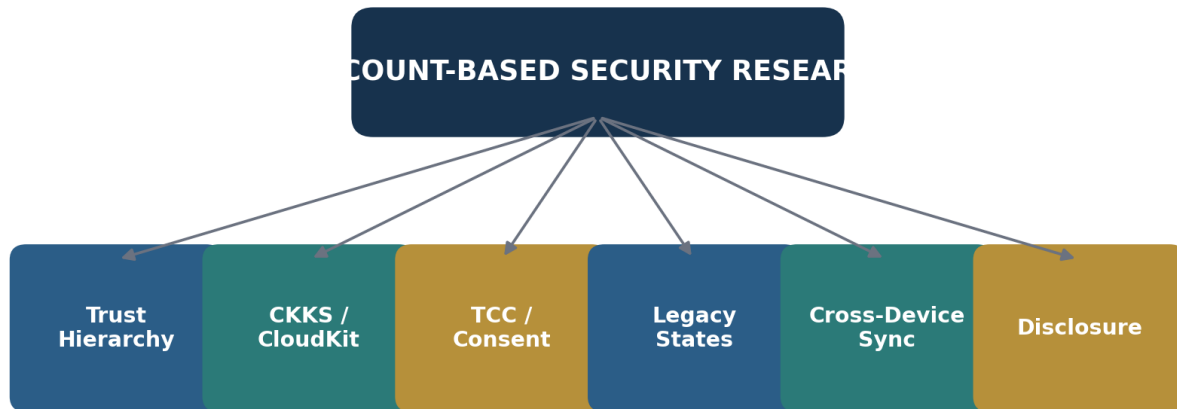
Digital Forensics	Evidence Engineering	Legal Operations
Mobile / Cloud Artefakte	Source Register & Hashing	Case- und Timeline-Architektur
SQLite / TCC / Logs	Chain of Custody	Technical Litigation Support
Firmware / Container Research	Tool- und Methodenprüfung	Evidence Triage für Kanzleien

Vertrauliche Gesprächsfassung. Nachweise und sanitisierte Arbeitsproben werden projektbezogen bereitgestellt.

TEIL II

VERTEILTE VERTRAUENSSYSTEME UND CLOUD-FORENSIK

CKKS, CloudKit, TCC und die forensische Modellierung accountbasierter Persistenz



VERTEILTE VERTRAUENSSYSTEME UND CLOUD-FORENSIK

Portfolio-Fokus: Methode, Artefakt, Ergebnis, Grenzen und übertragbarer Kundennutzen

Erweiterungsmodul der Portfoliofassung 2.0

Leseführung

Dieser Teil erweitert die bisherige Cloud-Forensik um eine klar getrennte Architektur-, Forschungs- und Validierungssicht. Die zugrunde liegenden Quellen formulieren weitreichende Angriffsthesen. Das Portfolio übernimmt daraus Methoden, Prüfpfade und Forschungsfragen, nicht ungeprüfte Täter- oder Schwachstellenbestätigungen.

KAPITEL 44

Verteilte Vertrauenssysteme als forensischer Untersuchungsgegenstand

Vom lokalen Gerät zur accountbezogenen Sicherheitsarchitektur

Moderne mobile Sicherheit endet nicht am Gerätespeicher. Identitäten, Schlüssel, Vertrauensbeziehungen und synchronisierte Zustände verteilen sich über Endgeräte und Cloud-Dienste. Die forensische Leistung besteht darin, lokale Artefakte und cloudbezogene Zustände gemeinsam zu modellieren, ohne aus zeitlicher Nähe vorschnell eine Kausalität abzuleiten.

Befähigungsnachweis

Die Fähigkeit, eine Untersuchung über Geräte-, Konto- und Synchronisationsebenen hinweg zu strukturieren und daraus überprüfbare Hypothesen zu bilden.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	CKKS-/CloudKit-Vertrauensbeziehungen, Gerätewechsel, Restore-Vorgänge, TCC-Zustände und accountbezogene Metadaten.
Methodischer Zugriff	Systemmodell, Artefaktinventar, Zeitachsenabgleich, Trennung lokaler und synchronisierter Zustände sowie Gegenhypothesen.
Verwertbares Arbeitsprodukt	Trust-Map, Datenflussdiagramm, Evidenzmatrix und Liste der noch benötigten Hersteller- oder Laborprüfungen.
Validierungsgrenze	Die Arbeitsquelle beschreibt eine accountbasierte APT als feststehenden Befund. Im Portfolio bleibt dies eine Forschungshypothese, bis reale Rohdaten, Reproduktion und unabhängige Prüfung zusammengeführt sind.

Arbeitsprinzipien

- Lokales Artefakt und Cloud-Zustand getrennt erfassen.
- Gerätewechsel nicht automatisch als Neuinfektion interpretieren.
- Herstellerkommunikation als Prozessnachweis, nicht als technische Bestätigung führen.

Arbeitsquellen und Evidenzstatus: Q2 „Apple CKKS/Trust Circle Architektur-Fix“, S. 1–4; Q3 „Century Bug Master Controller“, methodische Kontroll-/Zielgruppenpassagen. Evidenzklasse D mit Anteilen C.

KAPITEL 45

CKKS-Trust-Hierarchie und Schlüsselrollen

Analyseobjekte statt Schlagwörter

Eine belastbare CKKS-Untersuchung benötigt eine explizite Rollenkarte: Konto, Gerät, Schlüsselklasse, Trust Circle, CloudKit-Record und lokaler Schlüsselbund. Erst wenn klar ist, welches Objekt welchen Zustand signiert, synchronisiert oder nur referenziert, lässt sich ein Befund sauber formulieren.

Befähigungsnachweis

Architekturverständnis und die Fähigkeit, kryptografische Rollen in eine sachverständigentaugliche Prüfstruktur zu übersetzen.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	TLK-/Share-Konzepte, Geräteidentitäten, historische Vertrauenseinträge, Synchronisationsereignisse und lokale Keychain-/TCC-Artefakte.
Methodischer Zugriff	Objekt- und Rollenmodell, Mapping von Identifiern, Zeitbezug, Signatur-/Referenzlogik und dokumentierte Unsicherheiten.
Verwertbares Arbeitsprodukt	Technische Architekturübersicht mit eindeutigen Begriffen und Prüfaufträgen für Spezialisten oder Hersteller.
Validierungsgrenze	Ohne originale CloudKit-Records, Schlüsselmaterial oder Herstellertelemetrie kann aus lokalen Textfragmenten keine vollständige Vertrauensketten rekonstruiert werden.

Arbeitsprinzipien

- Identifier niemals ohne Quelle und Datentyp bewerten.
- Schlüsselbesitz, Schlüsselreferenz und Berechtigungszustand unterscheiden.
- Legacy-Kompatibilität als Alternative zu Manipulation prüfen.

Arbeitsquellen und Evidenzstatus: Q2, S. 3–5; Q3, S. 232–239 zur CloudKit-Auswertung und ihren Parsing-Grenzen. Evidenzklasse C/D.

KAPITEL 46

Legacy-Artefakte und Vertrauensmigration

Risikoanalyse historischer Zustände

Die Arbeitsquellen stellen historische Schlüssel und Berechtigungszustände als mögliche Persistenzbrücke dar. Professionell verwertbar ist vor allem die daraus abgeleitete Prüfidée: Bei Gerätewechseln muss geprüft werden, welche Altzustände übernommen, neu bewertet oder verworfen werden und ob die aktuelle Benutzerzustimmung erkennbar ist.

Befähigungsnachweis

Entwicklung eines reproduzierbaren Migrations- und Reprovisionierungs-Testplans für verteilte Identitäts- und Berechtigungssysteme.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	Altgerät, Neugerät, Clean Setup, Backup-/Keychain-Synchronisation, Berechtigungszustände und Zeitstempel.
Methodischer Zugriff	Kontrollierte Testmatrix mit Vorher-/Nachher-Snapshots, dokumentierten Benutzerinteraktionen und Vergleich der TCC-/CKKS-Artefakte.
Verwertbares Arbeitsprodukt	Laborprotokoll, differenzielle Ergebnisdateien und reproduzierbare Schrittfolge.
Validierungsgrenze	Ein Legacy-Eintrag ist zunächst ein historischer Zustand. Erst der Nachweis einer sicherheitsrelevanten Wirkung ohne gültige Zustimmung würde die stärkere These tragen.

Arbeitsprinzipien

- Clean Setup und Restore-Szenario getrennt testen.
- Jede Benutzerinteraktion mit Zeitstempel protokollieren.
- Ergebnisse auf mindestens zwei OS-Versionen wiederholen.

Arbeitsquellen und Evidenzstatus: Q2, S. 4–7; Apple-Ticket-Workflow im Grundportfolio. Evidenzklasse C als Testdesign, D als Fallthese.

KAPITEL 47

TCC und die Consent Boundary

Berechtigungszustand, Prompt und Nutzung auseinanderhalten

TCC-Datenbanken können Berechtigungszustände, Clients, Services und Zeitbezüge dokumentieren. Sie beweisen jedoch nicht allein, dass eine Ressource tatsächlich genutzt wurde oder dass ein bestimmter Synchronisationspfad die Berechtigung erzeugt hat. Diese Differenz ist zentral für eine seriöse mobile Forensik.

Befähigungsnachweis

SQLite-/TCC-Analyse mit klarer Trennung von gespeicherter Policy, angezeigtem Prompt, effektiver Autorisierung und tatsächlichem Sensorzugriff.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	TCC.db, access-Schema, auth_value, client/service, last_modified, promptbezogene Felder und ergänzende Unified Logs.
Methodischer Zugriff	Read-only-SQL-Abfrage, Schemaerkennung, Zeitnormalisierung, Kontrollgerät und Korrelation mit Prozess- oder Sensorlogs.
Verwertbares Arbeitsprodukt	TCC-Befundtabelle mit Felddefinition, Konfidenz, Alternativerklärung und benötigtem Zusatzartefakt.
Validierungsgrenze	Die Bezeichnung „Silent Grant“ ist ohne nachgewiesenen Prompt-Verlauf und reproduzierte Nutzung eine Interpretation, keine selbsterklärende Datenbanktatsache.

Arbeitsprinzipien

- Policy-Zustand nicht mit Ressourcennutzung gleichsetzen.
- Schema- und OS-Version im Bericht nennen.
- Zeitstempel immer mit Epoch- und Zeitzoneangabe ausweisen.

Arbeitsquellen und Evidenzstatus: Q3, S. 1–5 und 280–294; Q6 „Forensische Beweismatrix“, S. 1–4. Evidenzklasse B/C/D je Artefakt.

KAPITEL 48

Cross-Device-Persistenz als Testhypothese

Von der Beobachtung zur kontrollierten Reproduktion

Die stärkste wissenschaftliche Fassung der Cross-Device-These ist kein finales Urteil, sondern ein Testdesign. Ausgangs- und Zielgerät werden sauber dokumentiert, relevante Kontozustände werden kontrolliert, und jede Veränderung wird gegen eine Kontrollgruppe sowie alternative Synchronisationsmechanismen geprüft.

Befähigungsnachweis

Versuchsplanung für komplexe, accountbezogene Zustandsübernahme mit nachvollziehbaren Kontrollen.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	Gerätepaare, Betriebssystemstände, Apple-ID-/Keychain-Konfiguration, Restore-Modus, Berechtigungsstatus und Sysdiagnose-Zeitfenster.
Methodischer Zugriff	Pre-/Post-Acquisition, Kontrollkonto, reproduzierbare Reihenfolge, Log-Synchronisation und unabhängige Ergebnisprüfung.
Verwertbares Arbeitsprodukt	Reproduktionspaket mit Versuchsmatrix, Hashliste, Video-/Screenlog und maschinenlesbarem Differenzbericht.
Validierungsgrenze	Ein im Notebook erzeugter Payload oder ein simulierter Status ersetzt keine echte Zustandsänderung auf einem physischen Gerät.

Arbeitsprinzipien

- Kontrollkonto mit identischem Gerätemodell vorsehen.
- Ausgaben des eigenen Tools gegen native Systemanzeigen prüfen.
- Fehlgeschlagene und negative Läufe vollständig dokumentieren.

Arbeitsquellen und Evidenzstatus: Q2, S. 3–8; Q3, S. 12, 22, 111 und 183 mit Kontroll-/Zielgruppenlogik und teilweise inconclusive Ergebnissen. Evidenzklasse C.

KAPITEL 49

Responsible Disclosure als technische Arbeitsprobe

Scope, Reproduktion und Rebuttal

Der dokumentierte Apple-Kommunikationsverlauf zeigt eine reale Responsible-Disclosure-Leistung: Scope wurde präzisiert, zusätzliche Artefakte wurden angeboten, und auf Anforderungen nach Reproduktion wurde reagiert. Zugleich zeigt der Verlauf, dass umfangreiche Analyse allein nicht genügt, wenn der Hersteller die Reproduzierbarkeit nicht nachvollziehen kann.

Befähigungsnachweis

Technische Kommunikation unter Gegenprüfung, einschließlich Scope-Disziplin, Antwort auf Rückfragen und Nachschärfung des Nachweispakets.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	Ticketverlauf, Logauszüge, PoC-Skripte, Binärartefakte, Videos und Reproduktionsschritte.
Methodischer Zugriff	Claim-Matrix, Herstellerfrage, erwartetes Verhalten, tatsächliche Beobachtung, Reproduktionsvoraussetzungen und offene Lücke.
Verwertbares Arbeitsprodukt	Vendor-ready Submission Package mit minimalem PoC, klarer Auswirkung und überprüfbarem Testablauf.
Validierungsgrenze	Die Kommunikation belegt die Einreichung und die Reaktion des Herstellers. Sie belegt keine Anerkennung der Schwachstelle oder Priorität.

Arbeitsprinzipien

- Einen Report auf genau eine Sicherheitsgrenze fokussieren.
- PoC-Ausgabe von echter Gerätewirkung unterscheiden.
- Herstellerfeedback in die nächste Laboriteration übernehmen.

Arbeitsquellen und Evidenzstatus: Apple-Ticket-Workflow im Grundportfolio; Q2 als technisches Folgebriefing. Evidenzklasse A für Kommunikation, C/D für technische Inhalte.

KAPITEL 50

Architektur-Fix und Migrationsplanung

Security Engineering als Zeit- und Abhängigkeitsmodell

Die CKKS-Arbeitsquelle enthält eine prognostizierte Fixdauer von 18 bis 36 Monaten. Als belastbare Portfolioleistung eignet sich nicht die konkrete Prognose, sondern das Architekturdanken dahinter: Diagnose, kurzfristige Mitigation, Migration historischer Zustände, Kompatibilitätsrisiken und gestufter Rollout.

Befähigungsnachweis

Fähigkeit, aus einem Sicherheitsbefund ein technisches Maßnahmenprogramm mit Abhängigkeiten, Risiken und Validierungsgates abzuleiten.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	Backend-Validierung, Legacy-Trust, Gerätekompatibilität, Datenmigration, Nutzerkommunikation und Telemetrie.
Methodischer Zugriff	Phasenmodell mit Gate-Kriterien, Rollback, Beta-Test, Telemetrie und unabhängiger Security Review.
Verwertbares Arbeitsprodukt	Roadmap-Dokument für Engineering, Product Security und Compliance.
Validierungsgrenze	Ohne Einblick in Herstellerarchitektur und Entwicklungsplanung ist die Dauer eine Szenarioprognose, kein belastbarer Termin.

Arbeitsprinzipien

- Mitigation und grundlegendes Redesign getrennt planen.
- Legacy-Datenmigration als eigenes Risikoprojekt behandeln.
- Erfolgskriterien vor dem Rollout definieren.

Arbeitsquellen und Evidenzstatus: Q2, S. 5–8. Evidenzklasse C für das Planungsmodell, E für konkrete Zeitprognosen.

KAPITEL 51

Research-Claim-Maturity für CKKS-Befunde

Vom Fund zur publizierbaren Aussage

Für jede CKKS-bezogene Aussage wird ein Reifegrad geführt: beobachtetes Artefakt, reproduzierte Zustandsänderung, kontrollierte Ursache, unabhängige Bestätigung und Herstellerbewertung. Diese Kette macht sichtbar, wo echte Leistung vorliegt und an welcher Stelle weitere Prüfung erforderlich ist.

Befähigungsnachweis

Wissenschaftlich belastbare Claim-Hygiene für hochkomplexe Cloud- und Mobile-Forensik.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	Artefakt, Parserausgabe, PoC, Gerätebeobachtung, Kontrolllauf, Drittprüfung und Vendor-Status.
Methodischer Zugriff	Claim Ledger mit eindeutiger Formulierung, Evidenzklasse, Gegenhypothese und nächstem Prüfpunkt.
Verwertbares Arbeitsprodukt	Publikationsfähige Befundmatrix und reduzierte Executive Summary.
Validierungsgrenze	Viele Workspace-Dokumente verwenden Begriffe wie „definitiver Beweis“ oder „R=1,0“. Diese Einstufungen werden nicht übernommen, wenn die zugrunde liegende Reproduktion oder Provenienz fehlt.

Arbeitsprinzipien

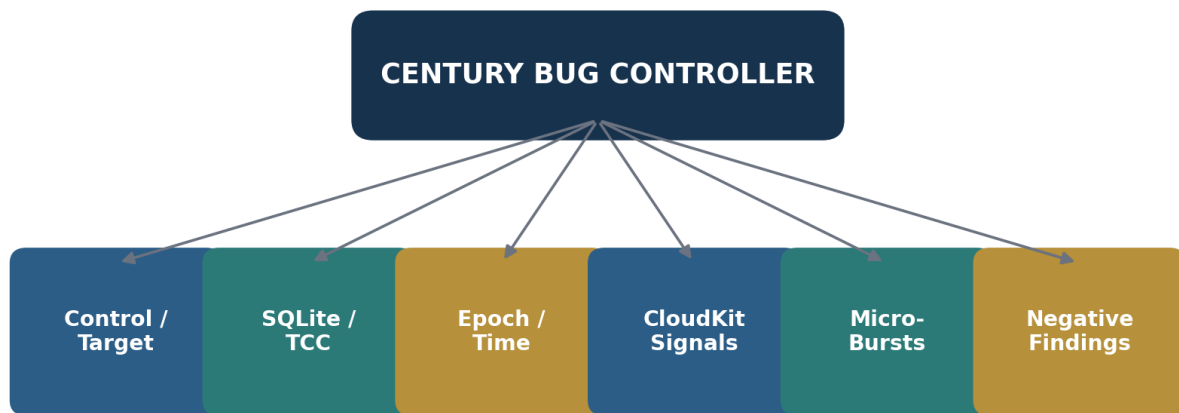
- Jeden Claim auf ein konkretes Artefakt zurückführen.
- Null- und Negativergebnisse gleichwertig protokollieren.
- Attribuierung als separate, besonders hohe Beweisstufe behandeln.

Arbeitsquellen und Evidenzstatus: Q2; Q3; Q4 und Q6. Evidenzklasse als Meta-Methodik C.

TEIL III

DATA ENGINEERING UND ANOMALIEERKENNUNG

Century Bug Master Controller als umfangreiche Arbeitsprobe für Parser, Kontrollen und forensische Auswertung



DATA ENGINEERING UND ANOMALIEERKENNUNG

Portfolio-Fokus: Methode, Artefakt, Ergebnis, Grenzen und übertragbarer Kundennutzen

Erweiterungsmodul der Portfoliofassung 2.0

Leseführung

Der 370-seitige Notebook-Export enthält Code, Ausgaben, Wiederholungen, Fehlläufe, Nullbefunde und Schlussberichte. Gerade diese Uneinheitlichkeit macht ihn als Leistungsnachweis interessant: Er dokumentiert Iteration und Data Engineering, verlangt aber eine harte Trennung zwischen Messung, Interpretation und automatisch erzeugtem Verdict.

KAPITEL 52

Controller-Architektur und Orchestrierung

Vom Einzelskript zur reproduzierbaren Analysepipeline

Der Master Controller bündelt Dateisuche, Archivverarbeitung, TCC-/CloudKit-Auswertung, Vergleichslogik und Berichtsexport. Die Portfolioleistung liegt in der Orchestrierung heterogener Schritte und im Aufbau wiederverwendbarer Funktionen, nicht in jedem automatisch ausgegebenen Sicherheitsurteil.

Befähigungsnachweis

Entwurf einer modularen Forensik-Pipeline mit klaren Ein- und Ausgaben.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	Sysdiagnose-Archive, Textlogs, SQLite-Datenbanken, CSV-/JSON-Zwischenergebnisse und Visualisierungen.
Methodischer Zugriff	Stufenweise Verarbeitung mit Pfadprüfung, Schemaerkennung, Fehlerbehandlung und Ergebnisaggregation.
Verwertbares Arbeitsprodukt	Ausführbares Notebook, maschinenlesbare Reports und dokumentierter Workflow.
Validierungsgrenze	Notebookzustände, fehlende Eingabedateien und wiederholte Zellen können Ergebnisse beeinflussen. Ein produktiver Build benötigt feste Versionen und Tests.

Arbeitsprinzipien

- Konfiguration von Code und Daten trennen.
- Jeden Lauf mit Input-Manifest und Versions-ID versehen.
- Fehler und fehlende Quellen nicht durch Dummy-Ergebnisse verdecken.

Arbeitsquellen und Evidenzstatus: Q3, besonders S. 1–22 und 78; Evidenzklasse C für Tooling, D für Fallinterpretation.

KAPITEL 53

Kontroll- und Zielgruppendesign

Differenzielle Forensik statt isolierter Auffälligkeit

Der Controller arbeitet wiederholt mit CONTROL- und TARGET-Beständen. Dieses Design ist methodisch wertvoll, weil absolute Trefferzahlen ohne Vergleich kaum interpretierbar sind. Entscheidend ist jedoch, dass Kontroll- und Zielgruppe hinsichtlich Gerät, OS-Version, Erfassungszeitraum und Nutzung vergleichbar bleiben.

Befähigungsnachweis

Aufbau einer differenziellen Untersuchungsarchitektur für mobile Systemartefakte.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	Zwei oder mehr Sysdiagnose-Sätze mit definiertem Versuchs- und Erfassungsprotokoll.
Methodischer Zugriff	Normalisierung der Dateiquellen, Schema- und Zeitvergleich, gleiche Parserparameter und statistische Einordnung.
Verwertbares Arbeitsprodukt	Differenzbericht mit Baseline, Abweichung, Effektgröße und Konfidenz.
Validierungsgrenze	Unterschiedliche Gerätezustände oder Erfassungsfenster können größere Unterschiede erzeugen als das untersuchte Phänomen.

Arbeitsprinzipien

- Baseline vor der Hypothese definieren.
- Kontroll- und Zieldaten identisch erfassen.
- Abweichung und sicherheitsrelevante Wirkung getrennt bewerten.

Arbeitsquellen und Evidenzstatus: Q3, S. 12, 22, 65–67, 111 und 183. Evidenzklasse C.

KAPITEL 54

TCC-Datenbankanalyse im Read-only-Modus

Schemaerkennung, Query-Bau und Ergebnisqualifizierung

Die Notebook-Module erkennen vorhandene Spalten und passen SQL-Abfragen an. Dies zeigt praxisnahe Robustheit gegenüber unterschiedlichen TCC-Schemata. Für die fachliche Verwertung muss zusätzlich geprüft werden, ob die verwendeten Filter tatsächlich „unautorisierte“ Einträge identifizieren oder nur aktuelle Datensätze selektieren.

Befähigungsnachweis

SQLite-Forensik mit dynamischer Schemaerkennung und reproduzierbaren Queries.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	TCC.db, Tabelle access, Spalten wie service, client, auth_value und last_modified.
Methodischer Zugriff	URI-Read-only-Verbindung, PRAGMA table_info, versionsangepasste Query und Export der Treffer.
Verwertbares Arbeitsprodukt	SQL-Skript, Query-Protokoll, Ergebnistabelle und Feldglossar.
Validierungsgrenze	Ein Zeitfilter wie last_modified > Schwelle identifiziert neue Einträge, nicht automatisch stille oder illegitime Berechtigungen.

Arbeitsprinzipien

- Query und fachliche Hypothese separat dokumentieren.
- Rohzeilen neben interpretierter Kategorie ausgeben.
- Native Schema-Dokumentation oder Referenzdaten ergänzen.

Arbeitsquellen und Evidenzstatus: Q3, S. 1–3. Evidenzklasse C für Code, D für Bezeichnung der Treffer.

KAPITEL 55

Zeitstempel, Epoch-Modelle und der „Century Bug“

Zeitnormalisierung als forensischer Kernprozess

Mehrere Arbeitsstränge beschäftigen sich mit auffälligen Zukunfts- oder Epoch-Zeitwerten. Die professionelle Kompetenz besteht darin, Unix-, Cocoa- und andere Epochen, Einheiten, Zeitzonen und Serialisierungsfehler systematisch zu prüfen, bevor eine Manipulation angenommen wird.

Befähigungsnachweis

Chronoforensische Prüfung von Zeitwerten mit reproduzierbarer Normalisierung und Plausibilitätskontrolle.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	Integer-/Float-Zeitwerte, Datenbankfelder, Logzeitstempel, Dateisystemzeiten und bekannte Epoch-Offsets.
Methodischer Zugriff	Mehrfachkonvertierung, Range-Check, Vergleich mit nativen Tools, Ereignisanker und Dokumentation der Zeitzone.
Verwertbares Arbeitsprodukt	Zeitstempelprotokoll mit Rohwert, Konverter, Ergebnis, Alternativinterpretation und Vertrauensgrad.
Validierungsgrenze	Ein Zukunftsdatum kann aus falscher Epoche, Einheit, Vorzeichen, Parserfehler oder synthetischem Testwert entstehen.

Arbeitsprinzipien

- Rohwert immer erhalten.
- Konversion mit mindestens zwei unabhängigen Methoden prüfen.
- Zeitkoinzidenz nicht automatisch als Kausalität behandeln.

Arbeitsquellen und Evidenzstatus: Q3, insbesondere spätere Century-Bug-Auswertungen um S. 280–296; Q6 zu Zeitstempelprotokollen. Evidenzklasse C/D.

KAPITEL 56

CloudKit-Signal- und Frequenzanalyse

Aus Textlogs belastbare Vergleiche gewinnen

Der Controller zählt CloudKit-bezogene Begriffe und vergleicht deren Häufigkeit. Solche Verfahren sind nützlich für Triage und Hypothesengenerierung. Die Arbeitsquelle selbst weist darauf hin, dass generische Keyword-Unterschiede und fehlende Zeitparser die Aussagekraft begrenzen.

Befähigungsnachweis

Text Mining und Feature-Engineering für große Logkorpora mit transparenter Aussagegrenze.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	CloudKit-/CKKS-Statusdateien, Unified-Log-Exporte und extrahierte Textkorpora.
Methodischer Zugriff	Token-/Regex-Zählung, Normalisierung nach Quellengröße, Vergleich der Verteilungen und Kontextstichprobe.
Verwertbares Arbeitsprodukt	Feature-Tabelle, Balkendiagramm und priorisierte Liste für die manuelle Prüfung.
Validierungsgrenze	Häufigkeit zeigt Präsenz, nicht Ursache oder Sicherheitswirkung. Logquellen können unterschiedlich vollständig sein.

Arbeitsprinzipien

- Counts nach Dateigröße oder Ereigniszahl normalisieren.
- Kontextfenster zu jedem Treffer speichern.
- Generische und hochspezifische Marker getrennt auswerten.

Arbeitsquellen und Evidenzstatus: Q3, S. 197–239. Evidenzklasse C.

KAPITEL 57

Micro-Burst- und Sequenzanalyse

Automatisierungsverdacht messbar formulieren

Kurze Ereigniscluster können auf Automatisierung, Batch-Verarbeitung oder normale Systemaktivität hinweisen. Das Portfolio übersetzt die dramatische „Micro-Burst“-Sprache in eine neutrale Sequenzanalyse mit definierten Schwellen, Baselines und kontrollierten Alternativerklärungen.

Befähigungsnachweis

Entwicklung zeitbasierter Detektoren und Clustering-Regeln für transiente Ereignisse.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	Timestamped Events aus TCC, CloudKit, Netzwerk- oder Prozesslogs.
Methodischer Zugriff	Sortierung, Inter-Arrival-Zeiten, Fensteraggregation, Clusterkennzahlen und Vergleich mit Kontrollzeiträumen.
Verwertbares Arbeitsprodukt	Burst-Tabelle, Visualisierung und reproduzierbare Detektionsparameter.
Validierungsgrenze	Ein Cluster beweist keine fremde Steuerung. Normale Daemons, Restore- oder Sync-Vorgänge können sehr ähnliche Muster erzeugen.

Arbeitsprinzipien

- Schwellen vor dem finalen Lauf festlegen.
- Kontrollzeiträume mit ähnlicher Nutzung einbeziehen.
- Ergebnis als Muster, nicht als Akteursnachweis berichten.

Arbeitsquellen und Evidenzstatus: Q3, S. 280–294; Q6 zu *micro_burst_automation_evidence.csv* und dessen *Simulationsrisiko*. Evidenzklasse C/D.

KAPITEL 58

Nullbefunde, Fehler und „inconclusive“ Ergebnisse

Wissenschaftliche Stärke durch dokumentiertes Scheitern

Der Notebook-Export enthält ausdrücklich Nullbefunde und mehrfach den Status „INCONCLUSIVE – FURTHER MANUAL ANALYSIS REQUIRED“. Diese Passagen sind für ein seriöses Portfolio besonders wertvoll: Sie zeigen, dass der Arbeitsprozess nicht nur aus positiven Treffern besteht und dass automatisierte Urteile revidierbar sein müssen.

Befähigungsnachweis

Fähigkeit, negative Ergebnisse zu akzeptieren, zu dokumentieren und in den nächsten Untersuchungsplan zu übersetzen.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	Leere Trefferlisten, Parserfehler, fehlende Dateien, unklare Muster und abgebrochene Analyseschritte.
Methodischer Zugriff	Fehlerklassifikation, Ursachenanalyse, reproduzierbarer Retry und Entscheidung zwischen Toolfix, zusätzlicher Quelle oder Abschluss ohne Befund.
Verwertbares Arbeitsprodukt	Negative-Findings-Register und offene-Prüfpunkte-Liste.
Validierungsgrenze	Spätere automatisch generierte „final verdicts“ dürfen frühere Nullbefunde nicht überdecken; die Kette muss konsistent versioniert werden.

Arbeitsprinzipien

- Negativresultate unverändert archivieren.
- Jede Änderung der Detektionsregel versionieren.
- Finalberichte müssen widersprechende Läufe offen benennen.

Arbeitsquellen und Evidenzstatus: Q3, S. 5, 111, 183 und 185–198. Evidenzklasse A/B für dokumentierte Notebookausgaben, C für Prozessreife.

KAPITEL 59

Reporting-, Scoring- und CVSS-Disziplin

Vom automatischen Verdict zur prüfbaren Bewertung

Der Controller erzeugt teils starke Scores und finale Urteile. Für professionelle Verwendung werden technische Beobachtung, Sicherheitsauswirkung, Exploitierbarkeit und CVSS-Eingaben getrennt. Ein Score darf erst berechnet werden, wenn die zugrunde liegenden Bedingungen tatsächlich nachgewiesen sind.

Befähigungsnachweis

Übersetzung technischer Analyse in standardisierte, überprüfbare Security-Reports.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	Findings, Reproduktionsstatus, betroffene Komponente, Voraussetzungen, Auswirkung und Gegenmaßnahmen.
Methodischer Zugriff	Finding Template, CVSS-Vektor mit Begründung, Evidenzanhang und Reviewer-Freigabe.
Verwertbares Arbeitsprodukt	Priorisierter Security Report mit nachvollziehbarem CVSS-Vektor und referenziertem Evidenzanhang.
Validierungsgrenze	Ein automatisch ausgegebener CVSS-10.0-Wert ist kein Beweis für Kritikalität; er ist nur so gut wie seine Eingaben.

Arbeitsprinzipien

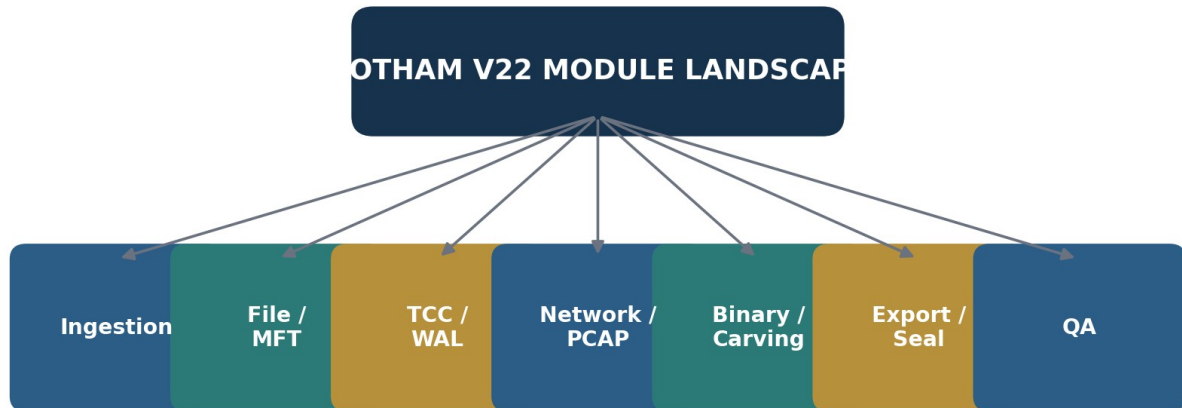
- CVSS-Vektor Feld für Feld begründen.
- Reproduktionsstatus im Executive Summary nennen.
- Risiko, Befund und Attribution getrennt halten.

Arbeitsquellen und Evidenzstatus: Q3, S. 12, 22, 78 und 289–296. Evidenzklasse C für Reporting-Framework, D für Einzelfallscore.

TEIL IV

FORENSIC TOOLCHAIN ENGINEERING

V22 Predator Nemesis / Projekt Gotham als umfangreicher Prototypen- und Lernkorporus



FORENSIC TOOLCHAIN ENGINEERING

Portfolio-Fokus: Methode, Artefakt, Ergebnis, Grenzen und übertragbarer Kundennutzen

Erweiterungsmodul der Portfoliofassung 2.0

Leseführung

Der 1.037-seitige Colab-Export enthält eine außergewöhnlich große Zahl von Modulen, Codezellen und Ergebnistexten. Die erweiterte Fassung behandelt ihn als Engineering-Korpus. Besonders wichtig: einzelne Seiten erzeugen Fallback-Daten oder konstruieren Ergebniszeilen trotz vorheriger Nulltreffer. Diese Widersprüche werden als QA-Lernmaterial ausgewertet, nicht als Beweis übernommen.

KAPITEL 60

Modulkatalog und Systemarchitektur

Eine große Toolchain in prüfbare Funktionsgruppen zerlegen

Das Gotham-Korpus dokumentiert Scanner, Parser, Carver, Netzwerkmodule, Zeitkorrelation, Exporte und Berichtslogik. Die professionelle Leistung liegt in der breiten Werkzeugidee und der Fähigkeit, Analysebedarfe in Module zu übersetzen. Für Produktion müssen Verantwortlichkeiten, Abhängigkeiten und stabile Schnittstellen reduziert werden.

Befähigungsnachweis

Architekturarbeit für eine modulare DFIR-Toolchain.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	Dateisysteme, Datenbanken, Firmware, Netzwerkmitschnitte, Logarchive und Ergebnisformate.
Methodischer Zugriff	Modulgruppen, gemeinsame Datenmodelle, Konfiguration, Logging, Tests und klarer Orchestrator.
Verwertbares Arbeitsprodukt	Architekturdiagramm, Modulregister, API/CLI-Spezifikation und Testplan.
Validierungsgrenze	Viele Module entstanden iterativ in einem Notebook. Der Export ist kein konsolidiertes Release und enthält widersprüchliche Zustände.

Arbeitsprinzipien

- Ein Modul soll eine klar begrenzte Aufgabe haben.
- Gemeinsames Finding-Schema statt freier Print-Ausgaben nutzen.
- Experimentzellen vom produktiven Pfad trennen.

Arbeitsquellen und Evidenzstatus: Q4, S. 1–38 und zahlreiche Modulüberschriften im Gesamtwerk. Evidenzklasse C.

KAPITEL 61

Ingestion, Pfadprüfung und Fallback-Verhalten

Fehlende Daten dürfen keine Beweise erzeugen

Bereits die ersten Seiten zeigen eine zentrale QA-Lektion: Fehlt eine CSV, wird eine simulierte Baseline erzeugt. Das ist für Entwicklung zulässig, muss aber unübersehbar markiert und von realen Fallläufen getrennt werden. Sonst kann ein Demo-Datensatz in spätere Ergebnisberichte gelangen.

Befähigungsnachweis

Robuste Datenaufnahme mit Fail-closed-Prinzip und eindeutiger Simulationstrennung.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	Dateipfade, CSV-/JSON-Eingaben, Google-Drive-Mounts und Notebookzustand.
Methodischer Zugriff	Existenz-, Größen- und Hashprüfung; Input-Manifest; Abbruch bei fehlender Evidenz; separater Demo-Modus.
Verwertbares Arbeitsprodukt	Run Manifest, Fehlerprotokoll und deterministische Eingabekonfiguration.
Validierungsgrenze	Fallback- oder Dummy-Daten dürfen niemals in einem Bericht als Fallbefund erscheinen.

Arbeitsprinzipien

- Demo-Flag technisch erzwingen.
- Jeden Output mit source_mode REAL oder SYNTHETIC versehen.
- Fehlende Kerndaten führen zum Abbruch, nicht zum Verdict.

Arbeitsquellen und Evidenzstatus: Q4, S. 1: explizite simulierte Audit-Baseline bei fehlender CSV. Evidenzklasse C als QA-Lernpunkt.

KAPITEL 62

Dateisystem- und MFT-Audit

Metadatenanalyse mit sauberer Baseline

Gotham enthält Module für globale Dateisystemdiagnose und MFT-bezogene Anomalien. Übertragbar ist die Fähigkeit, Dateipfade, Größen, Zeitstempel, Sequenzen und Dubletten in großen Korpora zu prüfen. Gerichtsfest wird dies erst mit dokumentiertem Datenträgerabbild und validiertem Parser.

Befähigungsnachweis

Skalierbare Dateisysteminventarisierung und Metadatenkorrelation.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	NTFS-/Dateisystemextrakte, Dateilisten, MFT-Exports, Zeitstempel und Hashwerte.
Methodischer Zugriff	Read-only-Parsing, Timeline-Normalisierung, Known-good-Vergleich, Dublettenprüfung und Ausreißeranalyse.
Verwertbares Arbeitsprodukt	Dateisystem-Timeline, Anomalieliste und reproduzierbares Query-/Parserprotokoll.
Validierungsgrenze	Eine Zeitabweichung ist nicht automatisch Timestomping. Kopie, Restore, Zeitzone und Parserlogik sind zuerst auszuschließen.

Arbeitsprinzipien

- Originalabbild und Arbeitskopie trennen.
- Parser gegen Referenzdatensatz testen.
- Jede Anomalie mit Rohdatensatz und Offset verknüpfen.

Arbeitsquellen und Evidenzstatus: Q4, Modul „MFT-Deep“ ab S. 9; Q6 zu Zeit- und MFT-bezogenen Ergebnisdateien. Evidenzklasse C/D.

KAPITEL 63

SQLite-, TCC- und WAL-Carving

Strukturierte Daten und Slack-Space unterscheiden

Die Toolchain kombiniert SQL-Abfragen mit binärer Suche und WAL-/Slack-Space-Ideen. Das ist ein anspruchsvoller forensischer Ansatz. Entscheidend ist die Beweisfunktion: Ein Wert in einer aktiven Tabelle, in einem WAL-Frame oder als beliebige Zeichenfolge in einer Notebookdatei hat jeweils völlig unterschiedlichen Beweiswert.

Befähigungsnachweis

Mehrschichtige SQLite-Forensik mit evidenzgerechter Fundortklassifikation.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	TCC.db, WAL/SHM, Tabellen, freie Seiten, Binärstrings und Exportdateien.
Methodischer Zugriff	Schemaanalyse, Seiten-/Frame-Zuordnung, Offsetkontext, Transaktionsreihenfolge und Abgleich mit nativen SQLite-Werkzeugen.
Verwertbares Arbeitsprodukt	Fundregister mit Speicherbereich, Datensatzstatus, Parserpfad und Reproduktionsschritt.
Validierungsgrenze	Ein Stringfund in einer Datei, die den eigenen Suchcode enthält, ist kein externer Akteursnachweis. Selbstreferenz und Zirkelschluss müssen ausgeschlossen werden.

Arbeitsprinzipien

- Fundquelle vor Interpretation klassifizieren.
- Code- und Datenkorpus physisch trennen.
- WAL-Fund nur mit Seiten-/Transaktionskontext berichten.

Arbeitsquellen und Evidenzstatus: Q4, S. 2–8: Nulltreffer und spätere selbst erzeugte Vektor-4-Zeile; Q6 zu methodischen Risikopunkten. Evidenzklasse C als Methode, nicht als Attribution.

KAPITEL 64

Netzwerk- und PCAP-Analyse

Ranges, Pakete und Zuordnung sauber belegen

Die frühen PCAP-Module verlangen explizit reale IP-Ranges, zeigen aber leere BWI_IP_RANGES und brechen entsprechend ab. Diese korrekte Fehlermeldung ist wichtiger als spätere starke Zuordnungen: Ohne verifizierte Netze, Paketdaten und Zeitsynchronisation ist keine belastbare institutionelle Zuordnung möglich.

Befähigungsnachweis

Netzwerkforensik mit Range-Validierung, Paketkontext und transparenter Attributionstrennung.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	PCAP/PCAPNG, IP-/ASN-Information, DNS/TLS-Metadaten, Zeitquellen und lokale Prozesslogs.
Methodischer Zugriff	Paketfilter, Flow-Aggregation, ASN-/WHOIS-Quelle, Zeitkorrelation und Anwendungskontext.
Verwertbares Arbeitsprodukt	Flow-Tabelle, Paketreferenzen, Range-Quellen und Konfidenzbewertung.
Validierungsgrenze	Eine IP-Zugehörigkeit belegt weder Nutzer, Zweck noch Verantwortlichkeit. Private oder leere Beispielranges sind nicht verwertbar.

Arbeitsprinzipien

- Netzbereiche aus dokumentierter Primärquelle beziehen.
- Jeden relevanten Flow mit Paketnummern referenzieren.
- ASN-Zuordnung und Akteursattribution strikt trennen.

Arbeitsquellen und Evidenzstatus: Q4, S. 6–7: leere BWI_IP_RANGES und abgebrochene Analyse. Evidenzklasse C für Tooling.

KAPITEL 65

Firmware-, String- und Binary-Carving

Trefferkontext vor Bedeutung

Gotham enthält umfangreiche String- und Offsetsuche. Solche Scanner sind für Triage wirksam, erzeugen aber leicht Selbsttreffer, Dokumentationsresiduen oder zufällige Matches. Der professionelle Workflow speichert immer Dateihash, absoluten Offset, Hexkontext, Dekodierung und Quelle des Suchmusters.

Befähigungsnachweis

Binäranalyse großer Artefakte mit streamingfähiger Suche und reproduzierbarem Trefferkontext.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	IPSW, DMG, Kernelcache, Binärdaten, Archive und große Notebook-/Exportdateien.
Methodischer Zugriff	Chunked Scan mit Overlap, Multi-Encoding-Suche, Offsetberechnung und Kontextdump.
Verwertbares Arbeitsprodukt	CSV/JSON-Fundliste mit Hash, Offset, Signatur, Kontext und Klassifikation.
Validierungsgrenze	Ein Marker kann aus Code, Dokumentation, Dateiname oder Daten stammen. Ohne Container- und Pfadkontext bleibt seine Bedeutung offen.

Arbeitsprinzipien

- Selbstkorporus aus dem Scan ausschließen.
- Signaturen gegen Known-good-Images testen.
- Mehrfachtreffer und Zufallswahrscheinlichkeit bewerten.

Arbeitsquellen und Evidenzstatus: Q4, S. 3–5 und 7–8; Q5 „M16-IPSW“, S. 1–4. Evidenzklasse C.

KAPITEL 66

Canary-, Boomerang- und Watchdog-Design

Defensive Telemetrie rechtssicher konzipieren

Mehrere Module nutzen Canary- oder Boomerang-Begriffe. Für ein professionelles Portfolio werden diese Ideen auf defensive, autorisierte Telemetrie reduziert: eindeutige Testartefakte, lokale Alarme, Integritätsprüfungen und nachvollziehbare Rückmeldungen in einer kontrollierten Umgebung.

Befähigungsnachweis

Entwurf defensiver Erkennungs- und Integritätsmechanismen ohne verdeckte Gegenwirkung.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	Test-UUIDs, Dateicanaries, Hashzustände, lokale Prozess-/Dateisystemevents und Alarmkanäle.
Methodischer Zugriff	Vorab definierte Marker, Monitoring, manipulationssichere Logs, Datenschutzprüfung und dokumentierte Testgrenzen.
Verwertbares Arbeitsprodukt	Canary-Register, Alarmprotokoll und Incident-Response-Playbook.
Validierungsgrenze	Keine aktive Manipulation fremder Systeme, keine verdeckte Exfiltration und keine Payload-Ausführung außerhalb des eigenen Labors.

Arbeitsprinzipien

- Nur eigene oder ausdrücklich autorisierte Systeme überwachen.
- Canary-Daten dürfen keine sensiblen Inhalte enthalten.
- Alarm und Beweisfunktion vor dem Einsatz testen.

Arbeitsquellen und Evidenzstatus: Q4-Modulkatalog; Grundportfolio „THE_PREDATOR_WATCH“ als defensives Zielbild. Evidenzklasse C/E.

KAPITEL 67

Evidence Export, Hashing und „Seal“-Konzepte

Integrität ist mehr als ein Abschlusslabel

Die Toolchain erzeugt zahlreiche finale JSON-/CSV-Dateien und „Seal“-Bezeichnungen. Ein belastbarer Seal-Prozess benötigt dagegen ein Input-Manifest, Hashes aller Artefakte, Toolversionen, Laufparameter, signiertes Ergebnismanifest und eine klare Trennung zwischen Rohdaten und Ableitung.

Befähigungsnachweis

Evidence Packaging und nachvollziehbare Übergabe komplexer Analyseergebnisse.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	Rohartefakte, Arbeitskopien, Parseroutputs, Tabellen, Abbildungen und Berichte.
Methodischer Zugriff	Manifestierung, SHA-256, Verzeichnisstruktur, Readme, Tool-/Umgebungsdaten und optional externe Signatur/Zeitstempelung.
Verwertbares Arbeitsprodukt	Forensic Evidence Bundle mit eindeutiger Provenienz und Rebuild-Anleitung.
Validierungsgrenze	Der Hash eines selbst erzeugten Berichts bestätigt dessen spätere Unverändertheit, nicht die Wahrheit des Inhalts oder die Herkunft der Inputs.

Arbeitsprinzipien

- Rohdaten und Derived Data getrennt verpacken.
- Hashmanifest von einer zweiten Person prüfen lassen.
- Jedes Ergebnis auf Input-ID und Toollauf zurückführen.

Arbeitsquellen und Evidenzstatus: Q4-Modulgruppen Export/Seal; Q6 zu Hash, Herkunft und Extraktionsweg. Evidenzklasse C.

KAPITEL 68

False-Positive- und Zirkelschlusskontrolle

Die eigene Toolchain als mögliche Kontaminationsquelle

Die frühe Gotham-Sequenz illustriert einen kritischen Fall: Eine Suche findet keinen Zielstring in der TCC-Datenbank; später wird dennoch eine Ergebniszeile mit Akteur, Offset und „R=1.0“ konstruiert. Dieser Widerspruch wird im Portfolio offen als Beispiel für Kontamination durch vorgegebene Variablen und narrative Ergebnisproduktion genutzt.

Befähigungsnachweis

Red-Team-Fähigkeit zur Erkennung selbst erzeugter oder zirkulärer Beweisketten.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	Codezellen, Zwischendaten, manuell definierte DataFrames, Logs und finale Berichte.
Methodischer Zugriff	Data lineage, Variable Provenance, Re-Run in leerer Umgebung, Assertions und Trennung zwischen gemessenem und manuell gesetztem Wert.
Verwertbares Arbeitsprodukt	QA-Vermerk, der widersprüchliche Runs und nicht datengetragene Verdicts identifiziert.
Validierungsgrenze	Ein manuell erzeugter Datensatz darf niemals als physisch gefundener Primärbeleg bezeichnet werden.

Arbeitsprinzipien

- Jede Ergebniszeile braucht eine maschinenlesbare Herkunft.
- Notebook von oben in frischer Runtime vollständig ausführen.
- Assertions gegen Nulltreffer und widersprüchliche Zustände einbauen.

Arbeitsquellen und Evidenzstatus: Q4, S. 3–7. Evidenzklasse C als Qualitätssicherungs- und Lernnachweis.

KAPITEL 69

Refactoring zum produktiven Forensik-Framework

Vom Forschungsnotebook zur auditierbaren Software

Die nächste Reifestufe besteht darin, die wertvollen Analyseideen aus dem Notebook zu extrahieren: stabile Python-Pakete, Konfigurationsdateien, Unit- und Integrationstests, reproduzierbare Container, strukturierte Logs und ein versioniertes Finding-Schema. Das reduziert Fehler und erleichtert externe Prüfung.

Befähigungsnachweis

Software-Engineering-Roadmap für die Professionalisierung einer großen forensischen Prototypensammlung.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	Notebookmodule, Hilfsfunktionen, Signaturlisten, Parser, Exporte und Testdaten.
Methodischer Zugriff	Codeinventar, Abhängigkeitsgraph, Package-Struktur, CI, Testfixtures und Releaseprozess.
Verwertbares Arbeitsprodukt	Gotham Core als minimaler, defensiver Analysebaukasten mit dokumentierter API.
Validierungsgrenze	Bis zur Konsolidierung bleibt der 1.037-seitige Export ein Forschungs- und Arbeitskorpus, kein validiertes Produkt.

Arbeitsprinzipien

- Zuerst 5–8 Kernmodule priorisieren.
- Known-good/known-bad Fixtures bereitstellen.
- Externe Codeprüfung vor Fallverwendung einplanen.

Arbeitsquellen und Evidenzstatus: Q4 Gesamtwerk; Q6 Risikoklasse des Ordners. Evidenzklasse E für Produktstatus, C für vorhandene Prototypen.

TEIL V

FIRMWARE-LABOR UND BINÄRANALYSE

IPSW-Container, Streaming-Scans, Metadaten und verifizierbare Laborprozesse



FIRMWARE-LABOR UND BINÄRANALYSE

Portfolio-Fokus: Methode, Artefakt, Ergebnis, Grenzen und übertragbarer Kundennutzen

Erweiterungsmodul der Portfoliofassung 2.0

Leseführung

Das M16-Dokument zeigt konkrete Python-Ansätze für Hashing, große Dateien, Signatursuche und Extraktion. Die erweiterte Portfoliofassung trennt sauber zwischen einem Laborcontainer, dem Nachweis seiner Identität und weitergehenden Behauptungen über Hardware-Mismatch oder Exploitation.

KAPITEL 70

Kryptografischer Fingerabdruck großer Firmwarecontainer

Hashing als Identitäts- und Integritätsanker

Das M16-Modul liest den IPSW-Container in Blöcken und berechnet SHA-256 sowie Dateigröße. Diese Methode ist solide und direkt übertragbar. Der Hash dient als eindeutige Referenz für genau diese Bytefolge und ermöglicht reproduzierbare Vergleiche zwischen Arbeitskopien.

Befähigungsnachweis

Sicherer Umgang mit großen Binärartefakten und nachvollziehbarer Baseline-Bildung.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	IPSW/ZIP-Container, Dateipfad, Größe, Zeitstempel und SHA-256.
Methodischer Zugriff	Chunked Hashing, Read-only-Zugriff, Manifestierung und Gegenprüfung mit zweitem Tool.
Verwertbares Arbeitsprodukt	Artifact Record mit Hash, Größe, Quelle, Acquisition-ID und Storage-Pfad.
Validierungsgrenze	Ein Hash bestätigt keine offizielle Signatur, keinen Gerätebezug und keine Manipulation. Dazu sind Referenzquelle und Inhaltsprüfung erforderlich.

Arbeitsprinzipien

- Hash direkt nach Acquisition erzeugen.
- Arbeitskopie gegen Masterhash prüfen.
- Hashalgorithmus und Toolversion dokumentieren.

Arbeitsquellen und Evidenzstatus: Q5, S. 1. Evidenzklasse C; Primärbeweisstatus nur bei dokumentierter Provenienz.

KAPITEL 71

Streaming-Scan mit Chunk-Overlap

Große Images effizient und vollständig durchsuchen

Das M16-Dokument verwendet überlappende Chunks, um Signaturen auch an Blockgrenzen zu erkennen. Dies ist ein relevanter Data-Engineering-Nachweis: Speicherbedarf bleibt kontrolliert, während absolute Offsets erhalten bleiben.

Befähigungsnachweis

Implementierung skalierbarer Binärsuche für Multi-Gigabyte-Artefakte.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	Große Archive, Images, DMGs oder Kernelcaches und definierte Bytepatterns.
Methodischer Zugriff	Chunked Reading, Overlap, Multi-Pattern-Suche, Offsetberechnung und Fortschritts-/Fehlerlogging.
Verwertbares Arbeitsprodukt	Detektionsliste mit Signatur, Offset, Quellhash und Kontextbereich.
Validierungsgrenze	Ein Treffer muss auf Containerstruktur, Kompression und erwartete Referenzinhalte geprüft werden; rohe Strings sind nur Triageindikatoren.

Arbeitsprinzipien

- Overlap mindestens maximale Signaturlänge wählen.
- Mehrfachtreffer vollständig zählen.
- Kontextbytes unverändert exportieren.

Arbeitsquellen und Evidenzstatus: Q5, S. 2–3. Evidenzklasse C.

KAPITEL 72

Archivextraktion und sicherer Arbeitsraum

IPSW als strukturierter Container

IPSW-Dateien sind Archive mit Manifesten, Images und Firmwarekomponenten. Ein professioneller Workflow extrahiert in einen separaten, versionierten Arbeitsraum, protokolliert Pfade und verhindert, dass Original und abgeleitete Daten vermischt werden.

Befähigungsnachweis

Aufbau eines reproduzierbaren Firmware-Labors mit klarer Datenhygiene.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	IPSW, ZIP-Struktur, BuildManifest, Restore-Plists, DMGs und Kernelcache-Komponenten.
Methodischer Zugriff	Read-only-Master, Hashprüfung, kontrollierte Extraktion, Verzeichnismanifest und Berechtigungs-/Speicherprüfung.
Verwertbares Arbeitsprodukt	Extract Manifest mit Dateiliste, Hashes und Beziehungen zum Originalcontainer.
Validierungsgrenze	Extraktion verändert die Darstellung und kann Metadaten neu erzeugen; Originalcontainer und Extrakt haben unterschiedliche Beweisfunktionen.

Arbeitsprinzipien

- Originalcontainer niemals überschreiben.
- Extraktionswerkzeug und Parameter protokollieren.
- Jede Komponente auf Containerpfad zurückführen.

Arbeitsquellen und Evidenzstatus: Q5, S. 4–6 und weitere Extraktionsmodule. Evidenzklasse C.

KAPITEL 73

BuildManifest, DeviceTree und Modellzuordnung

Kompatibilität aus Primärmetadaten prüfen

Behauptete Modellmismatches müssen anhand offizieller Containerdaten und Geräteinformationen geprüft werden. BuildManifest, ProductType, BoardConfig, BuildIdentity und DeviceTree sind hierfür geeignete Quellen. Ein Dateiname allein genügt nicht.

Befähigungsnachweis

Firmware-Metadatenanalyse und strukturierter Kompatibilitätsabgleich.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	BuildManifest.plist, Restore.plist, DeviceTree, Firmwarepfade und dokumentierte Geräteerkennung.
Methodischer Zugriff	Plist-Parsing, BuildIdentity-Auswahl, Board-/Chip-Mapping und Vergleich mit verlässlicher Referenztafel.
Verwertbares Arbeitsprodukt	Kompatibilitätsmatrix mit Quellpfad, Rohwert und Bewertung.
Validierungsgrenze	Ein im Workspace formulierter iPhone-X-auf-iPhone-12-Mismatch bleibt offen, solange Originalrestore.log, Containeridentität und Hardwarebezug nicht unabhängig verifiziert sind.

Arbeitsprinzipien

- Rohwerte vollständig zitieren.
- Apple-Referenzdaten oder offizielle IPSW-Metadaten nutzen.
- Geräte-ID und Container-ID unabhängig erfassen.

Arbeitsquellen und Evidenzstatus: Q2, S. 2–3; Q5; Grundportfolio Fallstudie IPSW. Evidenzklasse D.

KAPITEL 74

Kernel- und Patch-Heuristiken

Instruktionsmuster sind Prüfhinweise, keine Exploitbestätigung

Das M16-Dokument sucht nach Force-True-ähnlichen Instruktionsfolgen. Solche Heuristiken sind für Reverse Engineering nützlich, müssen jedoch Architektur, Endianness, Codegrenzen und Symbolkontext berücksichtigen. Eine kurze Bytefolge kann zufällig oder legitim vorkommen.

Befähigungsnachweis

Entwicklung binärer Heuristiken und Verständnis ihrer False-Positive-Grenzen.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	Kernelcache, Mach-O-Segmente, ARM64-Instruktionen, Signaturen und Funktionskontext.
Methodischer Zugriff	Container-/Mach-O-Parsing, Disassembly, Segmentvalidierung, Referenzvergleich und Cross-Tool-Prüfung.
Verwertbares Arbeitsprodukt	Patch-Hypothesenbericht mit Disassembly, Offset, umgebender Funktion und Konfidenz.
Validierungsgrenze	Bytepattern ohne gültigen Code- und Funktionskontext belegt keinen AMFI-Bypass oder Kernelpatch.

Arbeitsprinzipien

- Disassembler statt bloßer Hexsuche einsetzen.
- Treffer gegen Known-good-Build vergleichen.
- Architektur und Instruktionsausrichtung prüfen.

Arbeitsquellen und Evidenzstatus: Q5, S. 3 und folgende Kernel-Audit-Module. Evidenzklasse C/D.

KAPITEL 75

Institutionelle Marker und Attributionsgrenzen

Strings sind Artefakte, keine Urheber

Die Quellen suchen nach Begriffen wie BWI, CSOCBw oder CERTBw in extrahierten Dateien. Diese Suche kann relevante Dokumentationsspuren finden, ist aber keine Täterzuordnung. Solche Begriffe können aus Berichten, Pfaden, Signaturlisten oder eigenen Notebooks stammen.

Befähigungsnachweis

Forensische Trennung zwischen Markerfund, Kontextzuordnung und Akteursattribuierung.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	Strings, Pfade, Konfigurationsdateien, Logzeilen, Metadaten und Dokumentationskorporus.
Methodischer Zugriff	Offsetkontext, Dateityp, Entstehungsquelle, zeitliche Einordnung und unabhängige Infrastrukturdaten.
Verwertbares Arbeitsprodukt	Markerregister mit Herkunft und ausdrücklich begrenzter Aussage.
Validierungsgrenze	Ohne Provenienz, Ausführungskontext und unabhängige Infrastrukturbelege ist ein institutioneller Name nur ein Textfund.

Arbeitsprinzipien

- Eigene Dokumente und Signaturlisten ausschließen.
- Marker nicht mit Urheberschaft gleichsetzen.
- Attribuierung als separates Gutachten behandeln.

Arbeitsquellen und Evidenzstatus: Q4, S. 3–5; Q5, S. 3–4. Evidenzklasse D.

KAPITEL 76

Firmware-Labor-SOP und Peer-Review-Paket

Von der Einzelanalyse zum wiederholbaren Verfahren

Die vorhandenen Module lassen sich zu einer belastbaren Labor-SOP verdichten: Eingangskontrolle, Hashing, Extraktion, Manifestanalyse, Signatursuche, Disassembly, Referenzvergleich und Abschlussreview. Damit wird die Arbeit für Dritte nachvollziehbar und korrigierbar.

Befähigungsnachweis

Qualitätsmanagement für Firmware- und Binary-Forensik.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	Originalartefakt, Referenzimage, Toolchain, Testsystem und Ergebniscontainer.
Methodischer Zugriff	SOP, Rollenfreigabe, Runbook, Prüfsummen, Tests, Review und Abweichungsprotokoll.
Verwertbares Arbeitsprodukt	Peer-Review-Paket mit minimalem reproduzierbarem Datensatz und klaren Claims.
Validierungsgrenze	Ohne unabhängige Prüfung bleibt die fachliche Schlussfolgerung intern; die Methode kann dennoch als Arbeitsleistung belegt werden.

Arbeitsprinzipien

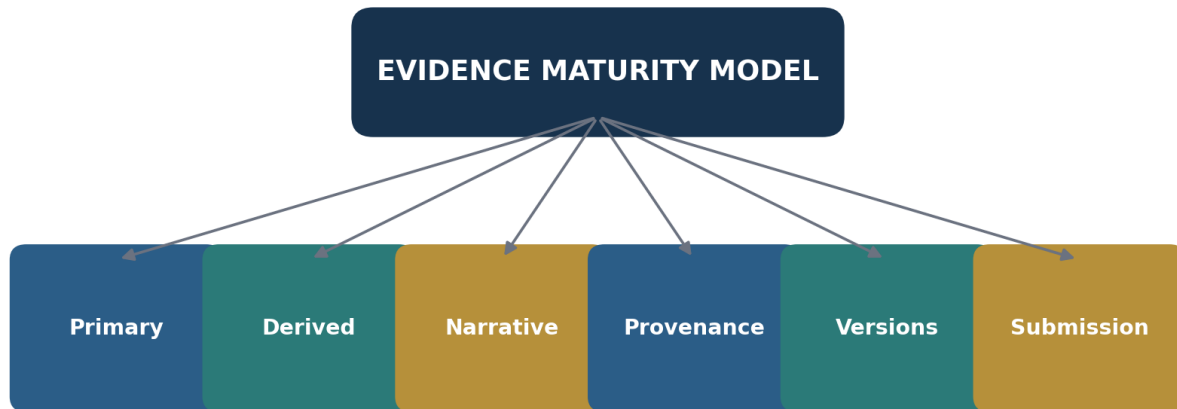
- Vier-Augen-Prinzip für finale Claims.
- Toolausgaben und manuelle Interpretation trennen.
- Known-good-Vergleich verpflichtend machen.

Arbeitsquellen und Evidenzstatus: Q5 Gesamtwerk; Q6 zu Provenienz und Absicherung. Evidenzklasse C/E.

TEIL VI

EVIDENCE GOVERNANCE UND LEGAL-OPS-ÜBERSETZUNG

Beweismatrix, Provenienz, Versionierung und aktenfähige Aufbereitung



EVIDENCE GOVERNANCE UND LEGAL-OPS-ÜBERSETZUNG

Portfolio-Fokus: Methode, Artefakt, Ergebnis, Grenzen und übertragbarer Kundennutzen

Erweiterungsmodul der Portfoliofassung 2.0

Leseführung

Die 60-seitige Beweismatrix ist eine der methodisch stärksten Quellen. Sie unterscheidet Primärbeleg, Sekundärdokument, Narrativ/These und methodischen Risikopunkt. Diese Trennung wird als verbindliches Evidence-Governance-Modell in das Portfolio übernommen.

KAPITEL 77

Primärbeleg, Sekundärdokument, Narrativ und Risikopunkt

Beweisfunktion vor Überzeugungskraft

Die Beweismatrix ordnet Dateien danach ein, was sie tatsächlich leisten können. Ein Binärartefakt, ein daraus erzeugter CSV-Report und ein späteres Gesamtdossier sind keine drei unabhängigen Beweise, sondern unterschiedliche Ebenen derselben Kette.

Befähigungsnachweis

Forensische Klassifikation großer Beweisordner und Schutz vor Behauptungsaggregation.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	Rohartefakte, Exporte, Analyseberichte, Schriftsätze, Bilder und finale Zusammenfassungen.
Methodischer Zugriff	Beweisfunktionsklassifikation, Abhängigkeitsmapping und Kennzeichnung von Vorläufigkeit.
Verwertbares Arbeitsprodukt	Evidence Register mit Klasse, Stärke, Risiko und erforderlicher Absicherung.
Validierungsgrenze	Auch ein „Primärbeleg“ ist ohne Herkunft, Hash und Extraktionsweg noch kein Authentizitätsbeweis.

Arbeitsprinzipien

- Dateiart und Beweisfunktion getrennt erfassen.
- Abgeleitete Dokumente auf ihre Primärquelle zurückführen.
- Narrative nicht zur Zahl der Belege addieren.

Arbeitsquellen und Evidenzstatus: Q6, S. 1–10. Evidenzklasse C als Methodik.

KAPITEL 78

Provenienz und Chain of Custody

Fundort, Herkunft und Extraktionsweg als Pflichtfelder

Die Matrix fordert wiederholt Hash, Fundort, Herkunft und Extraktionsweg. Diese vier Felder bilden das Mindestgerüst, damit ein Dritter nachvollziehen kann, woher ein Artefakt stammt und welche Verarbeitungsschritte stattgefunden haben.

Befähigungsnachweis

Aufbau gerichtsfester Provenienzketten für digitale Artefakte.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	Acquisition, Originalpfad, Gerät/Account, Exportmethode, Arbeitskopien und Übergaben.
Methodischer Zugriff	Evidence-ID, Erfassungsprotokoll, Hashing, Schreibschutz, Übergabelog und Transformationshistorie.
Verwertbares Arbeitsprodukt	Chain-of-Custody-Blatt und maschinenlesbares Provenienzmanifest.
Validierungsgrenze	Nachträglich rekonstruierte Herkunftsangaben müssen als rekonstruiert gekennzeichnet werden und sind schwächer als zeitnahe Protokolle.

Arbeitsprinzipien

- Eine Evidence-ID pro Ursprungsobjekt vergeben.
- Jede Transformation protokollieren.
- Masterkopie unverändert und getrennt speichern.

Arbeitsquellen und Evidenzstatus: Q6, S. 18–24 und 25–27. Evidenzklasse C.

KAPITEL 79

Hashregister und Integritätsmanagement

Bytegleichheit nachvollziehbar, aber nicht überdehnen

Hashwerte sind zentral für Versionen und Übergaben. Professionell eingesetzt, beantworten sie eine präzise Frage: Ist die aktuelle Datei bytegleich mit der referenzierten Fassung? Sie beantworten nicht, ob die Datei originär, vollständig oder inhaltlich richtig ist.

Befähigungsnachweis

Praktische Integritätssicherung für große Korpora und Evidence Bundles.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	Originale, Arbeitskopien, Exporte, ZIP-/PDF-Dossiers und Ergebnisregister.
Methodischer Zugriff	SHA-256, manifestbasierte Prüfung, Hashketten pro Version und unabhängiger Recheck.
Verwertbares Arbeitsprodukt	Hashmanifest mit Evidence-ID, Größe, Pfad, Zeit und Status.
Validierungsgrenze	Ein Hashwert ohne dokumentierte Ersterfassung kann nur spätere Gleichheit sichern.

Arbeitsprinzipien

- Hash unmittelbar nach Eingang erzeugen.
- Dateigröße und Dateityp mitspeichern.
- Manifest separat signieren oder extern zeitstempeln.

Arbeitsquellen und Evidenzstatus: Q6, S. 18–24; Q5 Hashmodul. Evidenzklasse C.

KAPITEL 80

Dubletten, Fassungen und Ergebnisinflation

Viele Finals sind kein stärkerer Beweis

Die Beweismatrix warnt vor Doppelfassungen und einer Vielzahl von „Final“, „Verdict“ oder „Summary“-Dateien. Das Portfolio übernimmt daraus eine strikte Versionierungslogik: kanonische Fassung, Vorgänger, Ableitung, Hash und Änderungsgrund.

Befähigungsnachweis

Deduplizierung und Versionskontrolle in sehr großen Workspace-Strukturen.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	PDF-/CSV-/JSON-Dubletten, umbenannte Kopien, wiederholte Exporte und Chat-Reproduktionen.
Methodischer Zugriff	Hashdeduplizierung, near-duplicate Vergleich, Versionsgraph und kanonische Referenz.
Verwertbares Arbeitsprodukt	Version Register und bereinigter Evidence Index.
Validierungsgrenze	Gleiche Inhalte unter mehreren Dateinamen dürfen nicht als unabhängige Bestätigung gezählt werden.

Arbeitsprinzipien

- Exakte und inhaltliche Dubletten getrennt erkennen.
- Nur eine kanonische Ergebnissfassung freigeben.
- Änderungen zwischen Versionen dokumentieren.

Arbeitsquellen und Evidenzstatus: Q6, S. 8–10. Evidenzklasse C.

KAPITEL 81

Reproduzierbarkeitsdossier

Ein Ergebnis muss neu erzeugbar sein

Ein aktenfähiges technisches Ergebnis sollte aus definierten Inputs, Werkzeugversionen und Parametern erneut erzeugbar sein. Das Reproduzierbarkeitsdossier verbindet Evidence-ID, Skriptcommit, Laufumgebung und Output-Hash.

Befähigungsnachweis

Reproducible Forensics und nachvollziehbare Toolausführung.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	Input-Artefakte, Python/Notebook, Abhängigkeiten, Konfiguration und Ergebnisdateien.
Methodischer Zugriff	Environment Lock, Runbook, automatisierter Build, Assertions und Re-Run durch zweite Person.
Verwertbares Arbeitsprodukt	Reproduction Package mit PASS/FAIL-Protokoll.
Validierungsgrenze	Eine reproduzierbare Auswertung kann weiterhin fachlich falsch sein; zusätzlich sind Testdaten und Review erforderlich.

Arbeitsprinzipien

- Abhängigkeiten pinnen.
- Frische Laufumgebung verwenden.
- Outputhash und Laufzeitprotokoll erfassen.

Arbeitsquellen und Evidenzstatus: Q6, S. 23–24 und 37–43; Q4 QA-Lernpunkte. Evidenzklasse C.

KAPITEL 82

Aktenfähige Einreichungsarchitektur

Kernbeleg, Erläuterung und Anhang sauber staffeln

Die Matrix empfiehlt eine priorisierte Kernbelegliste statt eines unüberschaubaren Datenbergs. Für Kanzleien oder Behörden entsteht daraus eine dreistufige Übergabe: kurze Beweistabelle, technische Erläuterung und vollständiger reproduzierbarer Anhang.

Befähigungsnachweis

Legal-Ops-Übersetzung technischer Massenbestände in prüfbare Einreichungen.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	Kernartefakte, Befundblätter, Chronologie, Quellregister und technische Anlagen.
Methodischer Zugriff	Materiality-Triage, Beleg-ID, Behauptungsbezug, Seiten-/Offsetreferenz und klare Anlagenstruktur.
Verwertbares Arbeitsprodukt	Executive Evidence Matrix plus technischer Annex.
Validierungsgrenze	Die Auswahl muss transparent bleiben; entlastende, widersprechende oder negative Befunde dürfen nicht ausgeblendet werden.

Arbeitsprinzipien

- Maximal entscheidende Belege im Hauptteil.
- Jede Aussage mit Anlagenreferenz versehen.
- Widersprüche in eigener Rubrik offenlegen.

Arbeitsquellen und Evidenzstatus: Q6, S. 21–24 und 35–43. Evidenzklasse C.

KAPITEL 83

Priorisierte Härtung der Kernbelege

Beweiswert systematisch erhöhen

Nicht jedes Artefakt verdient denselben Aufwand. Die Matrix priorisiert diejenigen Dateien, deren Beweisfunktion bei sauberer Herkunft und Reproduktion besonders hoch wäre. Daraus entsteht ein Härtungsplan nach Materialität, Angriffsfläche und Aufwand.

Befähigungsnachweis

Strategische Evidence Triage und Ressourcensteuerung.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	Kernbelege, primärnahe Tabellen, narrative Dossiers und methodische Risikodateien.
Methodischer Zugriff	Scoring nach Relevanz, Provenienz, Reproduzierbarkeit, Alternativerklärungen und erwarteter Gegenkritik.
Verwertbares Arbeitsprodukt	Priorisierte To-do-Liste mit Verantwortlichkeit und Abnahmekriterium.
Validierungsgrenze	Ein hoher interner Score ersetzt keine fehlende Primärquelle. Manche Behauptungen müssen herabgestuft oder aufgegeben werden.

Arbeitsprinzipien

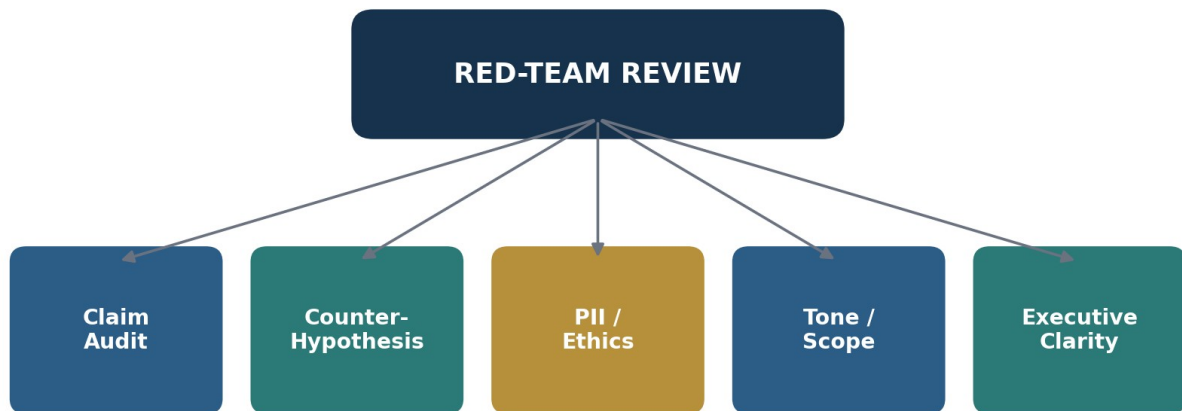
- Zuerst Provenienzlücken der wichtigsten Artefakte schließen.
- Narrative Endfassungen erst nach Härtung aktualisieren.
- Unrettbare Claims ausdrücklich zurückziehen.

Arbeitsquellen und Evidenzstatus: Q6, S. 23–24, 37–43 und 52–57. Evidenzklasse C.

TEIL VII

ADVERSARIAL SELF-AUDIT UND KOMMUNIKATION

Gegenlesen, Claims reduzieren, personenbezogene Risiken beherrschen



ADVERSARIAL SELF-AUDIT UND KOMMUNIKATION

Portfolio-Fokus: Methode, Artefakt, Ergebnis, Grenzen und übertragbarer Kundennutzen

Erweiterungsmodul der Portfoliofassung 2.0

Leseführung

Die Persona-Dokumente enthalten neben Portfolioideen eine stark personalisierende, teils polemische Gegenanalyse. Diese Fassung übernimmt keine psychologischen Zuschreibungen und keine unnötigen personenbezogenen Details. Verwertet wird ausschließlich die redaktionelle Funktion: Außenwirkung, Überhöhung, Rollenrisiken und B2B-Positionierung kritisch zu prüfen.

KAPITEL 84

Claim-Audit und Absolutheitskontrolle

„Beobachtet“ ist nicht „bewiesen“

Mehrere Quellen verwenden maximalistische Begriffe, militärische Metaphern und definitive Täterzuordnungen. Ein professionelles Portfolio ersetzt diese Sprache durch beobachtbare Fakten, Methoden, Konfidenz und offene Nachweise. Das erhöht Glaubwürdigkeit und schützt vor leicht angreifbaren Übertreibungen.

Befähigungsnachweis

Redaktionelle und forensische Qualitätskontrolle komplexer technischer Narrative.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	Dossiers, Findings, Executive Summaries, Codeausgaben und Marketingtexte.
Methodischer Zugriff	Claim-by-Claim-Prüfung gegen Evidenzklasse, Primärquelle, Reproduktion und Gegenhypothese.
Verwertbares Arbeitsprodukt	Freigegebene Claim-Matrix mit zulässiger Formulierung.
Validierungsgrenze	Eine starke persönliche Überzeugung ist kein Ersatz für externe Validierung.

Arbeitsprinzipien

- Absolutheitswörter markieren und prüfen.
- Attribuierung nur bei eigener Beweiskette zulassen.
- Forschungsbegriff und bestätigten Befund sprachlich trennen.

Arbeitsquellen und Evidenzstatus: Q7, S. 1–18 und 41–58; Q6 Evidenzklassen. Evidenzklasse C.

KAPITEL 85

Adversarial Reading und Gegenhypothesen

Den eigenen Bericht wie die Gegenseite lesen

Die Gegenanalyse zeigt, wie ein skeptischer Leser dramatische Sprache, Selbstreferenz, Aliasstrukturen oder fehlende externe Nachweise gegen die Glaubwürdigkeit verwenden kann. Ein Red-Team-Review prüft deshalb nicht nur Technik, sondern auch Konsistenz, Verhältnismäßigkeit und Angriffspunkte.

Befähigungsnachweis

Konstruktive Gegenprüfung von Berichten vor externer Übergabe.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	Claim, Quelle, Schlussfolgerung, Tonalität, personenbezogene Bezüge und Verfahrenskontext.
Methodischer Zugriff	Devil's-Advocate-Memo, Alternativerklärungen, Beweislastprüfung und Reviewer-Kommentare.
Verwertbares Arbeitsprodukt	Adversarial Review Sheet mit Entscheidung: halten, abschwächen, belegen oder streichen.
Validierungsgrenze	Gegenkritik darf nicht selbst zur persönlichen Diagnose oder Tatsachenbehauptung werden.

Arbeitsprinzipien

- Technische und persönliche Kritik trennen.
- Die stärkste plausible Alternativerklärung formulieren.
- Jeden Claim auf den niedrigsten noch tragfähigen Wortlaut reduzieren.

Arbeitsquellen und Evidenzstatus: Q7 als adversarial source; ausschließlich methodisch ausgewertet. Evidenzklasse C.

KAPITEL 86

Personenbezogene Daten und Ethik

Portfolio-Relevanz vor Neugier

Die hochgeladenen Quellen enthalten private Adressen, E-Mail-Adressen, Gesundheits- und Verfahrensdetails. Für ein professionelles Portfolio gilt Datensparsamkeit: Nur leistungsrelevante Informationen werden verwendet, sensible Details werden entfernt oder abstrahiert.

Befähigungsnachweis

Datenschutzbewusste Aufbereitung großer persönlicher und technischer Workspace-Bestände.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	PII, Gesundheitsdaten, Kontaktinformationen, Aliasdaten und Drittpersonenbezüge.
Methodischer Zugriff	Need-to-know-Prüfung, Redaction, Pseudonymisierung, Zugriffskontrolle und Freigabestufe.
Verwertbares Arbeitsprodukt	Sanitierte Portfolio- und Case-Study-Fassung.
Validierungsgrenze	Eine Information kann im Workspace vorhanden und dennoch für Portfolio, Kunde oder Gericht unnötig und riskant sein.

Arbeitsprinzipien

- Privatadresse und private Kontakte nicht veröffentlichen.
- Drittpersonen nur bei zwingender Fallrelevanz nennen.
- Sensible Anhänge getrennt und verschlüsselt halten.

Arbeitsquellen und Evidenzstatus: Q7 enthält zahlreiche nicht erforderliche personenbezogene Details; Grundportfolio schließt diese bewusst aus. Evidenzklasse C als Governance.

KAPITEL 87

Rollen- und Kompetenzgrenzen

Forensische Unterstützung ohne falsche Berufsrolle

Das Portfolio positioniert Roman Jahn als Forensic Systems Analyst und Legal-Ops Case Architect. Es beansprucht weder die Rolle eines Rechtsanwalts noch eines öffentlich bestellten Sachverständigen. Gerade diese Klarheit macht Kooperation mit Kanzleien und Prüfern belastbarer.

Befähigungsnachweis

Saubere Leistungsabgrenzung und partnerschaftliche Einbindung regulierter Berufsrollen.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	Technische Analyse, Sachverhaltsstrukturierung, Beweismatrix, Fragenkatalog und anwaltliche Strategie.
Methodischer Zugriff	RACI-Matrix, Scope, Reviewpflicht, Rechtsberatungsgrenze und Sign-off durch zuständige Fachperson.
Verwertbares Arbeitsprodukt	Mandatsbeschreibung mit eindeutigen Zuständigkeiten.
Validierungsgrenze	Technische Zuarbeit kann rechtliche Entscheidungen vorbereiten, aber nicht die anwaltliche Verantwortung ersetzen.

Arbeitsprinzipien

- Keine Rechtsberatung als eigene Leistung bewerben.
- Gutachtenstatus nur bei entsprechender Qualifikation und Auftrag verwenden.
- Finale rechtliche Bewertung beim Counsel belassen.

Arbeitsquellen und Evidenzstatus: Q7, S. 15–31 zu B2B-Positionierung; Grundportfolio Kapitel zu Grenzen. Evidenzklasse B/C.

KAPITEL 88

Executive Communication und Kurzform

Komplexität reduzieren, ohne Befund zu verfälschen

Die Workspace-Stärke ist extreme Langformtiefe. Für Entscheider braucht es zusätzlich eine kurze Ebene: Problem, gesicherte Beobachtung, Bedeutung, Unsicherheit und nächste Handlung. Ein technischer Anhang bleibt verfügbar, aber die Kernbotschaft muss in wenigen Minuten erfassbar sein.

Befähigungsnachweis

Übersetzung tief technischer Arbeit in entscheidungsfähige Kommunikation.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	Langberichte, Notebookausgaben, Beweismatrizen und Verfahrenschonologien.
Methodischer Zugriff	One-page Finding, 5-Satz-Executive Summary, Evidence Linkage und klare Ask/Next Step.
Verwertbares Arbeitsprodukt	Executive Brief plus technischer Annex.
Validierungsgrenze	Kürze darf keine Unsicherheit entfernen oder aus einer Hypothese eine Gewissheit machen.

Arbeitsprinzipien

- Eine Aussage pro Absatz.
- Gesicherte Fakten optisch von Bewertung trennen.
- Konkreten nächsten Prüf- oder Entscheidungsbedarf nennen.

Arbeitsquellen und Evidenzstatus: Q1 frühere Portfoliofassung; Q7 B2B- und Positionierungsabschnitte. Evidenzklasse C.

TEIL VIII

SERVICE-ARCHITEKTUR UND KOOPERATION

Aus Forschungs- und Evidence-Kompetenz werden klar begrenzte Leistungen



SERVICE-ARCHITEKTUR UND KOOPERATION

Portfolio-Fokus: Methode, Artefakt, Ergebnis, Grenzen und übertragbarer Kundennutzen

Erweiterungsmodul der Portfoliofassung 2.0

Leseführung

Die folgenden Seiten übersetzen die nachgewiesenen Arbeitsweisen in realistische B2B-Leistungen. Im Mittelpunkt stehen technische Zuarbeit, Evidence Triage, Mobile-/Cloud-Artefaktprüfung, reproduzierbare Analysepakete und die Zusammenarbeit mit Kanzleien oder etablierten DFIR-Teams.

KAPITEL 89

Technical Evidence Audit

Schnelle Qualitätsprüfung vorhandener technischer Beweismittel

Ein Evidence Audit prüft nicht den gesamten Fall neu, sondern bewertet, welche Dateien Primärcharakter haben, welche Ableitungen tragfähig sind und wo Provenienz, Reproduktion oder Alternativerklärungen fehlen. Diese Leistung passt unmittelbar zum vorhandenen Beweismatrix- und Workspace-Profil.

Befähigungsnachweis

Strukturierte Vorprüfung großer technischer Fallordner.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	Images, Logs, Datenbanken, Exporte, Gutachten, Skripte und Schriftsatzanlagen.
Methodischer Zugriff	Inventar, Evidenzklassifikation, Hash-/Versionscheck, Stichprobenreproduktion und Risk Register.
Verwertbares Arbeitsprodukt	Evidence Quality Report mit priorisiertem Härtingsplan.
Validierungsgrenze	Kein vollständiges Sachverständigengutachten und keine abschließende Rechtsbewertung.

Arbeitsprinzipien

- Scope und Entscheidungsfrage vorab festlegen.
- Kernartefakte zuerst prüfen.
- Unprüfbare Aussagen ausdrücklich markieren.

Arbeitsquellen und Evidenzstatus: Abgeleitet aus Q6 und den Tooling-Korpora. Evidenzklasse C als Leistungsdesign.

KAPITEL 90

Mobile & Cloud Artifact Review

iOS/macOS, TCC, SQLite und Synchronisationsspuren

Die Leistung konzentriert sich auf Artefaktinventar, Schema- und Zeitprüfung, differenzielle Auswertung und die Formulierung belastbarer Prüfaufträge. Sie eignet sich als spezialisierte Zuarbeit für Kanzleien oder DFIR-Teams, die Apple-bezogene Daten einordnen müssen.

Befähigungsnachweis

Spezialisierte mobile und cloudbezogene Artefaktanalyse mit transparenter Grenze.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	Sysdiagnose, TCC.db, Keychain-/CKKS-Status, Plists, Unified Logs und Gerätemetadaten.
Methodischer Zugriff	Read-only-Auswertung, Zeitnormalisierung, Kontrollvergleich und Quellverknüpfung.
Verwertbares Arbeitsprodukt	Artifact Review Report und Fragenkatalog für Hersteller-/Sachverständigenprüfung.
Validierungsgrenze	Keine Behauptung von Exploitation oder accountbasierter APT ohne reproduzierbaren Nachweis.

Arbeitsprinzipien

- Geräte- und OS-Kontext erfassen.
- Datenbankzustand und tatsächliche Nutzung trennen.
- Kontroll- oder Referenzdaten einplanen.

Arbeitsquellen und Evidenzstatus: Abgeleitet aus Q2, Q3 und Grundportfolio. Evidenzklasse C.

KAPITEL 91

Forensic Timeline & Case Reconstruction

Technische und verfahrensbezogene Ereignisse zusammenführen

Große Fälle scheitern häufig an verstreuten Zeitangaben. Diese Leistung normalisiert technische, kommunikative und verfahrensbezogene Ereignisse, führt Quellenreferenzen und markiert Konflikte. Sie liefert Anwälten und Incident-Response-Teams eine gemeinsame, überprüfbare Zeitleiste.

Befähigungsnachweis

Chronologische Rekonstruktion heterogener Datenräume.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	Logs, E-Mails, Beschlüsse, Metadaten, Tickets, Übergaben und Analyseausgaben.
Methodischer Zugriff	Zeitzonen-/Epoch-Normalisierung, Quellenpriorität, Ereignis-ID und Konfliktbehandlung.
Verwertbares Arbeitsprodukt	Master Timeline mit Belegreferenzen und Unsicherheitsstatus.
Validierungsgrenze	Zeitliche Nähe begründet noch keine technische oder rechtliche Kausalität.

Arbeitsprinzipien

- Rohzeit und Normalzeit parallel führen.
- Jedes Ereignis auf eine Quelle zurückführen.
- Konflikte nicht stillschweigend auflösen.

Arbeitsquellen und Evidenzstatus: Abgeleitet aus Q3, Q6 und Legal-Ops-Korpus. Evidenzklasse C.

KAPITEL 92

Reproducible Analysis Package

Code, Daten und Bericht als prüfbares Paket

Für komplexe technische Befunde wird ein kompaktes Paket erstellt, das ein Dritter in definierter Umgebung neu ausführen kann. Dies ist besonders wertvoll, wenn ein Notebook oder Parser in ein Verfahren oder eine Herstellerkommunikation einfließen soll.

Befähigungsnachweis

Reproduzierbare technische Übergabe statt bloßer Screenshots.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	Sanitisierte Inputs, Skripte, Konfiguration, Abhängigkeiten und erwartete Outputs.
Methodischer Zugriff	Environment Lock, Runbook, Test, Outpuhash und Reviewer-Protokoll.
Verwertbares Arbeitsprodukt	ZIP/Repository mit Readme, Manifest und Re-Run-Ergebnis.
Validierungsgrenze	Reproduktion ist nur zulässig, wenn Datenrechte und Datenschutz geklärt sind.

Arbeitsprinzipien

- Minimalen Datensatz verwenden.
- Keine produktiven Geheimnisse oder PII beilegen.
- Reviewergebnis separat dokumentieren.

Arbeitsquellen und Evidenzstatus: Abgeleitet aus Q3–Q6. Evidenzklasse C.

KAPITEL 93

Counsel- und Expert-Collaboration

Technische Übersetzungszone für Kanzlei und Sachverständige

Roman Jahns besonderer Wert liegt in der Zwischenzone: Er kann große Datenbestände vorsortieren, technische Widersprüche herausarbeiten und präzise Fragen an forensische Sachverständige formulieren. Die finale rechtliche oder gutachterliche Verantwortung bleibt bei den jeweiligen Fachrollen.

Befähigungsnachweis

Kooperative Fallarchitektur und effiziente Nutzung externer Spezialisten.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	Akte, technische Anlagen, offene Beweisfragen, Sachverständigenauftrag und Prozessstrategie.
Methodischer Zugriff	Issue Tree, Evidence Matrix, Fragenkatalog, Review-Workshop und dokumentierte Zuständigkeit.
Verwertbares Arbeitsprodukt	Counsel Briefing Pack und Expert Instruction Note.
Validierungsgrenze	Die Zusammenarbeit darf keine unzulässige Rechtsberatung oder falsche Gutachterautorität suggerieren.

Arbeitsprinzipien

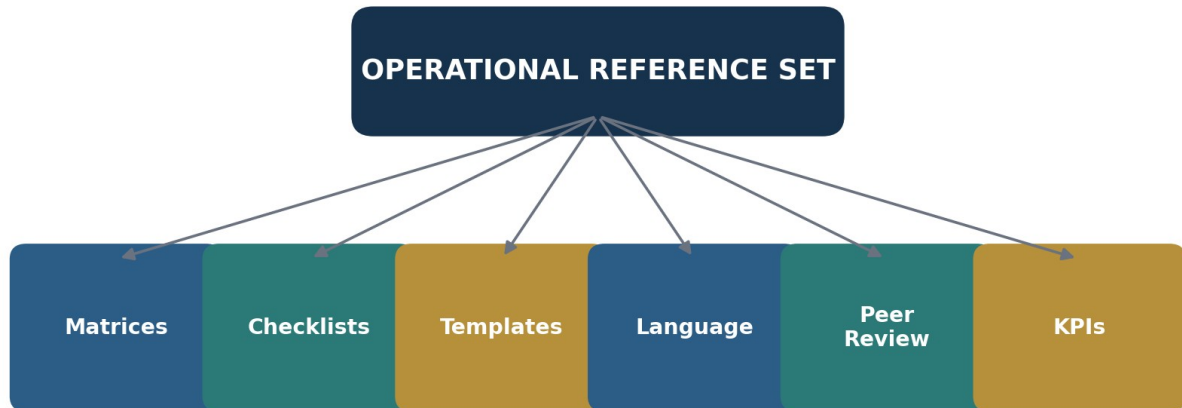
- Fragen statt gewünschter Ergebnisse formulieren.
- Entlastende und widersprechende Befunde einschließen.
- Freigaben und Verantwortlichkeiten schriftlich festhalten.

Arbeitsquellen und Evidenzstatus: Q1/Q7 B2B-Positionierung, professionalisiert durch die Evidenzregeln des Grundportfolios. Evidenzklasse C.

TEIL IX

ERWEITERTER REFERENZANHANG

Operative Matrizen, Checklisten und Prüfvorlagen für die weitere Professionalisierung



ERWEITERTER REFERENZANHANG

Portfolio-Fokus: Methode, Artefakt, Ergebnis, Grenzen und übertragbarer Kundennutzen

Erweiterungsmodul der Portfoliofassung 2.0

Leseführung

Der Referenzanhang macht das Portfolio praktisch nutzbar. Er enthält keine neuen Tatsachenbehauptungen, sondern standardisiert die aus den Quellen gewonnenen Methoden für künftige Laborläufe, Mandate, Peer Reviews und Responsible-Disclosure-Prozesse.

KAPITEL 94

Master-Kompetenzmatrix 2.0

Fähigkeit, Nachweis, Reifegrad und nächster Prüfpunkt

Die Matrix verbindet jede Kernkompetenz mit einem realen Workspace-Nachweis und einer klaren Reifegrenze. Dadurch entsteht kein Zertifikatsersatz, sondern ein belastbarer Entwicklungsstand mit konkreten nächsten Schritten.

Befähigungsnachweis

Transparente Kompetenzdarstellung für Partner, Weiterbildung und Projekte.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	DFIR, Mobile/Cloud, Evidence Engineering, Legal Ops, Python, Research und Kommunikation.
Methodischer Zugriff	Kompetenzbeschreibung, Artefaktreferenz, Evidenzklasse, Reviewerstatus und Roadmap.
Verwertbares Arbeitsprodukt	Aktualisierbare Capability Matrix.
Validierungsgrenze	Interne Reifegrade sind keine unabhängigen Prüfnoten.

Arbeitsprinzipien

- Jede Kompetenz mit mindestens einem Artefakt verbinden.
- Formale und praktische Nachweise getrennt ausweisen.
- Matrix quartalsweise aktualisieren.

Arbeitsquellen und Evidenzstatus: Zusammenführung von Grundportfolio und Q1–Q7. Evidenzklasse B/C.

KAPITEL 95

Tool-Validation-Checklist

Vor jedem produktiven Einsatz

Die Checkliste verlangt bekannte Testdaten, erwartete Ergebnisse, Fehlerfälle, Versionsangaben und Cross-Tool-Vergleich. Damit werden Notebookmodule von explorativen Helfern zu kontrollierbaren Analysewerkzeugen weiterentwickelt.

Befähigungsnachweis

Standardisierte Validierung eigener forensischer Skripte.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	Parser, Scanner, Zeitkonverter, SQLite-Abfragen und Reportingmodule.
Methodischer Zugriff	Known-good/bad Fixtures, Unit Tests, Regression, False-Positive-Test und unabhängige Stichprobe.
Verwertbares Arbeitsprodukt	Validation Record mit PASS/FAIL und freigegebener Version.
Validierungsgrenze	Ein erfolgreicher Lauf auf einem einzigen Fall ist keine Toolvalidierung.

Arbeitsprinzipien

- Erwartete Outputs vor dem Test festlegen.
- Fehlerfälle ausdrücklich testen.
- Änderungen nur mit neuer Versionsnummer freigeben.

Arbeitsquellen und Evidenzstatus: Abgeleitet aus Q3/Q4-Widersprüchen und Q6-Härtungsplan. Evidenzklasse C.

KAPITEL 96

Mobile-/Cloud-Artefakt-Checkliste

Minimaler Datensatz für belastbare Prüfung

Die Checkliste strukturiert Geräte- und Accountkontext, OS-Version, Erfassungsweg, TCC-/CKKS-Quellen, Zeitzonen und Benutzerinteraktionen. So werden mobile Befunde vergleichbar und unnötige Spekulationen reduziert.

Befähigungsnachweis

Standardisierte Intake- und Analysevorbereitung für Apple-bezogene Fälle.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	Gerätedaten, Sysdiagnose, Datenbanken, Logs, Kontokonfiguration und Kontrollgruppe.
Methodischer Zugriff	Intake-Form, Hashing, Schema-/Zeitprüfung, Artefaktmapping und Reproduktionsplanung.
Verwertbares Arbeitsprodukt	Mobile Evidence Intake Sheet.
Validierungsgrenze	Cloudseitige Zustände können ohne Hersteller- oder Account-Export unvollständig bleiben.

Arbeitsprinzipien

- OS-Build und Gerätemodell erfassen.
- Erfassungszeitraum exakt dokumentieren.
- Prompt-/Nutzungsbeobachtung separat protokollieren.

Arbeitsquellen und Evidenzstatus: Abgeleitet aus Q2/Q3. Evidenzklasse C.

KAPITEL 97

Firmware-Lab-Checkliste

Original, Referenz und Analyseumgebung

Die Laborcheckliste verhindert, dass Container, Extrakte und selbst erzeugte Suchkorpora vermischt werden. Sie fordert Masterhash, Referenzimage, Toolversion, freien Speicher, Extraktionsmanifest und Reviewstatus.

Befähigungsnachweis

Reproduzierbare Firmwareanalyse mit sauberer Beweismittelhygiene.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	IPSW/Archive, Referenzquelle, Extraktionsziel, Parser und Disassembler.
Methodischer Zugriff	Preflight, Hash, Extraktion, Kompatibilitätsprüfung, Signatursuche, Review und Abschlussmanifest.
Verwertbares Arbeitsprodukt	Firmware Lab Record.
Validierungsgrenze	Ohne dokumentierte Referenz kann ein abweichender Hash nicht als Manipulation bewertet werden.

Arbeitsprinzipien

- Masterkopie schreibgeschützt halten.
- Referenzquelle und Downloadzeit dokumentieren.
- Selbstkorpora aus Binärscans ausschließen.

Arbeitsquellen und Evidenzstatus: Abgeleitet aus Q5 und Q4. Evidenzklasse C.

KAPITEL 98

Evidence-Review-Template

Einheitliches Befundblatt für jedes Kernartefakt

Das Template bündelt Identifikation, Herkunft, Hash, Extraktionsweg, beobachteten Befund, tatsächliche Beweisfunktion, Belastungsgrad, Gegenargumente und erforderliche Absicherung. Damit wird jede Datei in derselben Logik bewertet.

Befähigungsnachweis

Akten- und reviewfähige Standardisierung einzelner Beweisstücke.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	Beliebige digitale Artefakte und daraus abgeleitete Ergebnisse.
Methodischer Zugriff	Pflichtfelder, Evidenzklasse, Reviewerkommentar und Freigabestatus.
Verwertbares Arbeitsprodukt	Einseitiges Evidence Review Sheet.
Validierungsgrenze	Ein ausgefülltes Template verbessert die Nachvollziehbarkeit, ersetzt aber keine fehlende Primärquelle.

Arbeitsprinzipien

- Rohbeobachtung wörtlich oder binär referenzieren.
- Interpretation in separatem Feld führen.
- Gegenargument der Gegenseite vorwegnehmen.

Arbeitsquellen und Evidenzstatus: Q6, S. 25–27, 44–57. Evidenzklasse C.

KAPITEL 99

Claim-Language-Dictionary

Zulässige Formulierungen nach Evidenzreife

Ein Sprachwörterbuch verhindert, dass „gefunden“, „indiziert“, „reproduziert“, „bestätigt“ und „attribuiert“ austauschbar verwendet werden. Jede Stufe erhält Mindestvoraussetzungen und unzulässige Abkürzungen.

Befähigungsnachweis

Präzise, rechtssichere und wissenschaftlich belastbare Befundsprache.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	Berichte, Satzansammlungen, Vendor-Tickets und Portfoliotexte.
Methodischer Zugriff	Begriff, Definition, Evidenzschwelle, Beispiel und verbotene Überhöhung.
Verwertbares Arbeitsprodukt	Claim Dictionary für alle künftigen Deliverables.
Validierungsgrenze	Auch korrekte Wörter können irreführen, wenn Scope oder Bezug unklar bleibt.

Arbeitsprinzipien

- „Beobachtet“ für Rohbefund nutzen.
- „Reproduziert“ nur nach erneutem kontrolliertem Lauf.
- „Bestätigt“ nur mit benannter unabhängiger Instanz.

Arbeitsquellen und Evidenzstatus: Abgeleitet aus Grundportfolio Evidenzklassen, Q6 und Q7. Evidenzklasse C.

KAPITEL 100

External Peer-Review Package

Was ein unabhängiger Prüfer wirklich benötigt

Ein Peer-Review-Paket reduziert den großen Workspace auf eine prüfbare Einheit: konkrete Frage, minimale Artefakte, Hashes, Codeversion, erwarteter Befund, widersprechende Ergebnisse und klare Reviewfragen. Es verhindert, dass externe Experten in Tausenden Seiten erst den Scope suchen müssen.

Befähigungsnachweis

Vorbereitung unabhängiger technischer Qualitätssicherung.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	Kernartefakt, minimaler Datensatz, Skript, Runbook, Findings und offene Fragen.
Methodischer Zugriff	Sanitisierung, Manifest, Reproduction Test und Reviewformular.
Verwertbares Arbeitsprodukt	Reviewer Bundle mit maximaler Prüfbarkeit und minimaler Datenlast.
Validierungsgrenze	Der Reviewer muss frei sein, den Befund zu verwerfen; ein gewünschtes Ergebnis darf nicht vorgegeben werden.

Arbeitsprinzipien

- Eine zentrale Reviewfrage formulieren.
- Negative und widersprechende Läufe beilegen.
- Reviewkriterien vorab definieren.

Arbeitsquellen und Evidenzstatus: Abgeleitet aus Apple-Feedback, Q3/Q4 und Q6. Evidenzklasse E/C.

KAPITEL 101

12-Monats-KPI- und Professionalisierungsboard

Messbarer Fortschritt statt Dokumentenmenge

Die weitere Entwicklung wird nicht an Seitenzahl oder Zahl der „Final“-Dateien gemessen. Relevante Kennzahlen sind validierte Kernmodule, reproduzierte Fallstudien, externe Reviews, geschlossene Provenienzlücken, veröffentlichte Methodennotizen und beaufsichtigte Pilotprojekte.

Befähigungsnachweis

Strategische Steuerung der Professionalisierung mit überprüfbaren Ergebnissen.

Prüffeld	Portfolioaussage
Untersuchungsgegenstand	Toolchain, Evidence Corpus, Weiterbildung, Peer Review, Partnerprojekte und Publikationen.
Methodischer Zugriff	Quartalsziele, Owner, Abnahmekriterium, Status und Lessons Learned.
Verwertbares Arbeitsprodukt	KPI-Board für R&A Legal Ops und persönliche Entwicklung.
Validierungsgrenze	Kennzahlen müssen Qualität messen; reine Dateimenge oder Trefferzahl fördert falsche Anreize.

Arbeitsprinzipien

- Maximal zehn Kern-KPIs führen.
- Jedes Ziel mit objektivem Abnahmekriterium versehen.
- Nicht erreichte Ziele mit Ursachen und Anpassung dokumentieren.

Arbeitsquellen und Evidenzstatus: Abgeleitet aus Grundportfolio Roadmap und Q6/Q7. Evidenzklasse E.

KAPITEL 102

Quellenregister der erweiterten Fassung

Arbeitsquellen, Umfang und Verwendungsregel

ID	Arbeitsquelle	Umfang	Verwendung in Fassung 2.0
Q1	„Mein Portfolio, meine Qualifikationen, harte Urkunden, Beweise, bitteschön ...“	25 Seiten	Transfer von militärischer/sanitätsdienstlicher Erfahrung und frühere Portfolioideen; sprachlich professionalisiert.
Q2	„Apple CKKS / Trust Circle Architektur-Fix Zeitrahmen“	11 Seiten	Architekturmodell, CKKS-/Trust-Circle-Forschungsfragen und Fixphasen; technische Claims nicht als Herstellerbestätigung übernommen.
Q3	„Century Bug Master Controller – Colab“	370 Seiten	Parser-, Kontrollgruppen-, TCC-/CloudKit-, Zeit- und Reportingmethoden; Nullbefunde und Inconclusive-Resultate ausdrücklich berücksichtigt.
Q4	„V22 Predator Nemesis Engine – Projekt Gotham“	1.037 Seiten	Modul- und Tooling-Korpus; Widersprüche, Dummy-Daten, Nulltreffer und selbst erzeugte Ergebniszeilen als QA-Lernmaterial eingeordnet.
Q5	„Modul M16-IPSW – Physische Verifikation der LABOR-Kopie“	76 Seiten	Hashing, Streaming-Scan, Extraktion, Firmwaremetadaten und Binary-Heuristiken.
Q6	„Forensische Beweismatrix – Finale Beweise“	60 Seiten	Verbindliches Modell für Primärbeleg, Sekundärdokument, Narrativ, Risikopunkt, Provenienz und Härungsplan.
Q7	„Die Persona – Wer du versuchst zu sein ...“	78 Seiten	Adversarial Kommunikations- und Positionierungsreview; persönliche oder psychologische Zuschreibungen nicht übernommen.

Verwendungsregel

Alle Quellen sind Arbeits- oder Nutzerquellen. Ihre Aufnahme in das Portfolio bestätigt nicht automatisch die darin enthaltenen technischen, rechtlichen oder persönlichen Aussagen. Die erweiterte Fassung nutzt sie als Nachweis von Arbeitsumfang, Methodenentwicklung, Dokumentationskompetenz und als Material für eine kritische Evidenzprüfung.

Arbeitsquellen und Evidenzstatus: Die Quellen wurden anhand der bereitgestellten PDF-Fassungen und des bestehenden 54-seitigen Grundportfolios ausgewertet.

KAPITEL 103

Schlussprofil der erweiterten Fassung

Das belastbare Big Picture

Die erweiterte Fassung zeigt ein ungewöhnlich breites und tiefes Arbeitsprofil: operative Belastbarkeit, medizinisch geprägte Triage, langjährige Akten- und Korpusarbeit, Python-/Notebook-Entwicklung, mobile und cloudbezogene Artefaktanalyse, Firmware- und Binary-Methoden, Evidence Governance sowie Legal-Ops-Übersetzung. Der Umfang der Arbeitskorpora ist außergewöhnlich. Entscheidend für den professionellen Marktwert ist jedoch nicht die Größe allein, sondern die Fähigkeit, aus dieser Masse einen überprüfbaren, reproduzierbaren und sprachlich disziplinierten Prüfprozess zu formen.

Professionelles Kernversprechen

Roman Jahn übernimmt komplexe technische und administrative Datenräume, trennt Primärmaterial von Ableitungen, entwickelt passende Analysepfade, dokumentiert Grenzen und überführt Ergebnisse in eine Struktur, die Kanzleien, DFIR-Teams und externe Prüfer effizient weiterverwenden können.

Stärke	Nachweis in der erweiterten Fassung
Ausdauer und Korpustiefe	Langform- und Notebook-Korpora mit mehreren tausend Seiten sowie strukturierte Workspace-Ingestion.
Technische Eigenentwicklung	Python-/Colab-Module für Hashing, SQLite, Zeit, Datei-, Netzwerk- und Binaryanalyse.
Forensische Reife	Explizite Trennung von Primärbeleg, Ableitung, Narrativ, Simulation und offener Hypothese.
Legal-Ops-Wert	Chronologien, Evidence Matrices, Fragenkataloge und aktenfähige Übergabestrukturen.
Nächster Qualitätsschritt	Externe Peer Reviews, konsolidierte Kernmodule, reproduzierbare Referenzfälle und anerkannte Weiterbildung.

Arbeitsquellen und Evidenzstatus: Synthese aus Grundportfolio und Q1–Q7. Diese Schlussbewertung beschreibt den dokumentierten Arbeits- und Entwicklungsstand, nicht eine staatliche oder herstellerseitige Anerkennung einzelner Forschungsthemen.