Hochschule Wismar
University of Applied Sciences
Technology, Business and Design
Fakultät für Ingenieurwissenschaften

Alternative Prüfungsleistung

IT-forensische Sicherung und Analyse sowie die Erstellung eines forensischen Gutachtens anhand eines fiktiven Vorfalls

Anschlag am Frankfurter Flughafen durch Umweltaktivisten

Modul: Forensik in Betriebs- und Anwendungssystemen
Sommersemester 2024

Eingereicht am: 7. Juli 2024

von: [redacted]

Inhaltsverzeichnis

1 Aufgabenstellung 4
2 Szenario 5
3 Planung 8
3.1 Vorgehensmodell 8
3.2 Auswahl der Geräte 9
3.3 Auswahl der Untersuchungswerkzeuge 9
3.4 Spurenlegung 9
4 Vorbereitung 12
4.1 Notebook 12
4.2 USB-Stick 13
4.3 Imageerstellung 14
5 Gutachten 15
5.1 Untersuchungsauftrag 16
5.2 Zusammenfassung der Untersuchung 16
5.3 Untersuchungsobjekte 18
5.3.1 Asservat 320/24-1 „Notebook“ 18
5.3.2 Asservat 320/24-2 „USB-Stick“ 19
5.4 Untersuchungswerkzeuge 19
5.5 Vorbereitung der Untersuchung 20
5.6 Untersuchung Asservat 320/24-1 „Notebook“ 22
5.6.1 Image-Integrität 23
5.6.2 Systeminformationen 23
5.6.3 Benutzerzuordnung 24
5.6.4 Medien und Dokumente 25
5.6.5 Browserverlauf 26
5.6.6 Verbundene Geräte 29
5.6.7 Kommunikation 31
5.6.8 Anwendungen 31
5.7 Untersuchung Asservat 320/24-2 „USB-Stick“ 31
5.7.1 Image-Integrität 31
5.7.2 Allgemeine Informationen 32
5.7.3 Medien und Dokumente 34
6 Fazit 35
7 Wiki Eintrag 37

Anhang A Fluchttürsteuerung 42

Anhang B Flucht- und Rettungsplan 43

Anhang C Grundstückplan Frankfurt Flughafen 44

Anhang D Übersicht Frankfurt Flughafen 45

Anhang E Gebäudeplan Frankfurt Flughafen 46

Anhang F Lageplan Frankfurt Flughafen 47

Anhang G Abus Alarmanlage 48

Anhang H EESec2 Alarmanlage 49

Anhang I Betriebsspezifische Schaltpläne 50

Anhang J Grundwissen Elektronik 51

Anhang K Stromversorgungsplan 52

Anhang L Bedienungsanleitung Notstromaggregat 53

Anhang M Flughafenordnung Frankfurt 54

Anhang N Ausweisordnung Frankfurt Flughafen 55

Anhang O Sicherheitsmanagement-System Frankfurt Flughafen 56

Anhang P Brandschutzordnung Frankfurt Flughafen 57

Anhang Q Struktur Fraport Group 58

Anhang R FraSec Unternehmensgruppe 59

Anhang S Organigramm Fraport AG 60

Anhang T Flugpläne Frankfurt Flughafen vom 17.05.2024 61

Anhang U Mietwagenbuchung 63

Quellverzeichnis 64

Abbildungsverzeichnis 66

Tabellenverzeichnis 67

Selbstständigkeitserklärung 68

1 Aufgabenstellung

Diese Praktikumsdokumentation ist ein Teil der Prüfungsleistung des Moduls „Forensik in Betriebs- und Anwendungssystemen“ des zweiten Fachsemesters im Masterstudiengang „IT-Sicherheit und Forensik“. Anhand eines eigen entworfenen Vorfalls soll eine forensische Analyse mittels auf Windows basierenden Forensik-Werkzeugen durchgeführt und die Vorgehensweise sowie die Ergebnisse als forensisches Gutachten aufbereitet werden. Dazu soll ein zeitbasiertes Szenario auf mindestens zwei Hardwarekomponenten ausgeführt und anschließend von jeder dieser Komponenten ein Image erstellt werden. Eine abschließende, kritische Bewertung der gewählten IT-forensischen Methode, der gewählten Forensik-Werkzeuge sowie der erlangten Ergebnisse ist ebenfalls Bestandteil dieser Ausarbeitung.

2 Szenario

Der Frankfurter Flughafen mit Sitz in Frankfurt am Main in Hessen wird von der Fraport AG betrieben und zählt zu den größten Verkehrsflughäfen Deutschlands [**2**]. Neben rund 148.500 Passagieren sowie 1.100 Start und Landungen pro Tag schlägt er täglich ca. 5.500 Tonnen Fracht um [**1**] und besitzt somit das größte Frachtaufkommen in ganz Europa [**2**]. Die Fraport AG beschäftigt um die 81.000 Mitarbeiter [**1**].

Am 17.05.2024 um 15:15 Uhr kam es zu einem Brandgeschehen in der Nähe der Hauptstromversorgung des Frankfurter Flughafens, sodass dieser in Teilen evakuiert werden musste und der Flugverkehr zeitweise eingestellt wurde. Folge des Brandes ist ein halbstündiger Stromausfall im Terminal 1. Betroffen von der Evakuierung waren rund 25.000 Passagiere und etwa 18.000 Mitarbeiter. Es kamen keine Personen zu schaden. Zudem mussten um die 120 Starts verschoben bzw. abgesagt sowie viele der ankommenden Flüge auf umliegende Flughäfen umgeleitet werden. Die Auswirkungen des Vorfalls wirkten sich noch weitere drei Tage auf den Tagesbetrieb des Flughafens aus. Der Schaden beläuft sich schätzungsweise auf insgesamt 1,2 Mio. Euro.

Nach nur zwei Stunden bekennt sich die linksextremistische Gruppierung „Die Pfifferlinge“ zu dem Vorfall. Der Frankfurter Flughafen liegt schon länger im Fokus der Umweltaktivisten, da der Neubau des Terminals 3 [**3**] großflächige Rodungen des umliegenden Waldes mit sich brachte. Bereits vor Baubeginn haben Gruppenmitglieder immer wieder Teile des Waldes belagert und sich an Bäume gekettet, um die Abholzung eben dieser zu verhindern. Bereits hier waren Einsätze der Polizei notwendig, um die Situation zu klären und aufzulösen. Das Bekennerschreiben der Gruppierung wurde auf der dafür bekannten Webseite „de.indymedia.org“ veröffentlicht und lautet wie folgt:

Abbildung 1: Bekennerschreiben der Gruppierung „Die Pfifferlinge“

Die Polizei Frankfurt am Main nimmt die Ermittlungen auf, da der Verdacht auf Brandstiftung gemäß § 306 StGB vorliegt. In der Nähe des Tatorts konnten leere Spiritusdosen sowie Reste von Anzündern sichergestellt werden. Diese Räumlichkeiten sowie der Tatort selbst sind nicht für die Öffentlichkeit zugänglich, sodass von einem Innentäter ausgegangen wird. Deswegen wird eine interne Befragung der Mitarbeiter der Fraport AG aufgesetzt, beginnend mit den Bereichen Facilitymanagement und Informationstechnik (IT). Dass „Die Pfifferlinge“ sich zu dem Anschlag bekennen und von einem Komplizen innerhalb der Fraport AG ausgegangen wird, hat sich bereits unter den Mitarbeitern herumgesprochen. Darüber hinaus berichten die Medien ausgiebig von dem Vorfall und stellen Spekulationen auf, wie solch etwas möglich sei. Der Herr Arnold Brandenburger, Mitarbeiter in der IT, berichtet deswegen den zuständigen Ermittlern, dass seine 29-jährige Kollegin, die Merle Braun, die seit drei Jahren ebenfalls in der IT der Fraport AG arbeitet, in einer Mittagspause mal erwähnte, dass sie sich aktiv um die Umwelt kümmere und sich mit einer Gruppe namens „Die Pfifferlinge“ öffentlich für die Natur und den Klimaschutz einsetze. Außerdem habe er als Administrator der Webserver bei seiner wöchentlichen Kontrolle verdächtige Anfragen über das Dienstnotebook der Frau Braun im Logging sehen können, die auf Beihilfe zum Vorfall schließen lassen.

Die Staatsanwaltschaft Frankfurt am Main forderte gem. § 94 Abs. 2 i. V. m. § 110 StPO ei-

ne Sicherstellung und Beschlagnahmung der relevanten Dokumente und IT-Komponenten ein. Bei der Durchsuchung des Arbeitsplatzes der Frau Braun am 19.05.2024 konnten ein Dienstnotebook sowie ein USB-Stick beschlagnahmt werden. Das Notebook befand sich im ausgeschalteten Zustand. Die beiden Asservate wurden der Dienststelle K33 „IT-Forensik Ermittlungsunterstützung“ der Polizei Frankfurt am Main übergeben, um eine IT-forensische Untersuchung durchzuführen.

3 Planung

3.1 Vorgehensmodell

Für die IT-forensische Untersuchung wird sich für das SAP-Vorgehensmodell entschieden, da es aufgrund seiner klaren und einfachen Struktur optimal zu dem beschriebenen Sachverhalt und den erforderlichen Untersuchungsmaßnahmen passt. Diese umfassen neben der IT-forensischen Datensicherung und der anschließenden Aufbereitung der Asservate, eine Auswertung hinsichtlich des Anschlags auf den Frankfurter Flughafen sowie das Verfassen eines IT-forensischen Gutachtens.

Die Sicherungsphase („Secure“) hat bereits bei der Durchsuchung des Arbeitsplatzes der Tatverdächtigen Merle Braun begonnen, da hier neben der forensischen Datensicherung auch die Sicherstellung möglicher Asservate, insbesondere von IT-Komponenten und Datenträgern, sowie die Dokumentation der vor Ort Situation bei der Tatverdächtigen verstanden werden kann. Es wurden Fotoaufnahmen durch die Polizeibeamten vom Arbeitsplatz, den beiden vorgefundenen Asservaten sowie möglicher Passworte gemacht. Darüber hinaus wurde bildlich festgehalten, dass sich das Notebook bei der Beschlagnahmung im ausgeschalteten Zustand befand. Der nächste Schritt der Sicherungsphase ist die IT-forensische Datensicherung, bei der sogenannte Images erstellt werden. Die Asservate werden dabei mittels Schreibschutz, auch als Writeblocker bezeichnet, an den Datensicherungsarbeitsplatz angeschlossen, um mögliche Veränderungen zu verhindern. Sollten Veränderungen unabdingbar sein, werden diese vorab mit dem zuständigen Ermittler abgesprochen und dokumentiert. Zur Prüfung der Integrität der Asservate sowie der Images werden bei der Sicherung MD5- und SHA1-Hashwerte generiert. Als Sicherungsmethode wird sich für die physische Sicherung entschieden, um neben dem aktuellen Zustand auch gelöschte und versteckte Daten einsehen zu können.

In der Analysephase („Analyse“) werden die Images als Vorbereitung für die eigentliche Auswertung technisch aufbereitet, d.h. der Systemzustand sowie die Daten werden in eine für den Menschen lesbare Form gebracht. Nach der Aufbereitung findet die Durchführung der Auswertung statt, die bereits eng mit der Interpretation der dabei vorgefundenen bzw. nicht vorliegenden Spuren korrespondiert. Es sollen Indizien, jedoch bestenfalls Beweise, gefunden werden, die die Tatverdächtige Merle Braun be- oder auch entlasten. Diese müssen dahingehend geprüft werden, ob sie in einen Zusammenhang mit dem Anschlag auf den Frankfurter Flughafen gebracht werden können und wie diese untereinander in Verbindung stehen.

Bei der abschließenden Präsentation („Present“) wird das IT-forensische Gutachten erstellt, das neben der Methodik auch die einzelnen gewonnenen Erkenntnisse aufzeigt. Eine abschließende Bewertung der aus dem Gutachten resultierenden Ergebnisse ist nicht Gegenstand des Untersuchungsauftrags.

3.2 Auswahl der Geräte

Aus dem gewählten Szenario lassen sich unmittelbar die zu untersuchenden Geräte ableiten. Die Tatverdächtige Merle Braun agiert als Innentäterin und gibt geheime Informationen und Dokumente als Tatvorbereitung aus dem Firmennetz der Fraport AG an die weiteren Mitglieder der Gruppe „Die Pfifferlinge“ weiter. Dementsprechend werden ein Notebook, welches den Arbeitsrechner der Tatverdächtigen darstellt, und ein USB-Stick als Untersuchungsobjekte ausgewählt. Mittels des USB-Sticks werden die Dokumente vom Notebook aus dem Firmennetz herauskopiert und anschließend nach außen getragen. Die Nutzung von Cloud-Diensten ist per Dienstanweisung der Fraport AG untersagt. Mithilfe von Blacklists wird das Aufrufen solcher Webseiten und Dienste unterbunden. Darüber hinaus ist die Verwendung von privater Hard- und Software für dienstliche Zwecke ebenfalls strengstens untersagt.

Bei dem Notebook handelt es sich um einen Acer des Typs „MM1-571“, auf welchem das Betriebssystem „Windows 10 Home“ installiert ist. Der USB-Stickt ist von der Marke „Kingston“ und weist eine Gesamtspeicherkapazität von 8 GB auf. Beide Geräte werden durch einen der Autoren bereitgestellt.

3.3 Auswahl der Untersuchungswerkzeuge

Für die Imageerstellung des USB-Sticks wird das kostenlose Sicherungstool „FTK Imager“ der Firma „Exterro“ verwendet. Außerdem wird der Software Writeblocker „SAFE Block“ der Firma „ForensicSoft“ eingesetzt.

Da die Festplatte des Notebooks nicht ausgebaut werden kann, wird sich für eine Sicherung mittels PALADIN EDGE der Firma „SUMURI“ entschieden. PALADIN beinhaltet u.a. die PALADIN Toolbox, mit der Images von internen Festplatten erstellt werden kann. Bei PALADIN handelt es sich um eine modifizierte „Live“-Linux-Distribution basierend auf Ubuntu, die sich in Polizeibehörden als Sicherungswerkzeug etabliert hat.

Zur Aufbereitung und Untersuchung der Geräte wird die Software „Magnet AXIOM“ der Firma „Magnet Forensics“ gewählt. Es wird sich für AXIOM entschieden, da bei der Auswertung insbesondere digitale Artefakte bezüglich des Browserverlaufs und möglicher Kommunikationsmittel erwartet werden und sich AXIOM erfahrungsgemäß für solche digitalen Artefakte besonders eignet. Zudem biete es die Möglichkeit die Windows Registry auszuwerten, um digitale Artefakte in Bezug auf die Verbindung des USB-Sticks mit dem Notebook zu finden.

3.4 Spurenlegung

Neben den internen Dokumenten, die von der Tatverdächtigen Merle Braun vom Notebook aus dem Firmennetz der Fraport AG auf einen USB-Stick kopiert werden, werden zum Szenario passende Suchanfragen durchgeführt und entsprechende Webseiten und Onlineartikel

aufgerufen. Die Suchanfragen dienen neben der Tatvorbereitung auch zum Recherchieren der Reaktion der Medien und der Gesellschaft nach dem Anschlag.

Des Weiteren wird die Kommunikation zwischen der Tatverdächtigen und den weiteren Mitgliedern der Gruppe „Die Pfifferlinge“ über das Notebook realisiert. Als Kommunikationsplattform wird sich für den Onlinedienst „Discord“ für Instant Messaging, Chat, Sprach- und Videokonferenzen entschieden. Hierüber erfolgt die Planung des Anschlags sowie der Informationsaustausch innerhalb der Gruppierung „Die Pfifferlinge“. Um das Szenario möglichst realistisch zu halten, wird Discord über den Browser geöffnet, da die lokale Installation der Anwendung zu auffällig wäre. Des Weiteren ist die Einrichtung einer nicht freigegebenen Software auf Dienstrechnern verboten und wird somit technisch unterbunden.

Um die Tatvorbereitung realistisch und über einen längeren Zeitraum zu simulieren, wird die Spurenlegung innerhalb des Zeitraums vom 27.04.2024 bis zum 18.05.2024 durchgeführt. Tabelle 1 zeigt eine chronologische Aufreihung dieser. Dabei wird eine Arbeitswoche von fünf Tagen berücksichtigt, sodass nach fünf Tagen bewusst zwei Tage lang keine Spuren gelegt werden. Der 17.05.2024 wird bewusst als Tattag gewählt. Hierbei handelt es sich um den Beginn des Pfingstwochenendes und den damit verbundenen Pfingstferien einiger Bundesländer. An diesem Tag ist mit vermehrtem Flugverkehr zu rechnen, was die Gruppierung „Die Pfifferlinge“ ausnutzt, um einen möglichst großen Schaden und eine hohe Medienaufmerksamkeit zu erreichen.

Datum	**Aktionen**
27.04.2024	Kommunikation im Discord Suchanfragen: KRITIS Ausfall Auswirkungen KRITIS Ausfall Schadenshöhe KRITIS Notfallplan
28.04.2024	Suchanfragen: Frankfurt Flughafen Stromversorgung Frankfurt Flughafen Notstrom
29.04.2024	Speicherung von Dokumenten Kommunikation in Discord
30.04.2024	Suchanfragen: Trafobrand in der Industrie Stromausfall/Blackout in der Industrie
01.05.2024	Speicherung von Dokumenten Kommunikation in Discord Suchanfragen: Funktionsweise Notstromaggregat Ausschalten Notstromaggregat

	Stromversorgung vollständig kappen
04.05.2024	Suchanfragen: Alarmanlage deaktivieren Fluchttüren Alarmanlage ausschalten Elektriker Werkzeug
05.05.2024	Suchanfragen: Auto mieten Frankfurt am Main Google Maps Frankfurt Flughafen Autovermietung anonym Elektriker Arbeitskleidung
06.05.2024	Suchanfragen: Frankfurt Flughafen Bahnhof Frankfurt Flughafen Flugplan 17.05 Frankfurt Flughafen Umspannwerk Was macht ein Umspannwerk
08.05.2024	Kommunikation in Discord Speicherung von Dokumenten
17.05.2024	Anschlag am Frankfurter Flughafen
18.05.2024	Suchanfragen: Frankfurt Flughafen Stromausfall Mai 2024 Frankfurt Flughafen Die Pfifferlinge Frankfurt Flughafen Stromausfall Reaktionen Frankfurt Flughafen Stromausfall Kritik Frankfurt Flughafen Stromausfall Daten und Fakten Frankfurt Flughafen Stromausfall Schaden Frankfurt Flughafen Stromausfall Reportage Wer sind Die Pfifferlinge
19.05.2024	Durchsuchung des Arbeitsplatzes

Tabelle 1: Zeitlicher Verlauf des Szenarios mit vorbereitenden und nachgelagerten Handlungen

4 Vorbereitung

4.1 Notebook

In Vorbereitung für die Spurenlegung wird das Notebook über die Windows eigenen Einstellungen zurückgesetzt. Es wird die Option ausgewählt, alle persönlichen Daten zu entfernen und Windows 10 Home neu aus der Cloud herunterzuladen und anschließend zu installieren. Die ausgewählten Optionen können den Abbildungen 2, 3 sowie 4 entnommen werden.

Abbildung 2: Wiederherstellung über die Windows eigene Funktion

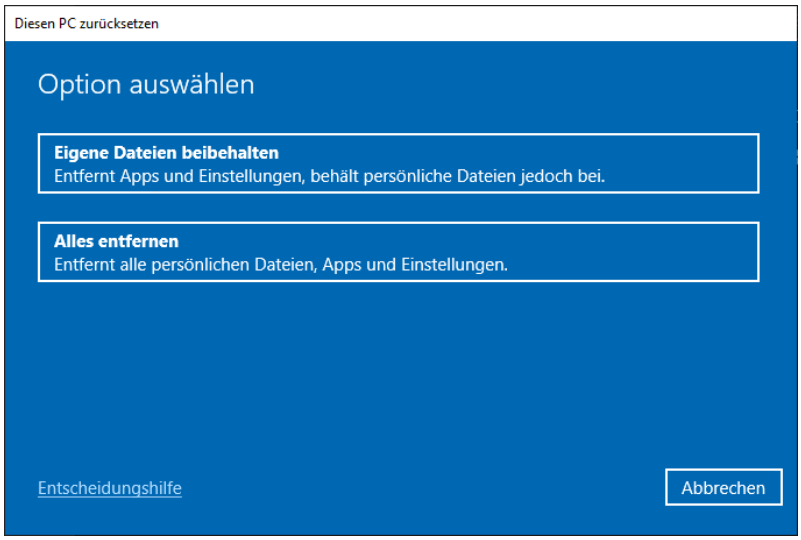


Abbildung 3: Wahl der Option beim Zurücksetzen des Systems

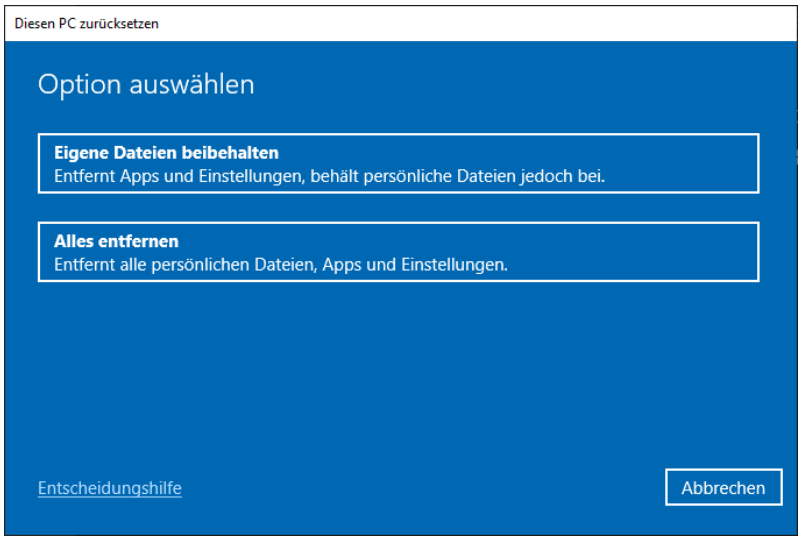


Abbildung 4: Wahl der Option bei der erneuten Installation von Windows

Nach der Neuinstallation wird ein Konto mit administrativen Rechten namens „Admin“ eingerichtet. Das Administratorenkonto wird ausschließlich für die Einrichtung des Notebooks verwendet, darunter auch die Durchführung aller verfügbaren Windows Updates. Dies liegt darin begründet, dass alle Spuren, die durch die Neuinstallation entstehen, von den gezielt gelegten Spuren des Szenarios zu unterscheiden sein sollen. Auf dem Notebook befinden sich nur die bei der Neueinrichtung durch Windows standardmäßig bereitgestellten Anwendungen. Es werden keine zusätzlichen Programme installiert.

Die Dokumente, die im Zuge der Spurenlegung vom Notebook auf den USB-Stick gespeichert werden, werden mit Hilfe eines zweiten, nicht für das Szenario relevanten USB-Stick auf dem Notebook platziert.

Nachdem das Notebook fertig eingerichtet ist, wird ein Benutzerkonto mit Namen „Merle Braun“ angelegt, das das Nutzerkonto der Tatverdächtigen innerhalb der Firmenumgebung darstellt und dementsprechend keine administrativen Rechte besitzt. Alle der in Kapitel 3.4 beschriebenen Spuren werden mit diesem Nutzerkonto gelegt.

4.2 USB-Stick

Der USB-Stick wird in Vorbereitung auf das Szenario mit dem kostenlosen Tool „Disk Wipe“ gewiped, d.h. vollständig mit Nullen überschrieben. Darüber hinaus wird dieser auf das Dateisystem „NTFS“ formatiert. Durch das Wipen wird sichergestellt, dass der USB-Stick komplett bereinigt wird und keine Spuren oder Fragmente von vorherigen Daten vorliegen.

Das Dateisystem „NTFS“ wird gewählt, da es sich dabei um ein gängiges Dateisystem unter Windows handelt. Des Weiteren kann die Verschlüsselung einer Partition unter VeraCrypt nur dann ohne vorherige Formatierung erfolgen, wenn das Dateisystem in NTFS

vorliegt. Da die Verschlüsselung des USB-Sticks nach der Spurenlegung erfolgt, d.h. die Partition bereits Daten enthält, muss das Dateisystem zwangsweise als NTFS formatiert werden.

Nachdem alle relevanten Spuren auf dem USB-Stick gelegt wurden, wird die Partition „1“ des USB-Sticks mit Hilfe des Tools „VeraCrypt“ verschlüsselt. Als Verschlüsselungsalgorithmus wird AES (Advanced Encryption Standard) gewählt. Das Passwort für die Entschlüsselung lautet „DiePfifferlinge95“.

4.3 Imageerstellung

Für die Sicherung des Notebooks wird das Tool „PALADIN EDGE“ verwendet. Dazu wird ein bootfähiges USB-Laufwerk erstellt, das es ermöglicht das Notebook über das USB-Laufwerk zu starten anstatt wie gewöhnlich über die interne Festplatte. Dieses Laufwerk enthält entweder ein bootfähiges Betriebssystem oder eine entsprechende Software. Das ISO-Abbild von PALADIN EDGE wird von der Herstellerwebseite heruntergeladen und im Anschluss mittels des Tools „Rufus“ ein bootfähiger USB-Stick erstellt. Über diesen wird das Notebook gestartet. Für die Sicherung wird das Sicherungstool „Imager“ aus der „PALADIN TOOLBOX“ verwendet. Als Optionen werden keine Fragmentierung und keine Kompression ausgewählt. Das Image wird im E01-Dateiformat erzeugt und direkt auf eine externe Festplatte geschrieben, die mit dem Notebook verbunden ist. Nach der Imageerstellung werden die von PALADIN bereitgestellten Logdateien bezüglich der Hashwerte kontrolliert, um so die Integrität des Images zu überprüfen.

Das Image des USB-Sticks wird mittels des Sicherungstools „FTK Imager“ im E01-Dateiformat erstellt. Dafür wird an der Forensik-Workstation ein Software Writeblocker gestartet, der alle Schreibzugriffe auf die noch nicht besetzten USB-Schnittstellen sperrt. So kann sichergestellt werden, dass die Integrität des USB-Sticks beim Verbinden mit der Forensik-Workstation nicht kompromittiert wird. Auch hier wird das Image ohne Kompression und ohne Fragmentierung erzeugt. Im Anschluss an die Imageerstellung werden wiederum die vom Sicherungstool errechneten Hashwerte überprüft, um die Integrität des USB-Sticks an sich und des erstellten Images zu gewährleisten.

Hinweise zum Gutachten

Das Gutachten in Kapitel 5 stellt ein in sich abgeschlossenes Dokument dar. Der Lesbarkeit halber werden die Anhänge des Gutachtens im Anhang der Praktikumsdokumentation dargestellt. Dabei handelt es sich primär um die gefundenen Dokumente, die im Zusammenhang mit dem Sachverhalt stehen. Diese werden aufgrund ihres Umfangs, falls notwendig, nur auszugsweise abgedruckt, um einen Einblick in die Inhalte und die damit verbundene Relevanz für das Szenario zu erlangen.

5 Gutachten

IT-forensisches Gutachten

Kriminalpolizei Frankfurt am Main

Auftraggeber

Staatsanwaltschaft Frankfurt am Main

Aktenzeichen

Js 2024/0517/MB2533

Sachverständige

Bob Andrews, Justus Jonas, Peter Shaw

Abschluss

24.05.2024

Polizei Präsidium Frankfurt am Main, Zur Kaffeekanne 4a, 60316 Frankfurt am Main

5.1 Untersuchungsauftrag

Die Staatsanwaltschaft Frankfurt am Main beauftragt im Rahmen eines Brandanschlags am Frankfurter Flughafen die forensische Sicherung, Aufbereitung und Auswertung der unter 5.3 aufgeführten Asservate. Darüber hinaus soll ein IT-forensisches Gutachten erstellt werden. Der vorgegebene Bearbeitungszeitraum ist vom 20.05.2024 bis zum 24.05.2024 angesetzt.

Im Rahmen der Untersuchung gilt es die nachstehenden Fragestellungen zu beantworten:

Asservat 320/24-1 „Notebook“

- Kann das Notebook in Verbindung mit der Tatverdächtigen gebracht werden?
- Kann die Tatverdächtige in Verbindung mit der Gruppierung „Die Pfifferlinge“ gebracht werden?
- Welche externen Datenträger wurden an das Notebook angeschlossen?
- Kann über das Notebook eine Kommunikation mit der Gruppierung „Die Pfifferlinge“ identifiziert werden?
- Können zur Tat vorbereitende Handlungen auf dem Notebook identifiziert werden?
- Kann ein Datenabfluss über das Notebook festgestellt werden?

Asservat 320/24-2 „USB-Stick“

- Können zur Tat relevante Dokumente auf dem USB-Stick festgestellt werden?
- Kann eine Verwendung des USB-Sticks durch die Tatverdächtige nachgewiesen werden?
- Kann eine Verbindung mit dem Asservat 320/24-1 „Notebook“ identifiziert werden?

5.2 Zusammenfassung der Untersuchung

Asservat 320/24-1 „Notebook“

Auf dem sichergestellten Notebook kann ein Benutzerkonto mit dem Namen „Merle Braun“ identifiziert werden, das durch ein Passwort geschützt ist. Dieses Benutzerkonto besitzt keine administrativen Rechte. Ob ausschließlich die Tatverdächtige auf dieses Benutzerkonto Zugriff hat, ist nicht bekannt.

Innerhalb des Webbrowsers „Microsoft Edge“ kann ein vermehrter Zugriff auf die Anwendung „Discord“ festgestellt werden. Dabei handelt es sich um einen Onlinedienst der zum Chatten und für Sprach- und Videokonferenzen genutzt werden kann. Eine lokale Installation auf dem Notebook wurde nicht gefunden. Es können insgesamt drei Kanäle auf dem Discord Server namens „Die Pfifferlinge“ erkannt werden, darunter auch einer

mit dem Namen „flughafen-frankfurt“. Dieser besitzt die meisten Zugriffe. Eine Einsicht in die Kommunikation sowie in die weiteren Teilnehmer ist nicht möglich. Augenscheinlich existiert eine Verbindung zwischen der Tatverdächtigen Merle Braun und der Gruppierung „Die Pfifferlinge“.

An dem Notebook wurde ein USB-Stick der Marke „Kingston“ angeschlossen, bei dem es sich um das Asservat 320/24-2 „USB-Stick“ handelt. Dies kann anhand der Volume Seriennummer festgestellt werden. Eine Verbindung mit dem Benutzerkonto „Merle Braun“ bestand erstmalig am 29.04.2024 und zuletzt am 08.05.2024. Zu weiteren externen Speichermedien bestand keine Verbindung.

Weitere Austauschplattformen oder Kommunikationsmittel, als die von der Fraport AG bereitgestellten Anwendungen „OneDrive“ zum Austauschen von Dokumenten und „Microsoft Outlook“ als Mailclient, können nicht identifiziert werden. Auf OneDrive kann nur mittels interner IP-Adresse, d.h. lediglich aus dem Firmennetz der Fraport AG, zugegriffen werden. Die Schlagwortsuche über das Outlook Konto der Tatverdächtigen Merle Braun führte zu keinem Ergebnis. Ein Datenabfluss über diese beiden Anwendungen kann ausgeschlossen werden. Auch findet sich kein Hinweis auf eine andere Anwendung, die zu einem Datenabfluss sensibler Dokumente und Informationen verwendet werden konnte.

Vor dem 17.05.2024 wurden vermehrt Suchanfragen in Google über den Webbrowser „Microsoft Edge“ durchgeführt, die u.a. im Zusammenhang mit der Unterbrechung von kritischen Stromversorgungen sowie der Handhabung des Alarmsystems des Frankfurter Flughafens stehen. Darüber hinaus können Google Maps Ansichten zu den Umspannwerken des Frankfurter Flughafens festgestellt werden. Diese Handlungen stehen augenscheinlich mit dem Brand des Frankfurter Flughafens in Verbindung.

Asservat 320/24-2 „USB-Stick“

Auf dem USB-Stick können Dokumenten identifiziert werden, die den Aufbau und die Struktur des Frankfurter Flughafens zeigen sowie Inhalte zum Thema Elektrotechnik und der Handhabung der Alarmanlage des Frankfurter Flughafens. Da diese Informationen in keinem Zusammenhang mit dem Aufgabenbereichs der Tatverdächtigen Merle Braun stehen, handelt es sich hierbei augenscheinlich um Dokumente, die zur Tatvorbereitung benötigt wurden.

Die Verwendung des USB-Sticks durch die Tatverdächtige sowie die Verbindung mit dem Asservat 320/24-1 „Notebook“ können durch die Artefakte auf dem Notebook nachgewiesen werden.

5.3 Untersuchungsobjekte

5.3.1 Asservat 320/24-1 „Notebook“

Hersteller: Acer

Typ: MM1-571 series

Typkennung: MM1-571-MS2612

Model: N15W4

Seriennr.: [redacted]

Abbildung 5: Asservat 320/24-1 „Notebook“ Vorderseite

Abbildung 6: Asservat 320/24-1 „Notebook“ Rückseite

Das Asservat besitzt ein CD-/DVD-Laufwerk und einen SD-Karten Slot. Hier können keine zusätzlichen externen Speichermedien festgestellt werden. Auf der Vorderseite befindet sich ein roter Aufkleber mit einer abgebildeten Hand.

5.3.2 Asservat 320/24-2 „USB-Stick“

Hersteller: Kingston

Speicherkapazität: 8 GB

Model: DTSE9

Seriennr.: -

Besonderheit: silberfarben

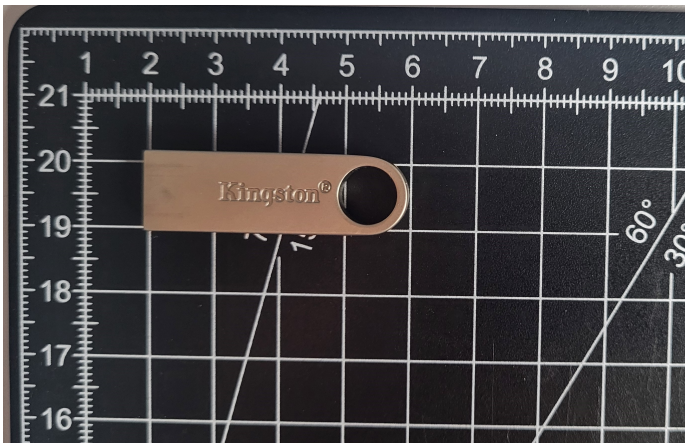


Abbildung 7: Asservat 320/24-2 „USB-Stick“ Vorderseite

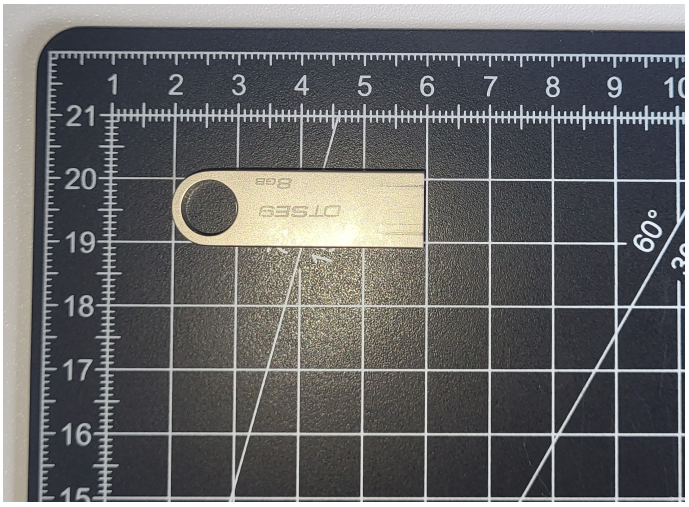


Abbildung 8: Asservat 320/24-2 „USB-Stick“ Rückseite

5.4 Untersuchungswerkzeuge

In Tabelle 2 findet sich eine Auflistung der im Rahmen der Untersuchung verwendeten Sicherungs- und Analyseanwendungen und die jeweils eingesetzte Versionierung. Für die

Dokumentation der Ergebnisse werden Bildschirmaufnahmen aus dem Untersuchungswerkzeug „Magnet AXIOM“ angefertigt.

Hersteller	**Anwendung**	**Version**	**Zweck**
ForensicSoft	SAFE Block	1.0.0.109	Schreibschutz
Exterro	FTK Imager	4.7.1.2	Sicherung
Sumuri	PALADIN EDGE	8.01	Sicherung
Magnet Forensics	AXIOM	8.0.1	Aufbereitung, Auswertung

Tabelle 2: Verwendete Untersuchungswerkzeuge

5.5 Vorbereitung der Untersuchung

Die Sicherung des Asservats 320/24-1 „Notebook“ erfolgt mittels PALADIN EDGE, die Sicherung des Asservats 320/24-2 „USB-Stick“ mit dem FTK Imager.

Beide Asservate werden mit Magnet AXIOM aufbereitet. Bei der Aufbereitung wird die in AXIOM integrierte Schlüsselwortsuche eingesetzt. Dabei wird die folgende Schlagwortliste, die vom Auftraggeber bereitgestellt wurde, verwendet:

- Pfifferlinge
- Flughafen
- Anschlag
- Stromausfall
- Strom
- Brand
- Feuer
- Frankfurt am Main

Durch die Schlagworte können Artefakte, die in Bezug zu dem Sachverhalt stehen, einfacher und schneller identifiziert werden.

Weiterhin werden die nachstehenden Kategorien für die Analyse von Bilddateien durch Magnet.AI ausgewählt. Bei Magnet.AI handelt es sich um die in AXIOM enthaltene KI, die Objekte in Bildern erkennen und klassifizieren kann.

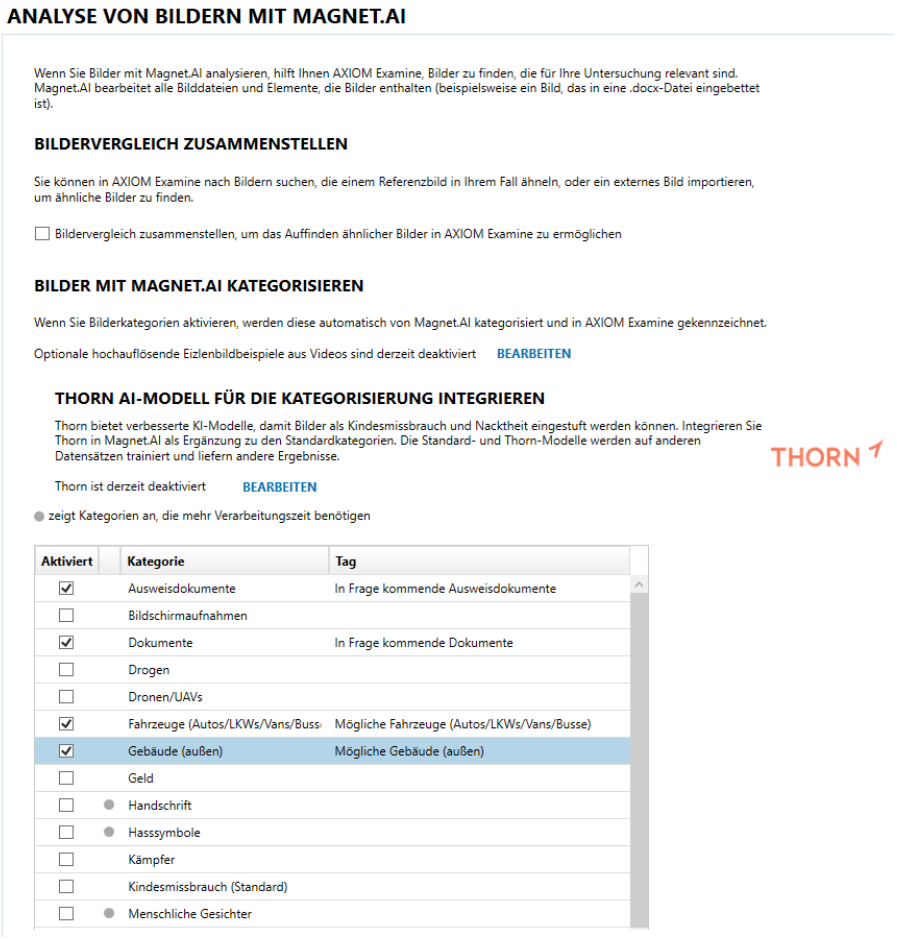


Abbildung 9: Kategorisierung mittels Magnet.AI in AXIOM

Das Asservat 320/24-2 „USB-Stick“ weist eine Verschlüsselung der Partition „1“ auf. Diese kann innerhalb von AXIOM mit dem bekannten Passwort „DiePfifferling95“ entschlüsselt werden. Dazu wird der Persönliche Iterationsfaktor (kurz PIM) „485“ mitgegeben. Bei dem PIM handelt es sich um einen Iterationsmultiplikator, der von der Anwendung „VeraCrypt“ verwendet wird, wenn die Länge des vergebenen Passworts weniger als 20 Zeichen entspricht. VeraCrypt ist eine kostenlose Anwendung, die zur vollständigen oder partiellen Verschlüsselung von Speichermedien, wie Festplatten oder USB-Sticks, verwendet werden kann. Der Wert „485“ bildet die von VeraCrypt standardmäßig vergebene Mindestgröße der PIM bei Containern ab.

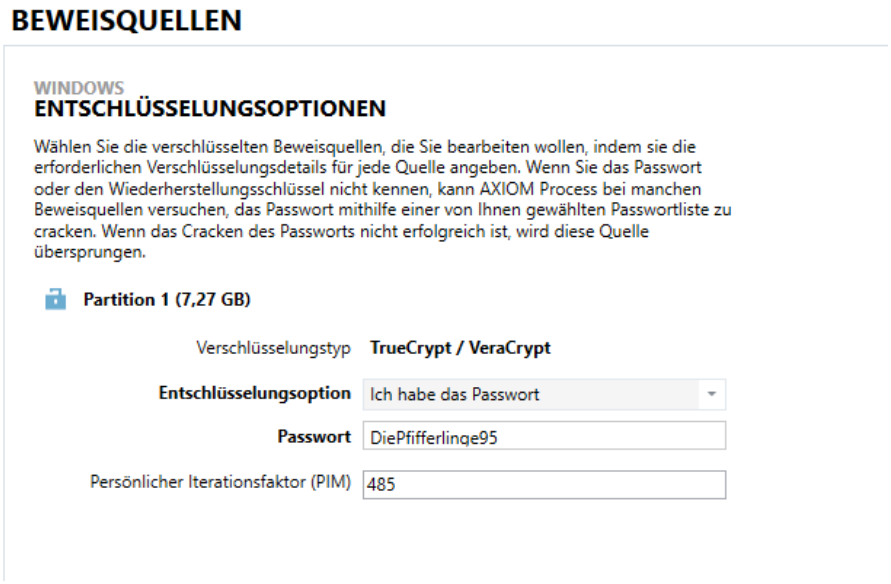


Abbildung 10: Entschlüsselung der Partition „1“ des USB-Sticks in AXIOM

5.6 Untersuchung Asservat 320/24-1 „Notebook“

Auf dem Asservat werden insgesamt 604.348 Artefakte festgestellt, die wie nachstehend abgebildet klassifiziert wurden.

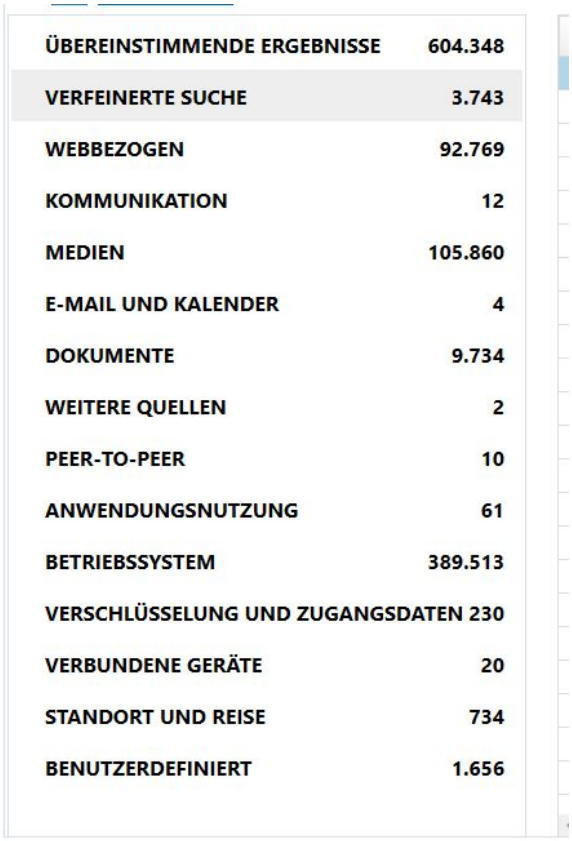


Abbildung 11: Übersicht der Artefakte des Notebooks

5.6.1 Image-Integrität

Die Integritätsprüfung wird mittels der von PALADIN bereitgestellten Logdateien durchgeführt. Hier werden die MD5- und SHA1-Hashes des Images und des Asservats dokumentiert.

```
**************************
Verification
**************************
MD5 hash stored in file:                92edb1a6a307b7e31194afdf25fedc52
MD5 hash calculated over data:          92edb1a6a307b7e31194afdf25fedc52
SHA1 hash stored in file:               13b0b178948856e2be9eab8a1a4dbe4208f81029
SHA1 hash calculated over data:         13b0b178948856e2be9eab8a1a4dbe4208f81029
```

Abbildung 12: Hashes aus PALADIN zur Integritätsprüfung

Diese sind identisch. Somit stellt das Image eine 1:1 Kopie des Asservats dar und die Integrität ist gegeben.

5.6.2 Systeminformationen

Das Notebook weist insgesamt vier Partitionen auf. Die vierte Partition besitzt eine Größe von 466 GB und ist ein NTFS Dateisystem.

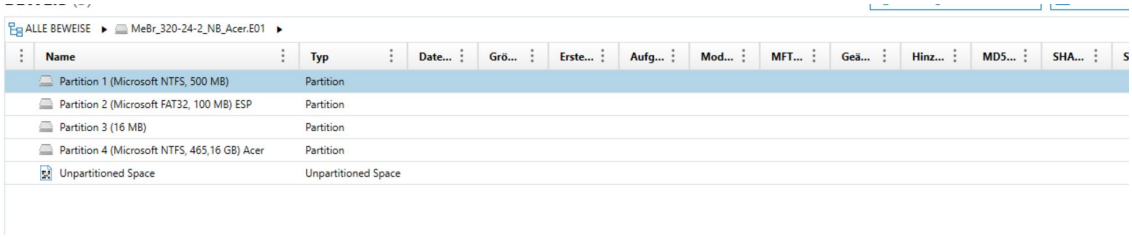


Abbildung 13: Vorhandene Partitionen des Notebooks

Hier befindet sich das installierte Betriebssystem, das ein „Windows 10 Home“ ist. Der Computername lautet „LAPTOP-6V59GTNV“. Das Asservat wurde am 19.05.2024 um 11:56:29 Uhr das letzte Mal heruntergefahren. An diesem Tag fand die Sicherstellung des Asservates statt.

Windows 10 Home (2009)

ARTEFAKTINFORMATIONEN

Betriebssystem	**Windows 10 Home (2009)**
Versionsnummer	**6.3**
Installiert/aktualisiert – Datum/Zeit	**26.03.2024 20:01:18,000**
Produktschlüssel	[redacted]
Besitzer	**Admin**
Angezeigter Computername	**LAPTOP-6V59GTNV**
Computername	**LAPTOP-6V59GTNV**
DHCP-DNS-Server	**192.168.2.1**
Betriebssystemversion	**Core**
Build-Nummer	**19045**
Produkt-ID	**00325-80562-17503-AAOEM**
Zuletzt heruntergefahren – Datum/Zeit	**19.05.2024 11:56:29,000**
System Root	**C:\WINDOWS**
Pfad	**C:\WINDOWS**
Zeit des letzten Zugriffs aktiviert	**System Managed - Last Access Updates Enabled**
Kontrollsettyp	**Current**
Typ	Betriebssystem
Objekt-ID	385898

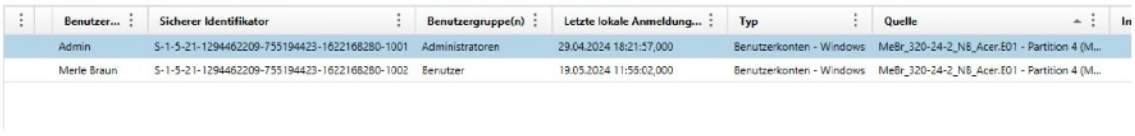
BEWEISINFORMATIONEN

Quelle	MeBr_320-24-2_NB_Acer.E01 - Partition 4 (Microsoft NTFS, 465,16 GB) Acer\Windows\System32\config\SOFTWARE

Abbildung 14: Systeminformationen des Notebooks

5.6.3 Benutzerzuordnung

Die Identifizierung der angelegten Benutzerkonten erfolgt mittels der Windows-Registry. Bei der Windows-Registry (z.Dt. Registrierungsdatenbank) handelt es sich um die zentrale Struktur des Windows Betriebssystems, die u.a. die Einstellungen und Konfigurationen enthält. Das Notebook besitzt zwei Benutzerkonten, darunter auch eines mit dem Namen „Merle Braun“.



Benutzer...	Sicherer Identifikator	Benutzergruppe(n)	Letzte lokale Anmeldung...	Typ	Quelle	In
Admin	S-1-5-21-1294462209-755194423-1622168280-1001	Administratoren	29.04.2024 18:21:57,000	Benutzerkonten - Windows	MeBr_320-24-2_NB_Acer.E01 - Partition 4 (M...	
Merle Braun	S-1-5-21-1294462209-755194423-1622168280-1002	Benutzer	19.05.2024 11:56:02,000	Benutzerkonten - Windows	MeBr_320-24-2_NB_Acer.E01 - Partition 4 (M...	

Abbildung 15: Angelegte Benutzerkonten des Notebooks

Der SID (Security Identifier), der eine eindeutige Kennung von Benutzern und Objekten unter Windows darstellt, lautet beim Benutzerkonto „Merle Braun“ „S-1-5-21-1294462209-755194423-1622168280-1002“. Dieses besitzt keine administrativen Rechte und war das letzte Mal am 19.05.2024 um 11:56:02 Uhr angemeldet. Dies deckt sich mit dem Zeitpunkt

des letzten Herunterfahrens des Notebooks. Das Benutzerkonto „Merle Braun“ war somit das zuletzt angemeldete Konto. Das Benutzerkonto „Admin“ war zuletzt am 29.04.2024 um 18:21:57 Uhr angemeldet und verfügt über Administratorrechte.

5.6.4 Medien und Dokumente

Auf dem Notebook werden vermehrt Zugriffe auf Bild- und PDF-Dateien festgestellt. Die Dateinamen stehen augenscheinlich entweder mit Plänen des Frankfurter Flughafens im Zusammenhang, darunter bspw. ein Gebäudeplan oder der Flugplan für den 17.05.2024, oder mit Handbüchern aus dem Bereich der Gebäudesicherheit oder Stromversorgung. Im Folgenden findet sich eine tabellarische Darstellung der identifizierten Medien- und Dokumentdateien. Diese können dem Anhang entnommen werden.

Ordner	**Dateiname**	**Dateityp**
`04_Fluchtwegeplan`	Fluchttürsteuerung	pdf
	Fluchtwegeplan	jpg
`05_Grundstuckplan_Frankfurt_Flughafen`	Grundstückplan Frankfurt Flughafen	png
	Uebersicht-airport-city-frankfurt	pdf
`06_Gebäudeplan Frankfurt Flughafen`	Gebäudeplan Frankfurt Flughafen	pdf
	Lageplan Besucherzentrum Fraport	jpg
`07_Handbuch_Alarmanlage`	Abus Alarmanlage	pdf
	EESec2 Handbuch Alarmanlage	pdf
`08_Stromversorgung`	Betriebsspezifische Schaltpläne	pdf
	Grundwissen Elektronik	pdf
	Stromversorgungsplan	jpg
`09_Handbuch_Notstromaggregat`	Bedienungsanleitung Eisemann Notstromaggregat	pdf
`10_Flughafenordnung`	C2.2 Umwelt-, Sicherheits- und Schutzregeln	pdf
	C4.3 Ausweisordnung	pdf
	C4.6 Sicherheitsmanagement-Systems des Verkehrsflughafens	pdf
	C4.8 Brandschutzordnung	pdf

11_Struktur_und_Organigramm	Fraport Group Struktur	jfif
	FraSec Sicherheitsdienst	png
	Gesamtorganigramm Fraport	pdf
12_Flugplan_17.05_-_15_15	Abflüge 17.05	pdf
	Ankünfte 17.05	pdf
13_Mietwagenbuchung	Mietwagenbuchung	pdf

Tabelle 3: Identifizierte Medien und Dokumente mit verdächtigem Inhalt

Auf diese Dateien wurde lokal mit dem Benutzerkonto „Merle Braun“ in einem Zeitraum vom 29.04.2024 bis zum 08.05.2024 zugegriffen.

Pfad	Pfadt...	Datum/Zeit...	Benu...	Typ	Quelle
C:\Users\Public\Documents\04_Fluchtwegeplan\04 Fluchtweg...	Drive	2024-05-01 15:38:23	Merle Braun	Dateien und Ordner, auf die lokal zugegriffen...	MeBr_320-24-2_NB_Acer.E01 - Partition 4 (Microsoft...
C:\Users\Public\Documents\05_Grundstuckplan_Frankfurt_Flu...	Drive	2024-04-29 20:25:49	Merle Braun	Dateien und Ordner, auf die lokal zugegriffen...	MeBr_320-24-2_NB_Acer.E01 - Partition 4 (Microsoft...
C:\Users\Public\Documents\06_Gebaudeplan_Frankfurt_Flugh...	Drive	2024-04-29 20:25:31	Merle Braun	Dateien und Ordner, auf die lokal zugegriffen...	MeBr_320-24-2_NB_Acer.E01 - Partition 4 (Microsoft...
C:\Users\Public\Documents\07_Handbuch_Alarmanlage\07 H...	Drive	2024-05-01 15:39:00	Merle Braun	Dateien und Ordner, auf die lokal zugegriffen...	MeBr_320-24-2_NB_Acer.E01 - Partition 4 (Microsoft...
C:\Users\Public\Documents\11_Struktur_und_Organigramm\1...	Drive	2024-05-08 18:44:40	Merle Braun	Dateien und Ordner, auf die lokal zugegriffen...	MeBr_320-24-2_NB_Acer.E01 - Partition 4 (Microsoft...

Abbildung 16: Lokaler Zugriff mit Benutzerkonto „Merle Braun“

Darüber hinaus kann der Download von weiteren Dokumenten, die augenscheinlich in Bezug zu der Stromversorgung des Frankfurter Flughafens stehen, von der Webseite „https://www.fraport.com“ ermittelt werden, die die offizielle Webseite der Fraport AG darstellt. Diese Dokumente befinden sich im Ordner „C:\Users\Merle Braun\Downloads“ und wurden am 28.04.2024 heruntergeladen.

Download-Quelle	Dateiname	Startzeit – Dat...	Gespeichert unter	Typ	Quelle
https://www.fraport.com/content/dam/fraport...	FAG_HVM-IE2_Hochlastzeitfenster-2024_01.pdf	28.04.2024 13:22:51,...	C:\Users\Merle Braun\Downloads\FAG_HVM-IE2_Ho...	Edge Chromium Downloads	MeBr_320-24-2_NB_Acer.E01 - Partition 4 (Microsoft...
https://www.fraport.com/content/dam/fraport...	FAG_Netzrelevante-Daten-2023.pdf	28.04.2024 13:22:02,...	C:\Users\Merle Braun\Downloads\FAG_Netzrelevant...	Edge Chromium Downloads	MeBr_320-24-2_NB_Acer.E01 - Partition 4 (Microsoft...
https://www.fraport.com/content/dam/fraport...	Stromnetz Strukturangaben 2023.pdf	28.04.2024 13:22:05,...	C:\Users\Merle Braun\Downloads\Stromnetz Struktu...	Edge Chromium Downloads	MeBr_320-24-2_NB_Acer.E01 - Partition 4 (Microsoft...

Abbildung 17: Download im Webbrowser „Microsoft Edge“

5.6.5 Browserverlauf

Der auf dem Asservat gesetzte Standardbrowser ist Microsoft Edge. Dieser wurde letztmalig am 18.05.2024 um 10:23:30 Uhr verwendet.

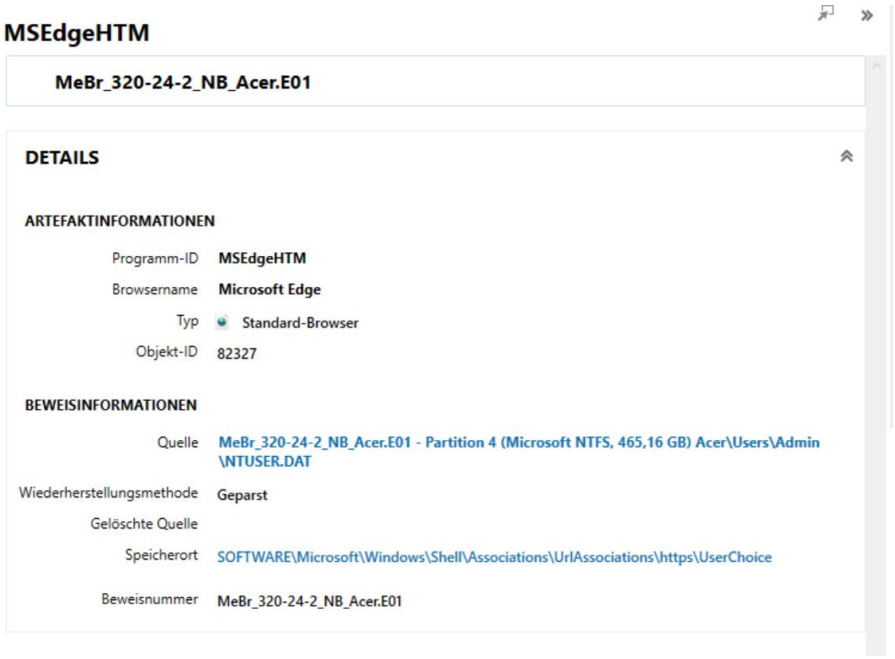


Abbildung 18: „Microsoft Edge“ als Standardbrowser des Notebooks

Innerhalb des Edge können Suchanfragen über die Suchmaschine „Google“ festgestellt werden. Betrachtet man die in AXIOM als „Google Suche“ klassifizierten Suchanfragen, decken sich diese mit den in Edge identifizierten Suchbegriffen, sodass darauf geschlossen werden kann, dass die Suchanfragen mittels Google im Edge Browser durchgeführt wurden. Die Google Suchanfragen erstrecken sich über einen Zeitraum vom 27.04.2024 bis zum 18.05.2024 und haben somit sowohl vor als auch nach der Tat stattgefunden. Hierbei können wesentliche inhaltliche Unterschiede identifiziert werden, die durch den nachfolgenden Auszug verdeutlicht werden sollen.

Suchbegriff	URL	Datum/Zeit	Typ	Artefakt	Quelle
kritis ausfall auswirkungen	https://www.google.com/search?...	27.04.2024 13:39:31...	Google Suche	Edge Chromium Web Visits	MeBr_320-24-2_NB_Acer.E01 - Partition 4...
kritis ausfall schadenshöhe	https://www.google.com/search?...	27.04.2024 13:48:17...	Google Suche	Edge Chromium Web Visits	MeBr_320-24-2_NB_Acer.E01 - Partition 4...
frankfurt flughafen stromversorgung	https://www.google.com/search?...	28.04.2024 13:07:40...	Google Suche	Edge Chromium Web Visits	MeBr_320-24-2_NB_Acer.E01 - Partition 4...
Bodenstromversorgung sabotage	https://www.google.com/search?...	28.04.2024 13:18:43...	Google Suche	Edge Chromium Web Visits	MeBr_320-24-2_NB_Acer.E01 - Partition 4...
Frankfurt Flughafen Notstromaggregat	https://www.google.com/search?...	28.04.2024 13:21:01...	Google Suche	Edge Chromium Web Visits	MeBr_320-24-2_NB_Acer.E01 - Partition 4...
trafobrand industrie	https://www.google.com/search?...	30.04.2024 15:50:23...	Google Suche	Edge Chromium Web Visits	MeBr_320-24-2_NB_Acer.E01 - Partition 4...
blackout industrie frankfurt	https://www.google.com/search?...	30.04.2024 15:55:38...	Google Suche	Edge Chromium Web Visits	MeBr_320-24-2_NB_Acer.E01 - Partition 4...
notstromaggregat industrie funktionsweise	https://www.google.com/search?...	01.05.2024 13:28:23...	Google Suche	Edge Chromium Web Visits	MeBr_320-24-2_NB_Acer.E01 - Partition 4...
stromversorgung unterbrechen	https://www.google.com/search?...	01.05.2024 13:35:31...	Google Suche	Edge Chromium Web Visits	MeBr_320-24-2_NB_Acer.E01 - Partition 4...
abus alarmanlage deaktivieren	https://www.google.com/search?...	04.05.2024 16:54:21...	Google Suche	Edge Chromium Web Visits	MeBr_320-24-2_NB_Acer.E01 - Partition 4...
alarmanlage eesec2 deaktivieren	https://www.google.com/search?...	04.05.2024 17:04:26...	Google Suche	Edge Chromium Web Visits	MeBr_320-24-2_NB_Acer.E01 - Partition 4...
alarmanlage ausschalten fluchttüren	https://www.google.com/search?...	04.05.2024 17:06:41...	Google Suche	Edge Chromium Web Visits	MeBr_320-24-2_NB_Acer.E01 - Partition 4...
auto mieten anonym frankfurt	https://www.google.com/search?...	05.05.2024 14:36:22...	Google Suche	Edge Chromium Web Visits	MeBr_320-24-2_NB_Acer.E01 - Partition 4...
umspannwerk frankfurt flughafen	https://www.google.com/search?...	06.05.2024 18:16:12...	Google Suche	Edge Chromium Web Visits	MeBr_320-24-2_NB_Acer.E01 - Partition 4...
frankfurt flughafen flugplan 17.05	https://www.google.com/search?...	06.05.2024 18:22:31...	Google Suche	Edge Chromium Web Visits	MeBr_320-24-2_NB_Acer.E01 - Partition 4...
Frankfurt Flughafen Stromausfall Reaktionen	https://www.google.de/search?sc...	18.05.2024 10:37:10...	Google Suche	Edge Chromium Web Visits	MeBr_320-24-2_NB_Acer.E01 - Partition 4...
Frankfurt Flughafen Stromausfall Schaden	https://www.google.de/search?q...	18.05.2024 10:37:21...	Google Suche	Edge Chromium Web Visits	MeBr_320-24-2_NB_Acer.E01 - Partition 4...
Die Pfifferlinge Frankfurt Stromausfall	https://www.google.de/search?q...	18.05.2024 10:37:59...	Google Suche	Edge Chromium Web Visits	MeBr_320-24-2_NB_Acer.E01 - Partition 4...
Wer sind die Pifferlinge	https://www.google.de/search?q...	18.05.2024 10:38:15...	Google Suche	Edge Chromium Web Visits	MeBr_320-24-2_NB_Acer.E01 - Partition 4...

Abbildung 19: Suchbegriffe in Google im Webbrowser „Microsoft Edge“

Zudem können Google Maps Anfragen, die sich auf die Umgebung rund um den Frankfurter Flughafen beschränken, gefunden werden. Diese wurden ebenfalls mit dem Edge Browser ausgeführt.

Suchanfrage	Datum/Zeit	Breit...	Läng...	Typ	Artefakt	Quelle
Flughafen Frankfurt (FRA), Frankfurt am Main	05.05.2024 14:30:14...	51.1967232	6.7928064	Google Maps Abfragen	Edge Chromium Web Visits	MeBr_320-24-2_NB_Acer.E01 - Partition 4 (Microsoft...
Flughafen Frankfurt	05.05.2024 14:30:15...	50.0377594	8.5565778	Google Maps Abfragen	Edge Chromium Web Visits	MeBr_320-24-2_NB_Acer.E01 - Partition 4 (Microsoft...
Aussichtsplattform Zeppelinheim Planespotting	05.05.2024 14:31:05...	50.0504	8.5792	Google Maps Abfragen	Edge Chromium Web Visits	MeBr_320-24-2_NB_Acer.E01 - Partition 4 (Microsoft...
50°09'33.2"N 8°44'07.2"E	06.05.2024 18:14:43...	50.15923	8.73533	Google Maps Abfragen	Edge Chromium Web Visits	MeBr_320-24-2_NB_Acer.E01 - Partition 4 (Microsoft...
50°05'32.0"N 8°37'07.0"E	06.05.2024 18:14:51...	50.092222	8.618611	Google Maps Abfragen	Edge Chromium Web Visits	MeBr_320-24-2_NB_Acer.E01 - Partition 4 (Microsoft...
Flughafen Frankfurt	06.05.2024 18:20:09...	50.040351	8.5557481	Google Maps Abfragen	Edge Chromium Web Visits	MeBr_320-24-2_NB_Acer.E01 - Partition 4 (Microsoft...
Frankfurt Bahnhof Flughafen, Frankfurt am Mai...	06.05.2024 18:20:19...	50.040351	8.5557481	Google Maps Abfragen	Edge Chromium Web Visits	MeBr_320-24-2_NB_Acer.E01 - Partition 4 (Microsoft...

Abbildung 20: Suchen in Google Maps im Webbrowser „Microsoft Edge“

Die beiden abgebildeten Koordinaten stellen augenscheinlich Umspannwerke in Frankfurt am Main dar.

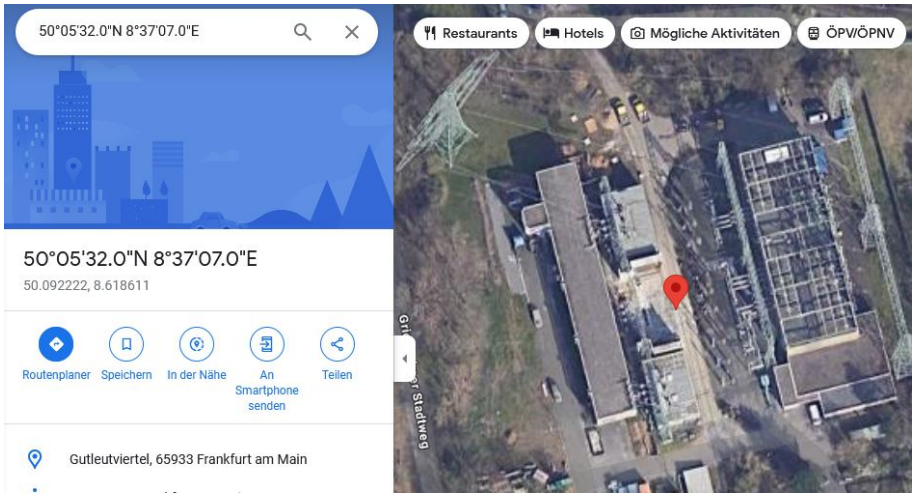


Abbildung 21: Koordinate „50°05’32.0”N 8°37’07.0”E“ in Google Maps

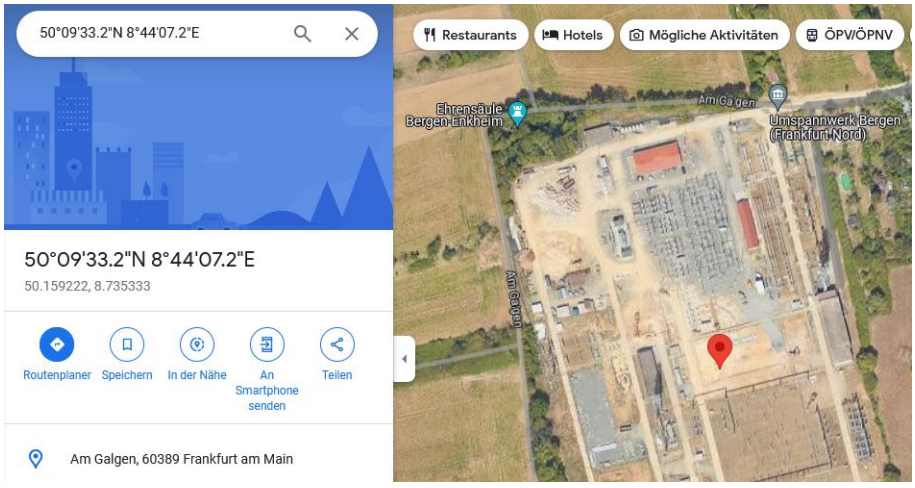


Abbildung 22: Koordinate „50°09’33.2”N 8°44’07.2”E“ in Google Maps

Ebenfalls über den Edge Browser können Aufrufe der Chat- und Kommunikationsplattform „Discord“ ausgemacht werden. Auf dem Server mit der Bezeichnung „Die Pfifferlinge“ können drei Chatkanäle identifiziert werden. Darunter auch ein Kanal, der „flughafen-frankfurt“ lautet. Auf diesen Kanal wurde insgesamt siebenmal zugegriffen.

URL	Zuletzt besuc...	Titel	Besuchsanzahl	Typ	Quelle
https://discord.com/	18.05.2024 10:38:25...	Discord | Ein Ort zum Treffen und zum Unterhalten	4	Edge Chromium Webverlauf	MeBr_320-24-2_NB_Acer.E01 - Partition 4 (Microsoft...
https://discord.com/login	08.05.2024 16:46:16...	Discord	5	Edge Chromium Webverlauf	MeBr_320-24-2_NB_Acer.E01 - Partition 4 (Microsoft...
https://discord.com/app	08.05.2024 16:46:47...	Discord	3	Edge Chromium Webverlauf	MeBr_320-24-2_NB_Acer.E01 - Partition 4 (Microsoft...
https://discord.com/channels/@me	18.05.2024 10:38:37...	• Discord | Freunde	4	Edge Chromium Webverlauf	MeBr_320-24-2_NB_Acer.E01 - Partition 4 (Microsoft...
https://discord.com/channels/1230...	08.05.2024 16:47:01...	Discord | #Allgemein | Die Pfifferlinge	5	Edge Chromium Webverlauf	MeBr_320-24-2_NB_Acer.E01 - Partition 4 (Microsoft...
https://discord.com/channels/1230...	27.04.2024 14:06:02...	Discord | #wald-und-wiesen-aktionen | Die Pfifferlin...	4	Edge Chromium Webverlauf	MeBr_320-24-2_NB_Acer.E01 - Partition 4 (Microsoft...
https://discord.com/channels/1230...	18.05.2024 10:38:49...	Discord | #flughafen-frankfurt | Die Pfifferlinge	7	Edge Chromium Webverlauf	MeBr_320-24-2_NB_Acer.E01 - Partition 4 (Microsoft...

Abbildung 23: Anwendung „Discord“ im Webverlauf von Edge

Der letzte Zugriff auf den Kanal „flughafen-frankfurt“ erfolgte am 18.05.2024.

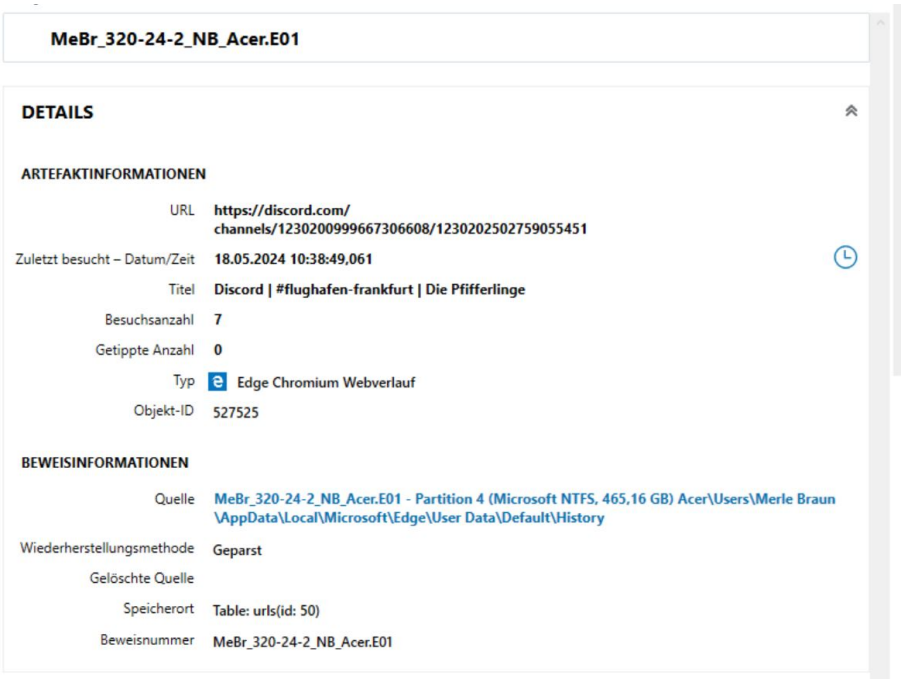


Abbildung 24: Details des Discord Kanals „frankfurt-flughafen“

5.6.6 Verbundene Geräte

Unter den mit dem Notebook verbundenen Geräten kann ein USB-Stick der Marke „Kingston“ erfasst werden. Der Zugriff auf diesen erfolgte mit dem Benutzerkonto „Merle Braun“. Die initiale Verbindung mit dem Asservat fand am 29.04.2024 um 18:24:17 Uhr statt, die letzte Verbindung am 08.05.2024 um 16:45:22 Uhr. Die Seriennummer lautet „001BFC3653 BCEEB0191BD8F3&0“.

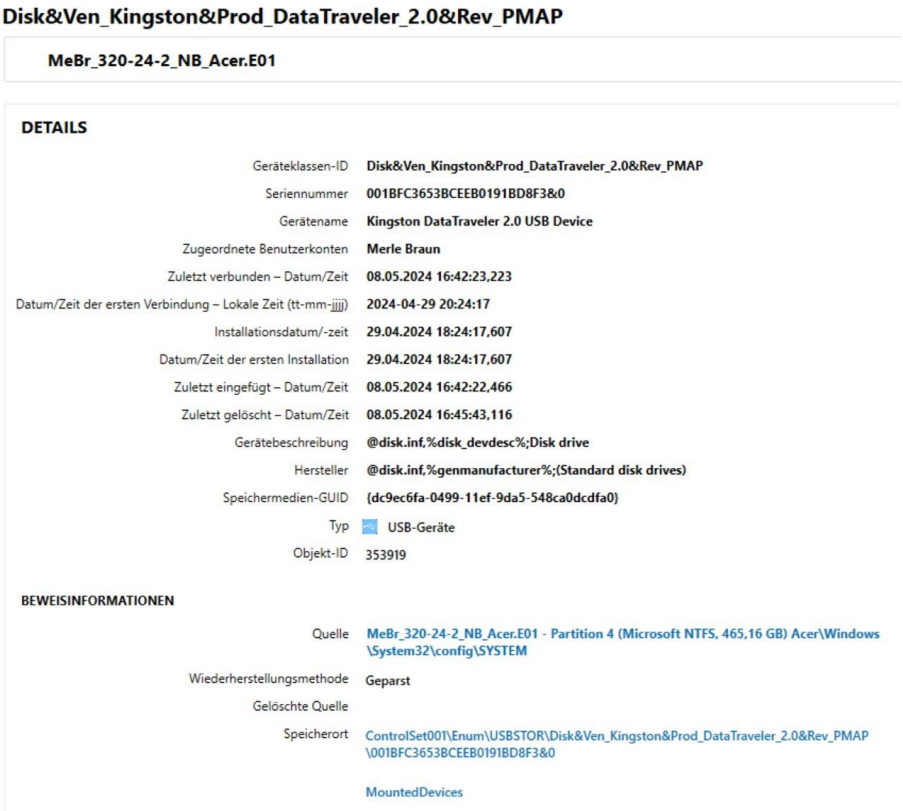


Abbildung 25: Verbundener Kingston USB-Stick

Diesem USB-Stick kann ein Volume mit der Seriennummer „5C785DA5“ zugeordnet werden. Es gehört zu einem Datenträger der Marke „Kingston“, dem Modell „DataTravler 2.0“ und wurde am 29.04.2024, 01.05.2024 und dem 08.05.2024 an dem Notebook verwendet. Die Seriennummer des Volumes deckt sich mit der des Asservats 320/24-2 „USB-Stick“.

Datum/Zeit d...	Hersteller	Modell	Seriennummer...	Typ	Quelle
01.05.2024 13:27:14...	Kingston	DataTraveler 2.0	5C785DA5	Windows-Ereignisprotokolle – Speichergerätereignisse	MeBr_320-24-2_NB_Acer.E01 - Partition 4 (...
01.05.2024 13:46:13...	Kingston	DataTraveler 2.0		Windows-Ereignisprotokolle – Speichergerätereignisse	MeBr_320-24-2_NB_Acer.E01 - Partition 4 (...
08.05.2024 16:42:22...	Kingston	DataTraveler 2.0	5C785DA5	Windows-Ereignisprotokolle – Speichergerätereignisse	MeBr_320-24-2_NB_Acer.E01 - Partition 4 (...
29.04.2024 18:26:39...	Kingston	DataTraveler 2.0		Windows-Ereignisprotokolle – Speichergerätereignisse	MeBr_320-24-2_NB_Acer.E01 - Partition 4 (...
08.05.2024 16:45:43...	Kingston	DataTraveler 2.0		Windows-Ereignisprotokolle – Speichergerätereignisse	MeBr_320-24-2_NB_Acer.E01 - Partition 4 (...
29.04.2024 18:24:17...	Kingston	DataTraveler 2.0	5C785DA5	Windows-Ereignisprotokolle – Speichergerätereignisse	MeBr_320-24-2_NB_Acer.E01 - Partition 4 (...

Abbildung 26: Volume Seriennummer zum Kingston USB-Stick

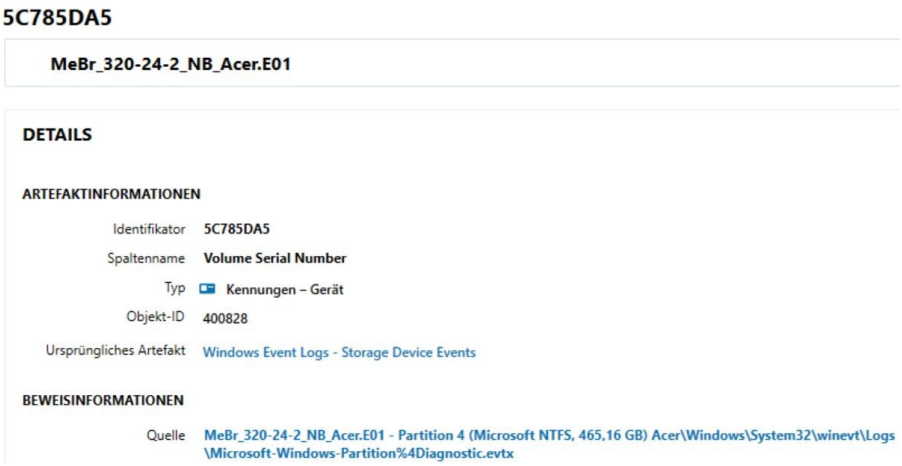


Abbildung 27: Volume zum Kingston USB-Stick

Der Anschluss weiterer externer Speichermedien kann nicht festgestellt werden.

5.6.7 Kommunikation

Die Fraport AG verwendet für die interne Kommunikation das Mailprogramm „Microsoft Outlook“ und für den Austausch von Dokumenten den Cloud-Dienst „Microsoft OneDrive“. Auf OneDrive kann nur mittels einer internen IP-Adresse zugegriffen werden, sodass der Zugriff von außerhalb der Organisation unterbunden wird. Der Aufruf anderer Cloud-Dienste, wie bspw. Dropbox oder Google Drive, wird über eine Blacklist verhindert. Bei einer Blacklist handelt es sich um einen Filter zum Ausschluss von Strukturen, wie z.B. IP-Adressen, Webseiten oder Mailadressen. Der Zugriff auf Social Media Plattformen, wie Facebook oder Instagram, wird ebenfalls über Blacklists eingeschränkt. Eine Volltextsuche über die Kommunikation innerhalb des Mailprogramms ergab keinen Treffer. Dabei wurden die Schlüsselworte unter 5.5 verwendet. Es können keine weiteren Kommunikationsmittel mit der Gruppierung „Die Pfifferlinge“ auf dem Notebook gefunden werden.

5.6.8 Anwendungen

Auf dem Asservat können neben den im Umfang eines Microsoft Windows Betriebssystems enthaltenen Standardprogramme keine zusätzlichen Programme identifiziert werden.

5.7 Untersuchung Asservat 320/24-2 „USB-Stick“

5.7.1 Image-Integrität

Die Integritätsprüfung wird mit Hilfe den vom FTK Imager bereitgestellten „Drive/Image Verify Results“ im Anschluss an die Imageerstellung durchgeführt. Es werden die MD5 und SHA-1 Hashes des Asservates vor der Imageerstellung, nach der Imageerstellung und die MD5- und SHA1-Hashes des Images berechnet und dokumentiert.

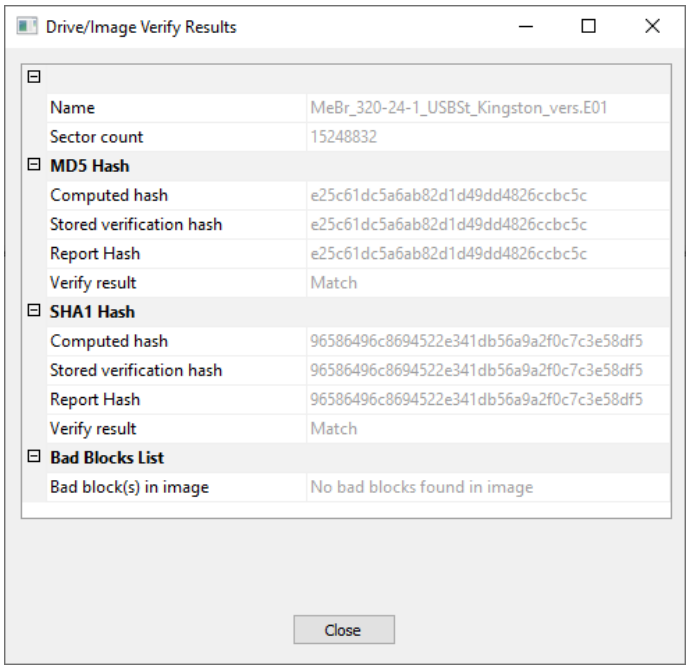


Abbildung 28: Hashes aus dem FTK Imager zur Integritätsprüfung

Die Hashwerte sind identisch. Somit ist die Integrität des Asservats und des Images gegeben.

5.7.2 Allgemeine Informationen

Auf dem Asservat befindet sich eine Partition mit dem Dateiformat „NTFS“, die verschlüsselt ist. Das Passwort ist bekannt und lautet „DiePfifferlinge95“. Durch das vorliegende Passwort kann AXIOM die Partition „1“ entschlüsseln und anschließend aufbereiten.

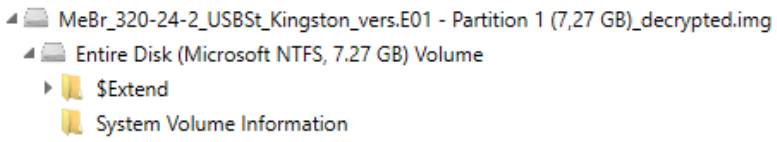


Abbildung 29: Vorhandene Partitionen des USB-Sticks

Die Partition „1“ hat eine Größe von 7,27 GB.

Die Seriennummern des Volumes lauten „5C785DA5“ und „565C78815C785DA5“. Damit handelt es sich um den USB-Stick der mit dem Asservat 320/24-1 „Notebook“ verbunden war.

ARTIFACT INFORMATION

Volume Serial Number	**5C785DA5**
Full Volume Serial Number	**565C78815C785DA5**
File System	**Microsoft NTFS**
Sectors per cluster	**8**
Bytes per sector	**512**
Starting Sector	**0**
Ending Sector	**15240254**
Total Sectors	**15240254**
Total Clusters	**1905031**
Free Clusters	**1886287**
Total Capacity (Bytes)	**7803006976**
Unallocated Area (Bytes)	**7726231552**
Allocated Area (Bytes)	**76775424**
Volume Name	**Volume**
Volume Offset (Bytes)	**0**
Artifact type	**File System Information**
Item ID	**1**

Abbildung 30: Seriennummern des Volumes des USB-Sticks

Logisch befinden sich die in Abbildung 31 dargestellten Dateien auf dem Asservat. Es sind keine gelöschten Daten vorhanden.

Name	Typ	Dateierweiterung	Größe (Byte)	Erstellt	Aufgerufen
Gesamtorganigramm Fraport.pdf	File	.pdf	51.528	08.05.2024 16:44:50,899	08.05.2024 16:44:50,899
FraSec Sicherheitsdienst.png	File	.png	796.702	08.05.2024 16:44:50,712	08.05.2024 16:44:50,884
Fraport Group Struktur.jfif	File	.jfif	277.031	08.05.2024 16:44:50,665	08.05.2024 16:44:50,696
C4.8 Brandschutzordnung.pdf	File	.pdf	840.445	08.05.2024 16:44:16,924	08.05.2024 16:44:16,955
C4.6 Sicherheitsmanagement-Systems des Verke...	File	.pdf	2.137.685	08.05.2024 16:44:16,721	08.05.2024 16:44:16,892
C4.3 Ausweisordnung.pdf	File	.pdf	834.655	08.05.2024 16:44:16,611	08.05.2024 16:44:16,705
C2.2 Umwelt-, Sicherheits- und Schutzregeln.pdf	File	.pdf	9.229.483	08.05.2024 16:44:16,142	08.05.2024 16:44:16,611
Bedienungsanleitung Eisemann Notstromaggre...	File	.pdf	10.882.640	08.05.2024 16:43:51,051	08.05.2024 16:43:52,051
Stromversorgungsplan.jpg	File	.jpg	488.917	08.05.2024 16:43:42,380	08.05.2024 16:43:42,427
Grundwissen Elektronik.pdf	File	.pdf	6.686.287	08.05.2024 16:43:41,755	08.05.2024 16:43:42,380
Betriebsspezifische Schaltpläne.pdf	File	.pdf	1.392.711	08.05.2024 16:43:41,536	08.05.2024 16:43:41,739
EESec2 Handbuch Alarmanlage.pdf	File	.pdf	7.840.320	01.05.2024 13:39:07,210	01.05.2024 13:39:07,929
Abus Alarmanlage.pdf	File	.pdf	314.765	01.05.2024 13:39:07,179	01.05.2024 13:39:07,194
Fluchtwegeplan.jpg	File	.jpg	238.099	01.05.2024 13:38:43,981	01.05.2024 13:38:44,012
Fluchttürsteuerung.pdf	File	.pdf	509.196	01.05.2024 13:38:43,887	01.05.2024 13:38:43,965
Lageplan Besucherzentrum Fraport.jpg	File	.jpg	306.118	29.04.2024 18:25:10,531	29.04.2024 18:25:10,546
Gebäudeplan Frankfurt Flughafen.pdf	File	.pdf	1.426.429	29.04.2024 18:25:10,374	29.04.2024 18:25:10,515
Uebersicht-airport-city-frankfurt.pdf	File	.pdf	3.681.500	29.04.2024 18:24:57,266	29.04.2024 18:24:57,594
Grundstückplan Frankfurt Flughafen.png	File	.png	1.987.629	29.04.2024 18:24:57,016	29.04.2024 18:24:57,250

Abbildung 31: Logisch vorhandene Dokumente auf dem USB-Stick

5.7.3 Medien und Dokumente

Es werden 218 Bilddateien gefunden, wobei 212 davon aus PDF-Dateien extrahiert wurden, die sich auf dem USB-Stick befinden. Bei den restlichen sechs Bilddateien handelt es sich um Dateien, die am 29.04.2024, 01.05.2024 und 08.05.2024 auf den USB-Stick gespeichert wurden. Wie aus den Inhalten und den Dateinamen zu entnehmen, haben vier der sechs Bilddateien einen Bezug zum Frankfurter Flughafen.

Abbild	Dateiname	Date...	Datum/Zeit der Erstellung
	Grundstückplan Frankfurt Flughafen.png	.png	29.04.2024 18:24:57,016
	Lageplan Besucherzentrum Fraport.jpg	.jpg	29.04.2024 18:25:10,531
	Fluchtwegeplan.jpg	.jpg	01.05.2024 13:38:43,981
	Stromversorgungsplan.jpg	.jpg	08.05.2024 16:43:42,380
	Fraport Group Struktur.jfif	.jfif	08.05.2024 16:44:50,665
	FraSec Sicherheitsdienst.png	.png	08.05.2024 16:44:50,712

Abbildung 32: Gespeicherte Bilddateien auf dem USB-Stick

Weiterhin können 13 Dokumente auf dem Asservat festgestellt werden. Dabei handelt es sich um die in Abbildung 33 aufgelisteten PDF-Dateien, die ebenfalls am 29.04.2024, 01.05.2024 und 08.05.2024 auf den USB-Stick gespeichert wurden.

Filename	Authors	File System Created Date...	File System Last Accessed D...
Uebersicht-airport-city-frankfurt.pdf	© Fraport AG - IFM-PG1	29.04.2024 18:24:57.000	29.04.2024 18:24:57.000
Gebäudeplan Frankfurt Flughafen.pdf		29.04.2024 18:25:10.000	29.04.2024 18:25:10.000
Fluchttürsteuerung.pdf		01.05.2024 13:38:43.000	01.05.2024 13:38:43.000
Abus Alarmanlage.pdf	megelhof	01.05.2024 13:39:07.000	01.05.2024 13:39:07.000
EESec2 Handbuch Alarmanlage.pdf	Ever Energy Group GmbH	01.05.2024 13:39:07.000	01.05.2024 13:39:07.000
Betriebsspezifische Schaltpläne.pdf	Landesumweltamt Nordrhein-Westfalen	08.05.2024 16:43:41.000	08.05.2024 16:43:41.000
Grundwissen Elektronik.pdf	\376\377\000B\000e\000r\000n\000h\...	08.05.2024 16:43:41.000	08.05.2024 16:43:42.000
Bedienungsanleitung Eisemann Notstromaggregat.pdf	Metallwarenfabrik Gemmingen GmbH	08.05.2024 16:43:51.000	08.05.2024 16:43:52.000
C4.3 Ausweisordnung.pdf		08.05.2024 16:44:16.000	08.05.2024 16:44:16.000
C4.6 Sicherheitsmanagement-Systems des Verkehrsflughafens.pdf	38321	08.05.2024 16:44:16.000	08.05.2024 16:44:16.000
C4.8 Brandschutzordnung.pdf		08.05.2024 16:44:16.000	08.05.2024 16:44:16.000
C2.2 Umwelt-, Sicherheits- und Schutzregeln.pdf	NAPS2	08.05.2024 16:44:16.000	08.05.2024 16:44:16.000
Gesamtorganigramm Fraport.pdf		08.05.2024 16:44:50.000	08.05.2024 16:44:50.000

Abbildung 33: Gespeicherte PDF-Dateien auf dem USB-Stick

Die Dokumente haben alle einen Bezug zum Frankfurter Flughafen oder stehen in Verbindung mit Stromversorgung und Brandschutz.

6 Fazit

Während der Sicherung, Aufbereitung und Auswertung der Asservate sind einige unvorhergesehene Probleme und Schwierigkeiten aufgetreten, die jedoch alle behoben werden konnten.

Aus unterschiedlichen Gründen konnte die interne Festplatte des Notebooks nicht ausgebaut werden, weshalb die Sicherung nicht wie geplant mittels FTK Imager durchgeführt werden konnte. Es musste also ein Tool gefunden werden, mit dem eine interne Festplatte ohne Ausbauen gesichert werden kann. Auf Grund von beruflicher Erfahrung wurde sich für PALADIN EDGE endschieden. Das Tool kann für den nicht kommerziellen Gebrauch kostenlos auf der Webseite des Herstellers heruntergeladen werden. Somit konnte eine anschließend reibungslose Sicherung des Notebooks durchgeführt werden.

Ein weiteres Problem trat bei der Aufbereitung des USB-Sticks mittels Magnet AXIOM auf. Da sich innerhalb des Szenarios für die Verschlüsselung des USB-Sticks entschieden wurde, muss dieser, um uneingeschränkten Zugriff auf die enthaltenen Daten zu bekommen, vor der Aufbereitung entschlüsselt werden. Das verwendete Passwort lautet „Die-Pfifferlinge95“ und besitzt weniger als 20 Zeichen. Die Entschlüsselung wird innerhalb von Magnet AXIOM ausgeführt. Dabei kam es zu der Fehlermeldung „Passwort oder PIM (oder beides) ist nicht korrekt“, obwohl diese unter der Angabe des korrekten Passworts erfolgte. Somit konnte nur der Persönlicher Iterationsfaktor (kurz PIM) zu der Fehlermeldung führen. Da initial nicht bekannt war, was und wofür der PIM ist, wurde das Feld bei der Entschlüsselung vorerst leer gelassen.

Nach einer Google Recherche konnte herausgefunden werden, dass es sich bei dem PIM um einen Iterationsfaktor bei der Ver- und Entschlüsselung handelt, der von VeraCrypt verwendet wird, damit die Anzahl an Iterationen nicht weniger als die standardmäßig definierte Mindestanzahl beträgt. Für Container beträgt der PIM den Mindestwert von 485. Nachdem für den PIM der Wert „485“ verwendet wurde, konnte der USB-Stick ohne weitere Probleme von Magnet AXIOM entschlüsselt und aufbereitet werden.

Als Kommunikationsmittel im Szenario wurde ein Discord Server für die Gruppierung „Die Pfifferlinge“ erstellt, der bei der Spurenlegung auf dem Notebook ausschließlich über den Webbrowser aufgerufen wurde. Zuvor war nicht bekannt, welche Artefakte von Discord innerhalb der Auswertung ersichtlich sein würden. Jedoch wurde davon ausgegangen, dass Chatnachrichten und Chatteilnehmer innerhalb der Aufbereitung nicht gefunden werden können, da sich diese Informationen in flüchtigen Speicherbereichen befinden. Schlussendlich reichten die in Bezug zu Discord identifizierten Artefakte aus, um der Tatverdächtigen den Kontakt mit den Mitgliedern der Gruppierung „Die Pfifferlinge“ nachweisen zu können. Dies liegt auch darin begründet, dass sowohl der Discord Server als auch die sich darauf befindenden Textkanäle während der Vorbereitung des Szenarios eindeutig benannt wurden.

Als letztes stellte die Analyse der Windows-Registry unter Magnet AXIOM eine Herausforderung dar. Da AXIOM neben der Aufbereitung der unterschiedlichen Artefakte auch die Möglichkeit bietet, die Registry in ihrem originalen Aufbau aufzurufen und zu analysieren, wurde sich lediglich für eine Auswertung mit AXIOM entschieden. Dies erfordert jedoch Kenntnisse über den Aufbau der Registry, genauer welche Daten sich in welchem Hive und unter welchem Schlüssel befinden. Des Weiteren ist die von AXIOM generierte Baumstruktur unübersichtlich. Vorteilhaft ist jedoch, dass die Inhalte der Registry mit aufbereitet werden und somit unter den Artefakten zu finden sind. Hierfür wird ebenfalls die Kenntnis benötigt, unter welcher der Kategorien die entsprechende Information angezeigt wird. Eine Zeitersparnis hätte durch die Analyse der Windows Registry mittels eines separaten Registry-Readers oder dem von X-Ways Forensics bereitgestellten Registry-Report erzielt werden können. Diese Tools bereiten die Registry in leicht lesbarer Form auf, sodass eine Analyse ohne fundierte Kenntnisse der Struktur und den Hives erfolgen kann.

Die Windows-Registry wurde u.a. für die Analyse der verbundenen externen Speichermedien des Notebooks verwendet. Dabei wurden der Anzeigename sowie die Seriennummer des verwendeten Kingston USB-Sticks identifiziert. Bei der Auswertung des Images des gesicherten USB-Sticks wurde die am Notebook ermittelte Seriennummer jedoch nicht festgestellt. Dies kann unterschiedliche Gründe haben. Oftmals kann die Seriennummer eines USB-Sticks auf Grund der Verwendung eines Writeblockers nicht gesichert werden. Letztendlich konnte die Verbindung des USB-Sticks mit dem Notebook anhand der Volume Seriennummer nachgewiesen werden. Diese befand sich in den Windows-Ereignisprotokollen zu den Speichergeräten und konnte dort eindeutig dem Kingston USB-Stick zugeordnet werden. Dort waren ebenfalls die drei unterschiedlichen Verbindungszeitpunkte zu erkennen.

Abschließend kann gesagt werden, dass die Planung und Vorbereitung des Szenarios sowie die Durchführung der forensischen Analyse sehr gut verlaufen sind. Das in Kapitel 3.1 beschriebene forensische SAP-Vorgehensmodell war für das Szenario gut gewählt. Die auftretenden Probleme und Schwierigkeiten konnten gut und zeitnah gelöst werden.

7 Wiki Eintrag

Hinweis

Der folgende Eintrag für das IT-Forensik Wiki der Hochschule Wismar stellt ein in sich abgeschlossenes Kapitel dar und steht in keinem Bezug zu der restlichen Praktikumsdokumentation. Deswegen beginnen die Nummerierungen zu Abbildungen, Tabellen und Quellangaben beim initialen Zähler. Die Quellen werden unmittelbar am Ende des Kapitels aufgeführt und nicht im Quellverzeichnis der Praktikumsdokumentation.

Thumbnail Cache unter Windows

Einleitung

Thumbnail Caches sind spezielle Dateien, die unter Windows erstellt und verwendet werden, um Vorschaubilder von Dateien, wie bspw. von Bildern oder Videos, im Windows Explorer schneller anzeigen zu können. Diese Caches beinhalten kleine Vorschauversionen von Dateien, den sogenannten Thumbnails, um diese nicht bei jedem Öffnen eines Ordners neu generieren zu müssen. Damit wird dem Benutzer eine Vorschau des Inhalts der Datei ermöglicht, ohne diese öffnen zu müssen. Dies macht das Durchsuchen und Verwalten von Dateien erheblich effizienter.[1][2]

Erstellung

Der Thumbnail Cache besteht aus einer Sammlung von Vorschaubildern, die automatisch erstellt werden, wenn ein Benutzer auf einen Ordner zugreift, der unterstützte Dateien enthält. Gleichzeitig wird bei jedem Ordnerzugriff überprüft, ob die Vorschaubilder bereits im Cache vorhanden sind. Sollte dies zutreffen, werden diese direkt aus dem Cache geladen, andernfalls neu generiert und im Cache abgelegt. Bei der Erstellung eines Thumbnails wird diesem eine eindeutige acht Byte lange ThumbnailcacheID zugeordnet, die zugleich den Namen des Thumbnails darstellt.[3]

Speicherung und Dateiformate

Die Cache-Dateien werden in Abhängigkeit der verschiedenen Windows-Versionen in unterschiedlichen Verzeichnissen auf der lokalen Festplatte gespeichert. Seit Windows Vista befinden sich die Cache-Dateien zentralisiert im Verzeichnis `C:\Users\<Benutzername>`

`\AppData\Local\Microsoft\Windows\Explorer` und werden als „thumbcache_*.db“ abgelegt, wobei die angegebene Zahl die Größe der gespeicherten Thumbnails in Pixeln angibt [1][2]. In früheren Windows-Versionen werden sie hingegen als versteckte Dateien mit dem Namen „thumbs.db“ im selben Dateipfad wie die Originaldateien gespeichert. Die Cache-Dateien sind in einer Datenbankstruktur organisiert und besitzen die Endung „*.db“ (Database File Format). Die Thumbnails selbst werden im Dateiformat JPEG (Joint Photographic Experts Group), BMP (Windows Bitmap) oder PNG (Portable Network Graphics) gespeichert.[4]

Abbildung 1 zeigt die Thumbnail Cache Dateien eines Windows 10 Benutzerkontos.

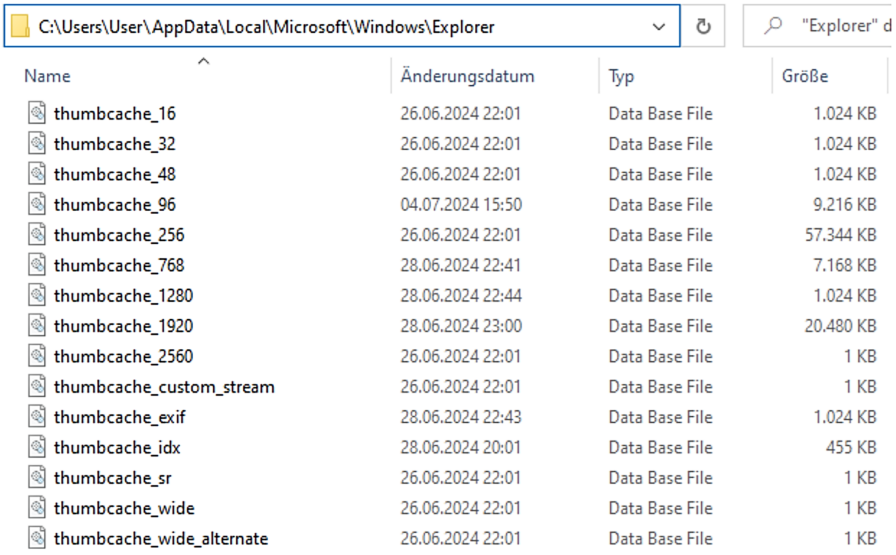


Abbildung 1: Beispiel Thumbnail Cache Dateien unter Windows 10

Abbildung 2 zeigt eine der verschiedenen Vorschaugrößen im Windows Explorer eines Windows 10 Betriebssystems. Wie zu erkennen, werden bei der Vorschauansicht Thumbnails der Bilddateien angezeigt.

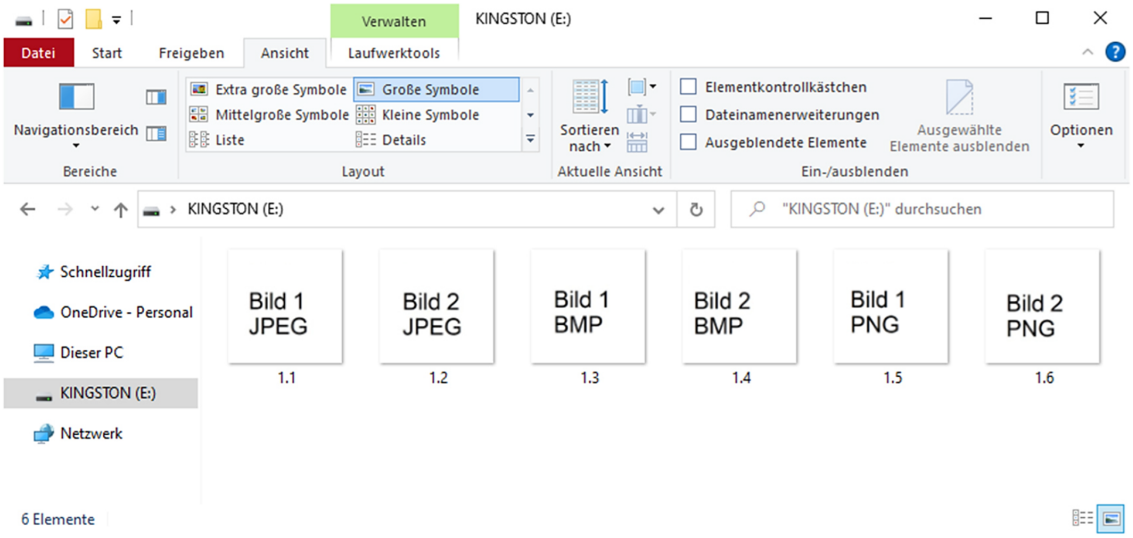


Abbildung 2: Ansicht „Große Symbole“

Struktur und Inhalt

Die Struktur der Datenbank umfasst eine Tabelle für Thumbnails. Diese enthält neben den eigentlichen Bilddaten der Thumbnails einen Index, der schnelle Zugriffe und die Verknüpfung von Dateipfaden und anderer Metadaten mit den gespeicherten Thumbnails ermöglicht, sowie die Metadaten selbst. Metadaten enthalten bspw. Informationen wie den Dateinamen, den Pfad zur Originaldatei, die Zeit des letzten Zugriffs und die Größe der Datei. Wenn eine Datei geändert oder gelöscht wird, kann das Betriebssystem anhand der Metadaten erkennen, ob das dazugehörige Vorschaubild im Cache aktualisiert oder entfernt werden muss. [5][6]

Tabelle 1 zeigt einen Überblick über den Thumbnail Cache seit seiner Einführung. Zu jeder Windows-Version wird angegeben, ob es sich bei der jeweiligen Cache-Datei um die thumbs.db oder um die thumbcache_*.db Datenbank handelt. Weiterhin wird ein Überblick darüber geboten, wo der Thumbnail Cache in Windows gespeichert wird und welche Metadaten er enthält.

Betriebssystem	**Dateiname**	**Speicherort**	**Metadaten**
Windows 95B	thumbs.db	Lokal im Ordner	
Windows ME Windows 2000	thumbs.db	Lokal im Ordner	Dateiname, Laufwerkbuchstabe, Speicherpfad
Windows XP Windows 2000	thumbs.db	Lokal im Ordner	Dateiname

Windows Vista	thumbcache_32, 96, 256, 1024	C:\Users\<username>\AppData\Local\Microsoft\Windows\Explorer	ThumbnailcacheID
Windows 7	thumbcache_32, 96, 256, 1024	C:\Users\<username>\AppData\Local\Microsoft\Windows\Explorer	ThumbnailcacheID, GUID, Laufwerkbuchstabe
Windows 8	thumbcache_16, 32, 48, 96, 256, 1024, wide	C:\Users\<username>\AppData\Local\Microsoft\Windows\Explorer	ThumbnailcacheID
Windows 10	thumbcache_16, 32, 48, 96, 256, 768, 1280, 1920, 2560, wide, wide_alternate	C:\Users\<username>\AppData\Local\Microsoft\Windows\Explorer	ThumbnailcacheID

Tabelle 1: Windows Thumbnail Cache in den verschiedenen Windows-Versionen

Bedeutung in der digitalen Forensik

Inkriminierte Bilddateien werden häufig mit Verbrechen wie Sexualdelikten, Drogendelikten, Waffendelikten oder Insider-Bedrohungen in Verbindung gebracht. Der Thumbnail Cache wurde dabei in Gerichtsverhandlungen als Beweismittel genutzt. Im Fall „Vereinigte Staaten von Amerika gegen S. Room“ (2006) wurde der Begriff „Thumbnail“ in der Rechtsprechung wie folgt definiert: „Der Begriff Thumbnail, der sich von der Skizze eines Künstlers ableitet, bezieht sich auf ein kleines Bild einer Grafikdatei, das angezeigt wird, um deren Identifizierung zu erleichtern.“ [1]

Bei der forensischen Untersuchung stehen den Ermittlern verschiedene Vorgehensweisen zur Verfügung. Zum einen kann mit Hilfe von Filtern innerhalb verschiedener forensischer Programme, wie z.B. EnCase oder X-Ways Forensics, eine rekursive Suche nach allen auf dem Betriebssystem gespeicherten Bilddateien durchgeführt werden. Zum anderen kann gezielt nach Bilddateien in einem bestimmten Benutzerverzeichnis gesucht werden, was einen guten Anhaltspunkt bei der Suche und Lokalisierung von inkriminierten Bilddateien bietet.

Da der Thumbnail Cache nutzerbezogen ist, hat jedes Windows Benutzerkonto seinen eigenen Cache. Gespeicherte Thumbnails stammen daher vermutlich von Dateien, die der Nutzer selbst verarbeitet hat und die wichtige Einblicke in das Verhalten eines Nutzers bieten. Viele Nutzer wissen nicht, dass der Thumbnail Cache existiert. Und da der Cache nicht automatisch aktualisiert wird, bleiben Thumbnails inkriminierter Dateien selbst dann erhalten, wenn die Originaldateien gelöscht wurden. Erst das manuelle Löschen des Thumbnail Caches oder die Verwendung der Windows Datenträgerbereinigung mit entsprechen-

der Option entfernen diese. [7] Das komplette Unterbinden des Zwischenspeicherns von Thumbnails ist seit Windows 8 nicht mehr möglich [8].

Quellen

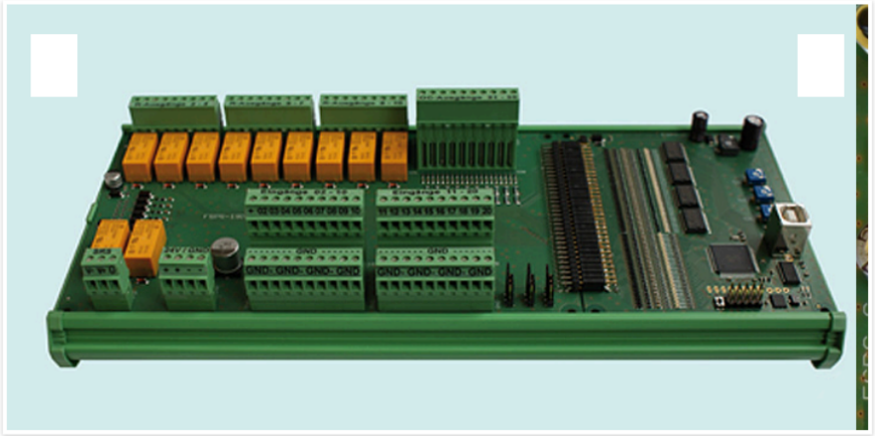
[1] „Forensic Analysis of Windows Thumbcache Files“ https://ssrn.com/abstract=2429795 [zuletzt besucht am 07.07.2024]
[2] „Windows thumbnail cache“ https://en.wikipedia.org/w/index.php?title=Windows_thumbnail_cache&oldid=945661331 [zuletzt besucht am 07.07.2024]
[3] „An Analysis of the Structure and Behaviour of the Windows 7 Operating System Thumbnail Cache“ https://www.researchgate.net/publication/262327134_An_analysis_of_the_structure_and_behaviour_of_the_Windows_7_operating_system_thumbnail_cache [zuletzt besucht am 07.07.2024]
[4] „Under My Thumbs – Revisiting Windows Thumb nail Databases and Some New Revelations About the Forensic Implications.“ http://computerforensics.parsonage.co.uk/downloads/UnderMyThumbs.pdf [zuletzt besucht am 07.07.2024]
[5] „Forming a Relationship be tween Artefacts identified in thumbnail caches and the remaining data on a storage device.“ https://www.researchgate.net/publication/262327215_Forming_a_Relationship_between_Artefacts_identified_in_thumbnai_caches_and_the_remaining_data_on_a_storage_device [zuletzt besucht am 07.07.2024]
[6] „Vorschaubild“ https://de.wikipedia.org/wiki/Vorschaubild [zuletzt besucht am 07.07.2024]
[7] „Windows Thumbnail Cache“ https://de.wikipedia.org/w/index.php?title=Windows_Thumbnail_Cache&oldid=193998229 [zuletzt besucht am 07.07.2024]
[8] „Thumbnail Preview will not disable for me in Windows 11“ https://answers.microsoft.com/en-us/windows/forum/all/thumbnail-preview-will-not-disable-for-me-in/af5a8da4-ded4-4720-a861-ea6bd9fea399 [zuletzt besucht am 07.07.2024]

A Fluchttürsteuerung

info@maniago.de +49 6131 581014

MANIAGO

Fluchttürsteuerung FSPS 20 / 30



Flucht- und Rettungswegmanagement im Objekt

Die FSPS ist eine Entwicklung speziell für Anwendungen im Flucht- und Rettungswegmanagement, welche mit einer nach EltVTR geprüften und zugelassenen Steuerung realisiert werden müssen.

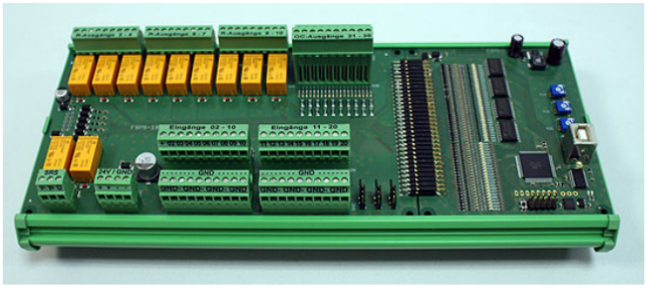


Foto: Fluchttürsteuerung FSPS 20 / 30

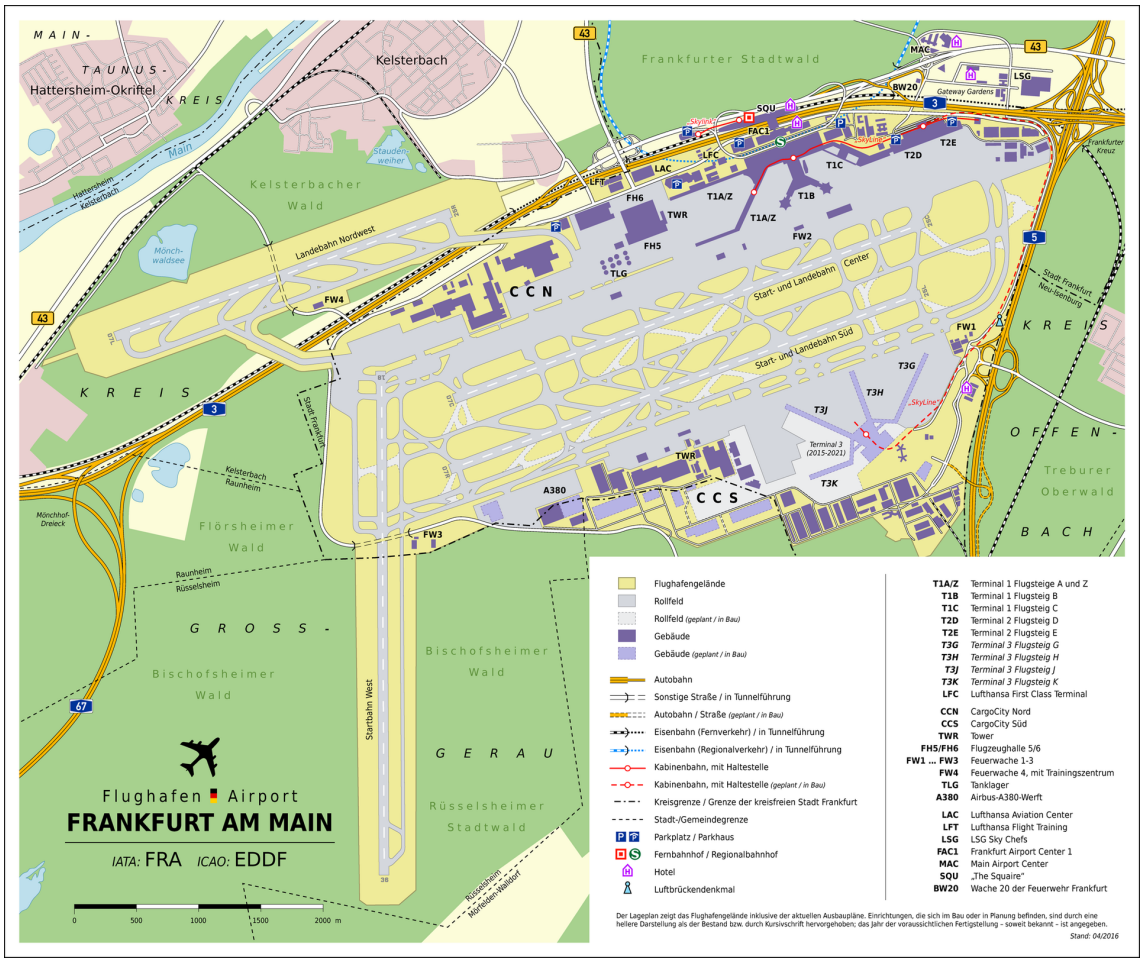
Die FSPS geht über den Standard üblicher Flucht- und Rettungswegsteuerungen hinaus.

[4]

B Flucht- und Rettungsplan

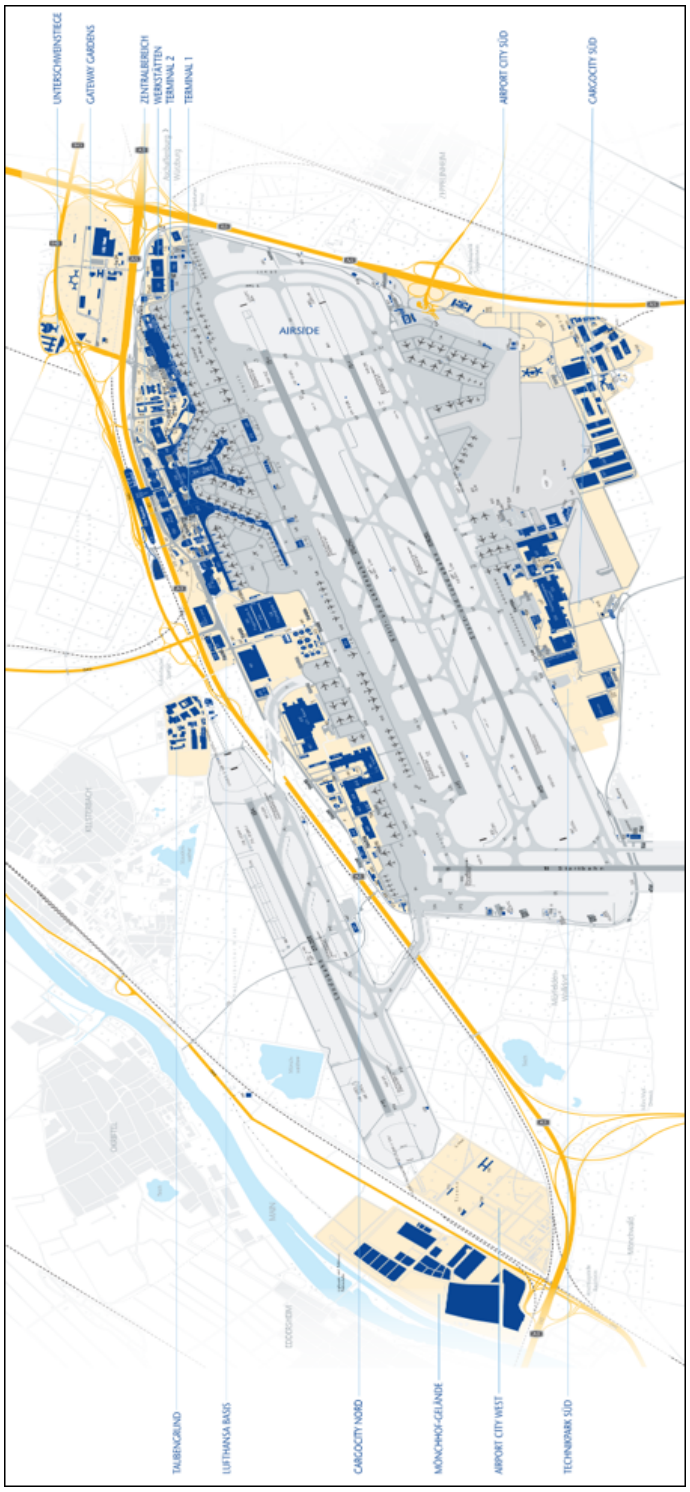
[5]

C Grundstückplan Frankfurt Flughafen



[6]

D Übersicht Frankfurt Flughafen

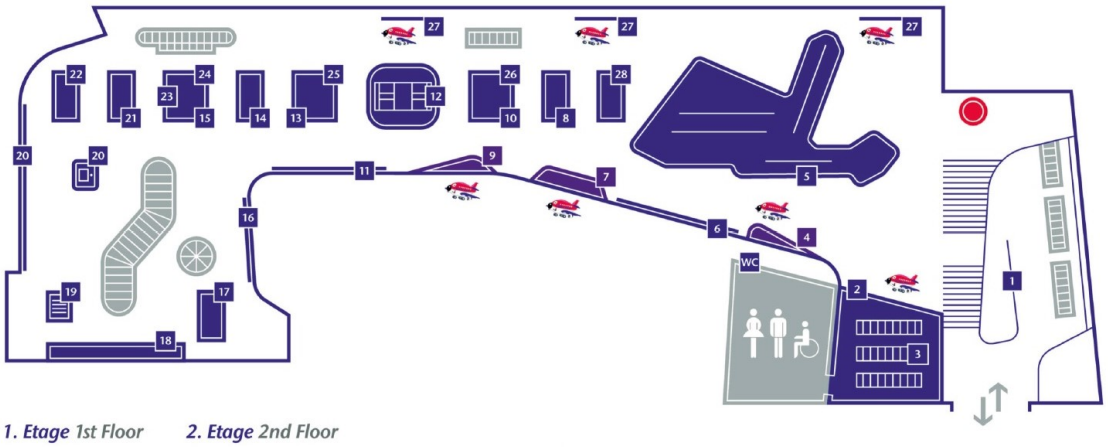


[7]

E Gebäudeplan Frankfurt Flughafen

[8]

F Lageplan Frankfurt Flughafen



1. Etage *1st Floor*

1 Empfangsbereich
Reception

2. Etage *2nd Floor*

Ihr Standort
You are here

Inhalte für Kinder
Content for Children

Sitzgelegenheiten
Seating

2 Movie Lounge
Movie Lounge

3 VR-Brillen
Virtual reality headsets

4 Kinderbereich Vorfeldkontrolle
Apron Control for Children

5 Airport City Modell
Airport City Model

6 Mitgezählt-Wand
Count-Up Wall

7 Kinderbereich An- und Abflug
Takeoff and Landing for Children

8 Frankfurt – Stadt der Luftfahrt
Frankfurt: the Aviation City

9 Kinderbereich Gaming
Gaming for Children

10 3D-Holographie Zeppelin-Ära
3D Hologram: The Zeppelin Era

11 Zeitstrahl
Timeline

12 Motion Ride
Motion Ride

13 Natur und mehr
Nature and More

14 FRA – Tor zur Welt
FRA: Gateway to the World

15 3D-Holographie Luftbrücke
3D Hologram: The Berlin Airlift

16 Marshaller's Game
Marshaller's Game

17 FRA Aktuell
FRA Latest

18 Berufe-Wand
Job Wall

19 Fraport – Internationale Konzernflughäfen
Fraport Group Airports Worldwide

20 The Globe
The Globe

21 FRA – Drehkreuz des Luftverkehrs
FRA: a Major Aviation Hub

22 Foto-Wand
Photo Wall

23 Terminal 3
Terminal 3

24 Fliegeralphabet
Spelling Alphabet Used in Aviation

25 Audiosäule Services
Audio Column: Services

26 Audiosäule Vielfalt
Audio Column: Diversity

27 Smart Windows
Smart Windows

28 Audiosäule Von Mensch zu Mensch
Audio Column: Helping Others

[9]

G Abus Alarmanlage

ABUS
Security Tech Germany

BEDIENUNGSANLEITUNG

Terxon LX

Perfekte Sicherheit für Wohnung, Haus und Gewerbe

CE

Inv. 1-497233

[10]

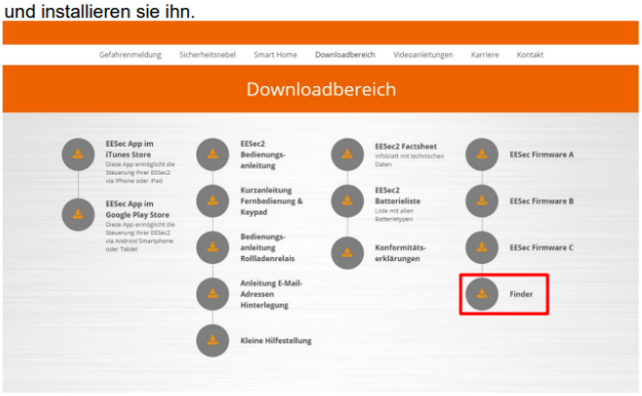
H EESec2 Alarmanlage

Zugriff auf das Webinterface der Alarmanlage

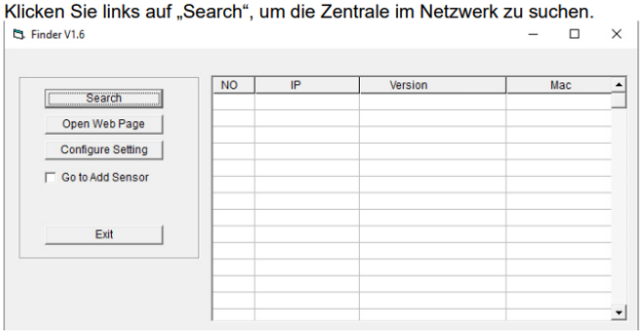
Die Zentrale wird über eine browsergestützte Benutzeroberfläche gesteuert, die wie eine Internetseite aufgebaut ist. Auf dieser Benutzeroberfläche können Sie alle Funktionen Ihrer Alarmanlage steuern, Sensoren hinzufügen oder bearbeiten, die Zentrale scharf oder unscharf stellen, überprüfen ob Fenster oder Türen offen stehen, sowie, falls vorhanden, die Live-Bilder Ihrer HD-Netzwerkkameras und Rekorder sehen.

Um das Hauptmenü der Zentrale mit Windows Clients zu öffnen, gehen Sie wie beschrieben vor:

1. Laden Sie sich von unserer Website www.eesec.de den Finder herunter und installieren sie ihn.



2. Klicken Sie links auf „Search“, um die Zentrale im Netzwerk zu suchen.



[11]

I Betriebsspezifische Schaltpläne

Schaltschrank 2

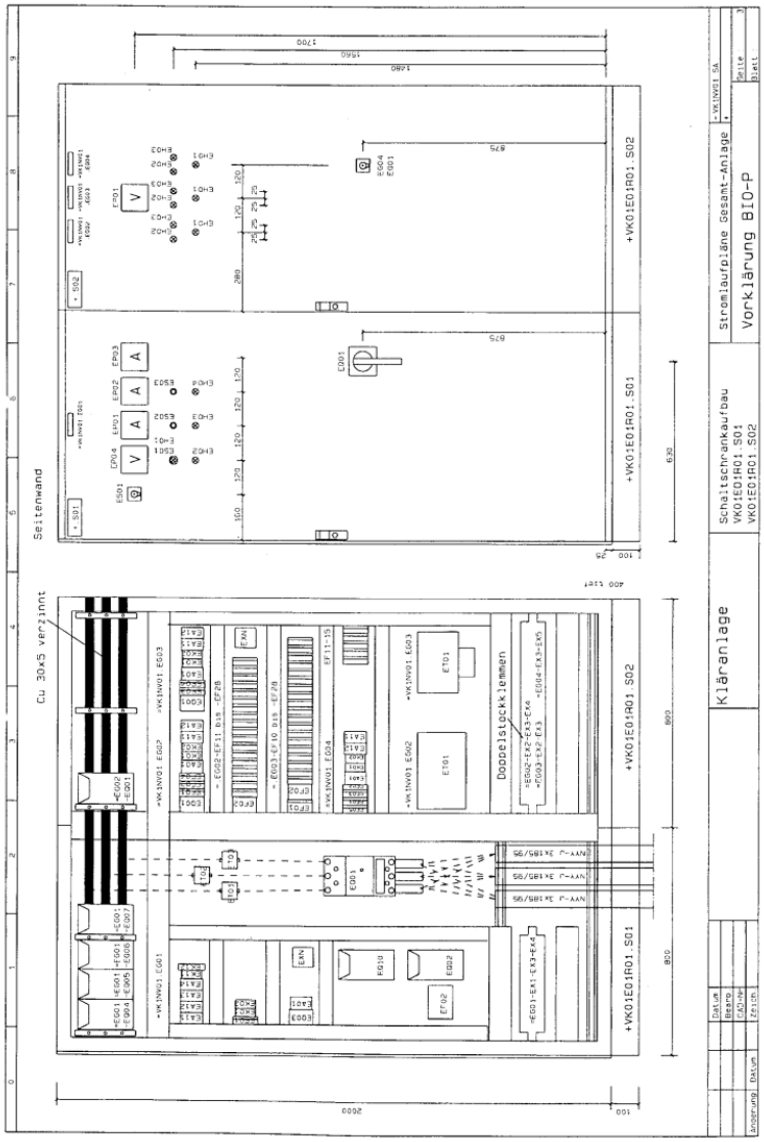


Abb. 7.10: Schaltschrank

[12]

J Grundwissen Elektronik

Grundwissen Elektronik

Release 0.1.6e

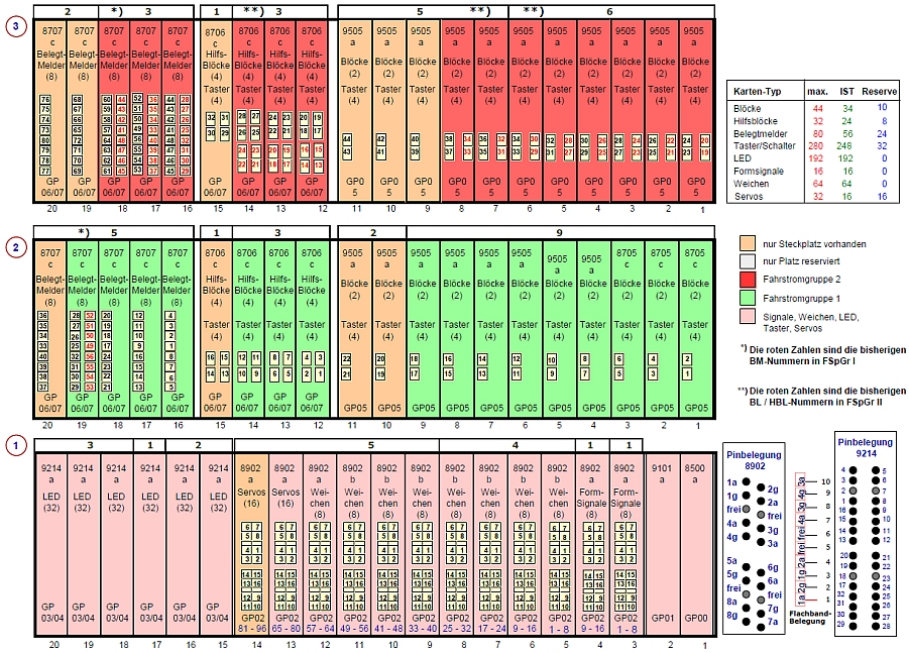
Aktualisiert am 02.12.2018

Bernhard Grotz

http://www.grund-wissen.de

[**13**]

K Stromversorgungsplan



[**14**]

L Bedienungsanleitung Notstromaggregat

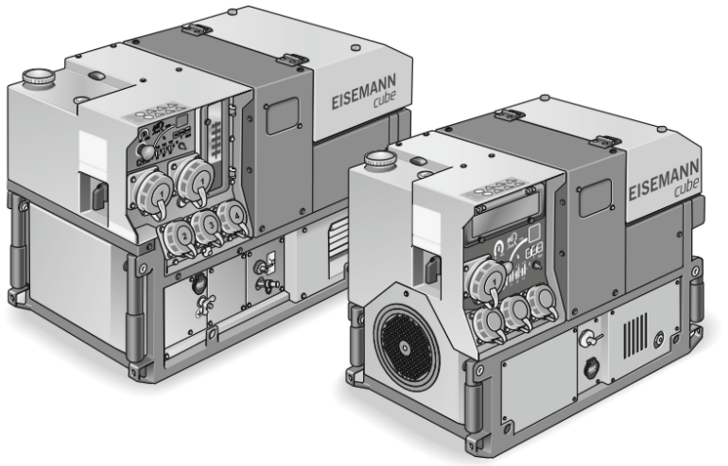
Original-Betriebsanleitung DE

Stromerzeuger

EISEMANN

BSKA 9E RSS Cube
BSKA 14E RSS Cube
BSKA 17EV RSS Cube PMG EFI

DIN 14685-1



Wichtig – vor jedem Start!

Lesen Sie diese Betriebsanleitung und das mitgeltende Motorhandbuch sorgfältig durch. Achten Sie stets darauf, dass alle Personen in Reichweite des Stromerzeugers einen geeigneten Gehörschutz tragen.

904212 – 2020-04

CE

Metallwarenfabrik Gemmingen GmbH
Industriestraße 1, D – 75050 Gemmingen
Tel.: +49 (0) 7267 806 0, Fax: +49 (0) 7267 806 100
www.metallwarenfabrik.com
info@metallwarenfabrik.com

[15]

M Flughafenordnung Frankfurt

6. Umwelt-, Sicherheits- und Schutzregeln

6.1 Notfallordnung der Fraport AG für den Verkehrsflughafen Frankfurt am Main (FRA Not)

Die Notfallordnung der Fraport AG (nachfolgend FRA Not genannt) regelt die Verfahrensweisen bei Notfällen im Bereich des Verkehrsflughafens Frankfurt/Main.

Sie beschreibt die gemäß Verordnung (EU) Nr. 139/2014 und ICAO Annex 14, Annex 19 zu treffende Vorbereitung auf schwere Störungen, Brand- und Explosionsereignisse, Unglücks- und Notfälle, kriminelle Handlungen sowie zu erwartende oder bereits eingetretene Flugunfälle auf oder in der Nähe des Verkehrsflughafens Frankfurt/Main. Ziel der in der FRA Not definierten Verfahren ist es, die Auswirkungen von Notfällen zu minimieren. Sie ist außerdem Bestandteil des übergeordneten Sicherheitsmanagementsystems, welches die Fraport AG in Erfüllung ihrer Verpflichtung nach § 45b Abs. 1 Satz 1 LuftVZO einzurichten und zu betreiben hat.

Die FRA Not enthält Verfahren zur koordinierten Vorgehensweise der an der Bewältigung eines Notfalls beteiligten internen und externen Stellen, soweit deren Einbindung erforderlich ist.

Für Beschäftigte der Fraport AG ist die FRA Not eine Dienstanweisung für das Verhalten und die Verfahrensweise bei Notfällen und stellt im Übrigen eine Konkretisierung des Hausrechts der Fraport AG dar.

6.2 Brandschutzregeln

Jeder muss durch Achtsamkeit und überlegtes Handeln zur Brandverhütung und im Brandfall zur Rettung von Menschen und Tieren zu einer raschen Brandbekämpfung beitragen.

6.2.1 Einleitung

Die Fraport AG hat eine Brandschutzordnung erstellt, um gesetzlichen Anforderungen aus Verkehrs-, Bau- und Brandschutzrecht zu entsprechen. Sie ist eine Ergänzung zum Teil II, Ziffer 5 "Sicherheitsbestimmungen" der Flughafenbenutzungsordnung. Die Brandschutzordnung ist die Zusammenfassung von Grundregeln zur Brandverhütung und den zu treffenden Selbsthilfemaßnahmen bei Bränden oder sonstigen Schadensereignissen (vgl. Abschnitt 7 und 8). Sie informiert über die Maßnahmen des vorbeugenden und abwehrenden Brandschutzes.

Diese Brandschutzregeln richten sich an alle Beschäftigten, Dienstleister und Kunden des Verkehrsflughafens Frankfurt/Main auf dem Flughafengelände.

6.2.2 Weitere Brandschutzordnungen auf dem Gelände der Fraport AG

Erbbauberechtigte, Firmen und Behörden im Bereich des Verkehrsflughafens Frankfurt/Main können eine eigene Brandschutzordnung erstellen, diese ist jedoch zuvor mit dem „Vorbeugenden Brand- und Explosionsschutz" der Fraport AG abzustimmen.

Die eigene Brandschutzordnung darf grundsätzlich nicht im Widerspruch zur Brandschutzordnung der Fraport AG stehen.

[16]

N Ausweisordnung Frankfurt Flughafen

C4.3
Ausweisordnung

Aufgrund des Luftsicherheitsgesetzes (LuftSiG), der Luftverkehrszulassungsordnung (LuftVZO) und der EU-Luftsicherheitsvorgaben ist die Fraport AG zur Sicherung des Flughafengeländes verpflichtet. Der Zugang und die Zufahrt zu den landseitigen und luftseitigen Bereichen sind deshalb nur berechtigten Personen zu gestatten.

Diese Ausweisordnung dient der Beschreibung des am Flughafen Frankfurt/Main gültigen Ausweissystems und den damit verbundenen Zugangs- und Zufahrtsregelungen.

Bei dieser Ausweisordnung handelt es sich um Weisungen des Flughafenunternehmers aufgrund des Teil 2 Ziffer 1.1 der behördlich genehmigten Flughafenbenutzungsordnung in Verbindung mit deren Anhängen, die von allen am Flughafen Frankfurt/Main tätigen Personen zu befolgen sind.

Diese Ausweisordnung ersetzt die Ausgabe von November 2019.

gez. Dr. Pierre Dominique Prümm gez. ppa. Alexander Laukenmann

Gültig ab: 01.01.2021
Ersteller: AVN-SR2
Freigeber: VI, AVN

[17]

O Sicherheitsmanagement-System Frankfurt Flughafen

Gesamtbewertung von SMS-relevanten Ereignissen

Die Prozesseigner / -verantwortlichen nehmen eine Einstufung der Ereignisse gemäß der in den Kapiteln 8.2.100 beschriebenen Klassifizierungen vor. Bei Bedarf kann vom SMS der Fraport AG ein entsprechendes Formblatt (8.1 SMS 4.2) zur Verfügung gestellt werden.

		Katastrophal Absturz A	Gefährlich Großbrand B	Hoch Unfall C	Niedrig Notverfahren D	Sehr gering E
Häufig	5	5A	5B	5C	5D	5E
Gelegentlich	4	4A	4B	4C	4D	4E
Gering	3	3A	3B	3C	3D	3E
Unwahrscheinlich	2	2A	2B	2C	2D	2E
Sehr unwahrscheinlich	1	1A	1B	1C	1D	1E

Abbildung 4: Toleranzmatrix des Fraport SMS basierend auf ICAO Doc. 9859, SMM III

Mit der Toleranzmatrix werden Entscheidungen über die Akzeptanz bzw. Toleranz von Risiken für die betriebliche Sicherheit transparent unterstützt.

Die Definition der Inhalte der Matrix erfolgt i.d.R. durch die Prozesseigner / -verantwortlichen und Bereichsleiter.

Sofern Bereichsleiter für ihre Organisationseinheit eine von den Richtlinien der ICAO und deren mitgeltenden Unterlagen, auf Grundlage des von ihnen definierten akzeptierten Risikoniveaus ALoR, eine abweichende Matrix im Rahmen der von ihnen durchgeführten Risikobewertungen angewandt haben, ist dieser Sachverhalt in der dazugehörigen Dokumentation unter Angabe der Gründe zu dokumentieren und dem SMS mitzuteilen.

8.2.2 Reaktive Risikobewertung (ERC Event Risk Classification)

Reaktive Sicherheitsbewertungen dienen u.a. der Validierung der Ergebnisse proaktiver (inklusive vorhersagender) Risikobewertungen sowie der Überprüfung der betrieblichen Sicherheit von (Teil-) Prozessen. Diese sind durch die jeweiligen Prozesseigner / -verantwortlichen vorzunehmen.

Darüber hinaus schätzt das SMS unter Einbindung der jeweiligen Prozesseigner / -verantwortlichen auf Grundlage der ihm vorliegenden Berichte und Meldungen die betriebliche Sicherheit bei der Flughafenbetriebsabwicklung ein.

Die reaktive Risikobewertung erfolgt in Form einer „Event Risk Classification", ERC und wird dokumentiert. Das Hauptziel der Bewertung nach der ERC Methodik ist eine schnelle Beurteilung, ob im Zusammenhang mit gemeldeten oder erfassten sicherheitsrelevanten Ereignissen umgehend Maßnahmen zur Reduzierung von Risiken notwendig sind. Diese Beurteilung erfolgt in der Regel innerhalb von 2-3 Tagen nach dem Ereignis und wird durch das SSO durchgeführt.

[18]

P Brandschutzordnung Frankfurt Flughafen

C4.8
Brandschutzordnung

Maßnahmen zur Verhütung von Bränden,
Verhalten bei Bränden und Notständen

Vorwort

Die Fraport AG hat diese Brandschutzordnung (BSO) erstellt, um gesetzlichen Anforderungen aus Verkehrs-, Bau-, Umwelt-und Brandschutzrecht zu entsprechen. *Sie ist eine Ergänzung zum Teil II, Ziffer 5 "Sicherheitsbestimmungen" der C2.1 Flughafen-Benutzungsordnung.* Die Brandschutzordnung ist die Zusammenfassung von Grundregeln zur Brandverhütung und der zu treffenden Selbsthilfemaßnahmen bei Bränden oder sonstigen Schadensereignissen. Sie informiert über die Maßnahmen des vorbeugenden und abwehrenden Brandschutzes.

Die Brandschutzordnung ist gemäß DIN 14096 gegliedert und richtet sich:

- in Abschnitt 1 an alle Besucher des Verkehrsflughafens Frankfurt/Main (**Teil A**),
- in Abschnitt 2 an alle Personen auf dem Gelände des Verkehrsflughafens Frankfurt/Main, die aufgrund ihres regelmäßigen Aufenthalts einen Flughafenausweis besitzen (**Teil B**),
- in Abschnitt 3 an alle Personen mit besonderen Brandschutzaufgaben auf dem Gelände des Verkehrsflughafens Frankfurt/Main (**Teil C**).

Die Brandschutzordnung dient:

- der Sicherheit der Fluggäste, Besucher und Beschäftigten
- dem Schutz der Umwelt
- der Erhaltung der Arbeitsplätze und dem Schutz der Unternehmenswerte

und somit den Interessen der Allgemeinheit.

Erbbauberechtigte, Firmen und Behörden im Bereich des Verkehrsflughafens Frankfurt/Main können eine eigene Brandschutzordnung erstellen, diese ist jedoch zuvor mit dem „Vorbeugenden Brandschutz" der Fraport AG abzustimmen.

Die eigene Brandschutzordnung darf nicht im Widerspruch zur Brandschutzordnung der Fraport AG stehen.

[**19**]

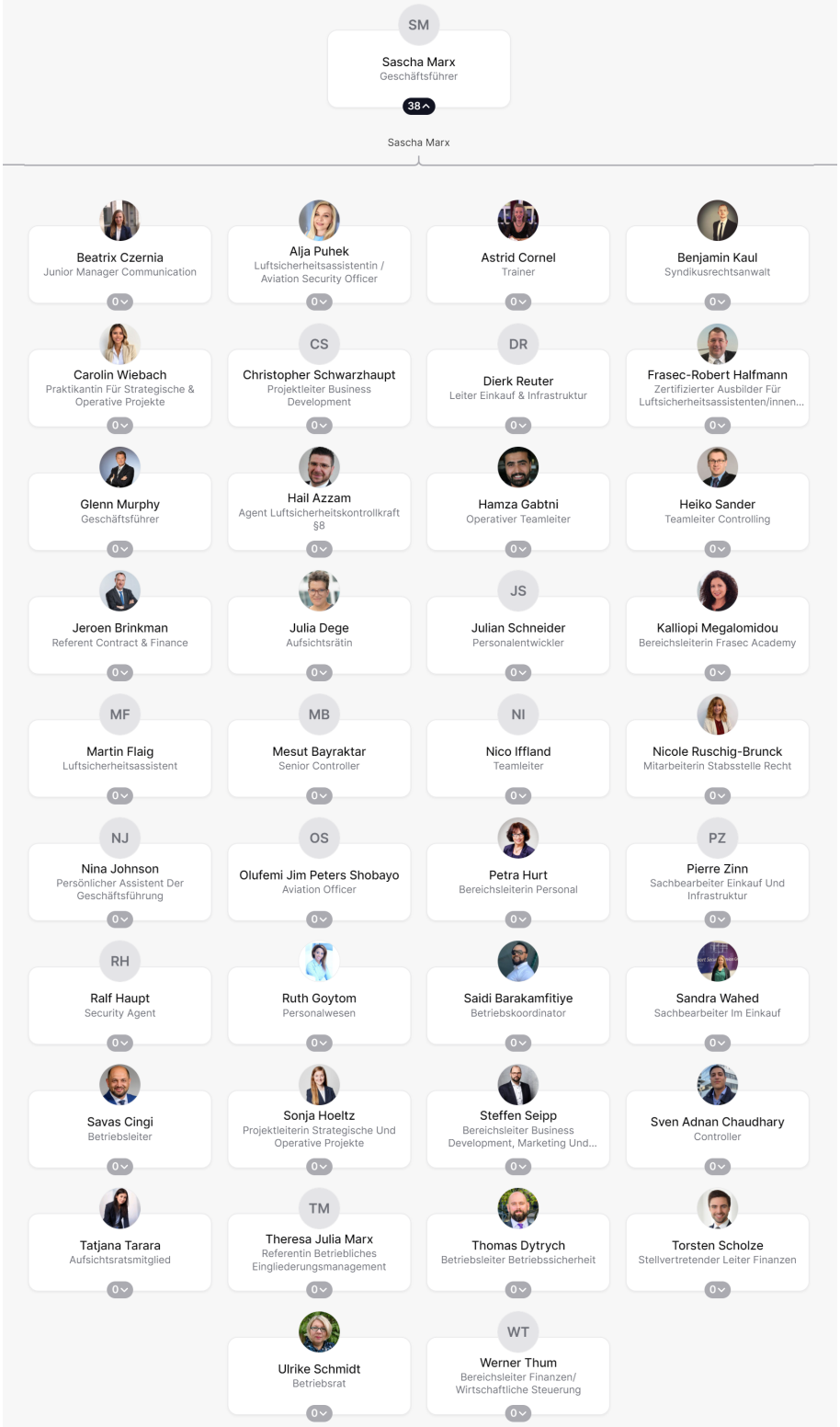
Q Struktur Fraport Group

Fraport-Konzernstruktur

	Dr. Stefan Schulte	Anke Giesen	Julia Kranenberg	Dr. Pierre Dominique Prümm	Prof. Dr. Matthias Zieschang
Segmente	International Activities & Services	Retail & Real Estate	Ground Handling	Aviation	
Strategische Geschäfts- und Servicebereiche	• Akquisitionen und Beteiligungen • Projekt Ausbau Süd	• Handels- und Vermietungs-management • Informations- und Kommunikationsdienst-leistungen	• Bodenverkehrsdienste	• Aviation • Zentrales Infrastruktur-management	• Integriertes Facility Management
Zentralbereiche	• Unternehmens-entwicklung, Umwelt und Nachhaltigkeit • Unternehmens-kommunikation	• Interne Revision • Rechtsangelegenheiten und Compliance	• Personalservice-leistungen		• Finanzen und Investor Relations • Investitions- und Projektcontrolling • Kosten- und Ergebniscontrolling • Rechnungswesen • Zentraler Einkauf und Bauvergabe
Wesentliche Konzern-Gesellschaften	• Fraport Slovenija • Fortaleza & Porto Alegre • Lima • Fraport Greece • Twin Star • Antalya	• Media Frankfurt • Fraport Immobilienservices	• FraGround • FraCareServices	• FraSec Aviation Security • FraSec Flughafen-sicherheit • FraSec Services	• Fraport Facility Services

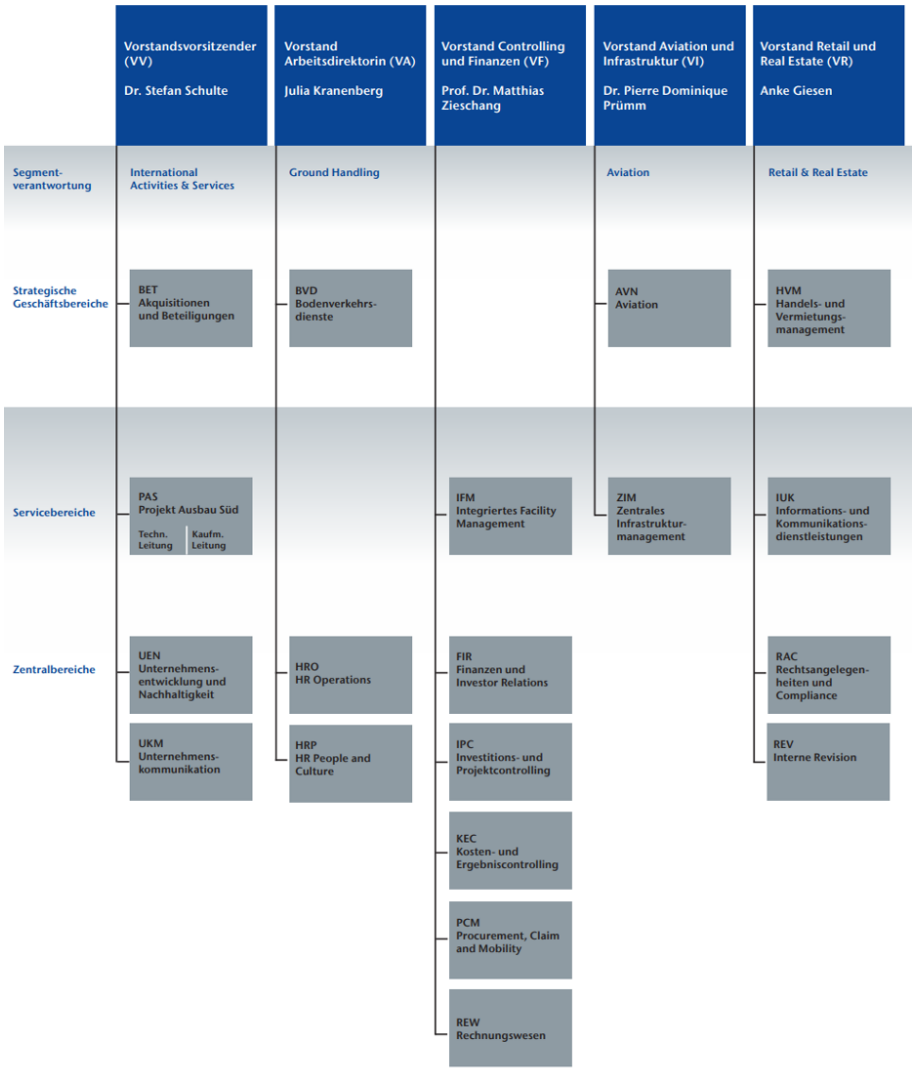
[**20**]

R FraSec Unternehmensgruppe



[**21**]

S Organigramm Fraport AG

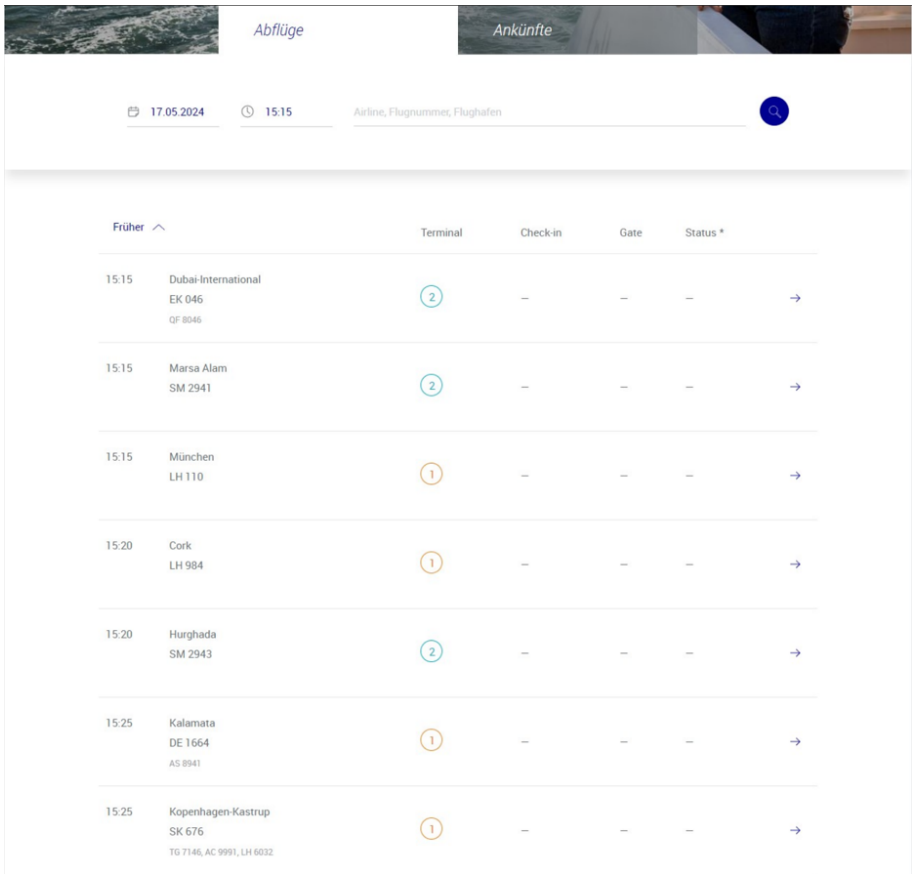


Die Bereiche Arbeitsmedizin (VA3), Arbeitsschutz (VA4) sowie Medizinische Dienste (VA5) sind direkt dem Vorstand Arbeitsdirektorin zugeordnet.

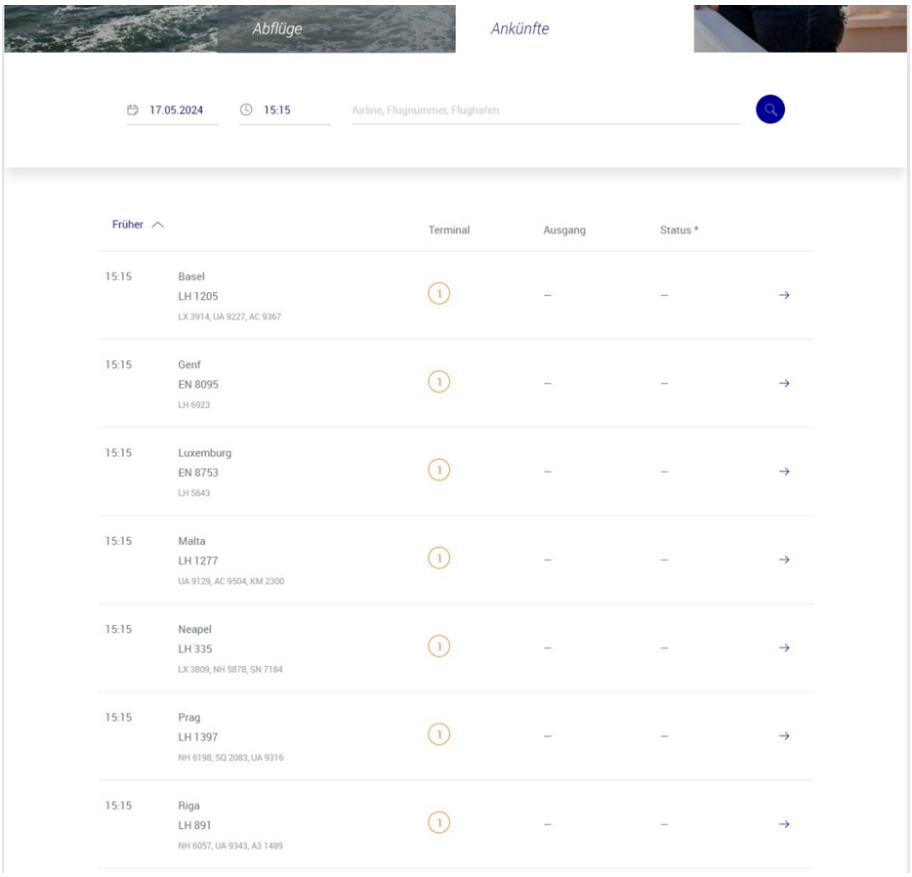
Es besteht ein Gemeinschaftsbetrieb zwischen der Fraport AG, der FRA-Vorfeldkontrolle GmbH (FRAVG) und der Fraport Ground Handling Professionals GmbH (FraGround). Die Arbeitsorganisation des Gemeinschaftsbetriebs wird in einer separaten Abbildung (Anhang 1) dargestellt und im Kooperationsvertrag beschrieben.

[**22**]

T Flugpläne Frankfurt Flughafen vom 17.05.2024



[**23**]


Abflüge
Ankünfte
17.05.2024
15:15
Airline, Flugnummer, Flughafen
Früher
Terminal
Ausgang
Status *
15:15 Basel LH 1205 LX 3914, UA 9227, AC 9367 1 – –
15:15 Genf EN 8095 LH 6923 1 – –
15:15 Luxemburg EN 8753 LH 5643 1 – –
15:15 Malta LH 1277 UA 9129, AC 9504, KM 2300 1 – –
15:15 Neapel LH 335 LX 3809, NH 5878, SN 7184 1 – –
15:15 Prag LH 1397 NH 6198, SQ 2083, UA 9316 1 – –
15:15 Riga LH 891 NH 6057, UA 9343, A3 1489 1 – –

[**24**]

U Mietwagenbuchung

Buchungsnummer: 33964957

Mietwagen

drucken | Termin exportieren | nicht mehr anzeigen

VW Passat oder ähnlich
Frankfurt am Main Flughafen
16.05.2024-19.05.2024

STARCAR

Reklamation/Schaden

gesamt 135,62 €
Preis für 3 Tage

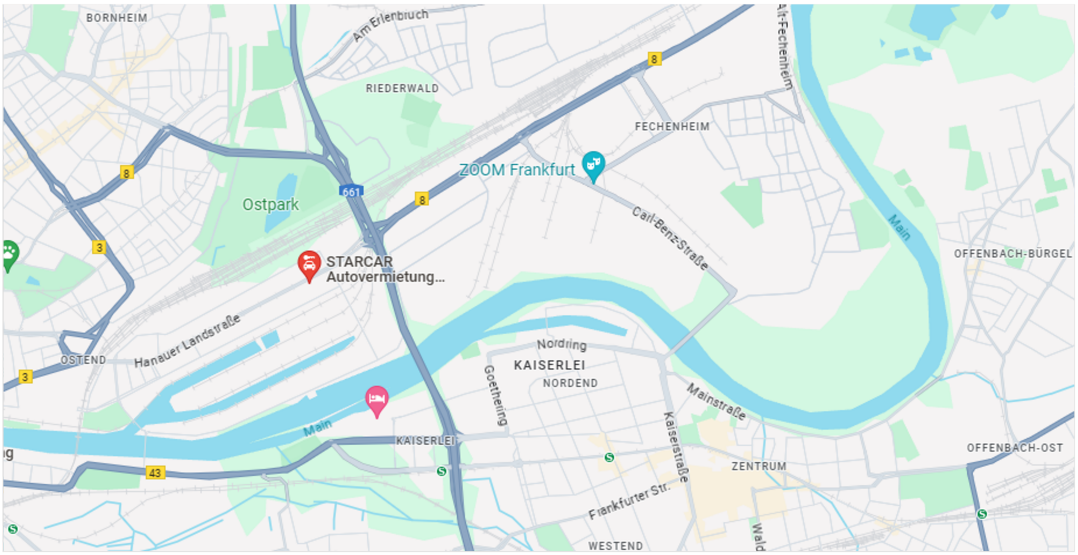
Fahrzeugdetails

Obere Mittelklasse, z.B. Ford Mondeo, BMW 2er Active Tourer (ACRISS-Code SDMR)

5 Sitze | 4 Türen | 3 Koffer | Manuell | Klima

Abholung & Rückgabe

Abholung		**Rückgabe**	
Wann?	Do., 16.05.2024, 12:00 Uhr	Wann?	So., 19.05.2024, 12:00 Uhr
Wo?	Hanauer Landstraße 208-2016 STARCAR Autovermietung 60314 Frankfurt am Main	Wo?	Hanauer Landstraße 208-2016 STARCAR Autovermietung 60314 Frankfurt am Main
Kontakt Station	+49 69 415030	Kontakt Station	+49 69 415030
Öffnungszeiten	06:30 – 23:00 Uhr	Öffnungszeiten	06:30 – 23:00 Uhr



Hinweise für den Hauptfahrer

Vom **Hauptfahrer** sind vor Ort ein gültiger Führerschein und ein **Personalausweis** oder **Reisepass** vorzuzeigen.

Ihr Vermieter **blockt** vor Ort eine **Kaution** (Höhe siehe Mietbedingungen) auf Ihrer **Kreditkarte**. Sie benötigen dafür Ihre Kreditkarten-**PIN**.
Debit- und Prepaidkarten, American Express sowie **Apple Pay** und **Google Pay** werden am Schalter oft **nicht akzeptiert**.

Quellverzeichnis

[1] https://www.fraport.com/de/konzern/ueber-uns/zahlen--daten-und-fakten1.html [zuletzt besucht am 29.06.2024]

[2] https://de.wikipedia.org/wiki/Flughafen_Frankfurt_Main [zuletzt besucht am 29.06.2024]

[3] https://terminal3.frankfurt-airport.com/ [zuletzt besucht am 29.06.2024]

[4] https://www.maniago.de/produkte/fluchttuersteuerung-fsps [zuletzt besucht am 05.07.2024]

[5] https://www.fs-architekten.de/projekte/fraport-geb-201-rba10-brandschutz\protect\@normalcr\relaxsanierung-25 [zuletzt besucht am 05.07.2024]

[6] https://commons.wikimedia.org/wiki/File:Frankfurt-Main_Airport_Map_DE.png [zuletzt besucht am 05.07.2024]

[7] https://static.fraport.de/ONLINE/pdfRH/uebersicht-airport-city-frankfurt.pdf [zuletzt besucht am 05.07.2024]

[8] https://b2b.frankfurt-airport.com/content/dam/fraport-travel/airport/dokumente/b2b/Immobilien/CargoCity.pdf/_jcr_content/renditions/original.media_file.download_attachment.file/CargoCity.pdf [zuletzt besucht 05.07.2024]

[9] https://www.fraport.com/content/dam/fraport-company/images/newsroom/pressemappe/besucherzentrum-30-06-2021/dokumente-de/BZ-lageplan.jpg/_jcr_content/renditions/original.media_file.download_attachment.file/BZ-lageplan.jpg [zuletzt besucht am 05.07.2024]

[10] https://c1.abus.com/var/ImagesPIM/d110001/medias/docus/9/Bedienungsanleitung_Terxon_LX.pdf [zuletzt besucht am 05.07.2024]

[11] https://alarmanlage.de/wp-content/uploads/2021/09/Handbuch_EESec2.pdf [zuletzt besucht am 05.07.2024]

[12] https://www.lanuv.nrw.de/veroeffentlichungen/sondersam/hndbetec/11_k7_web.pdf [zuletzt besucht am 05.07.2024]

[13] https://www.grund-wissen.de/elektronik/_downloads/grundwissen-elektronik.pdf [zuletzt besucht am 05.07.2024]

[14] http://www.muellerbahn.de/media/Rackbelegung.jpg [zuletzt besucht am 05.07.2024]

[15] https://www.drk-nrw.de/fileadmin/user_upload/DRK_in_NRW/NRW_Dokumente/verpflegungsmodul_nrw/betriebsanleitungen/eisemann/Bedienungsanleitung_Cube_9_14_17KVA.pdf [zuletzt besucht am 05.07.2024]

[16] https://sslapps.fraport.de/webportalAVS/pdf/Allgemeine-Flughafenordnung.pdf [zuletzt besucht am 05.07.2024]

[17] https://sslapps.fraport.de/webportalAVS/pdf/Ausweisordnung.pdf [zuletzt besucht am 05.07.2024]

[18] https://sslapps.fraport.de/webportalAVS/pdf/SMS-Ordnung.pdf [zuletzt besucht am 05.07.2024]

[19] https://www.fraport.com/content/dam/fraport-company/documents/geschaeftsfelder/service/richtlinien-und-zahlungsbedingungen/richtlinien/de/2024/C4.8%20Brandschutzordnung%20v2.0%20Teil%20B.pdf/_jcr_content/renditions/original.media_file.download_attachment.file/C4.8%20Brandschutzordnung%20v2.0%20Teil%20B.pdf [zuletzt besucht am 05.07.2024]

[20] https://www.geschaeftsbericht.fraport.de/annual-report/2022/de/zusammengefasster-lagebericht/grundlagen-des-konzerns/struktur/ [zuletzt besucht am 05.07.2024]

[21] https://theorg.com/org/frasec-unternehmensgruppe [zuletzt besucht am 05.07.2024]

[22] https://www.fraport.com/content/dam/fraport-company/documents/konzern/fraport/%C3%BCber-uns/Gesamtorganigramm%203_24%20D.pdf/_jcr_content/renditions/original.media_file.download_attachment.file/Gesamtorganigramm%203_24%20D.pdf [zuletzt besucht am 05.07.2024]

[23] https://www.frankfurt-airport.com/de/fluege-und-airlines/abfluege.html [zuletzt besucht am 17.05.2024]

[24] https://www.frankfurt-airport.com/de/fluege-und-airlines/ankuenfte.html [zuletzt besucht am 17.05.2024]

Abbildungsverzeichnis

1 Bekennerschreiben . . . 6
2 Wiederherstellung unter Windows . . . 12
3 Optionen beim Zurücksetzen . . . 12
4 Optionen der Neuinstallation . . . 13
5 Notebook Vorderseite . . . 18
6 Notebook Rückseite . . . 18
7 USB-Stick Vorderseite . . . 19
8 USB-Stick Rückseite . . . 19
9 Magnet.AI . . . 21
10 Entschlüsselung AXIOM . . . 22
11 Artefakte Notebook . . . 22
12 Hashes Notebook . . . 23
13 Partitionen Notebook . . . 23
14 Systeminformationen Notebook . . . 24
15 Benutzerkonten Notebook . . . 24
16 Lokaler Zugriff . . . 26
17 Download Edge . . . 26
18 Standardbrowser . . . 27
19 Suchbegriffe Google . . . 27
20 Suche Google Maps . . . 28
21 Erste Koordinate Google Maps . . . 28
22 Zweite Koordinate Google Maps . . . 28
23 Discord Edge . . . 29
24 Discord Kanal . . . 29
25 Kingston USB-Stick . . . 30
26 Seriennr. USB-Stick . . . 30
27 Volume USB-Stick . . . 31
28 Hashes USB-Stick . . . 32
29 Partition USB-Stick . . . 32
30 Seriennummer USB-Stick . . . 33
31 Dokumente USB-Stick . . . 33
32 Bilddateien USB-Stick . . . 34
33 PDF-Dateien USB-Stick . . . 34

Tabellenverzeichnis

1 Zeitlicher Verlauf Szenario 11
2 Untersuchungswerkzeuge 20
3 Dokumente 26

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbständig verfasst und keine anderen als die angegebenen Hilfsmittel benutzt habe. Die Stellen der Arbeit, die anderen Quellen im Wortlaut oder dem Sinn nach entnommen wurden, sind durch Angaben der Herkunft kenntlich gemacht. Dies gilt auch für Zeichnungen, Skizzen, bildliche Darstellungen sowie für Quellen aus dem Internet.

Ich erkläre ferner, dass ich die vorliegende Arbeit in keinem anderen Prüfungsverfahren als Prüfungsarbeit eingereicht habe oder einreichen werde.

Die eingereichte schriftliche Arbeit entspricht der elektronischen Fassung. Ich stimme zu, dass eine elektronische Kopie gefertigt und gespeichert werden darf, um eine Überprüfung mittels Anti-Plagiatssoftware zu ermöglichen.

Ort, Datum Unterschrift