HOCHSCHULE MITTWEIDA
University of Applied Sciences

Betriebssysteme

Windows Sicherheit

(Foliensatz ©Felix Fischer, M.Sc.)

Prof. Ronny Bodach; Leander Hoßfeld, B.Sc.

16.05.2023

Bundeskriminalamt

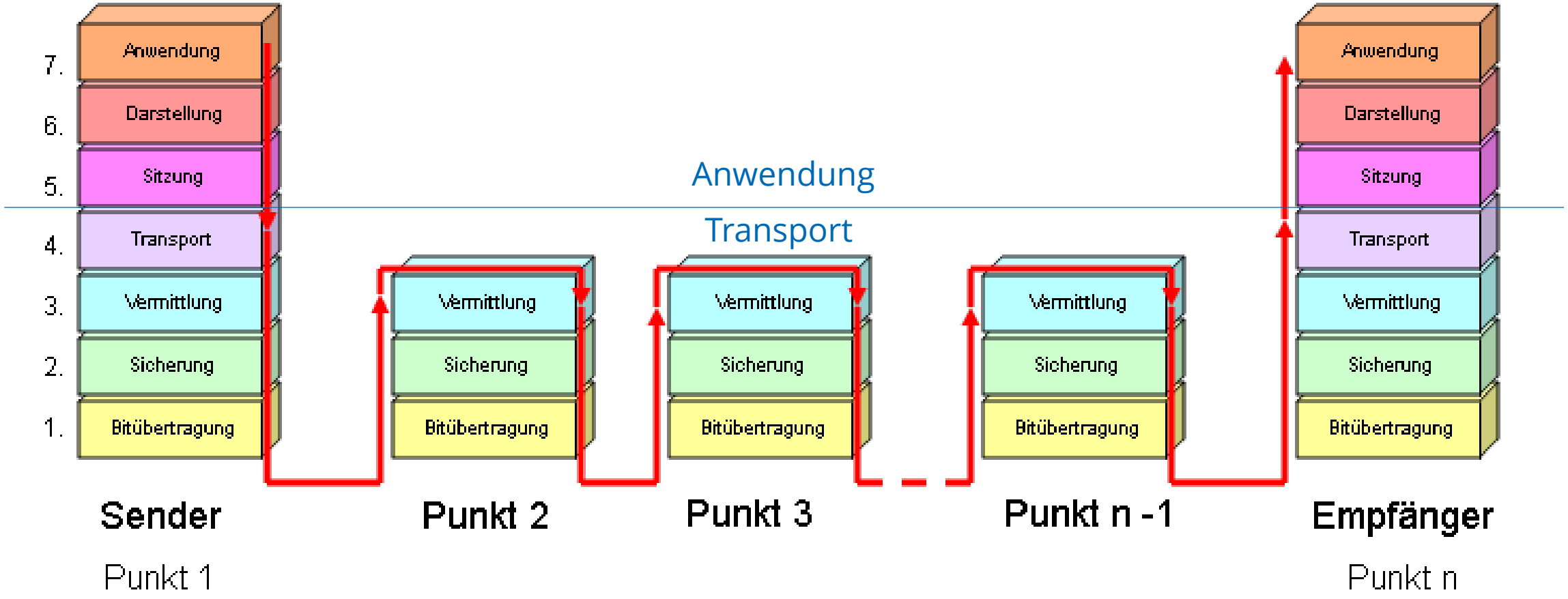
hossfeld@hs-mittweida.de

Agenda

1. Firewall
2. Netzwerk Zonen
3. Updates
4. Schutzmechanismen
5. EFS Verschlüsselung
6. VSS Volume Shadow Copy Service

Firewall

Wiederholung OSI-Modell
Open System Interconnection



Wiederholung OSI-Modell

- Application Layer
  - Informationsaustausch zwischen Anwendungen
  - Teilnehmer Identifikation
  - Teilnehmer Verifikation und Sicherheitschecks
- Presentation Layer
  - Aufbereiten der Daten für Applikation Layer für einfachen Zugriff
  - Datenformatierung
  - Kompression
  - Übertragungsverschlüsselung
- Session Layer
  - High-Level Synchronisation zwischen Anwendungen
  - Regelung der Übertragungskommunikation (Wer spricht? Wer hört zu?)

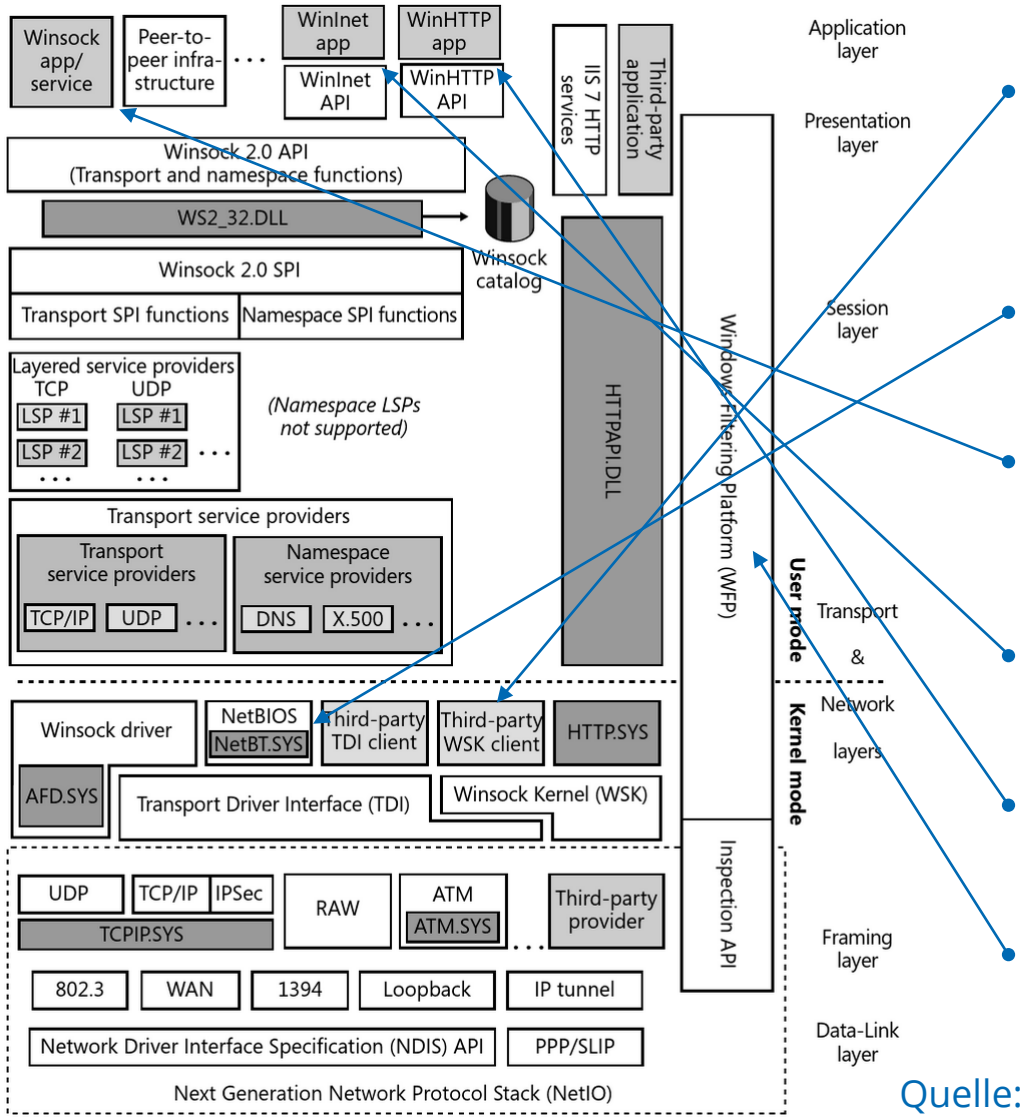
Wiederholung OSI-Modell

- Transport Layer
  - Paketisierung der Daten
  - Organisation der ankommenden Daten (Reihenfolge)
  - Bereitstellen eines rein logischen Datenstromzugangs für Session Layer
- Network Layer
  - Paketzustellung (Routing)
  - Internetworkkommunikation
  - Logischer Netzwerkaufbau
- Data-Link Layer
  - Datenübertragung innerhalb eines Netzwerks
  - Daten erreichen nächsten Knoten auf der Route zum Zielrechner
  - Kollisionserkennung bei Übertragung
- Physical Layer
  - Übertragung von Bits zum nächsten Kommunikationsgerät

OSI-Modell
Analogie zum Verstehen

- Application Layer — Nachrichtentext
- Presentation Layer — Sprache, Formatierung von Text, Tabellen, …
- Session Layer — Brieflayout, Formulierungsgrad (formell, informell)
- Transport Layer — Brief in Umschlag verpacken, Frankierung
- Network Layer — Postanschrift
- Data-Link Layer — Verteilungszentrum ordnet Brief Transportmittel zu
- Physical Layer — Postboten, LKWs, Flugzeuge transportieren Brief

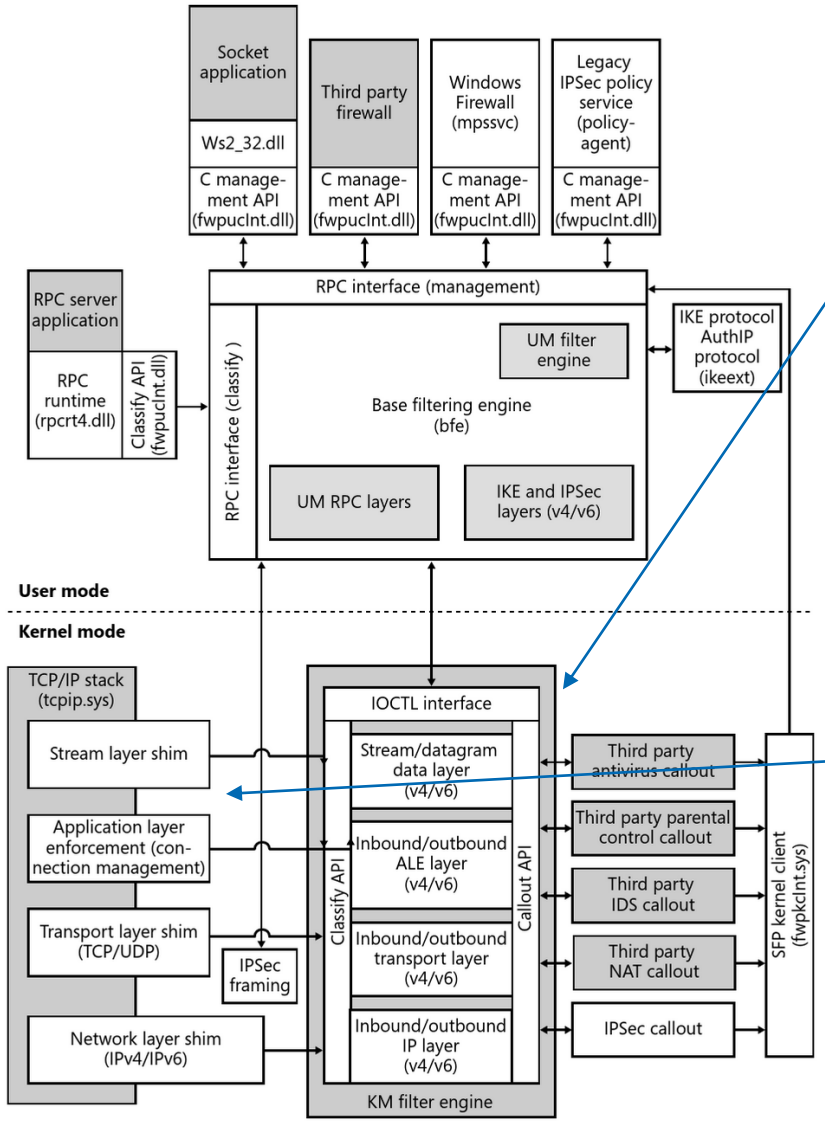
Windows Netzwerkkomponenten



- Windows Sockets
  - Funktionsweise von BSD-Sockets
  - Portierung von BSD/UNIX-Anwendungen
- NetBIOS
  - legacy, Abwärtskompatibilität
- Winsock
  - Client und Server Sockets für Windows-Anwendungen
- WinInet
  - API für FTP und HTTP
- WinHTTP
  - API für HTTP
- Windows Filtering Platform
  - Regeln für Netzwerkverkehr / -zugang

Quelle: Windows Internals

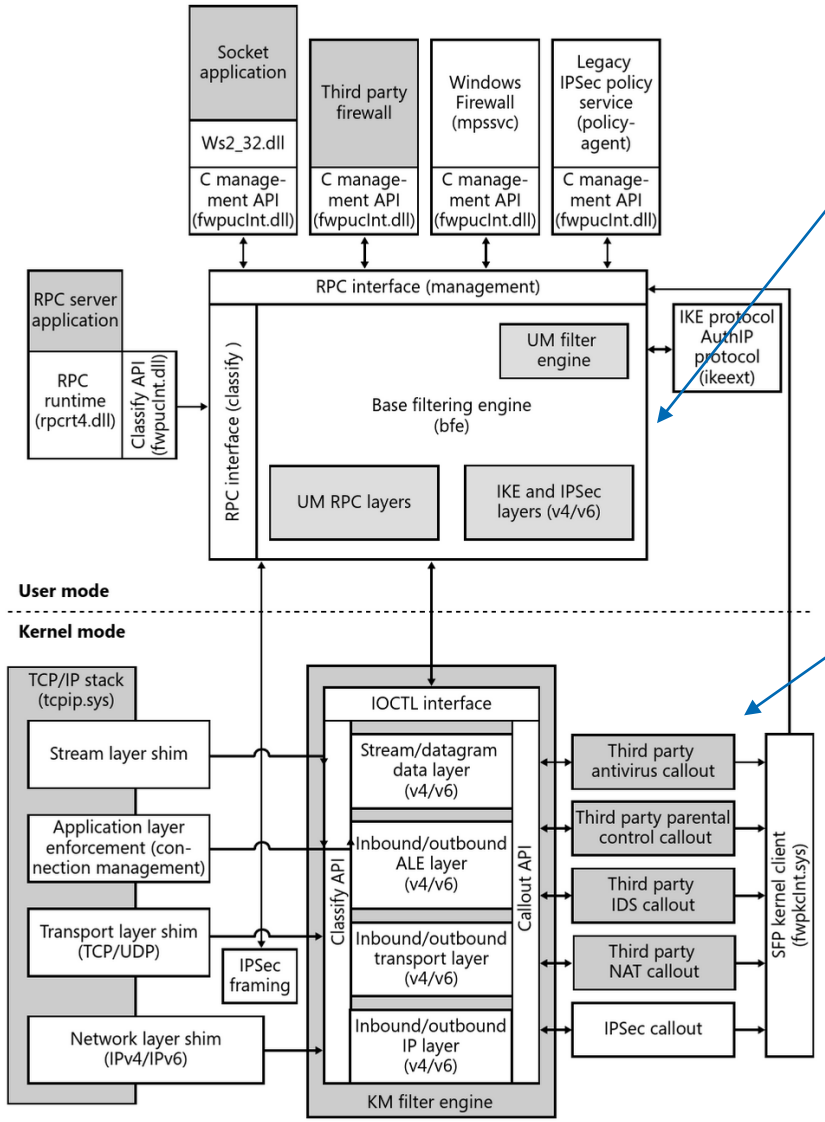
Windows Filtering Platform



- Filterung auf allen Levels des Network-Stacks
- Filter-Engine
  - User-Mode
    - RPC und IPSec Filter
    - Anwendungsorientiert
  - Kernel-Mode
    - TCP/UDP und IP Filter
    - Transportorientiert
- Shims
  - Normalisierung der Daten für Filter
  - Abfrage an Filter-Engine
  - Aktionsdurchführung (drop, pass, reject)

Quelle: Windows Internals

Windows Filtering Platform

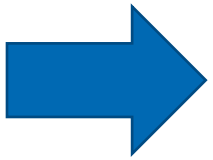


- Base Filtering Engine
  - Management aller WFP Operationen
  - Filter hinzufügen
  - Filter entfernen
  - Filterdatabase Security
- Callout Drivers
  - Deep Packet Inspection
  - Packet Modification (Sanitation)
  - Network Adress Translation (NAT)

Quelle: Windows Internals

Firewall Actions

- Pass
  - Normale Weiterleitung des Pakets
- Block / Drop
  - Löschen des Pakets
- Reject
  - Löschen des Pakets
  - Sender über Löschen informieren
  - Debuginformationen für Netzwerkadmin
  - Informationen für Angreifer
    - Firewall vorhanden und aktiv
    - Firewall Regel hat gegriffen
    - Admin eventuell informiert



Pass = erlaubt

Block = nicht erlaubt, Produktivbetrieb

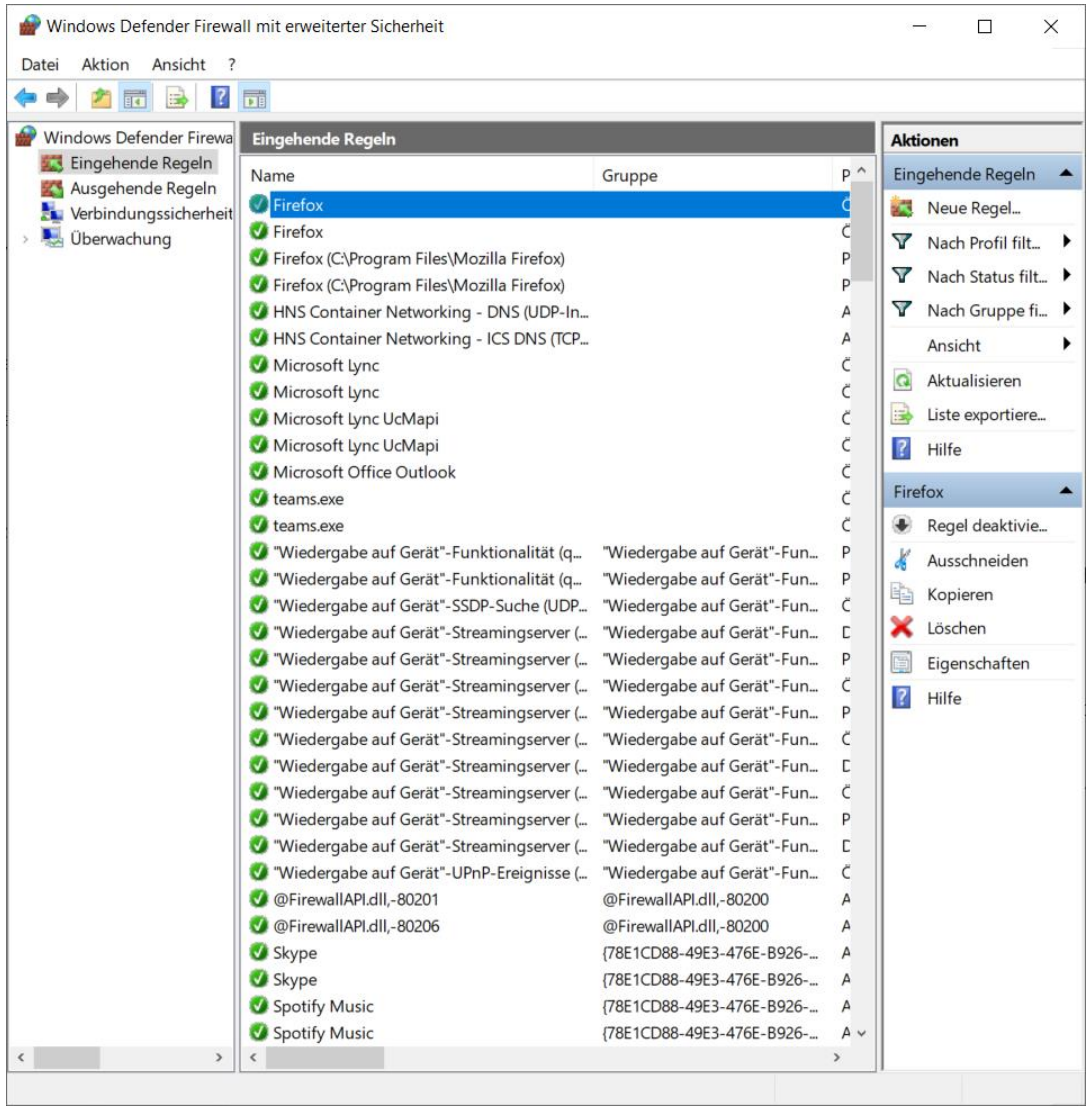
Reject = nicht erlaubt, Netzwerkkonstruktion

Filtermodus

- Whitelist (Allowlist)
  - Liste mit erlaubten Regeln
  - Alles andere Verboten
- Empfohlen für sicheres Design
- Aufwendig zu Beginn einzurichten
- Einrichtung wächst mit Nutzung
- Resistent gegen vergessene Ausnahmen / Spezialfälle
- Fail-Safe
- Beispiel: Haustürschloss

- Blacklist (Denylist)
  - Liste mit verbotenen Regeln
  - Alles andere erlaubt
- Anwenderfreundlich (Alles funktioniert zunächst)
- Einrichtung wächst mit Angriffswegen
- An alle Angriffswege muss gedacht werden
- Beispiel: Gesetzestexte

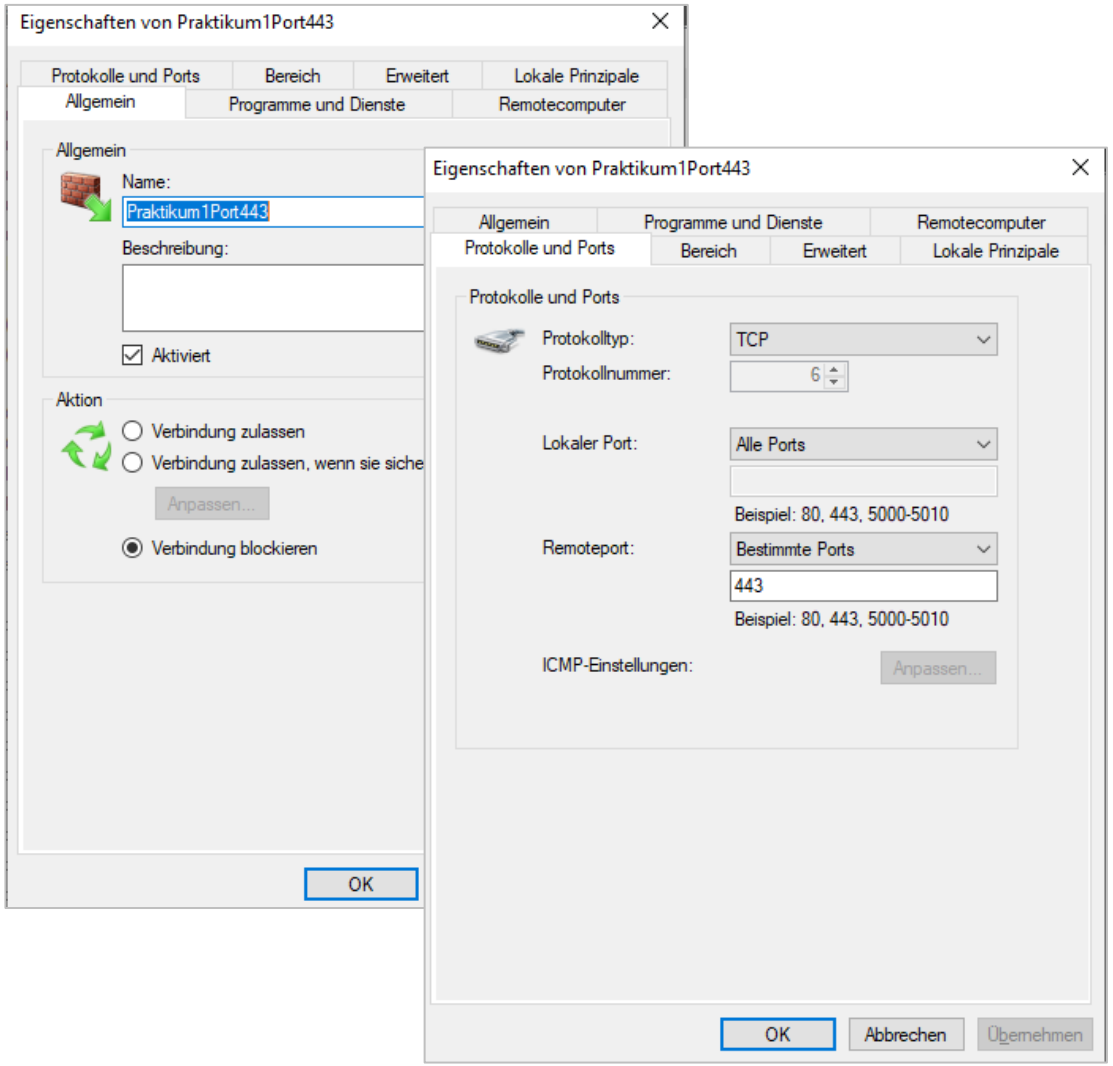
Windows Defender Firewall Regeln



Regeln basieren auf:

- Ports
  - eingehend
  - ausgehend
- IP-Adresse
  - Sender
  - Empfänger
- Transportprotokoll
  - TCP
  - UDP
- Richtung
  - eingehend
  - ausgehend
- Anwendung
- Netzwerkumgebung
  - privat (Heimnetzwerk)
  - öffentlich
- Benutzer
- Domaine

Windows Defender Firewall Regeln



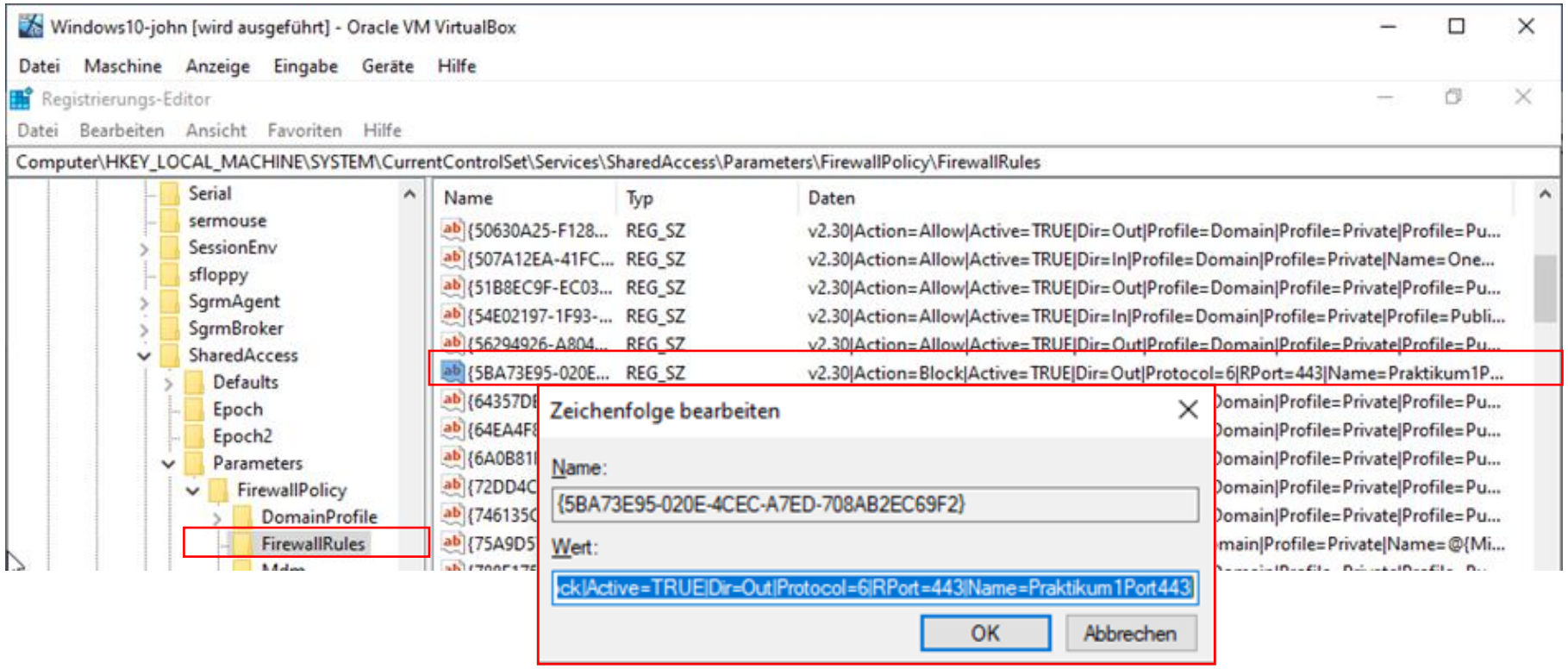
Regeln basieren auf:

- Ports
  - eingehend
  - ausgehend
- IP-Adresse
  - Sender
  - Empfänger
- Transportprotokoll
  - TCP
  - UDP
- Richtung
  - eingehend
  - ausgehend
- Anwendung
- Netzwerkumgebung
  - privat (Heimnetzwerk)
  - öffentlich
- Benutzer
- Domaine

Windows Defender Firewall Regeln

Firewall Regeln sind in der Registrierung abgelegt:

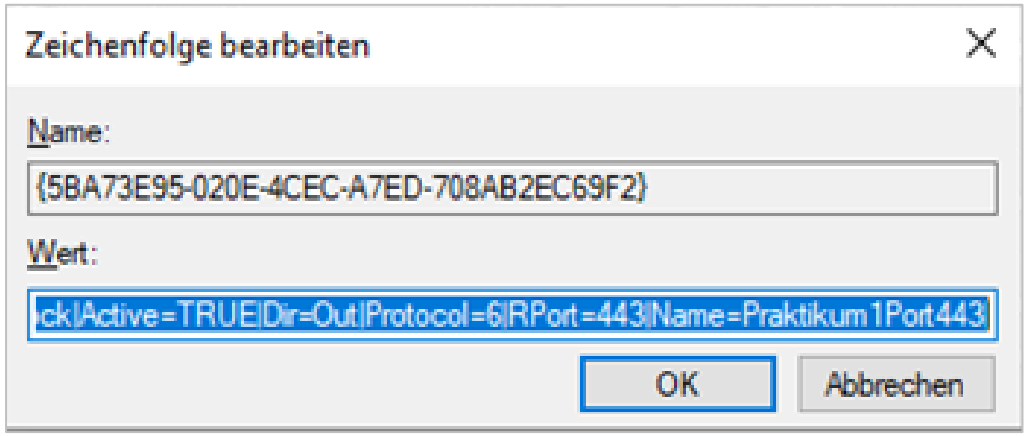
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SharedAccess\Parameters\FirewallPolicy\FirewallRules



Windows Defender Firewall Regeln

Eintragungen für Firewall Regeln in der Registrierung :

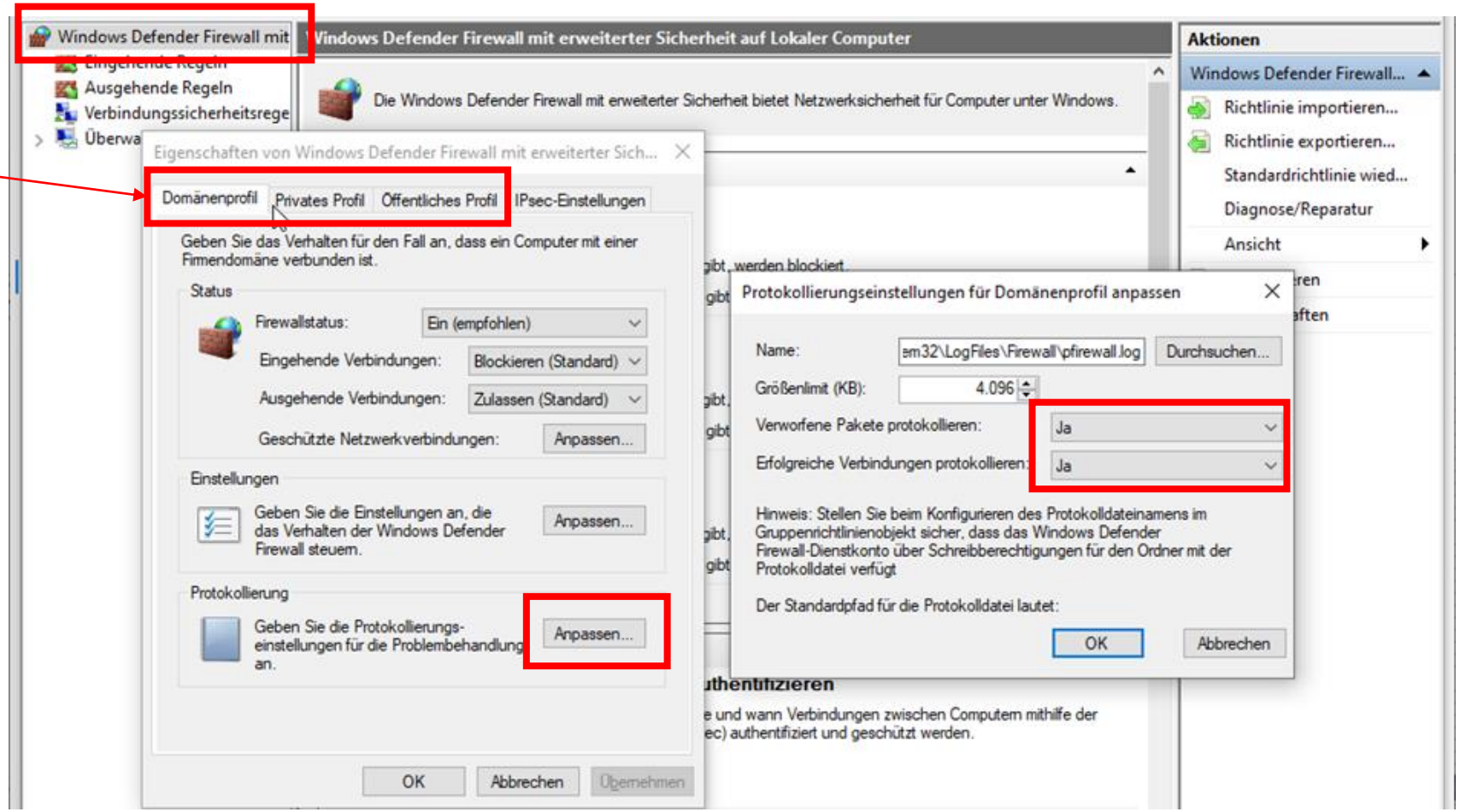
- Protocol:
  - 6 ist TCP
  - 17 ist UDP
  - 1 ist ICMP
- Lport: lokaler Port
- Rport: remote Port
- LA4 oder LA6: lokale IPv4 oder IPv6 Adresse
- RA4 oder RA6: remote IPv4 oder IPv6 Adresse
- App: Applikation für Regel-Match (application-specific rules unabhängig vom Port)
- Name: Regelname
- Profile: Firewall Profil für die Regel gilt (Domain, Private und Public)



Windows Defender Firewall Logs

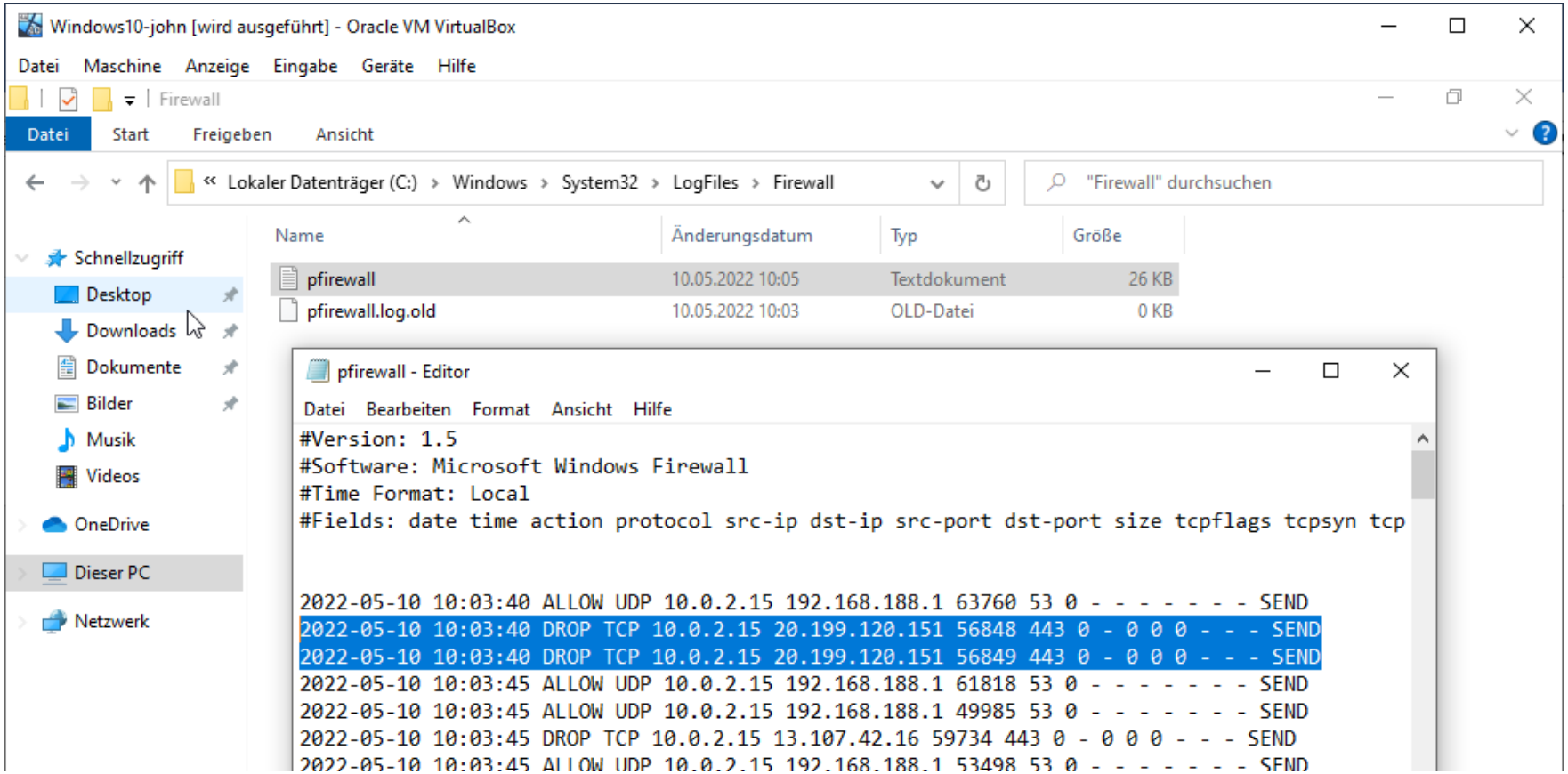
Firewall Logfiles müssen im Standard erst aktiviert werden:

- für alle drei Profile separat aktivieren



Windows Defender Firewall Logs

Standardpfad ist "%systemroot%\system32\logfiles\firewall\pfirewall.log„:



Netzwerk Zonen

Zone Identifier

- Windows XP SP2 Einführung alternativer NTFS Datenstrom "Zone.Identifier"
- NUR auf einem NTFS Dateisystem vorhanden!
- Zone.Identifier wird von Web Anwendungen generiert
- wird angelegt wenn Benutzer:

Dateien aus **anderen Sicherheitszone** --> im **lokalen Dateisystem speichert**

Zone Identifier

Es gibt 5 am häufigsten vorkommende Zonen-IDs:

0 - Lokale Computerzone, die vertrauenswürdigste Zone für Inhalte, die auf dem lokalen Computer vorhanden sind

1 - Lokale Intranetzone für Inhalte im Intranet einer Organisation

2 - Zone vertrauenswürdiger Sites für Inhalte auf Websites, die als seriöser oder vertrauenswürdiger gelten als andere Websites im Internet

3 - Internetzone für Websites im Internet, die keiner anderen Zone angehören

4 - Zone für eingeschränkte Sites für Websites, die möglicherweise unsicheren Inhalt enthalten

Zone Identifier

Browser Beispiele für Downloads:

Google Chrome:

```
[ZoneTransfer]
ZoneId=3
ReferrerUrl=http://referringurl.com/
HostUrl=http://referringurl.com/wpcontent/uploads/LOGO_NEW.png
```

Firefox:

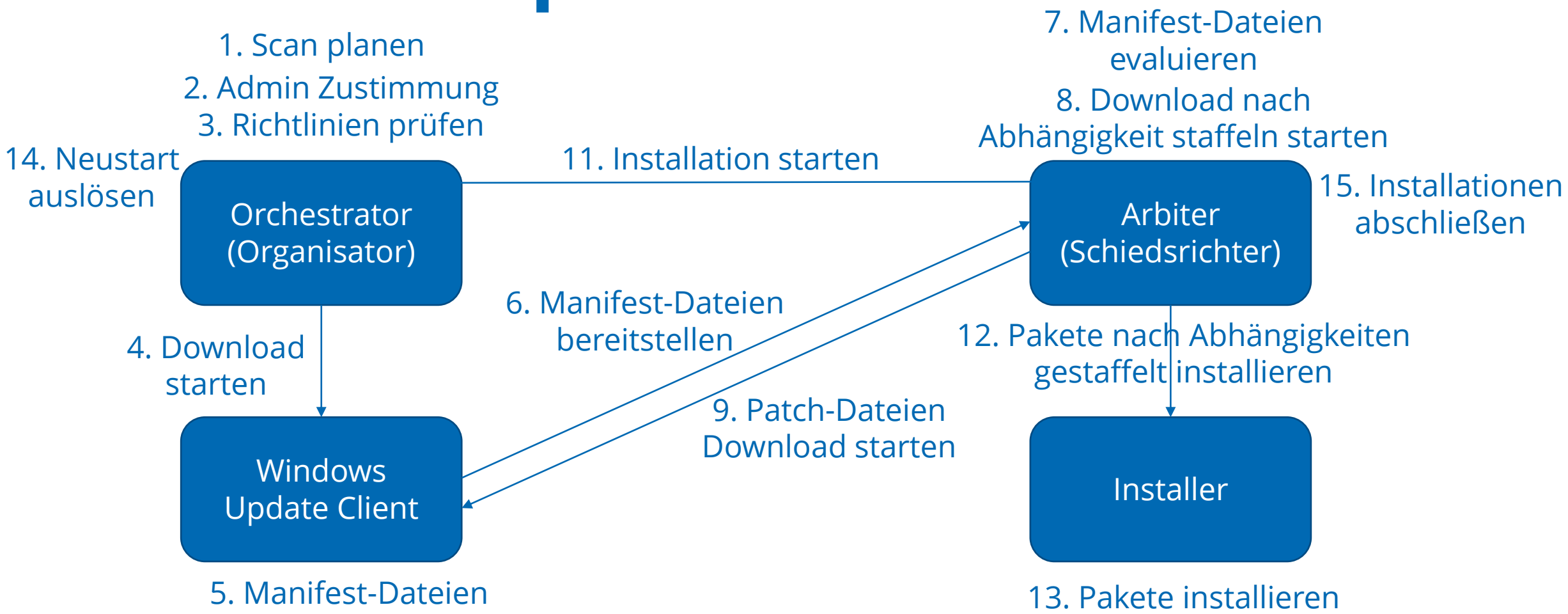
```
[ZoneTransfer]
ZoneId=3
```

Microsoft Edge:

```
[ZoneTransfer]
LastWriterPackageFamilyName=Microsoft.MicrosoftEdge_8wekyb3d8bbwe
ZoneId=3
```

Updates

Windows Updateablauf



Windows Update-Typen

- Feature Update
  - Halbjähriger Release
  - Neue Funktionen im Betriebssystem
- Cummulative Updates
  - 14-tägige Updates
  - Fehlerbehebung, Performance- und Sicherheitsupdates
- Security Update
  - Monatlich am 2. Donnerstag im Monat
  - Außerplanmäßig, bei sehr kritischen Schwachstellen
  - Sicherheitsupdate
- Servicing Stack Update (SSU)
  - Fehlerpatches für Spezialfälle
  - Vorbereitung vor eigentlichen Patch
- Compartibility and Reliability Update
  - Kompatibilitätsvorbereitung für Installationen
- Microcode Update
  - CPU-Schwachstellen Patch
  - Patches für Hardwareprobleme durch Microcode
- Intelligence Update for Defender Antivirus
  - Update Liste schädlicher Programme
  - Update Kennungen von Schadsoftware

Schutzmechanismen

AAA-System

- Authentication (Authentifikation)
  - Identifikation
  - Nachweis des Rechteanfragenden
- Authorization (Autorisierung)
  - Zugriff festlegen
  - Zugriff gewähren
- Accounting (Protokollierung)
  - Zugriff protokollieren
  - Auf was wurde zugegriffen?
  - Wann / Wie lange wurde darauf zugegriffen?

Wer bist du?

Du bist also Barack Obama?
Beweise es mir!

Das darfst du!

Du darfst:
drucken
die Datei X öffnen
diese Webseiten aufrufen
...

Das wird in den Akten hinterlegt.

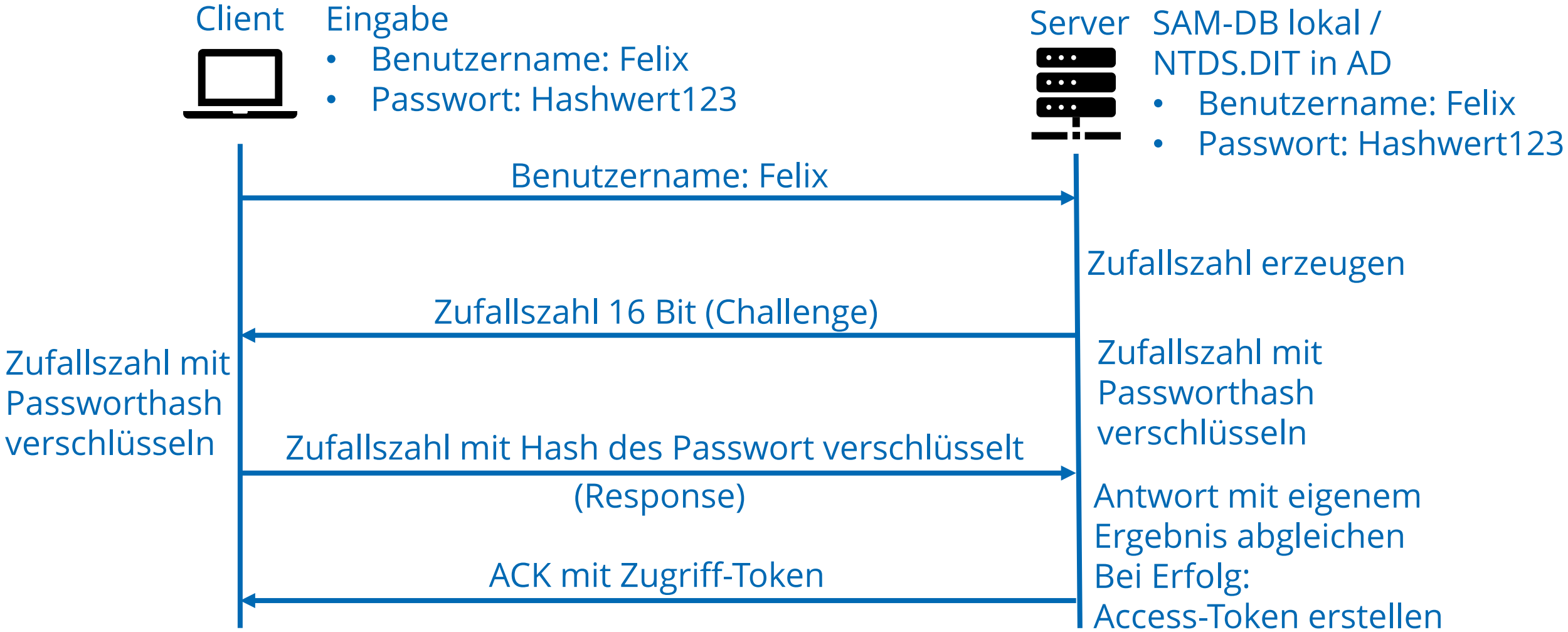
Person X hat Datei Y um 15:05 Uhr geöffnet.

Person Z hat um 16:04 Uhr folgende Anfrage an die Datenbank gestellt: ...

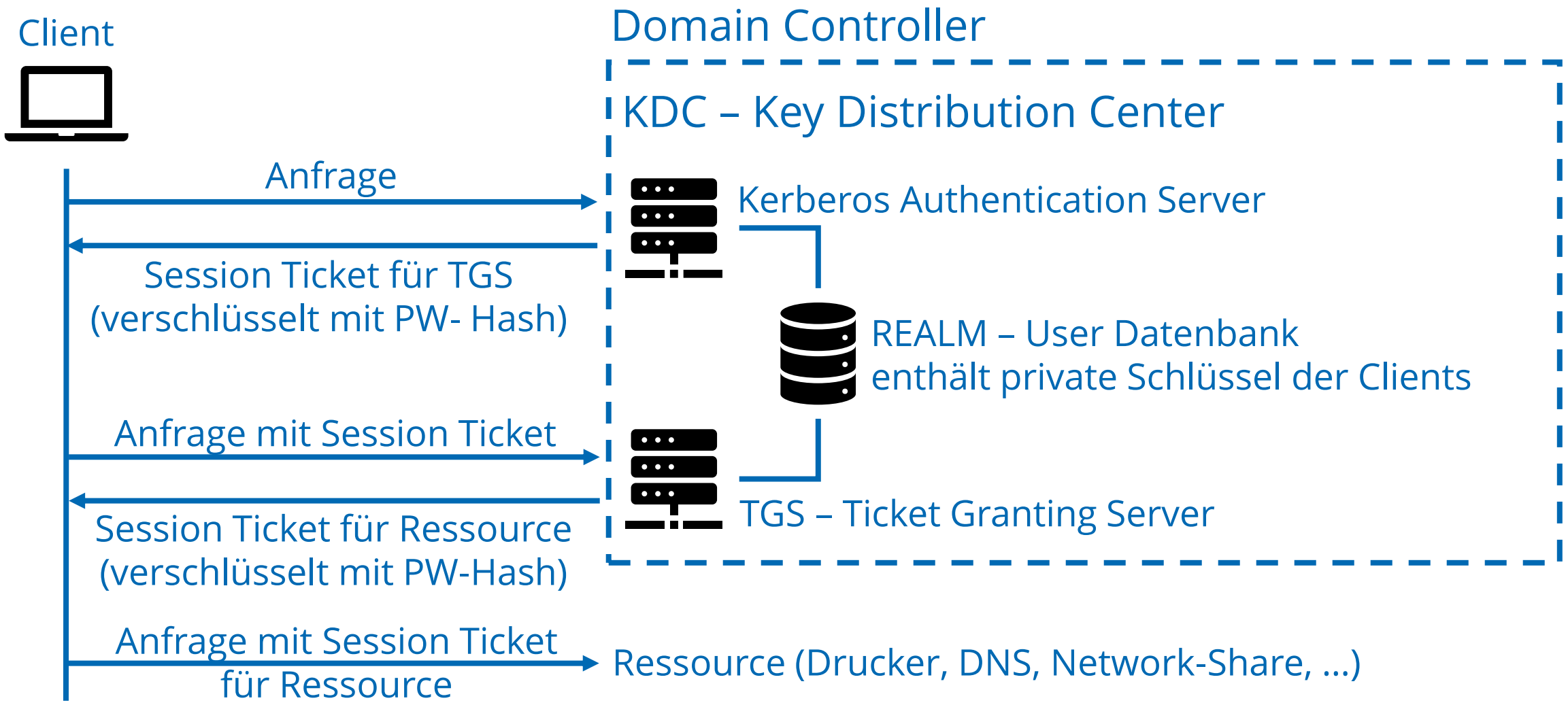
Authentifizierung unter Windows

- Privates Geheimnis
  - Passwort
  - PIN (gescheitertes Biometrisches Merkmal)
- Biometrisches Merkmal
  - Gesicht
  - Fingerabdruck
- Besitz
  - Keycard
- NT LAN Manager (NTLM)
  - Challenge and Response
- Kerberos
  - Gemeinsames Geheimnis

NT LAN Manager (NTLM)



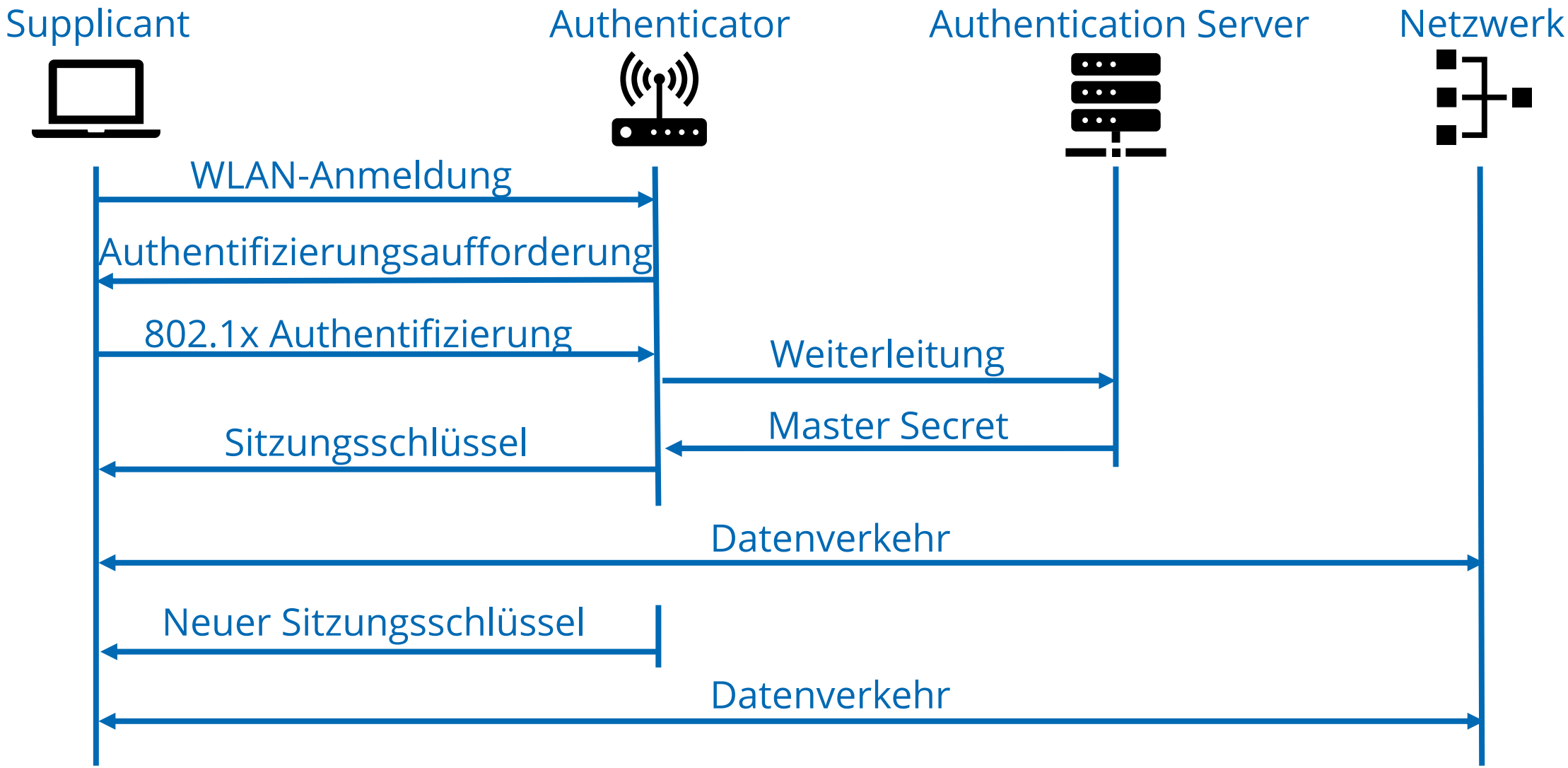
Kerberos



EAP und RADIUS

- Extensible Authentication Protokoll
- definiert in Standard IEEE 802.1x
- Integriert in Data-Link-Layer (OSI-Schicht 2)
- Ziele
  - Netzwerkzugang nur mit Authentifizierung
  - Protokollierung von Netzwerknutzung
- Bestandteile
  - Supplicant (Client)
  - Authenticator (Netzwerkschnittstelle)
  - Authentication Server (meistens RADIUS-Server)

EAP und RADIUS (Beispiel WLAN)



Windows Passwörter

- Maximal 127 Zeichen
- Unicode-Zeichensatz
- Gespeichert als Hash, jedoch stets ohne Salt
- Lan Manager-One-Way-Function (LM OWF)
  - Abwährtskompatibilität
  - Nur die ersten 14 Bytes des PW werden verwendet
  - DES-Hash, Keine Case-Sensitivität
- NT One-Way-Function (NT OWF)
  - Empfohlen, da sicherer
  - MD4-Hash

Windows Passwort umgehen

- PC mit Linux-Live-Stick starten
- Festplatte unter Linux einbinden
- Backup von /Windows/System32/Utilman.exe
- /Windows/System32/Utilman.exe durch /Windows/System32/cmd.exe überschreiben
- PC neu starten
- Erleichterte Bedienung öffnet CMD mit Systemrechten („Uhr“-Symbol in der rechten unteren Ecke)
- Befehl eingeben: „net user USERNAME NEUES_PASSWORT“
- Anmelden mit neuen Passwort

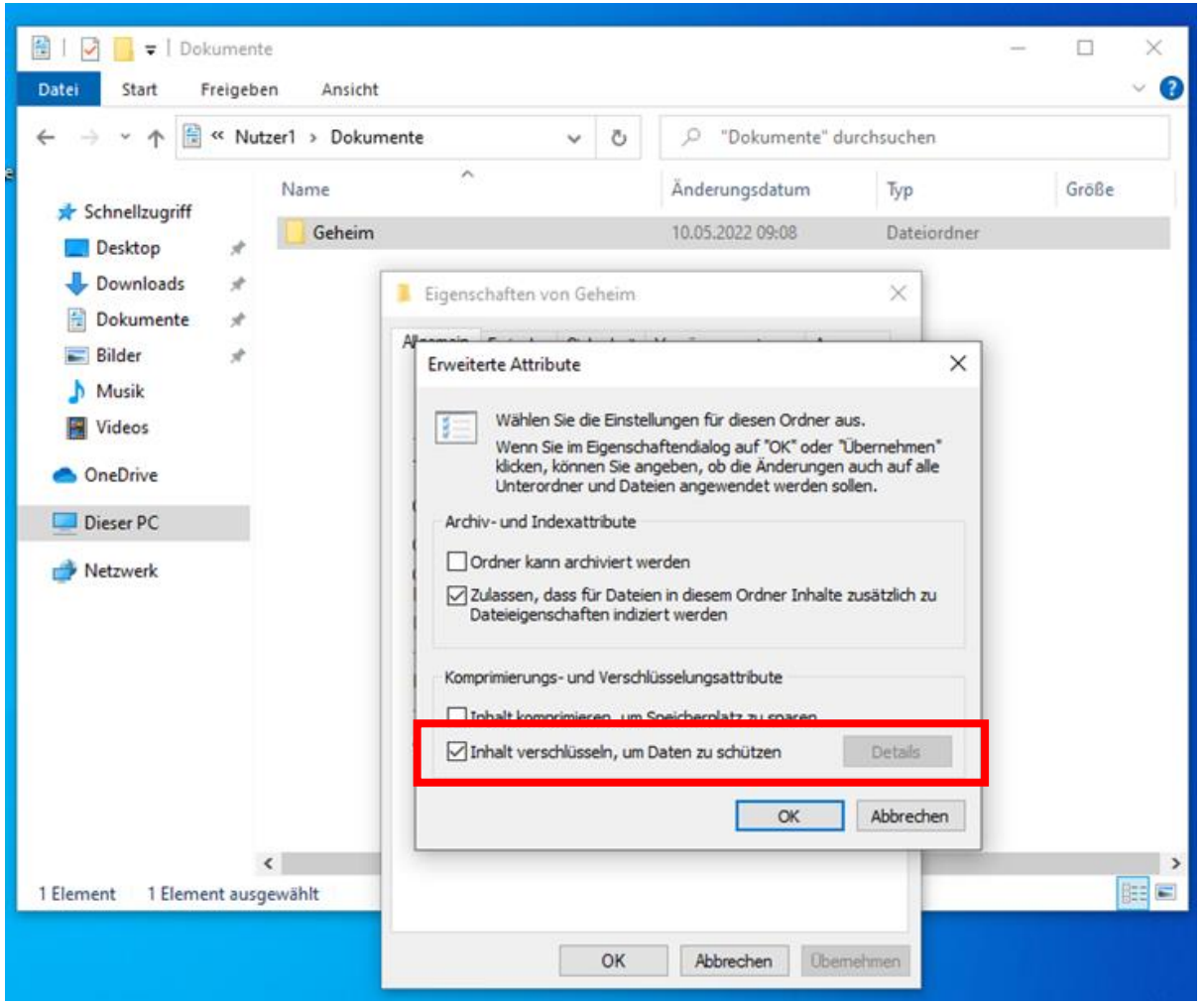
EFS Verschlüsselung

Betriebssystemspezifika Windows

EFS VERSCHLÜSSELUNG

Das **Encrypting File System (EFS)** kennzeichnet ein System der **Dateiverschlüsselung** auf **NTFS-Datenträgern**.

Dabei werden die Verschlüsselungsschlüssel an den Benutzer-Account gebunden!



Betriebssystemspezifika Windows

EFS VERSCHLÜSSELUNG

Datei per EFS verschlüsseln:

- System generiert einen zufälligen File Encryption Key (FEK)
- Datei wird mit FEK mittels AES chiffriert
- FEK wird mit asymmetrischen RSA-Algorithmus unter Benutzung des öffentlichen Schlüssels des Benutzers (SAM) verschlüsselt
- RSA-FEK mit der Datei zusammen abgespeichert

Datei lesen:

- FEK mittels des geheimen Schlüssels des Benutzers entschlüsseln
- Klartext der verschlüsselten Datei wiederherstellen

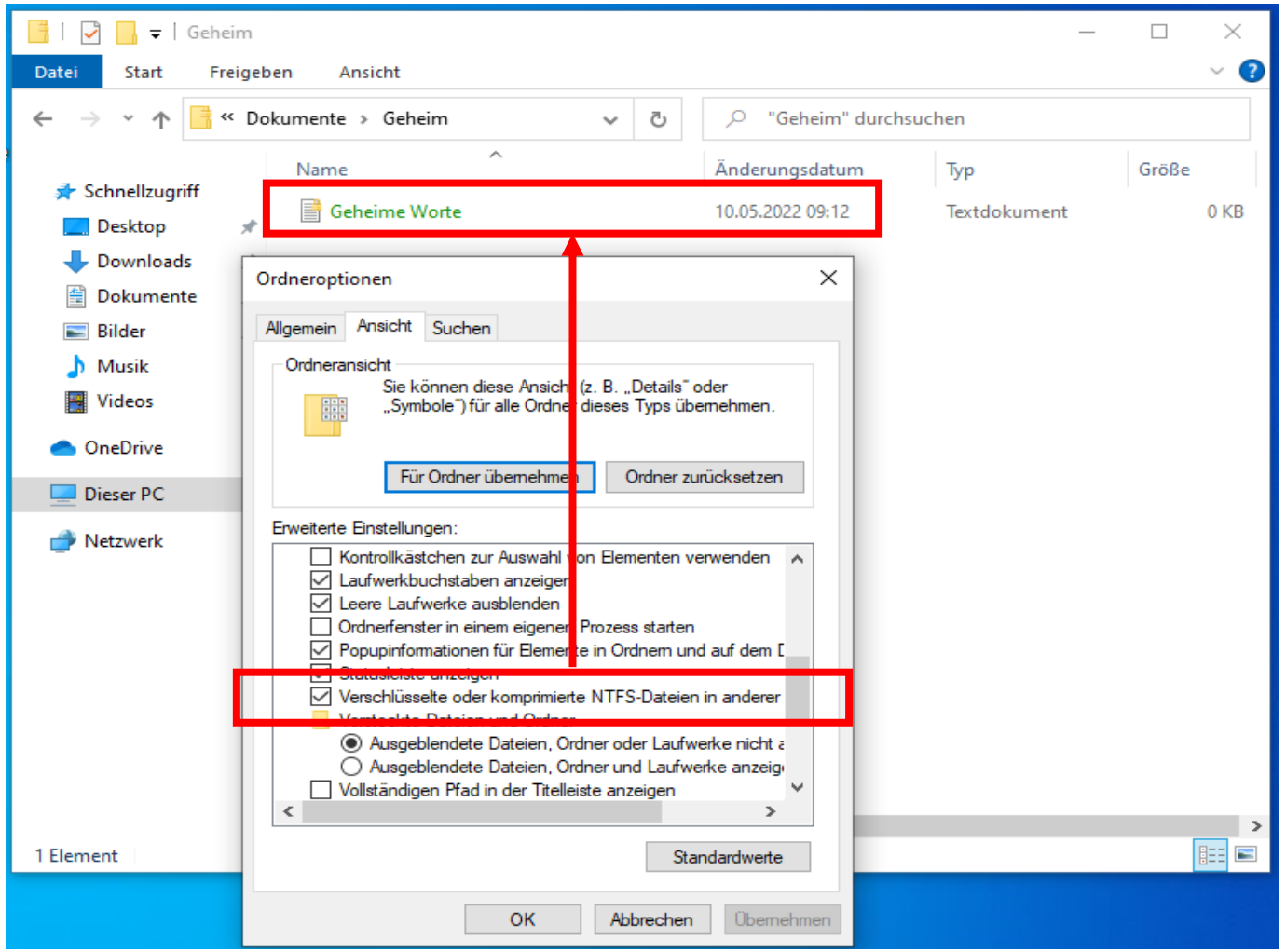
Betriebssystemspezifika Windows

EFS VERSCHLÜSSELUNG

EFS verschlüsselten Daten in forensischer Untersuchung finden:

- „Ansicht > Optionen“
- Register „Ansicht“
- Markieren von:

➢ „Verschlüsselte oder komprimierte NTFS-Dateien in anderer Farbe anzeigen“.



Betriebssystemspezifika Windows

EFS VERSCHLÜSSELUNG

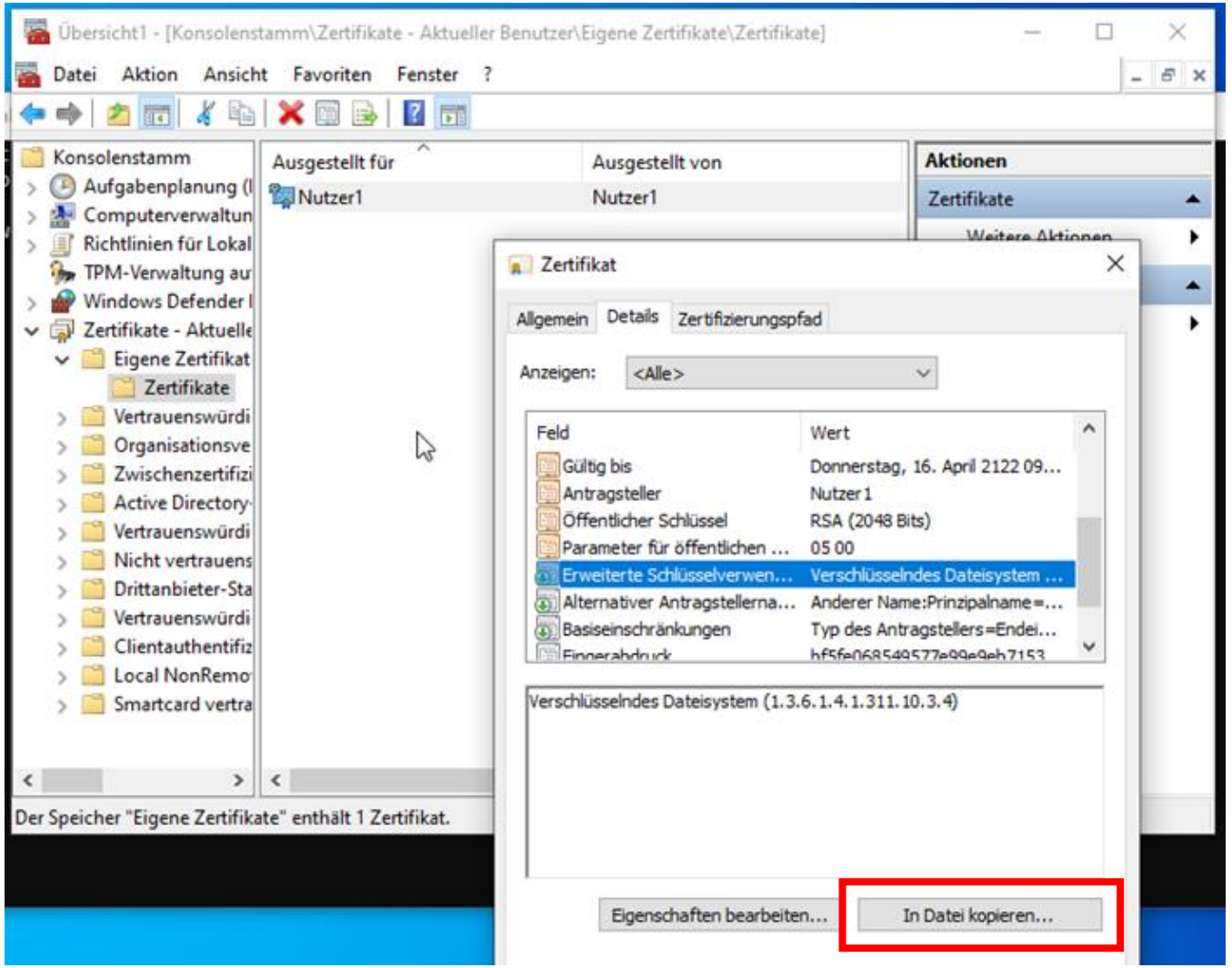
EFS verschlüsselte Daten in forensischer Untersuchung einsehen:

- mit Benutzerkennung an Rechner mit verschlüsselten Daten anmelden
- bedingt, dass man das Passwort des Benutzers kennt
- Unbekanntes Passwort knacken
- vom Benutzer den EFS Schlüssel als Zertifikat exportieren
- an der forensischen Untersuchungsmaschine importieren
- EFS verschlüsselten Dateien öffnen

Betriebssystemspezifika Windows

EFS VERSCHLÜSSELUNG

Zertifikat mit dem EFS Schlüssel exportieren:



Betriebssystemspezifika Windows

EFS VERSCHLÜSSELUNG

WICHTIG:

Die Nutzung einer Boot CD zum zurücksetzen des PW des Benutzers funktioniert in einem solchen Fall nicht, da beim Löschen der Benutzerkennwörter auch die Möglichkeit der Dechiffrierung der EFS Dateien verloren geht, da der FEK mit dem Passwort des Benutzers verschlüsselt wird.

Wahlweise kann man auch eine Virtualisierung des Asservates in Erwägung ziehen und die EFS verschlüsselten Daten nach Anmeldung am System mit der entsprechenden Benutzerkennung exportieren und damit für eine Untersuchung erlangen.

VSS - Volume Shadow Copy Service

Betriebssystemspezifika Windows

VOLUMENSCHATTENKOPIEN VSS

Seit Windows 2003 gibt es den sog. „Volume Shadow Copy Service“ (VSS)

- Hintergrunddienst der mehrere Versionen von Dateien vorhält
- Seit Windows 7 ist dieser Dienst standardmäßig aktiviert.
- gesicherten Daten werden im Verzeichnis „System Volume Information“ abgelegt
- Schattenkopien ersetzen „RestorePoints“-Funktionalität aus Windows-Versionen vor Vista

Schattenkopien dienen als einheitliche Datenquelle für zwei Funktionen:

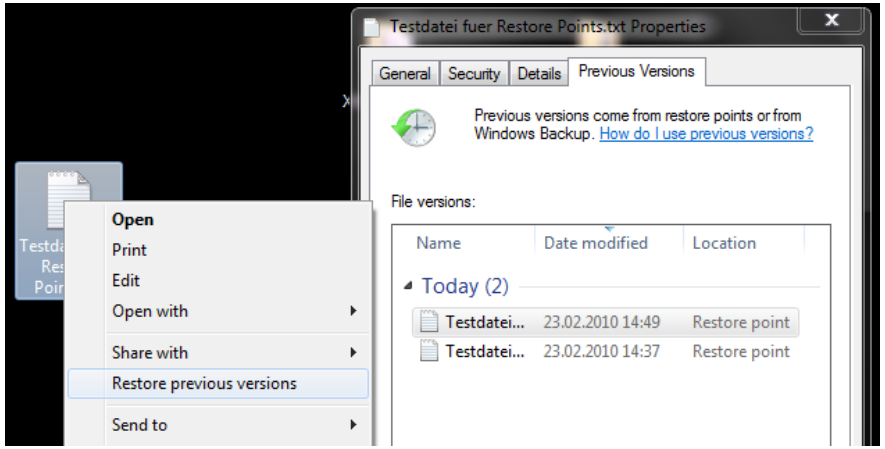
- RestorePoints (Wiederherstellungspunkte)
- PreviousVersions (Vorherige Versionen)

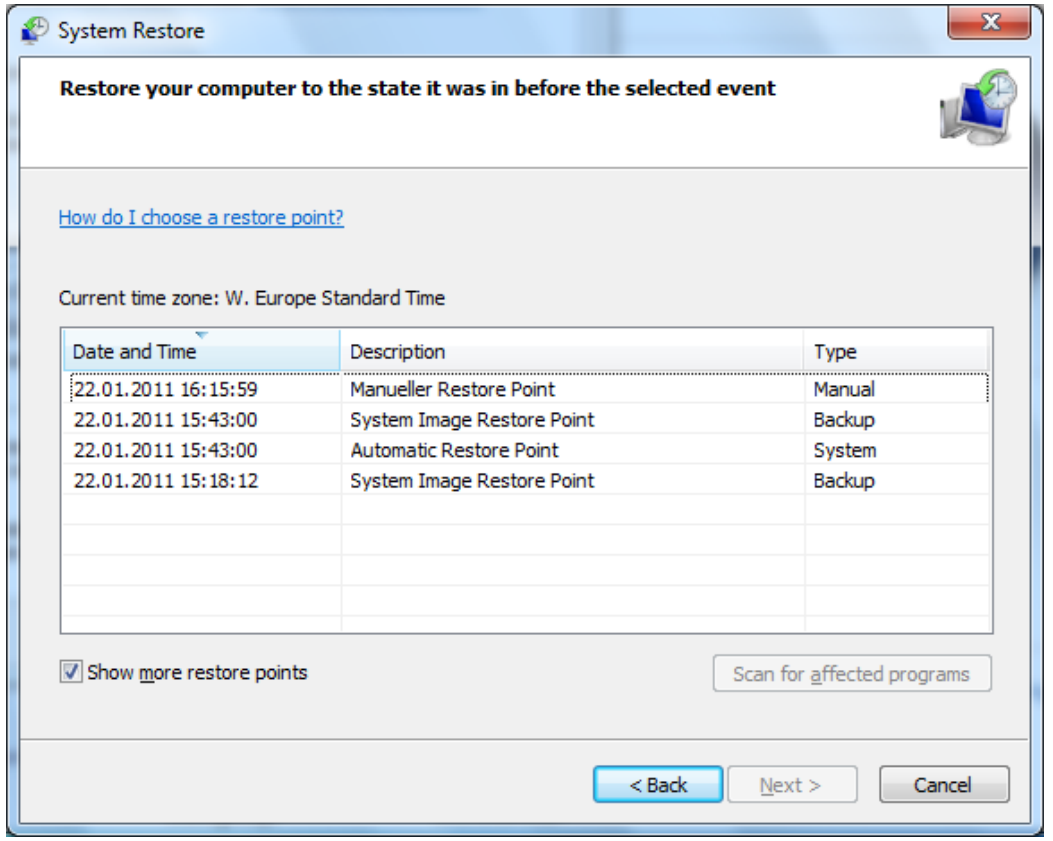
Betriebssystemspezifika Windows

VOLUMENSCHATTENKOPIEN VSS

Gespeicherte vorherige Versionen von Dateien können:

- An eine beliebige Stelle kopiert werden („Copy“)
- Wiederhergestellt werden und damit die aktuelle Fassung ersetzen („Restore“)





Betriebssystemspezifika Windows

VOLUMENSCHATTENKOPIEN VSS

Unter Windows 7 ff. etwa werden zu folgenden Ereignissen Schattenkopien erstellt:

- manuell erstellt
- alle 7 Tage automatisch
- vor einem Windows-Update oder der Installation eines unsignierten Treibers
- Anwendung, die eine Sicherung über die Windows-API anfordert

Daten aus Schattenkopien werden (standardmäßig) entfernt, wenn

- mehr als 5% des Speichers bei einer Partition >64GB
- mehr als 3% des Speichers bei einer Partition <64GB

belegt sind.

Betriebssystemspezifika Windows

VOLUMENSCHATTENKOPIEN VSS

- Schattenkopien bleiben erhalten, selbst wenn die zugehörigen Quelldateien gelöscht, gewiped oder verschlüsselt werden
- Frühere Versionen von Dateien können aus Schattenkopien wiederhergestellt werden
- Daher sind Schattenkopien ein wichtiges Element im Rahmen der Analyse gelöschter Dateien

Betriebssystemspezifika Windows

VOLUMENSCHATTENKOPIEN VSS

Wichtig für das Verständnis der Funktionsweise ist das sog. „Copy-on-Write“-Konzept: Änderungen in eine Schattenkopie werden nur dann geschrieben, wenn die Originaldatei geändert wurde.

Daher funktioniert die Erstellung eines kompletten RestorePoints auch so schnell! Es wird pro Schattenkopie nur die jeweils letzte Änderung an einer Datei gespeichert.

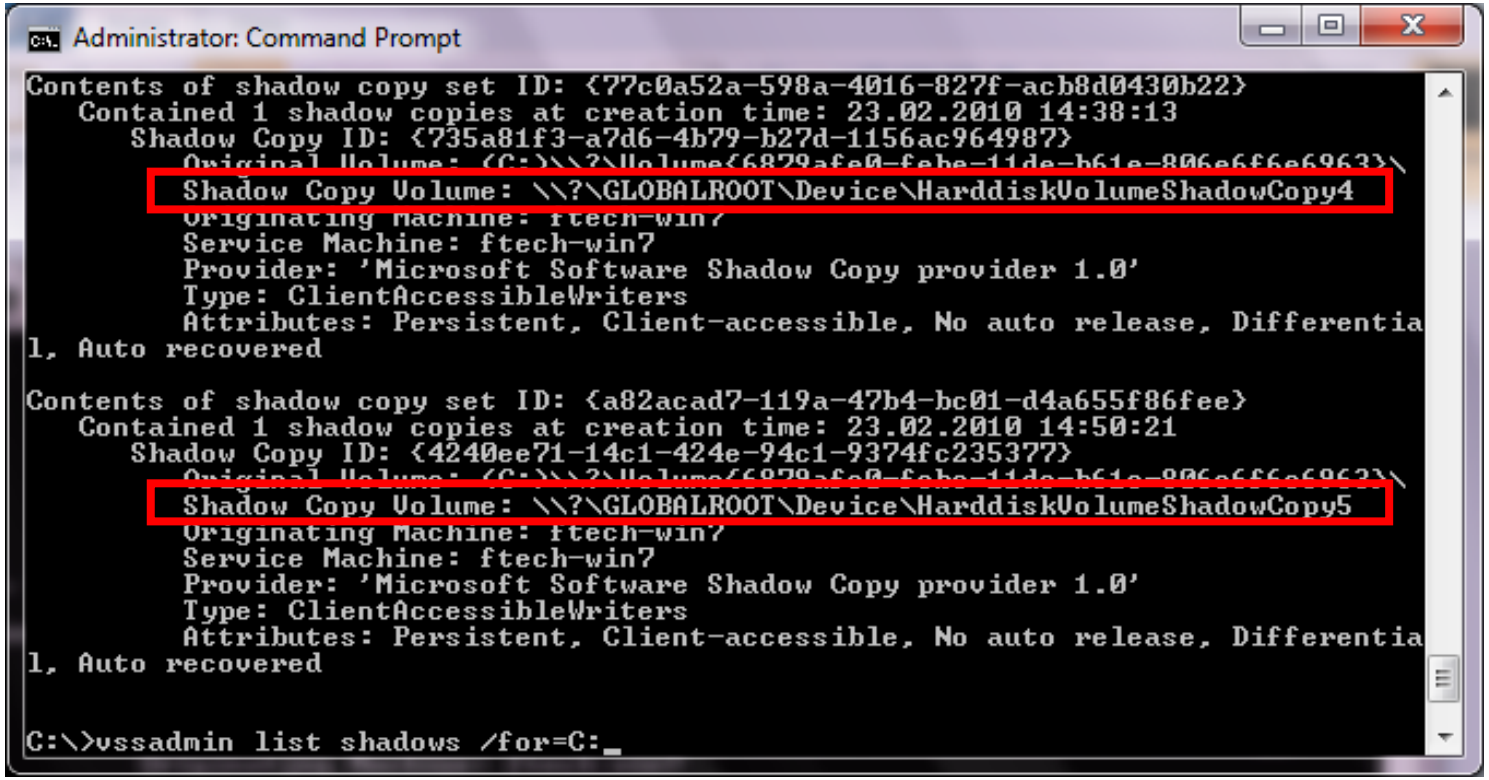
Als Konsequenz daraus wird also nicht jede Änderung gesichert, sondern nur falls zwischenzeitlich eine neue Schattenkopie angelegt wurde.

Betriebssystemspezifika Windows

VOLUMENSCHATTENKOPIEN VSS

In der Kommandozeile kann mit vssadmin list shadows /for=C: die Schattenkopien von Laufwerk C:\ aufgelistet werden.

Hierbei kann der Shadow Copy Volume Identifier herausgelesen werden.



Betriebssystemspezifika Windows

VOLUMENSCHATTENKOPIEN VSS

Anhand des Shadow Copy Volume Identifiers kann auf eine Schattenkopie live zugegriffen werden:

```
mklink/d c:\vss-test \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy4\
```

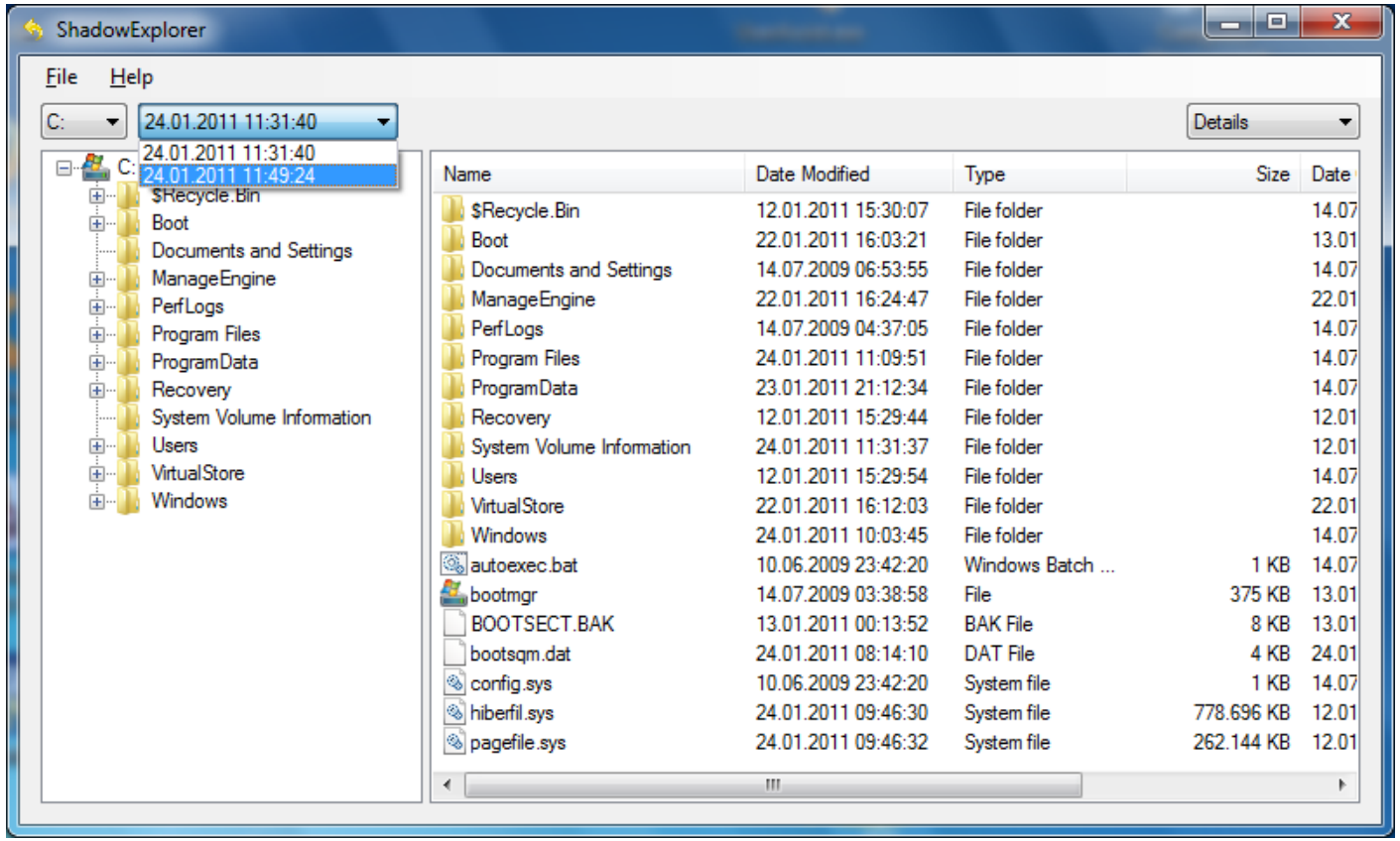
Der Befehl erstellt einen Link auf die Schattenkopie.

In „*c:\vss-test*“ befindet sich dann die Ordneransicht zum Zeitpunkt der Erstellung der Schattenkopie.

Betriebssystemspezifika Windows

VOLUMENSCHATTENKOPIEN VSS

Alternativ kann hierzu auch das kostenfreie Tool „ShadowExplorer“ genutzt werden:



Betriebssystemspezifika Windows

VOLUMENSCHATTENKOPIEN VSS

Der Shadow Copy Volume Identifier kann auch als Quelle für eine Image-Erstellung genutzt werden:

```
dd if=\\.\HarddiskVolumeShadowCopy4 of=d:\shadowrawkopie4.dd -localwrt
```

Erstellt ein Image auf Laufwerk D:\ des Rechners in der Datei shadowrawkopie4.dd.

- Image stellt die Sicht auf den Datenträger zum Zeitpunkt der Erstellung der Schattenkopie dar
- Image kann dann als logischer Datenträger in Forensik-Tools importiert und näher analysiert werden

Betriebssystemspezifika Windows

VOLUMENSCHATTENKOPIEN VSS

Das Image einer Shadow Copy hat dieselbe Größe wie die Quellpartition. Durch die potentiell hohe Anzahl von Shadow Copies ergeben sich damit sehr große Datenmengen, die auszuwerten sind:

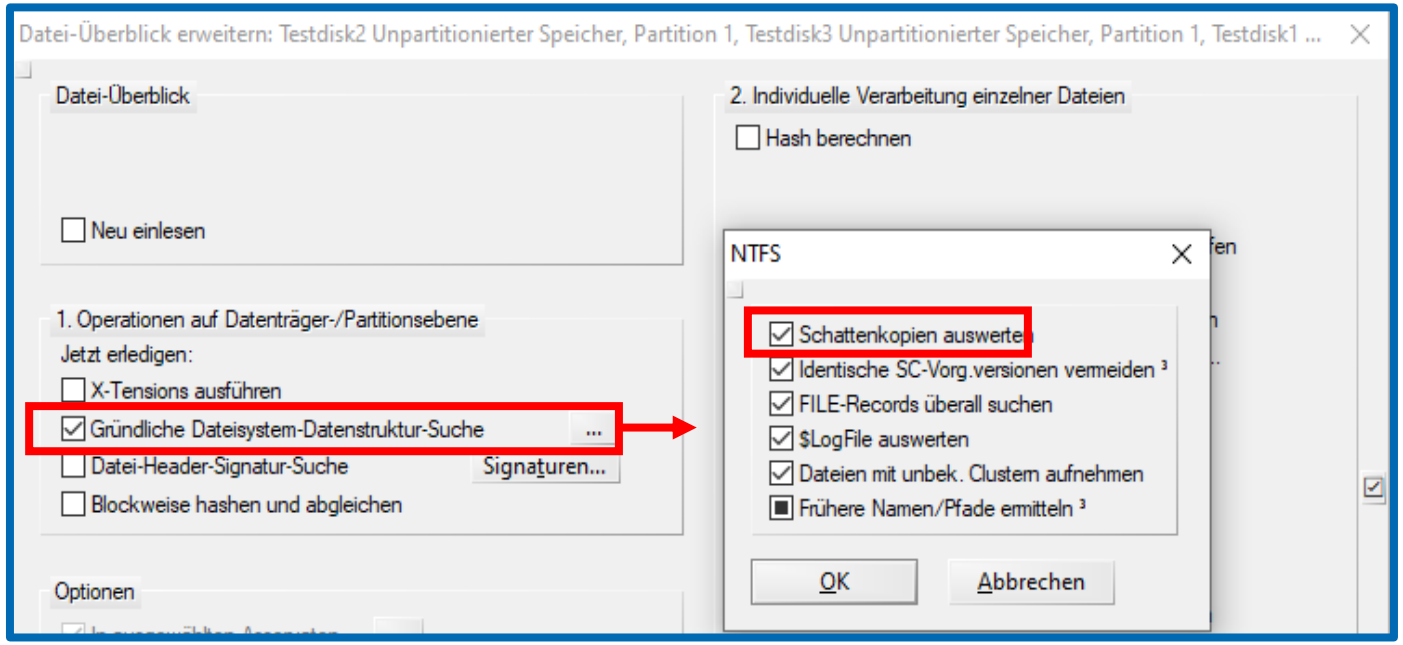
- Ggfs. Einschränkung möglich auf Basis des vermuteten Tatzeitraumes
- Durch Bildung von Hashsets und einen entsprechenden Abgleich können die bereits aus anderen Schattenkopien bekannten Dateiversionen ausgeblendet werden

Betriebssystemspezifika Windows

VOLUMENSCHATTENKOPIEN VSS

mit X-Ways Volumenschatten-kopien untersuchen:

- unter "Spezialist" -> "Dateiüberblick erweitern"
- Option "gründliche Dateisystem-Datenstruktur-Suche" aktivieren
- Aufbereitung von Schattenkopien zusätzlich zu anderen Optionen wie Aufbereitung von MFT-Record-Datensätzen, INDX-Puffern und $LogFiles durchgeführt

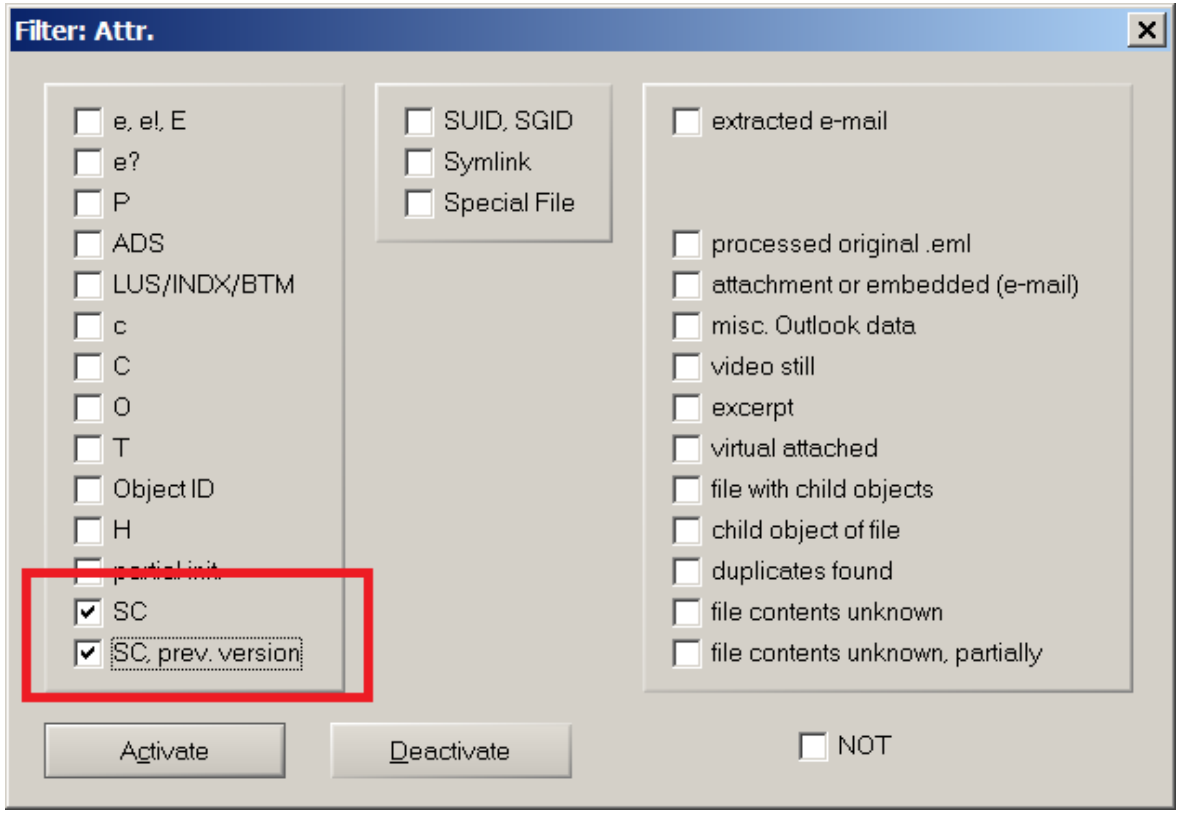


Betriebssystemspezifika Windows

VOLUMENSCHATTENKOPIEN VSS

Dateien im Verzeichnisbrowser auflisten, die aus "Schattenkopien" extrahiert wurden:

- mithilfe der Attributsspalte gefiltert nach "SC" (Dateien in Volumenschatten-kopien) und "SC, vorherige Version" (frühere Versionen von "SC") werden.
- Frühere Versionen von "SC" bezeichnet Dateien, die dem Volume-Snapshot bereits vor der Dateisystem-datenstruktur-Suche bekannt waren.

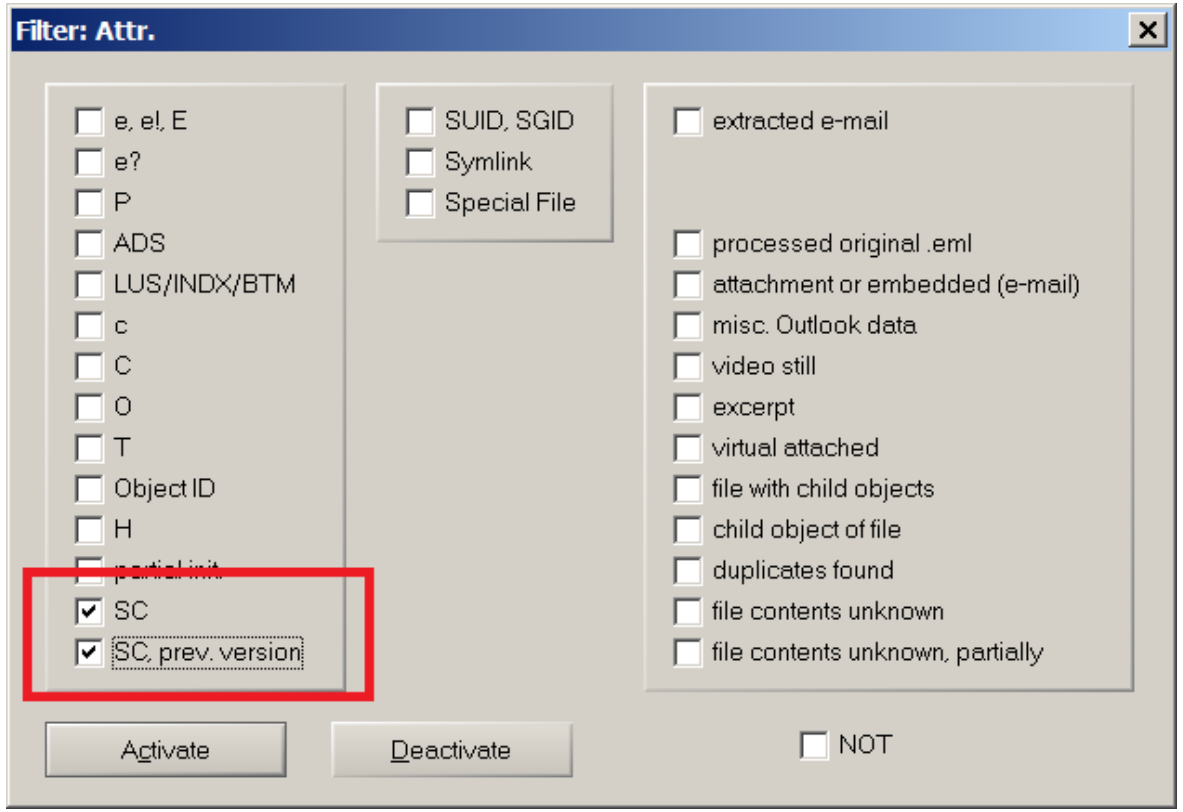


Betriebssystemspezifika Windows

VOLUMENSCHATTENKOPIEN VSS

Kombiniert man dies dann kreativ mit anderen Filteroptionen (wie Typ oder Datum) erhält man so konkrete geänderte Dateien, zu entsprechenden Zeitstempel.

z. B.: "Zeige mir alle Dateien einer Schattenkopie an, bei denen es sich um eine Bilddatei mit einem Änderungsdatum zwischen Datum X und Y handelt."



Zusammenfassung

Zusammenfassung

Das OSI-Modell strukturiert die Netzwerkkommunikation in verschiedene Ebenen mit entsprechenden Aufgabengebieten. Windows implementiert diese Ebenen in ihren Windows-Networkstack. Dieses ist auf Grund von Abwärtskompatibilität sehr komplex.

Zugriffsüberwachung übernimmt unter Windows die Windows Filtering Plattform. Diese integriert die Windows Firewall und die Antivirussoftware Windows Defender.

Der Windows Updateprozess teilt sich in Orchestrator, Windows Update Client, Arbiter und Installer auf.

Das AAA-Konzept gliedert sich in Authentification, Authorization und Accounting auf. Hierzu wurden verschiedene Authentifizierungsverfahren detaillierter betrachtet.

Vielen Dank für Ihre Aufmerksamkeit!

Leander Hoßfeld, B.Sc.
Wissenschaftlicher Mitarbeiter
Studierender Cybercrime/Cybersecurity (M.Sc.)
Seminargruppe: CY22wC-M
Matrikelnummer: 52212

Hochschule Mittweida | University of Applied Sciences
Technikumplatz 17 | 09648 Mittweida
Fakultät Angewandte Computer- und Biowissenschaften

T +49 (0) 3727 581748
M +49 (0) 17659592904
lhossfel@hs-mittweida.de
hossfeld@hs-mittweida.de

Besucheradresse: Haus 06 | Grunert-de-Jácome-Bau| Raum 6-031
Am Schwanenteich 4b | 09648 Mittweida

HOCHSCHULE MITTWEIDA
University of Applied Sciences

hossfeld@hs-mittweida.de