

Bachelor Thesis

Windows Server User Access Logging (UAL) als forensisches Artefakt – Möglichkeiten und Grenzen

eingereicht von:

Dario Ruberto

geboren am XX.XXX.XXXX in XXXXX

Studiengang IT-Forensik

Betreuer:

Prof. Dr.-Ing. Antje Raab-Düsterhöft

weitere Gutachter:

Prof. Dr.-Ing. habil. Andreas Ahrens

XXXXX, den XX.XXX.XXXX

Aufgabenstellung

Titel: Windows Server User Access Logging (UAL) als forensisches Artefakt – Möglichkeiten und Grenzen

Title: Windows Server User Access Logging (UAL) As a Forensic Artifact – Possibilities and Limitations

Die Zielsetzung dieser Bachelor-Thesis besteht darin, dass Windows Server User Access Logging (UAL) unter verschiedenen Windows Server Betriebssystemen und unter Anwendung verschiedener Testszenarien zu untersuchen. Es sollen der Informationsgehalt und die Robustheit des Artefakts bewertet werden sowie die damit verbundenen Möglichkeiten und Grenzen als ein mögliches forensisches Artefakt aufgezeigt werden. Die Herausforderungen bei der UAL besteht darin, dass es sich hierbei nicht um eine dedizierte Möglichkeit von Microsoft handelt um IT-Forensiker zu unterstützen, vielmehr handelt es sich um ein neues feature von Microsoft welche potenziell nützlichen Informationen für die IT-Forensik beinhaltet.

Kurzreferat

Diese Arbeit dient als Ausgangspunkt zur Untersuchung der Eignung des von Microsoft bereitgestellten User Access Logging (UAL) als IT-forensisches Artefakt, insbesondere im Hinblick auf die Robustheit und den damit verbundenen Informationsgehalt. Ziel ist es die Grenzen und Möglichkeiten zu beleuchten und somit einen Aufklärungsbeitrag in der IT-Forensik und IT-Sicherheit zu liefern.

IT-Forensische Untersuchungen variieren stark in ihrer Komplexität, mit steigender Komplexität eröffnet sich der Bedarf für neue Artefakt Quellen welche während der Untersuchung herangezogen werden können, um so die Untersuchung und Rekonstruktion des Tathergangs, über die Beweissicherung bis hin zur Aufklärung eingesetzt werden können. UAL protokolliert unter anderem benutzerspezifische Informationen, Zeitstempel, Details zur Software und gerätespezifische Informationen, somit stellt die UAL eine potenzielle Artefakt Quelle für Untersuchungen dar.

In dieser Arbeit wird die technische Grundlage zur UAL erörtert sowie die Methoden zur Gewinnung und Auswertung der potenziellen Artefakte dargelegt. Verschiedenste Testszenarien wurden in einer kontrollierten Testumgebung durchgeführt, um UAL-Artefakte zu generieren und die UAL-Artefakte im IT-Forensischen Kontext zu untersuchen und auszuwerten.

Die UAL-Artefakt Untersuchung und Auswertung in dieser Arbeit, belegt dessen Robustheit als potenzielles IT-Forensisches Artefakt das Abhängig der Fall-Komplexität als Artefakt in Betracht gezogen werden sollte. User Access Logging kann unabhängig der gespeicherten Artefakte keine vollständige Untersuchung ersetzen, dennoch Wissenslücken während einer Untersuchung schließen oder bestehende Annahmen bestärken.

Abstract

This work serves as a starting point for examining the suitability of the User Access Logging (UAL) provided by Microsoft as an IT forensic artifact, particularly with regard to its robustness and the associated information content. The aim is to shed light on the limits and possibilities and thus provide an educational contribution to IT forensics and IT security.

IT forensic investigations vary greatly in their complexity, with increasing complexity there is a need for new artifact sources that can be used during the investigation, so that the investigation and reconstruction of the crime, through the preservation of evidence and even the investigation can be used. UAL logs, among other things, user-specific information, timestamps, software details and device-specific information, making UAL a potential artifact source for investigations.

This work discusses the technical basis for UAL and presents the methods for obtaining and evaluating potential artifacts. A wide variety of test scenarios were carried out in a controlled test environment to generate UAL artifacts and to examine and evaluate the UAL artifacts in an IT forensic context.

The UAL artifact investigation and evaluation demonstrates its robustness as a potential IT forensic artifact that should be considered as an artifact depending on the case complexity. Regardless of the artifacts stored, user access logging cannot replace a complete investigation, but it can still close knowledge gaps during an investigation or reinforce existing assumptions.

Inhaltsverzeichnis

1	Einführung und Motivation des Themas	7
1.1	Gegenwertiger Stand der Forschung	9
1.2	Forschungsfragen.....	10
2	Grundlagen	11
2.1	Forensik.....	11
2.2	IT-Forensik	11
2.2.1	IT-Forensisches Artefakt	12
2.2.2	Allgemein Anforderungen forensische Untersuchung	12
2.2.3	IT-Forensische Untersuchung	13
2.3	User Access Logging (UAL)	15
2.3.1	Windows Server User Access Logging (UAL).....	15
2.3.2	Windows Server- und Service-Rollen Unterstützung	15
2.3.3	Protokollierung	17
2.3.4	Verfügbarkeit	19
2.3.5	Technische Grundlage Windows User Access Logging (UAL)	21
3	Testumgebung	31
3.1	Testumgebung.....	31
3.2	Werkzeuge	38
4	Untersuchung	40
4.1	Konkretisierung der Forschungsfragen	40
4.2	Testszenarien	41
4.3	Methoden.....	41
4.4	Untersuchung	42
4.4.1	Live-Untersuchung Windows Server 2019	42
4.4.2	Live-Untersuchung Windows Server 2012R2	46
4.4.3	Post-mortem-Untersuchung Windows Server 2019	49
4.4.4	Post-mortem-Untersuchung Windows Server 2012 R2	59

5	Ergebnisse	70
5.1	Auswertung und Bewertung	70
5.1.1	W-Fragen	73
5.2	Grenzen und Möglichkeiten	75
5.2.1	Grenzen des UAL-Artefakts	75
5.2.2	Möglichkeiten des UAL-Artefakts	76
5.3	Beantwortung der Forschungsfragen	77
6	Zusammenfassung und Ausblick	80
6.1	Konklusion	81
6.2	Fazit	82
	Literaturverzeichnis	83
	Abbildungsverzeichnis	89
	Tabellenverzeichnis	91
	Anlagenverzeichnis und Anlagen	92
	Anlage 1 – Testszenarien	93
	Anlage 2 – Get-UalOverview Windows Server 2019	96
	Anlage 3 – Get-UalOverview Windows Server 2012 R2	97
	Verzeichnis der Abkürzungen	98
	Selbstständigkeitserklärung	99

1 Einführung und Motivation des Themas

Die Digitalisierung schreitet unaufhaltsam voran, digitale Informationen sind in unserer heutigen Gesellschaft bedeutsam für alle Bereiche unseres Lebens obgleich Unternehmen, Regierung, Gesundheitswesen, Bildungsinstitutionen, Forschung, Wissenschaft oder Privathaushalt. Mit dem Fortschritt der Digitalisierung rückt die digitale Kriminalität auch bekannt als Cyberkriminalität in den Vordergrund. Identitätsdiebstahl, Datenmanipulation, Datenexfiltration (Datendiebstahl), Systemangriffe, Erpressungsversuche bis hin zur mutwilligen Zerstörung von fremdem digitalem Gedankengut. Die Aufklärung von derartigen Vorfällen fällt im Allgemeinen unter den Begriff der Computer Forensik, Digitale Forensik, Cyber-Forensik oder IT-Forensik. Die Untersuchung (in dieser Arbeit auch Analyse genannt) und Rekonstruktion eines Tathergangs (auch Ereignis genannt) über die Beweissicherung bis hin zur Aufklärung, kann in der Komplexität variieren, traditionelle, bereits bekannte und erprobte Artefakt Quellen sowie Programme/Software) (in dieser Arbeit auch Werkzeuge genannt) kommen zum Einsatz.

Mit steigender Komplexität eröffnet sich der Bedarf für neue Artefakt Quellen, User Access Logging (UAL) könnte eine potenzielle Artefakt Quelle darstellen. Aus Gründen der Lesbarkeit wird in der Folge dieser Arbeit die User Access Logging oftmals abgekürzt als UAL bezeichnet.

Mit der Veröffentlichung von Microsoft Windows Server 2012 im September 2012 [13] hat Microsoft UAL für Windows Server Betriebssystem als neue Funktion veröffentlicht, UAL ermöglicht die Protokollierung unter anderem benutzerspezifische Informationen, Zeitstempel, Details zur Software und gerätespezifische Informationen. UAL wird ausschließlich auf den Windows Server Betriebssystemen bereitgestellt, Windows Client Betriebssysteme wie beispielsweise Windows 10, bieten kein User Access Logging.

Im Jahr 2021 wurde auf dem jährlichen SANS DFIR (Digital Forensics and Incident Response) Summit & Training 2021, UAL zum ersten Mal im Rahmen einer renommierten Veranstaltung vor öffentlichem Publikum vorgestellt unter dem Titel „Where Have UAL Been“ [14] und erhielt im Rahmen der DFIR-Gemeinschaft erstmals Sichtbarkeit.

Diese Arbeit dient als Ausgangspunkt zur Untersuchung der Eignung des von Microsoft bereitgestellten User Access Logging als IT-forensisches Artefakt, insbesondere im Hinblick auf die Robustheit und den damit verbundenen Informationsgehalt. Ziel ist es die Grenzen und Möglichkeiten zu beleuchten und somit einen Aufklärungsbeitrag in der IT-Forensik und IT-Sicherheit zu liefern.

Die in dieser Arbeit erlangten Erkenntnisse basieren auf den in der Testumgebung generierten UAL-Artefakte. Die Erkenntnisse sind daher spezifisch für die in dieser Arbeit verwendeten Testumgebung und Werkzeuge verifiziert und gültig, eine Verallgemeinerung wird jedoch nicht ausgeschlossen.

Diese Arbeit beansprucht nicht eine vollständige und endgültige Analyse der Architektur, der Datenbanktechnologie, Funktionsweise oder Verkettung der UAL innerhalb der Windows Server Betriebssysteme zu sein.

Daher liegen spezifische Themenbereiche außerhalb des Fokus dieser Arbeit und werden nicht vertieft:

- Rechtlichen Datenschutzaspekte
- Implementierung von Schutzmaßnahmen
- Datenbanken im Allgemeinen
- Windows Betriebssysteme im Allgemeinen
- Windows Registry und Event Viewer im Allgemeinen
- Weitere verfügbare Werkzeuge (jedoch im Rahmen dieser Arbeit nicht verwendet)

1.1 Gegenwertiger Stand der Forschung

Microsoft veröffentlicht mit Windows Server 2012 das User Access Logging, welche in erster Linie für Administratoren zur Verfügung steht und unter anderem die Protokollierung benutzerspezifische Informationen, Zeitstempel, Details zur Software und gerätespezifische Informationen ermöglicht.

Das US-Sicherheitsunternehmen Crowdstrike berichtet in einem Blogeintrag zum Thema UAL, das bei gegenwertigen forensischen Analysen die UAL-Datenbanken oftmals nicht untersucht oder berücksichtigt werden, wodurch forensisch relevante Informationen übersehen werden können [50]. Eine Gesamtübersicht des gegenwertigen Standes der Forschung bietet die im Jahr 2021 vorgestellte Präsentation auf dem jährlichen SANS DFIR (Digital Forensics and Incident Response) Summit & Training 2021 unter dem Titel „Where Have UAL Been“ von Kevin Stokes und Brian Moran [14].

Unter anderem wird der Speicherort sowie der Datenbankaufbau der UAL beleuchtet, im Rahmen der Ausarbeitung von Kevin Stokes und Brian Moran wurde bekannt, dass sich der UAL-Datenbankinhalt nach der Extraktion in einem benutzerunfreundlichen Zustand befindet, wodurch ein Python Skript von Brian Moran mit dem Namen *KStrike* entwickelt und veröffentlicht wurde. *KStrike* ist ein sogenannter *Parser*, welcher die Analyse und Verarbeitung der Datenbankinformationen in einem benutzerfreundlichen Zustand ermöglicht. *KStrike* übernimmt ebenfalls automatisch die Zuordnung zu Windows-Services, -GUID und -Rollen [11].

Ein *UAL_Parser* als *Autopsy* [51] Python Plugin wurde von Mark McKinnon im Juli 2021 veröffentlicht [52] welcher auf dem *KStrike Parser* basiert, und es ermöglicht die Ergebnisse direkt mit *Autopsy* zu betrachten. In der wissenschaftlichen Literatur, Fachzeitschriften oder Fachbüchern, konnten keine Informationen zur UAL gefunden werden.

Die Analyse von UAL-Artefakten über einen Zeitraum von bis zu drei Jahren, rückwirkend zu analysieren, bietet potenzielle Vorteile. Zum aktuellen Zeitpunkt fehlen konkrete Anwendungs- oder Testszenarien, um den Nutzen der UAL als forensisches Artefakt zu verdeutlichen. Ebenfalls ist nicht belegt ob UAL-

Artefakte hinsichtlich ihres Informationsgehalts und ihrer Robustheit den allgemeinen Standardanforderungen forensischer Untersuchungen entsprechen.

1.2 Forschungsfragen

Im Rahmen dieser Arbeit dienen Forschungsfragen um eine systematische, zielgerichtete und fokussierte Untersuchung von UAL zu ermöglichen. Die Forschungsfragen sind darauf ausgerichtet einen Überblick über UAL zu vermitteln und decken sowohl die technischen Aspekte als auch die praktischen Aspekte ab. Diese Fragen werden den Ausgang dieser Arbeit maßgeblich prägen und werden deshalb im *Kapitel 8.1 - Konkretisierung der Forschungsfragen*, dieser Arbeit konkretisiert. Die Ausarbeitung und Klärung der Forschungsfragen wird dazu beitragen um UAL als ein mögliches forensisches Artefakt zu bewerten.

Forschungsfrage 1: Welche Informationen werden durch UAL protokolliert (Informationsgehalt) und wie lange werden diese gespeichert?

Forschungsfrage 2: Wie können UAL-Artefakte ausgelesen und extrahiert werden?

Forschungsfrage 3: Unterscheidet sich UAL-Funktionsweise sowie UAL-Artefakte von Windows Server 2019 und Windows Server 2012R2?

Forschungsfrage 4: Wie sind UAL-Artefakte zu interpretieren und kann den Anforderungen an die Erhebung von Daten gerecht werden (Robustheit)?

Forschungsfrage 5: Welche Grenzen gibt es bei UAL als forensisches Artefakt?

Forschungsfrage 6: Welche Möglichkeiten bietet UAL als forensisches Artefakt?

2 Grundlagen

Grundlagen zur Thematik sind wichtig, um ein rudimentäres Verständnis über die in dieser Arbeit behandelten Forschungsfragen zu vermitteln. Hierzu wird zu Beginn dieser Arbeit auf die wichtigsten Begrifflichkeiten eingegangen. Diese Sichtweise findet sich auch bei Geschonneck wieder:

Ein Dritter, der eventuell nicht über den gleichen technischen Sachverstand und Erfahrungsschatz verfügt, muss den Tätigkeiten, die während der Ermittlung durchgeführt wurden, Glauben schenken können. (Geschonneck, 2014 [17])

2.1 Forensik

Der Begriff Forensik entstammt der römischen Epoche und wird wie folgt beschrieben:

Forensik ist ein Sammelbegriff für wissenschaftliche und technische Arbeitsgebiete, in denen kriminelle Handlungen systematisch untersucht werden. Der Begriff stammt vom lateinischen forensis, zum Forum, Markt[platz] gehörig'. Gerichtsverfahren, Untersuchungen, Urteilsverkündungen sowie der Strafvollzug im antiken Rom wurden öffentlich und meist auf dem Marktplatz (Forum) durchgeführt. (Wikipedia, 2023 [15])

2.2 IT-Forensik

Der Begriff IT-Forensik setzt sich aus IT (Informationstechnik, englisch *Information Technology*) zusammen und Forensik (englisch *Forensic*) zusammen. Das BSI (Bundesamt für Sicherheit in der Informationstechnik) beschreibt IT-Forensik wie folgt:

IT-Forensik ist die streng methodisch vorgenommene Datenanalyse auf Datenträgern und in Computernetzen zur Aufklärung von Vorfällen unter Einbeziehung der Möglichkeiten der strategischen Vorbereitung insbesondere aus der Sicht des Anlagenbetreibers eines IT-Systems. (BSI, 2011 [16])

Das BSI beschreibt daher, die IT-Forensik in die Prozesse des IT-Betriebs zu verankern. Im Gegensatz zu Geschonneck welcher IT-Forensik auf den Nachweis und die Ermittlung von Straftaten oder Vorfällen im Bereich der Computerkriminalität einschränkt [18].

2.2.1 IT-Forensisches Artefakt

Bei IT-Forensischen Artefakten handelt es sich um digitale Artefakte, der Begriff Artefakt (aus dem lateinisch ars, artis ‚Handwerk‘, und factum, das Gemachte‘) [19]. Im Kontext der IT-Forensik handelt es sich bei Artefakten um eine Sammlung von digitalen (virtuellen) Daten, jede Aktion auf einem Digitalen System löst beabsichtigt oder unbeabsichtigte Prozesse aus welche Datenveränderungen, Datengenerierung oder Daten Eliminierung führen. Im Rahmen der IT-Forensischen Aufklärungsarbeit (Untersuchung) werden diese Artefakte gesichtet, gesichert, ausgewertet und dokumentiert. IT-Forensische Artefakte können dazu beitragen, Vorfälle nachzuvollziehen und zu rekonstruieren. Sie können unter anderem Informationen wie Konfigurationen, Aktivitäten, Ereignisse, Herkunftsinformationen (Aufzählung nicht abschließend) enthalten.

2.2.2 Allgemein Anforderungen forensische Untersuchung

Ein Grundverständnis über die allgemeinen Anforderungen an eine forensische Untersuchung ist notwendig, um Fehler bei der Erhebung und den Umgang mit Daten innerhalb einer Untersuchung zu vermeiden. Insofern wird in diesem Abschnitt ein rudimentäres Grundverständnis vermittelt nach welchen Anforderungen, Daten während einer Untersuchung erhoben werden, jedoch auch um der Frage, ob UAL als ein robustes Artefakt betrachtet werden kann ein Stück näher zu kommen. Der BSI [20] referenziert auf Geschonneck [21] und beschreibt die folgenden Anforderungen an die Erhebung von Daten mit folgenden Anforderungen:

- **Akzeptanz:** Bekannte Methoden, welche in der Fachwelt bekannt sind und im Allgemeinen akzeptiert sind zu bevorzugen, neue Verfahren oder Werkzeuge können eingesetzt werden jedoch ist die Methode und Vorgehensweise zu verteidigen.
- **Glaubwürdigkeit:** Die Funktion sowie die Robustheit der Methode und des Verfahrens müssen nachvollziehbare Ergebnisse liefern und plausibel erklärt werden können.

- **Wiederholbarkeit:** Es muss sichergestellt werden, dass bei einer erneuten Durchführung der Untersuchung auch eine dritte Person dieselben Ergebnisse erzielen würde.
- **Integrität:** Die Integrität der sichergestellten Daten muss jederzeit gewährleistet sein, es dürfen keine unbemerkten Veränderungen vorgenommen werden.
- **Ursache und Auswirkungen:** Die Methode muss zu einer logischen nachvollziehbaren Verbindung zwischen Ergebnissen und Beweisspuren führen.
- **Dokumentation:** Jeder Schritt muss angemessen, vollständig transparent und nachvollziehbar dokumentiert werden.

Ob UAL-Artefakte als Robust betrachtet werden können, hängt mit der Erfüllung der zuvor genannten Anforderungen zusammen. Im Rahmen dieser Arbeit werden UAL-Artefakte betrachtet, obwohl sie in der Fachwelt der IT-Forensik noch als unpopulär gelten. Hierdurch besteht nicht die Möglichkeit auf traditionelle und anerkannte forensische Methoden und Werkzeuge zurückgegriffen. Es werden Methoden und Werkzeuge verwendet welche neuartig sind und gegebenenfalls nicht alle oberhalb genannten Anforderungen gerecht werden.

2.2.3 IT-Forensische Untersuchung

Auf die allgemeine Vorgehensweise bei einer IT-Forensischen Untersuchung wird in dieser Arbeit nicht näher eingegangen. Um jedoch auch an dieser Stelle ein Grundverständnis zu vermitteln, wird auf den Leitfaden IT-Forensik des BSI verwiesen, welcher die Vorgehensweise einer forensischen Untersuchung in folgenden sechs Abschnitte unterteilt [22]:

1. Strategische Vorbereitung
2. Operationale Vorbereitung
3. Datensammlung
4. Untersuchung
5. Datenanalyse
6. Dokumentation

Untersuchungen können auf zwei Arten stattfinden:

1. Post-Mortem, der Begriff *post-mortem* (lateinsch für ‚nach dem Tod‘) [23].
2. Live, der Begriff *Live* steht für ‚lebend, unverzögert‘ [24].

Es handelt sich hierbei um zwei unterschiedliche Ansätze, bei der Post-Mortem-Untersuchung handelt es sich um eine Untersuchung auf einem Duplikat der betroffenen Datenträger, daher eine Offline-Kopie des Live-Systems somit kann eine Untersuchung in Ruhe und ohne Zeitdruck [25] stattfinden, ebenfalls ist eine Wiederherstellung jederzeit möglich im Falle einer Beschädigung der Datenträger Kopie während einer Untersuchung.

Laut IT-Forensik Wiki wird die Post-Mortem-Analyse wie folgt beschrieben:

Ein Vorfall wird im Rahmen einer Post-Mortem-Analyse nachträglich aufgeklärt. Die Post-Mortem-Analyse bezeichnet z.B. Untersuchung von Datenträgerabbildern, nichtflüchtigen Spuren, gelöschten oder unbenannten oder verschlüsselten Dateien von Massenspeichern. (IT-Forensik Wiki, 2018 [26])

Bei der Live-Analyse handelt es sich um die Untersuchung des Systems, während es noch aktiv ist, diese Art wird oft verwendet, wenn sich Informationen in flüchtigen Speichern befinden, welche beim Herunterfahren verloren oder beschädigt werden könnten, bei Vor-Ort Analysen in denen sofort gehandelt werden muss und keine Zeit für eine Post-Mortem-Analyse zur Verfügung steht (Aufzählung nicht abschließend). UAL-Arte selbst können sowohl im Post-Mortem Zustand sowie auch im Live-Zustand analysiert werden. Im Rahmen dieser Arbeit wird die Untersuchung sowohl im Live-Zustand wie auch im Post-Mortem Zustand durchgeführt.

Zum Ziel einer forensischen Untersuchung gehört die Beantwortung der folgenden W-Fragen [48]:

- Was ist geschehen?
- Wo ist es passiert?
- Wann ist es passiert?
- Wie ist es passiert?

2.3 User Access Logging (UAL)

2.3.1 Windows Server User Access Logging (UAL)

User Access Logging – es handelt es sich um eine integrierte Funktion in den Windows Server Betriebssystemen welche Client-Nutzerdaten (Endgerät, welches in einem Netzwerk mit einem Server kommuniziert [28]) zu Windows Server- und Service-Rollen protokolliert.

Die Protokollierung erfolgt nahezu in Echtzeit, die Protokolldaten werden mit einer Standardverzögerungszeit von 24 Stunden in eine spezifische Datenbank gespeichert und ermöglichen somit eine Informationsspeicherung von bis zu drei Jahren.

UAL wurde konzeptionell eingeführt, um Administratoren die Möglichkeit zu geben Windows Server Infrastrukturen im Punkto Serverressourcen-Lücken zu optimieren, Microsoft selbst hat keinen Zugriff auf diese Informationen, ebenfalls können keine Fehlerberichte exportiert oder direkt an Microsoft gesendet werden.

2.3.2 Windows Server- und Service-Rollen Unterstützung

Die folgende Server- und Service-Rollen werden von User Access Logging (UAL) unterstützt [27]:

- Active Directory Certificate Services (AD CS)
- Active Directory Rights Management Services (AD RMS)
- BranchCache
- Domain Name System (DNS)
- Dynamic Host Configuration Protocol (DHCP)
- Fax Server
- File Services

- File Transfer Protocol (FTP) Server
- Hyper-V
- Web-Server (IIS)
- Microsoft Message Queue (MSMQ) Service
- Network Policy and Access Services
- Print and Document Services
- Routing and Remote Access Service (RRAS)
- Windows Deployment Services (WDS)
- Windows Server Update Service (WSUS)

Während Microsoft über seine Microsoft Learn Website Informationen zu den verschiedenen Server- und Service-Rollen, welche von UAL unterstützt werden, bereitstellt [30], fokussiert sich diese Arbeit lediglich auf die für sie relevanten Rollen, diese werden falls relevant im Rahmen dieser Arbeit näher beschrieben. Für Informationen zu nicht im Fokus liegenden Server- und Service-Rollen ist die Microsoft Learn Webseite zu konsultieren [30].

2.3.3 Protokollierung

Microsoft veröffentlicht zur Frage welche benutzerspezifischen Informationen, Zeitstempel, Details zur Software und gerätespezifische Informationen von UAL protokolliert werden, die folgenden Informationen [27]:

- Benutzerspezifischen Informationen:

Data	Description
UserName	The user name on the client that accompanies the UAL entried from installed roles and products
ActivityCount	The number of times a particular user accessed a role or service.
FirstSeen	The date and time when a user first accesses a role or service.
LastSeen	The date and time when a user last accessed a role or service.
ProductName	The name of the software parent product, such as Windows, that is providing UAL data.
RoleGUID	The UAL assigned or registered GUID that represents the server role or installed product.
RoleName	The name of the role, component, or subproduct that is providing UAL data. This is also associated with a ProductName and a RoleGUID.
TenantIdentifier	A unique GUID for a tenant client of an installed role or product that accompanies the UAL data, if applicable.

Tabelle 1: Benutzerspezifischen Informationen [27]

- Gerätespezifische Informationen:

Data	Description
IPAddress	The IP address of a client device that is used to access a role or service.
ActivityCount	The number of times a particular device accessed the role or service.
FirstSeen	The date and time when an IP address was first used to access a role or service.
LastSeen	The date and time when an IP address was last used to access a role or service.
ProductName	The name of the software parent product, such as Windows, that is providing UAL data.
RoleGUID	The UAL-assigned or registered GUID that represents the server role or installed product.
RoleName	The name of the role, component, or subproduct that is providing UAL data. This is also associated with a ProductName and a RoleGUID.
TenantIdentifier	A unique GUID for a tenant client of an installed role or product that accompanies the UAL data, if applicable.

Tabelle 2: Gerätespezifische Informationen [27]

2.3.4 Verfügbarkeit

User Access Logging ist auf den von Microsoft veröffentlichten Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 sowie auf Windows Server 2022 Betriebssystemen verfügbar und standardmäßig im Betriebssystem integriert, eine Aktivierung ist nicht erforderlich, eine Deaktivierung als Administrator möglich. Der Windows Service mit dem Namen *User Access Logging Service* befindet sich unter der Windows Service Funktion und kann bei Bedarf gestartet, gestoppt oder neugestartet werden.

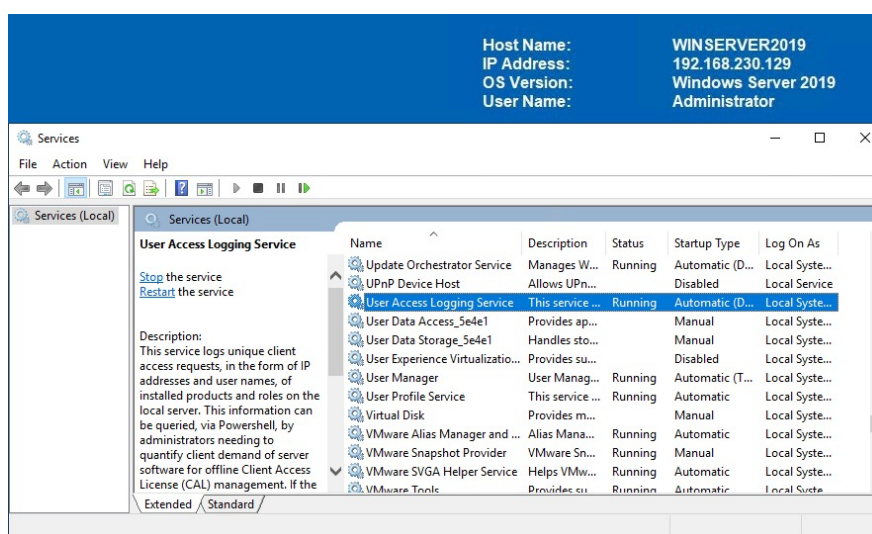


Abbildung 1: Windows Server 2019 - UAL Service

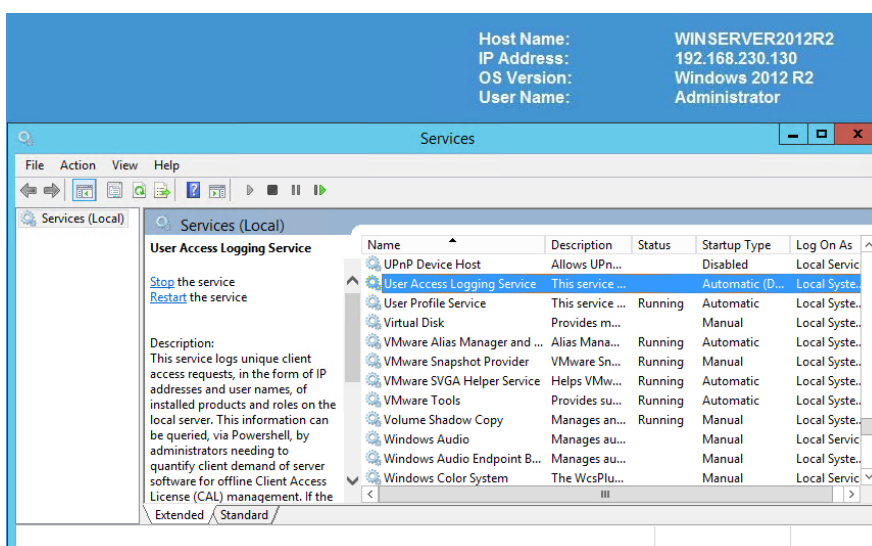


Abbildung 2: Windows Server 2012R2 - UAL Service

Ebenfalls kann der UAL-Service über *PowerShell* aktiviert bzw. deaktiviert werden sowie gestartet oder gestoppt werden:

PowerShell Befehl	Funktion
Enable-ual	UAL-Funktion aktivieren
Disable-ual	UAL-Funktion deaktivieren
Start-service ualsvc	UAL-Service starten
Stop-service ualsvc	UAL-Service stoppen

Tabelle 3: UAL-Service - PowerShell

Microsoft empfiehlt eine UAL-Deaktivierung bei Servern welche direkt mit dem Internet-Kommunizieren oder hohe Leistungsanforderungen haben. UAL wird nur empfohlen für Server, welche sich im eigenen Netzwerk dem sogenannten Intranet befinden ohne direkt Internetverbindung [27].

Microsoft hat das sogenannte *End-of-Life* von Windows Server 2012 sowie Windows Server 2012 R2 zum 10. Oktober 2023 bekannt gegeben. Ab diesem Moment wird Microsoft keine Produktunterstützung anbieten welches zur Folge hat das keine Updates, Fehlerbehebungen sowie technische Unterstützung und damit verbundenen technischen Veröffentlichungen angeboten werden [29]. Im Rahmen dieser Arbeit hat das *End-of-Life* von Windows Server 2012 R2 keinen Einfluss, es ist anzunehmen, dass trotz *End-of-Life* von Windows Server 2012 R2 weiterhin das Betriebssystem aktiv betrieben wird und somit die Erkenntnisse in Bezug auf Windows Server 2012 R2 und UAL aus dieser Arbeit weiterhin Bestand haben, Windows Server 2019 bleibt weiterhin als Microsoft unterstütztes Betriebssystem bis zum Zeitpunkt dieser Ausarbeitung gelistet und wird aktiv von Microsoft unterstützt.

2.3.5 Technische Grundlage Windows User Access Logging (UAL)

Microsoft veröffentlicht nur wenige Informationen über die Architektur von UAL, lediglich Administratorenwissen wird vermittelt, wie beispielsweise, die Verwaltung mittels UAL [33]. Im Rahmen dieser Arbeit wurde keine Fachliteratur identifiziert, welche dediziert Einblicke in die UAL-Architektur gibt wie beispielsweise welche DLL-Dateien [31] oder API-Schnittstellen [32] in Verbindung mit UAL stehen.

Ein Grundverständnis der Architektur ist jedoch hilfreich, um eine UAL-Bewertung und -Vergleichbarkeit auf beiden Windows Server Betriebssystemen (Windows Server 2019, Windows Server 2012 R2), welche für diese Arbeit ausgewählt wurden zu ermöglichen. Die technischen Informationen veröffentlicht in dieser Arbeit sind daher selbst erhoben und nicht als abschließend zu betrachten.

Um einen ersten Überblick über die UAL-Architektur zu erhalten wurden die Verzeichnisse der Windows Server Betriebssysteme durchsucht und lieferten folgende für das weitere Vorgehen relevanten Ergebnisse:

Betriebssystem	Filter (Suchwort)	Ergebnis	Verzeichnis
Windows Server 2019	UAL*.dll	ualprov.dll	C:\Windows\system32\
		ualapi.dll	C:\Windows\WinSxS\
		ualsvc.dll	
Windows Server 2012 R2	UAL*.dll	ualapi.dll	C:\Windows\SysWOW64\
		ualprov.dll	C:\Windows\system32\
		ualapi.dll	C:\Windows\WinSxS\
		ualsvc.dll	
		ualapi.dll	C:\Windows\SysWOW64\
		ualprov.dll	C:\Windows\system32\

Tabelle 4: UAL*.DLL Dateien

Dateien aus dem Verzeichnis *C:\Windows\assembly* sowie aus dem Verzeichnis *C:\Windows\Microsoft.NET* wurden nicht näher betrachtet, diese Ordner werden als Zwischenspeicher von .NET-Frameworks verwendet [34] und gehören somit mutmaßlich nicht zum UAL-Hauptmodul, sondern zur UAL-Sub-Modul.

Um ein klareres Verständnis zu gewährleisten, werden die angeführten Verzeichnisse damit ihrer Funktionen detailliert beschrieben:

Verzeichnis	Funktion
C:\Windows\system32	Kritisches Verzeichnis von Windows welches wichtige System Dateien beinhaltet [37].
C:\Windows\WinSxS	SxS ist die Abkürzung für Windows Side by Side, dieses Verzeichnis wird von Windows verwendet um Dateien zur Installation von Windows und Datensicherung dieser Versionen [38].
C:\Windows\SysWOW64	Verzeichnis welches ausschließlich auf 64-Bit Betriebssystemen vorhanden ist, dieses Verzeichnis enthält auch 32-Bit Komponenten, welche das Betriebssystem zum aktiven Betrieb benötigt [39].

Tabelle 5: Windows Verzeichnisse – Funktion

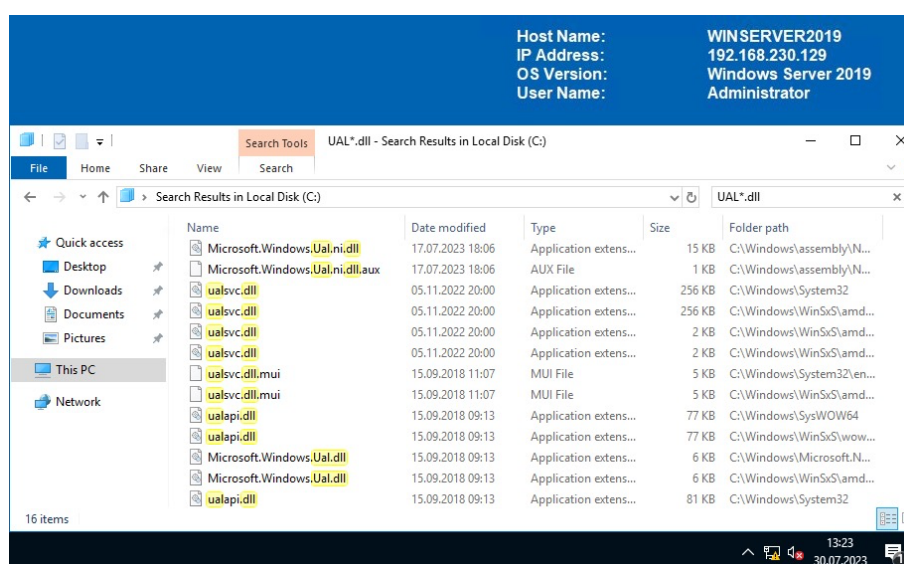


Abbildung 3: UAL*.DLL Dateien - Windows Server 2019

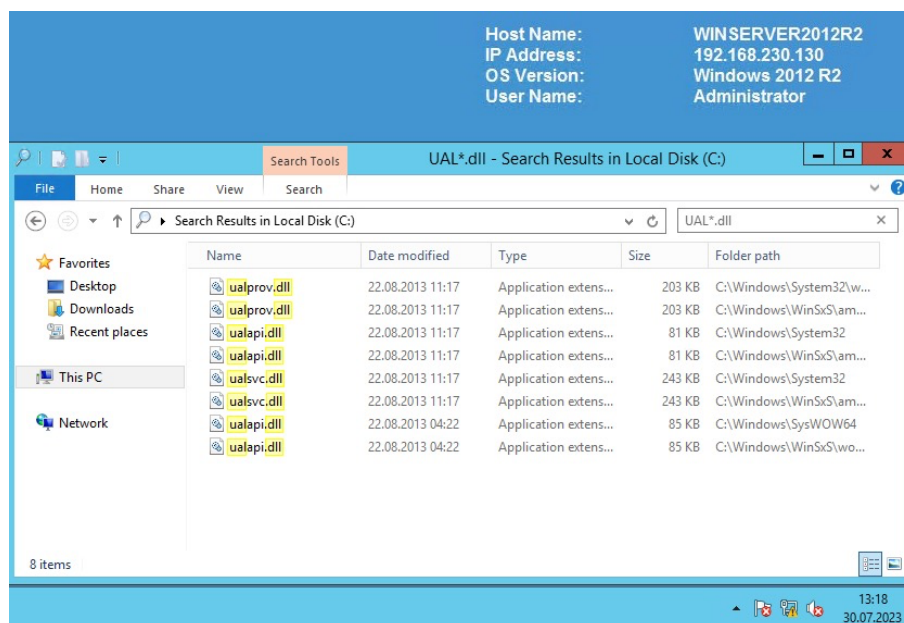


Abbildung 4: UAL*.DLL Dateien - Windows Server 2012 R2

Microsoft veröffentlicht keine dedizierten Informationen über die UAL-Architektur, somit werden die gefundenen DLL-Dateien mit Ghidra [35] untersucht, bei Ghidra handelt es sich um ein kostenloses open source Werkzeug, welches für Reverse Engineering [36] Aktivitäten entwickelt wurde.

Ghidra wurde hierzu auf den Windows 10 Client, Instanz 4 mit den Standard-Installationsoptionen installiert, die Detaillierte Beschreibung der Ghidra Installation und Funktionsweise kann auf der Herstellerseite [35] eingesehen werden, detaillierte Informationen der in dieser Arbeit verwendeten Version sind im *Kapitel 7.2 – Werkzeuge* referenziert.

Die DLL-Dateien der zwei Windows Server Betriebssysteme wurden exportiert und wie folgt umbenannt:

- Windows Server 2019 → ual*2019
- Windows Server 2012R2 → ual*2012

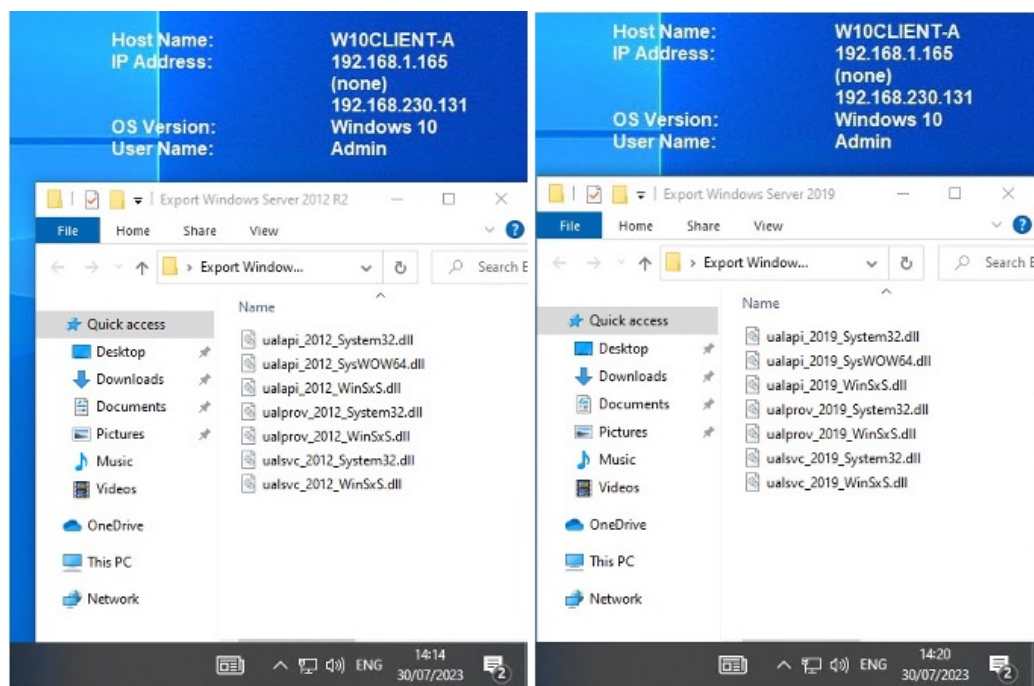


Abbildung 5: UAL*.DLL Dateien - Export

Die Umbenennung dient einer klaren Orientierung vor und während der Nutzung von Ghidra bei der Untersuchung der ual*2019/2012 DLL-Dateien:

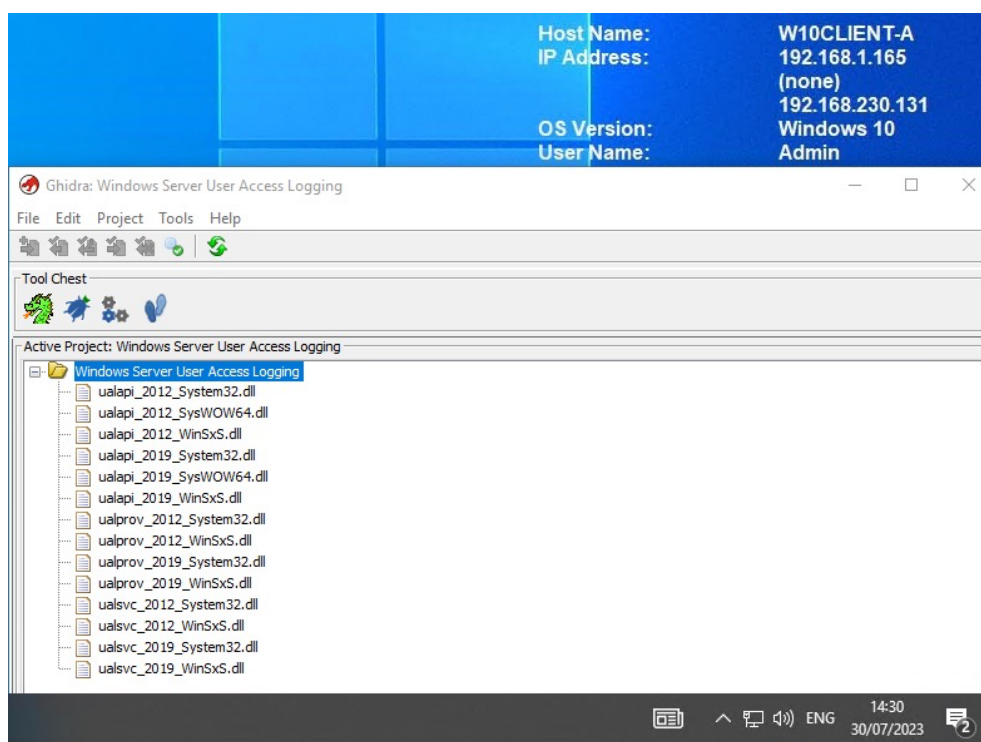


Abbildung 6: UAL*.DLL Dateien - Import Ghidra

Der *Ghidra Decompile* hat für die ual*2019/2012 DLL-Dateien die folgenden Ergebnisse geliefert (reduziert auf die mutmaßlich relevanten Ergebnisse):

DLL-Datei Name	Ergebnisse
ualapi_2012_System32.dll	Exports: UalInstrument, UalRegisterProduct, UalStart, UalStop
ualapi_2012_SysWOW64.dll	Exports: UalInstrument, UalRegisterProduct, UalStart, UalStop
ualapi_2012_WinSxS.dll	Exports: UalInstrument, UalRegisterProduct, UalStart, UalStop
ualapi_2019_System32.dll	Exports: UalInstrument, UalRegisterProduct, UalStart, UalStop
ualapi_2019_SysWOW64.dll	Exports: UalInstrument, UalRegisterProduct, UalStart, UalStop
ualapi_2019_WinSxS.dll	Exports: UalInstrument, UalRegisterProduct, UalStart, UalStop
ualprov_2012_System32.dll	Exports: DllRegisterServer, DllUnregisterServer
ualprov_2012_WinSxS.dll	Exports: DllRegisterServer, DllUnregisterServer
ualprov_2019_System32.dll	Exports: DllRegisterServer, DllUnregisterServer
ualprov_2019_WinSxS.dll	Exports: DllRegisterServer, DllUnregisterServer
ualsvc_2012_System32.dll	Exports: ServiceMain, SumSysprepCleanup
ualsvc_2012_WinSxS.dll	Exports: ServiceMain, SumSysprepCleanup
ualsvc_2019_System32.dll	Exports: ServiceMain, SumSysprepCleanup
ualsvc_2019_WinSxS.dll	Exports: ServiceMain, SumSysprepCleanup

Tabelle 6: UAL*.DLL Dateien - Ergebnisse Ghidra

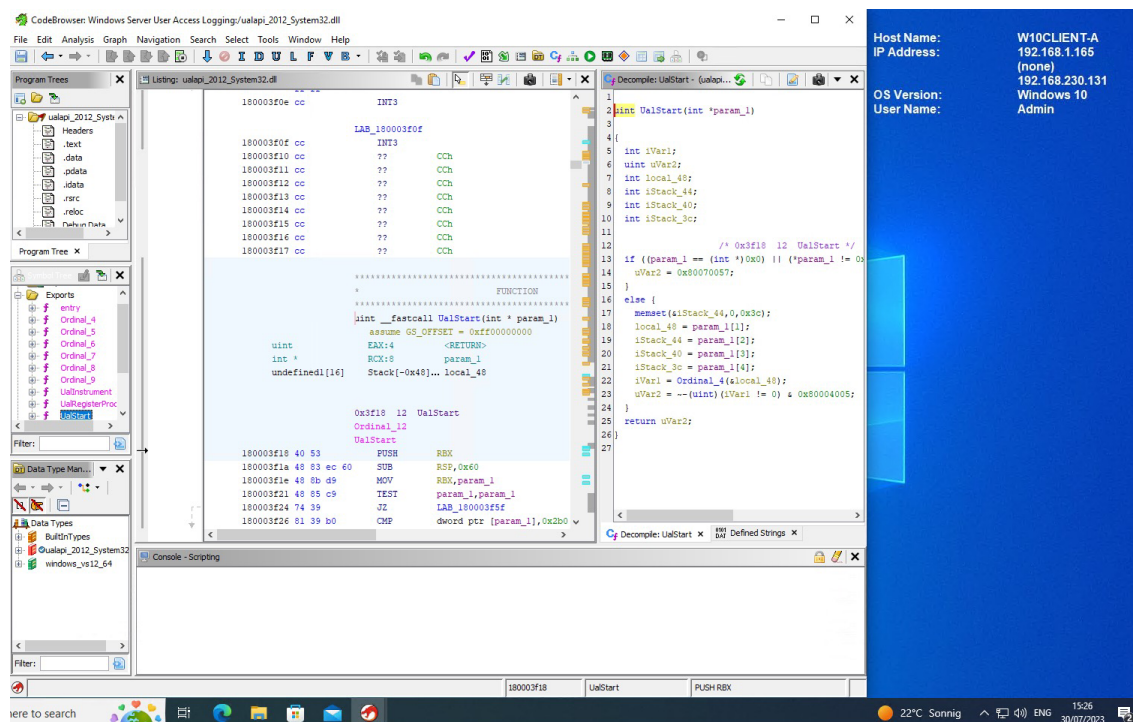


Abbildung 7: Ghirda - ualapi_2012_System32.dll exemplarisch

Die *Export Funktion* einer DLL-Datei ist wichtig da Informationen aus der DLL-Datei für andere Programme zur Verfügung gestellt werden, aufgrund der oben genannten Informationen, wird davon ausgegangen, dass die relevanten ual*2019/2012 DLL-Dateien sich im C:\Windows\system32 Verzeichnis befinden und die jeweils gleichnamigen ual*2019/2012 DLL-Dateien in den anderen Verzeichnissen lediglich Kopien im selben oder ähnlichen Zustand sind. Bei der *ualapi.dll* handelt es sich um einen sogenannten API-Wrapper [40] dieser ermöglicht einen vereinfachten Zugriff auf eine andere API [32] und dient somit als Vermittler zusätzlich wird der Entwicklungsaufwand bei Veränderungen im System minimiert.

Die oberflächliche Untersuchung mit Ghidra hat die Erkenntnis geliefert, dass die ual*2019/2012 DLL-Dateien im Verzeichnis C:\Windows\system32 bis auf kleine Änderungen im Quellcode aufgrund der unterschiedlichen Betriebssysteme dieselbe Funktion haben, somit kann abgeleitet werden, dass die UAL-Grundfunktion in Windows Server 2019 und Windows Server 2012 R2 eine Grundlage bietet für einen direkten Vergleich der UAL-Artefakte.

Unter Windows Services befindet sich der User Access Logging Service mit einem automatischen *Start-Typ, Automatic (Delayed Start)* welcher den UAL-Service startet (Information gültig für Windows Server 2019 sowie Windows Server 2012 R2).

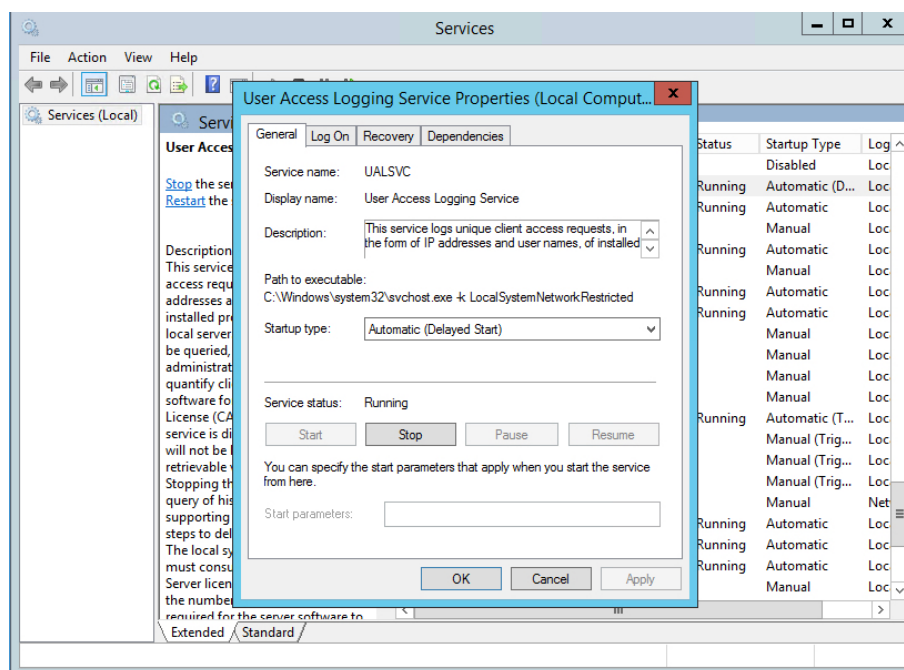


Abbildung 8: UAL-Service

Im Rahmen der zeitlichen Beschränkung dieser Arbeit war es nicht möglich den Anbieter zu identifizieren und herauszufinden, wo die *ualapi.dll*, *ualprov.dll*, *uapsvc.dll* verbraucht (verwendet) werden, insbesondere die Suche nach der GUID (Universally Unique Identifier) [41] war nicht erfolgreich.

Der UAL-Speicherort ist vordefiniert und befindet sich im Verzeichnis *C:\Windows\system32\LogFiles\Sum* [14] in diesem Verzeichnis befinden sich die UAL-Dateien, es handelt sich hierbei um *ESE (Extensible Storage Engine)* [42] Datenbank Dateien mit der Dateiendung *.mdb* in welche die gesammelten UAL-Informationen geschrieben werden [43]:

Name	Informationen	Speicherdauer
Current.mdb	Alle Informationen welche von der UAL-Funktion aufgezeichnet wurden (aktuell)	Letzten 24-Stunden des laufenden Jahres
{GUID}.mdb	Alle Informationen, welche von der UAL-Funktion aufgezeichnet wurden (Tägliche Kopie der Current.mdb Datenbankinformationen in diese {GUID}.mdb Datenbank), für jedes Kalenderjahr wird eine neue {GUID}.mdb erstellt	Insgesamt drei Jahre mit Current.mdb
SystemIdentity.mdb	Informationen über Dateien, Verzeichnisse, Rollen, Dienste, GUIDs und andere Ressourcen des Servers	Insgesamt drei Jahre

Tabelle 7: UAL-Datenbanken [43]

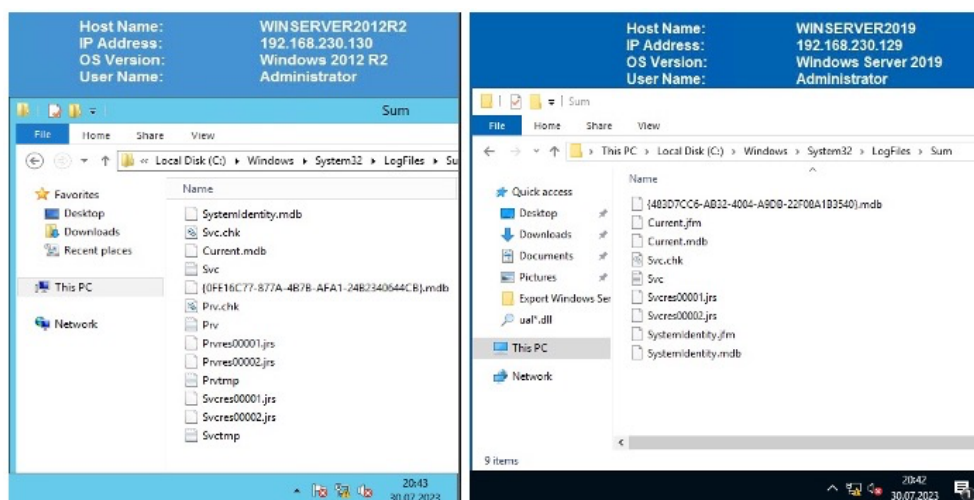


Abbildung 9: UAL-Datenbanken

Die aktuellen UAL-Informationen werden mit einer Verzögerung von 24 Stunden in die *Current.mdb* geschrieben. In der *Current.mdb* befinden sich die UAL-Informationen der letzten 24-Stunden, diese werden im Anschluss automatisch nach weiteren 24-Stunden in die Datenbank des aktuellen Jahres (*{GUID}.mdb*) verschoben. Die UAL-Informationen der letzten zwei Jahre werden in einer weiteren Datenbank aufbewahrt (*{GUID}.mdb*).

Die UAL-Informationen können mit Hilfe von *PowerShell cmdlets* über vordefinierte Befehle abgefragt und gesammelt werden. Microsoft veröffentlicht diese Information, welche ebenfalls spezifiziert werden können, um eine Informationsfilterung zu erreichen [33]:

PowerShell cmdlets	Funktion
Get-UalOverview	Provides UAL related details and history of installed products and roles.
Get-UalServerUser:	Provides client user access data for the local or targeted server.
Get-UalServerDevice:	Provides client device access data for the local or targeted server.
Get-UalUserAccess:	Provides client user access data for each role or product installed on the local or targeted server.
Get-UalDeviceAccess	Provides client device access data for each role or product installed on the local or targeted server.
Get-UalDailyUserAccess	Provides client user access data for each day of the year.
Get-UalDailyDeviceAccess	Provides client device access data for each day of the year.
Get-UalDailyAccess	Provides both client device and user access data for each day of the year.
Get-UalHyperV	Provides virtual machine data relevant to the local or targeted server.
Get-UalDns	Provides DNS client specific data of the local or targeted DNS server.
Get-UalSystemId	Provides system specific data to uniquely identify the local or targeted server.

Tabelle 8: Microsoft, Collect UAL Data [33]

Die UAL-Datenbanken sind durch die aktive UAL dauerhaft in Verwendung vom Windows Betriebssystem und dem UAL-Service, eine Kopie der aktiven Datenbank zu erstellen ist nur auf Umwegen möglich, siehe *Kapitel 8.4 - Untersuchung*.

Microsoft bietet nur begrenzte Informationen zur UAL-Architektur, um dennoch ein ganzheitliches Bild der UAL zu präsentieren wurde im Zuge der Recherche und Erarbeitung dieser Arbeit das folgende Schema entwickelt, welches die UAL-Architektur oberflächlich darstellt:

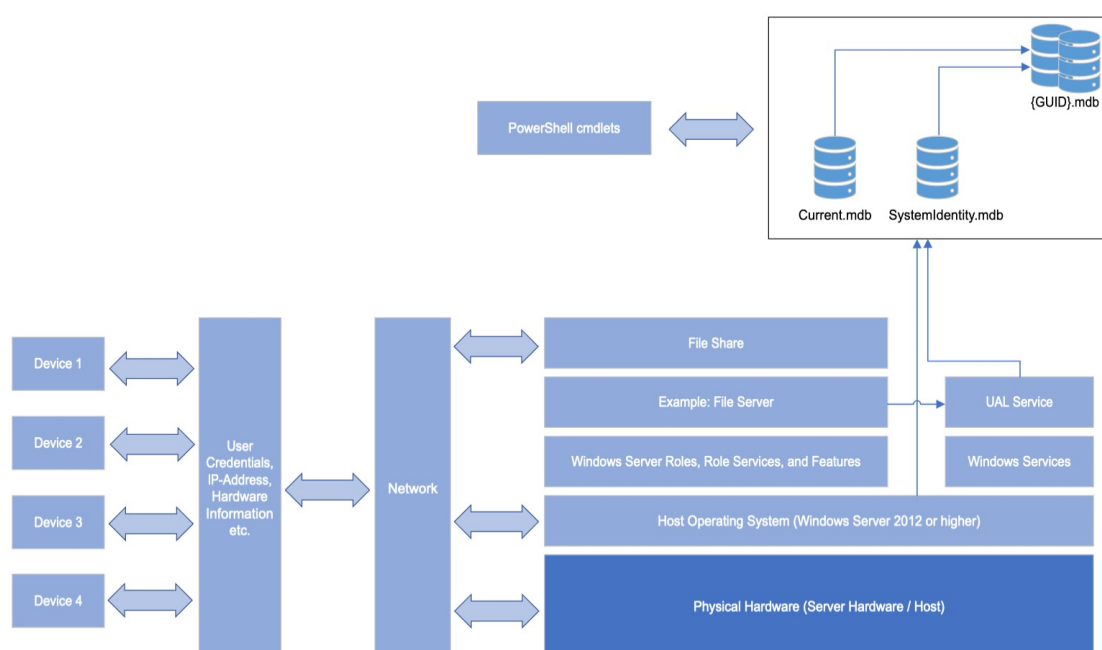


Abbildung 10: UAL-Architektur

3 Testumgebung

Die Testumgebung sowie die eingesetzten Werkzeuge sind in dieser Arbeit eng miteinander verbunden und ermöglichen es die Untersuchung in einer kontrollierten Umgebung welche reproduzierbaren Ergebnisse liefert durchzuführen.

3.1 Testumgebung

Die Testumgebung in dieser Arbeit baut auf einer leistungsfähigen Physischen mit Windows 10 betriebenen Workstation auf, welche als Host-System fungiert:

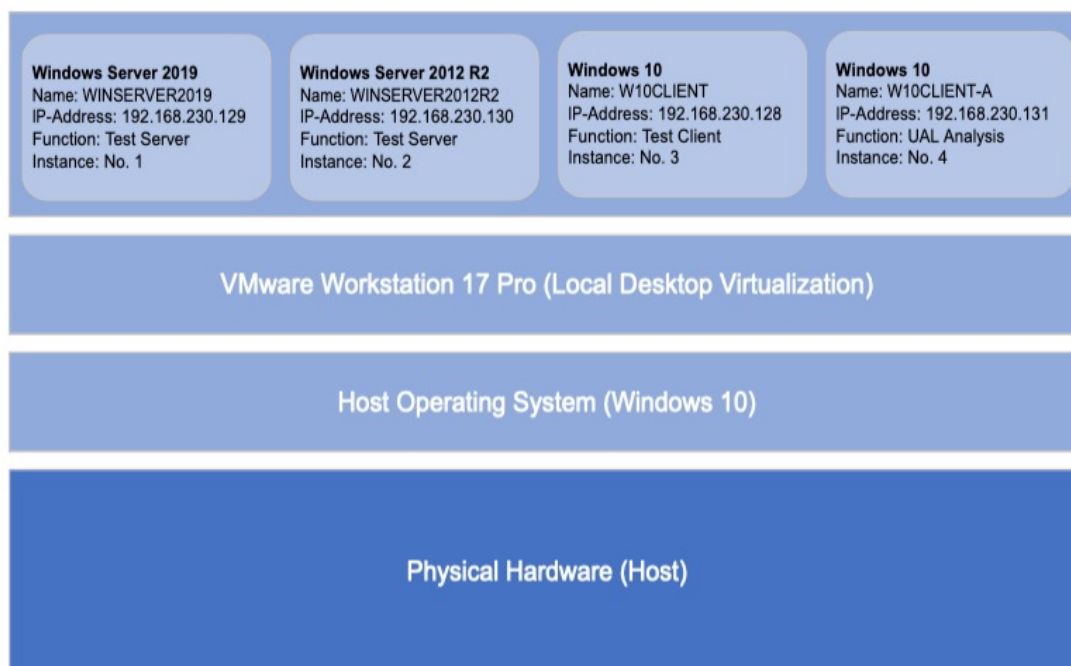


Abbildung 11: Testumgebung

Um den Betrieb verschiedener Betriebssystemumgebungen parallel zu ermöglichen, wurde auf die Lokale Desktop Virtualisierungslösung von VMware (VMware Workstation 17 Pro) zurückgegriffen, VMware bietet mit diesem Produkt eine flexible und skalierbare Lösung für virtuelle IT-Umgebung. Der Einsatz des VMware Workstation 17 Pro als Virtualisierungslösung ermöglicht es eine realitätsnahe physische IT-Umgebung virtuell abzubilden, welche den Betrieb von einzelnen virtuellen Instanzen parallel ermöglicht:

Instanz	Label	Zweck	Windows Rolle/Service
Instanz 1 (Instance 1)	Windows Server 2019 Name: WINSERVER2019 IP-Address: 192.168.230.129 Function: Test Server Instance: No. 1	Test-Server, Server Betriebssystem mit UA	File Server
Instanz 2 (Instance 2)	Windows Server 2012 R2 Name: WINSERVER2012R2 IP-Address: 192.168.230.130 Function: Test Server Instance: No. 2	Test-Server, Server Betriebssystem mit UAL	File Server
Instanz 3 (Instance 3)	Windows 10 Name: W10CLIENT IP-Address: 192.168.230.128 Function: Test Client Instance: No. 3	Client Betriebssystem, Test- Client für den Zugriff Instanz 1 & 2	Keine
Instanz 4 (Instance 4)	Windows 10 Name: W10CLIENT-A IP-Address: 192.168.230.131 Function: UAL Analysis Instance: No. 4	Client Betriebssystem zur Auswertung der UAL- Artefakte, Werkzeuge installiert	Keine

Tabelle 9: Virtuelle Instanzen

Die genannten Instanzen wurden mit den offiziellen Standardinstallationsmedien von Microsoft installiert, bei der Installation wurde die vorgeschlagene Standardeinstellung der Windows Betriebssystem Installationsroutine verwendet. Bei Instanz 1 (Windows Server 2019) wurde zusätzlich die Rolle *File Server* [44, 45] aktiviert, bei Instanz 2 (Windows Server 2012 R2) wurde ebenfalls die Rolle *File Server* [46, 47] aktiviert, um hierdurch eine Vergleichbarkeit der Ergebnisse auf beiden Betriebssystemen zu erreichen.

Ebenfalls wurde auf beide Server Betriebssysteme (Instanz 1 und 2) *RawCopy* heruntergeladen [12] und unter *C:\Windows\RawCopy* abgelegt.

Die folgenden Informationen gelten für Windows Server 2019 sowie für Windows Server 2012 R2:

Rolle	Funktion / Zweck
File Server	Ermöglicht es einem Server, Netzwerkdienste für das Speichern und Verwalten von Daten über ein Netzwerk zur Verfügung zu stellen, hierdurch wird der Zugriff auf gemeinsame Ressourcen erleichtert.

Tabelle 10: Funktion / Zweck - File Server

Es wurden pro Server Instanz jeweils ein Remote Shares (Netzwerkfreigabeordner) eingerichtet, welche direkt von der Windows 10-Client Instanz (Instanz 3) erreicht werden kann:

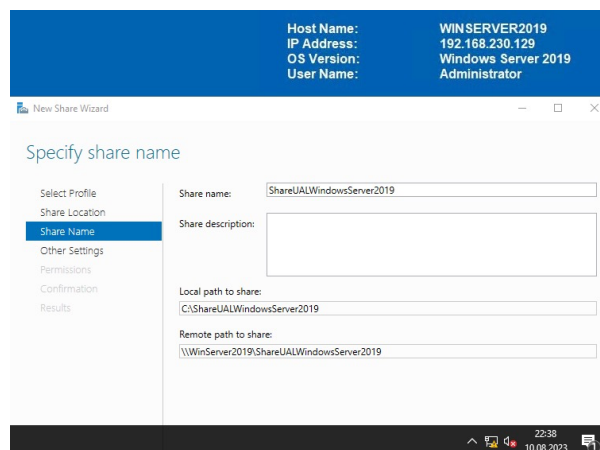


Abbildung 12: Share Windows Server 2019

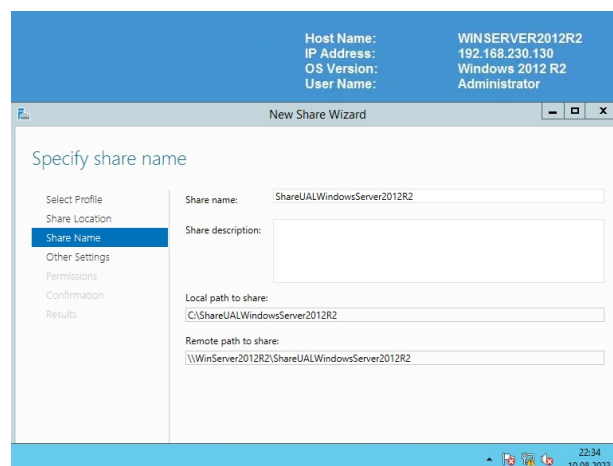


Abbildung 13: Share Windows Server 2012 R2

Um die Testszenarien durchzuführen, wurden auf den Server Instanzen (Instanz 1 und 2) zwei zusätzliche Benutzerkonten eingerichtet. Dies ermöglicht es, die UAL-Reaktion in Abhängigkeit zur Berechtigung des jeweiligen Benutzerkontos zu überprüfen. Eine Remote Verbindung (Fernverbindung) vom Windows 10 Client (Instanz 3) ist daher mit dem Benutzerkonto auf die gewünschte Server Instanz möglich.

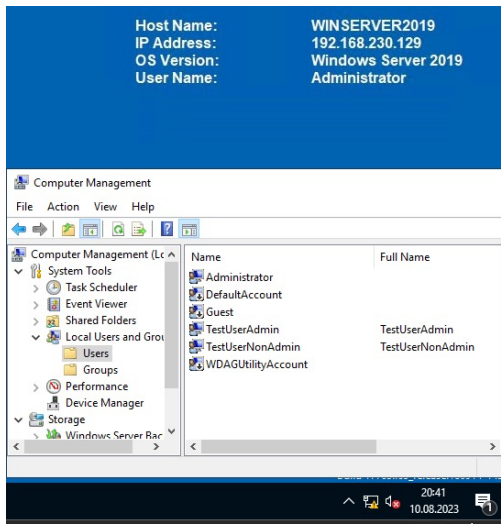
Instanz	Label	Benutzerkonto & Berechtigung
Instanz 1	Windows Server 2019 Name: WINSERVER2019 IP-Address: 192.168.230.129 Function: Test Server Instance: No. 1	Benutzerkonto: TestUserAdmin Berechtigung: Administratoren Rechte
		Benutzerkonto: TestUserNonAdmin Berechtigung: Keine Administratoren Rechte
		<div> Host Name: WINSERVER2019 IP Address: 192.168.230.129 OS Version: Windows Server 2019 User Name: Administrator </div> 

Tabelle 11: Windows Server 2019 - Benutzerkonto

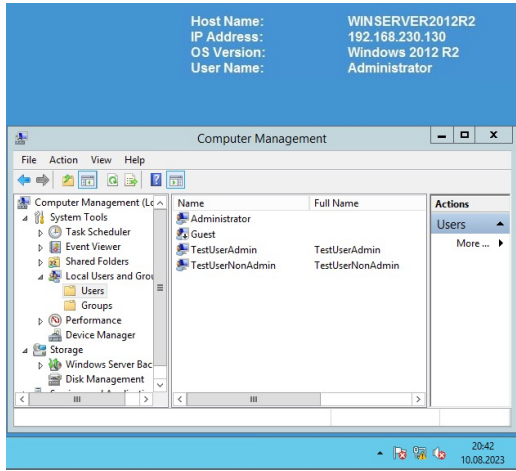
Instanz	Label	Benutzerkonto & Berechtigung
Instanz 2	Windows Server 2012 R2 Name: WINSERVER2012R2 IP-Address: 192.168.230.130 Function: Test Server Instance: No. 2	Benutzerkonto: TestUserNonAdmin Berechtigung: Keine Administratoren Rechte
		Benutzerkonto: TestUserAdmin Berechtigung: Administratoren Rechte
		

Tabelle 12: Windows Server 2012 R2 - Benutzerkonto

Um den Datenaustausch sowie die generelle Kommunikation zwischen den Instanzen über das virtuelle Netzwerk zu gewährleisten, wurden auf der Ebene des Windows Betriebssystems statische IP-Adressen zugewiesen. Hierfür wurde ein virtuelles Netzwerk mit VMware Workstation17 Pro eingerichtet:

Network:	vmnet0
Subnet IP:	192.168.230.0
Subnet mask:	255.255.255.0
Starting IP address:	192 . 168 . 230 . 128
Ending IP address:	192 . 168 . 230 . 254
Broadcast address:	192.168.230.255

Abbildung 14: Virtuelles Netzwerk

Jeder einzelnen virtuellen Instanz wurden spezifische Netzwerkeigenschaften zugewiesen, die endgültige Zuordnung lautet wie folgt:

Instanz 1

IP-Adresse: 192.168.230.129
Subnet: 255.255.255.0
Gateway: 192.168.230.1

Instanz 3

IP-Adresse: 192.168.230.128
Subnet: 255.255.255.0
Gateway: 192.168.230.1

Instanz 2

IP-Adresse: 192.168.230.130
Subnet: 255.255.255.0
Gateway: 192.168.230.1

Instanz 4

IP-Adresse: 192.168.230.131
Subnet: 255.255.255.0
Gateway: 192.168.230.1

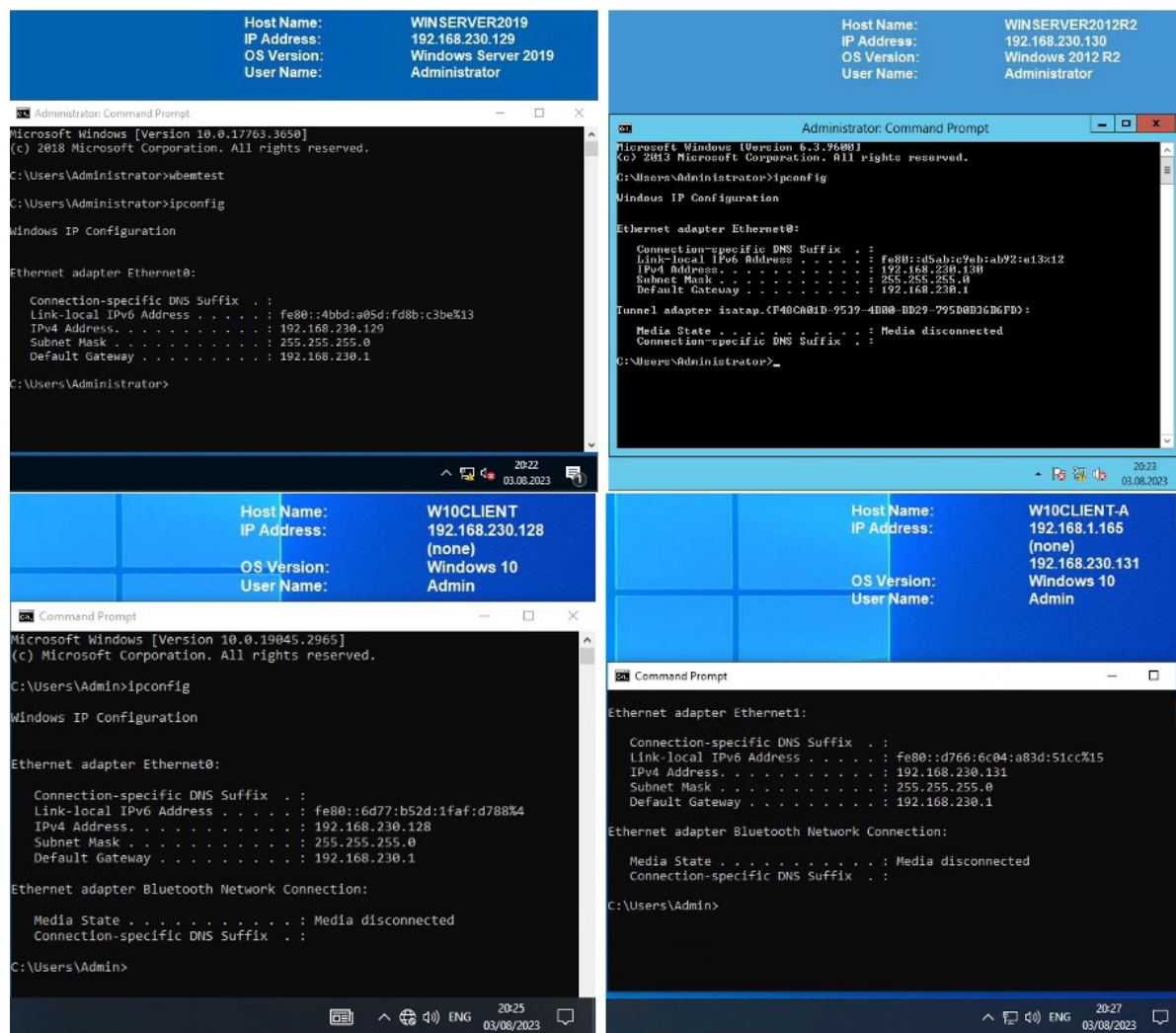


Abbildung 15: Netzwerkeigenschaften Virtuelle Instanzen

Im letzten Schritt wurden die bereits erstellten Remote Shares (Netzwerkfreigabeordner) auf dem Windows 10 Client (Instanz 3) eingebunden [49]:

- \\WinServer2019\ShareUALWindowsServer2019
- \\WinServer2012R2\ShareUALWindowsServer2012R2

Im Rahmen dieser Arbeit wurden die folgenden Windows Betriebssysteme eingesetzt und ermöglichen mit diesen Angaben eine exakte reproduktion der durchgeführten Untersuchungen und Ergebnissen:

Produkt: Microsoft Windows 10
Version: 10.0.19045 Build-19045.2965, 64-Bit
Lizenz: Vollversion
Sprache: Englisch
Veröffentlichung: 09. Mai 2023 [3]
Quelle: Microsoft Windows 10 [4]

Produkt: Microsoft Windows Server 2019 Standard Evaluation (Desktop Experience)
Version: 10.0.17763 Build-17763, 64-Bit
Lizenz: Evaluation 90-Tage
Sprache: Englisch
Veröffentlichung: 13. November 2018 [7]
Quelle: Microsoft Server 2019 [6]

Produkt: Windows Server 2019 PowerShell
Version: 5.1.17763.2931

Produkt: Microsoft Windows Server 2012 R2 (Standard Evaluation (Server with GUI))
Version: 6.3.9600 Build 9600, 64-Bit
Lizenz: Evaluation 90-Tage
Sprache: Englisch
Veröffentlichung: 25. November 2012 [5]
Quelle: Microsoft Server 2012 R2 [6]

Produkt: Windows Server 2012 R2 PowerShell
Version: 4.0

3.2 Werkzeuge

Bei der Auswahl der Werkzeuge wurde der aktuelle UAL-Forschungsstand, siehe *Kapitel 5.1 – Gegenwertiger Stand der Forschung*, berücksichtigt. Die Installation der Werkzeuge ist gemäß Herstellerinformationen erfolgt, welche der Herstellerseite insofern nicht näher beschrieben im Rahmen dieser Arbeit, siehe Quellenangabe, entnommen werden kann.

Zur optimalen Unterstützung und Ausführung der virtuellen Instanzen und geplanten Aktivitäten wurde folgendes Werkzeug auf dem physischen Host installiert und während der Untersuchung eingesetzt:

Produkt:	VMware Workstation 17 Pro
Version:	17.0.2 Build-21581411
Lizenz:	Vollversion
Sprache:	Englisch
Veröffentlichung:	20. April 2023 [1]
Quelle:	VMware Workstation 17 Pro [2]
Funktion:	Lokale Desktop Virtualisierungslösung

Um die Datenbank Extraktion auf den virtuellen Maschinen, Instanz 1 und 2 zu ermöglichen, wurde folgendes Werkzeug installiert und während der Untersuchung eingesetzt:

Produkt:	RawCopy
Version:	1.0.0.22
Lizenz:	Kostenlos
Sprache:	Englisch
Veröffentlichung:	30. Juli 2019 [12]
Quelle:	Github RawCopy [12]
Funktion:	Dateiextraktor

Um eine detaillierte Analyse der UAL durchzuführen, wurde auf der virtuellen Maschine, Instanz 4, die nachfolgenden Werkzeuge installiert und während der Untersuchung eingesetzt:

Produkt: Microsoft Excel 2016
Version: 10.0.4266.1001, 32-Bit
Lizenz: Vollversion
Sprache: Englisch
Veröffentlichung: 22. September 2015 [8]
Quelle: Microsoft Excel [9]
Funktion: Tabellenkalkulationslösung

Produkt: Python
Version: 3.11.4
Version: 3.11.5
Lizenz: Kostenlos, Open source
Sprache: Englisch
Veröffentlichung: 06. Juni 2023 [10]
Quelle: Python [10]
Funktion: Programmiersprache und Programmierwerkzeug
Info: Im Verlauf der Erstellung diese Arbeit wurde Python, Version 3.11.5 am 24. August 2023 veröffentlicht, nach der Veröffentlichung wurde Python, Version 3.11.5 installiert und verwendet

Produkt: Ghidra
Version: 10.3.2 Build PUBLIC
Lizenz: Kostenlos
Sprache: Englisch
Veröffentlichung: 11. Juli 2023
Quelle: Ghidra [35]
Funktion: Reverse Engineering Werkzeug

Produkt: KStrike
Version: 20210624
Lizenz: Kostenlos
Sprache: Englisch
Veröffentlichung: 24. Juni 2021 [11]
Quelle: Github KStrike [11]
Funktion: Python Skript analysiert UAL-Informationen

Bei der Auswahl von *KStrike* als Werkzeuge wurde der aktuelle UAL-Forschungsstand berücksichtigt. Der *UAL_Parser* [52], welcher als Plugin in Autopsy [51] integriert werden kann, fand keine Berücksichtigung, da er auf der Basis von *KStrike* entwickelt wurde. Die Alternative, *SumECmd* [53], wurde ebenfalls nicht in Erwägung gezogen, da es ausschließlich mit intakten (cleanen) Datenbanken arbeitet. Das spiegelt nicht immer die Realität wieder, in der man häufig auch mit beschädigten (dirty) Datenbanken konfrontiert ist. *KStrike* hingegen ist in der Lage, sowohl mit intakten als auch mit beschädigten Datenbanken effizient zu arbeiten.

4 Untersuchung

4.1 Konkretisierung der Forschungsfragen

Forschungsfrage 1: Welche Informationen werden durch die UAL protokolliert (Informationsgehalt) und wie lange werden diese gespeichert?

Konkretisierung: Können mit Hilfe der UAL als forensisches Artefakt die W-Fragen [48] beantwortet werden (Was ist geschehen; Wo ist es passiert; Wann ist es passiert; Wie ist es passiert)?

Forschungsfrage 2: Wie können UAL-Artefakte ausgelesen und extrahiert werden?

Konkretisierung: Vorstellung der Methoden zum Auslesen sowie extrahieren von UAL-Artefakten

Forschungsfrage 3: Unterscheidet sich die UAL-Funktion sowie die UAL-Artefakte von Windows Server 2012 R2 und Windows Server 2019?

Konkretisierung: Gibt es funktionelle Unterschiede der UAL-Funktion bei Windows Server 2012 R2 im Vergleich zu Windows Server 2019?

Konkretisierung: Gibt es Unterschiede der UAL-Artefakte bei Windows 2012 R2 im Vergleich zu Windows Server 2019?

<p>Forschungsfrage 4: Wie sind UAL-Artefakte zu interpretieren und kann den Anforderungen an die Erhebung von Daten gerecht werden (Robustheit)?</p> <p><u>Konkretisierung:</u> Wird UAL den Anforderungen gerecht in Bezug auf: Akzeptanz, Glaubwürdigkeit, Wiederholbarkeit, Integrität, Ursache und Auswirkung sowie Dokumentation [20,21]?</p>
<p>Forschungsfrage 5: Welche Grenzen gibt es bei der UAL als forensisches Artefakt?</p> <p><u>Konkretisierung:</u> Darstellung von technischen Grenzen.</p>
<p>Forschungsfrage 6: Welche Möglichkeiten bietet die UAL als forensisches Artefakt?</p> <p><u>Konkretisierung:</u> Darstellung von technischen Möglichkeiten.</p>

Tabelle 13: Konkretisierung der Forschungsfragen

4.2 Testszenarien

Sämtliche Testszenarien starten auf der Instanz 3, die mit dem Windows 10 Client-Betriebssystem betrieben wird initiiert und systematisch auf den beiden Windows Server Betriebssystemen, Instanz 1 (betrieben mit Windows Server 2019) und Instanz 2 (betrieben mit Windows Server 2012 R2) ausgeführt, wie Anlage 1 – Testszenarien, zu entnehmen ist.

4.3 Methoden

Die UAL-Untersuchung wird unter Anwendung von zwei verschiedenen Methoden durchgeführt:

- **Methode 1:** Live-Untersuchung mittels *PowerShell Cmdlets* direkt auf den Server Betriebssystemen (Instanz 1 und 2). Microsoft ermöglicht es, mit *PowerShell Cmdlets* Informationen zu erheben, unabhängig davon, ob das Betriebssystem und die Datenbank gerade verwendet werden oder nicht.
- **Methode 2:** Post-mortem-Analyse durch Verwendung einer Kopie der UAL-Datenbank. Diese Kopie wird mit *RawCopy* erstellt und anschließend mittels *KStrike* auf dem Windows Client (Instanz 4) analysiert. Dies ermöglicht eine tiefgehende Analyse auf einem dedizierten Analyse Client, auf welchem

bereits alle notwendigen Werkzeuge zur UAL-Analyse vorinstalliert sind. Diese Methode bietet zudem den Vorteil, dass sie eine externe und zeitlich flexible Analyse erlaubt, was dem gängigen Vorgehen in der Praxis entspricht [22].

4.4 Untersuchung

Die in *Kapitel 8.2* beschriebenen Testszenarien wurden auf beiden Server-Betriebssystemen (Instanz 1 und Instanz 2) durchgeführt. Die Untersuchung nach erfolgreicher Durchführung der Testszenarien erfolgt für jede Instanz in zwei Phasen:

Phase 1: Live-Analyse direkt auf dem Windows Server-Betriebssystem (Instanz 1 und Instanz 2)

Phase 2: Post-mortem-Analyse der UAL-Datenbank Kopien auf dem Windows 10 Analyse-Client (Instanz 4)

4.4.1 Live-Untersuchung Windows Server 2019

Für die Live-Untersuchung werden die von Microsoft bereitgestellten *PowerShell Cmdlets*, *Kapitel 6.3.5 – Technische Grundlagen Windows User Access Logging (UAL)* genutzt. Mittels *PowerShell Cmdlet Get-UalOverview* wurde ein Überblick über UAL-Rollen, welche unterstützt werden, gewonnen. Dabei wurden insgesamt 13 Windows-Rollen identifiziert, die in direktem Zusammenhang mit der UAL stehen. Detaillierte Informationen sind in *Anlage 2* aufgeführt, lediglich die Einträge welche einen *FirstSeen* sowie einen *LastSeen* aufweisen, verarbeiten tatsächlich aktive Zugriffe von Clients. Insbesondere der Eintrag mit dem *Role Name, File Server* ist im Kontext dieser Arbeit von Bedeutung. Somit bestätigt die Übersicht, welche durch *Get-UalOverview* geliefert wurde, die Rolle des *File Server* sowie des *Print and Document Services*.

```

Host Name:      WINSERVER2019
IP Address:     192.168.230.129
OS Version:     Windows Server 2019

PS C:\Users\Administrator> Get-UalOverview

FirstSeen      :
GUID           : 952285d9-edb7-4b6b-9d85-0c09e3da0bbd
LastSeen       :
ProductName     : Windows Server 2019 Standard Evaluation
RoleName       : Remote Access
PSComputerName :

FirstSeen      :
GUID           : c50fcc83-bc8d-4df5-8a3d-89d7f80f074b
LastSeen       :
ProductName     : Windows Server 2019 Standard Evaluation
RoleName       : Active Directory Certificate Services
PSComputerName :

FirstSeen      :
GUID           : c23f1c6a-30a8-41b6-bbf7-f266563dfcd6
LastSeen       :
ProductName     : Windows Server 2019 Standard Evaluation
RoleName       : FTP Server
PSComputerName :

FirstSeen      :
GUID           : d6256cf7-98fb-4eb4-aa18-303f1da1f770
LastSeen       :
ProductName     : Windows Server 2019 Standard Evaluation
RoleName       : Web Server
PSComputerName :

FirstSeen      : 20.07.2023 12:37:26
GUID           : 10a9226f-50ee-49d8-a393-9a501d47ce04
LastSeen       : 17.08.2023 22:24:30
ProductName     : Windows Server 2019 Standard Evaluation
RoleName       : File Server
PSComputerName :

FirstSeen      :
GUID           : 910cbaf9-b612-4782-a21f-f7c75105434a
LastSeen       :
ProductName     : Windows Server 2019 Standard Evaluation
RoleName       : BranchCache
PSComputerName :

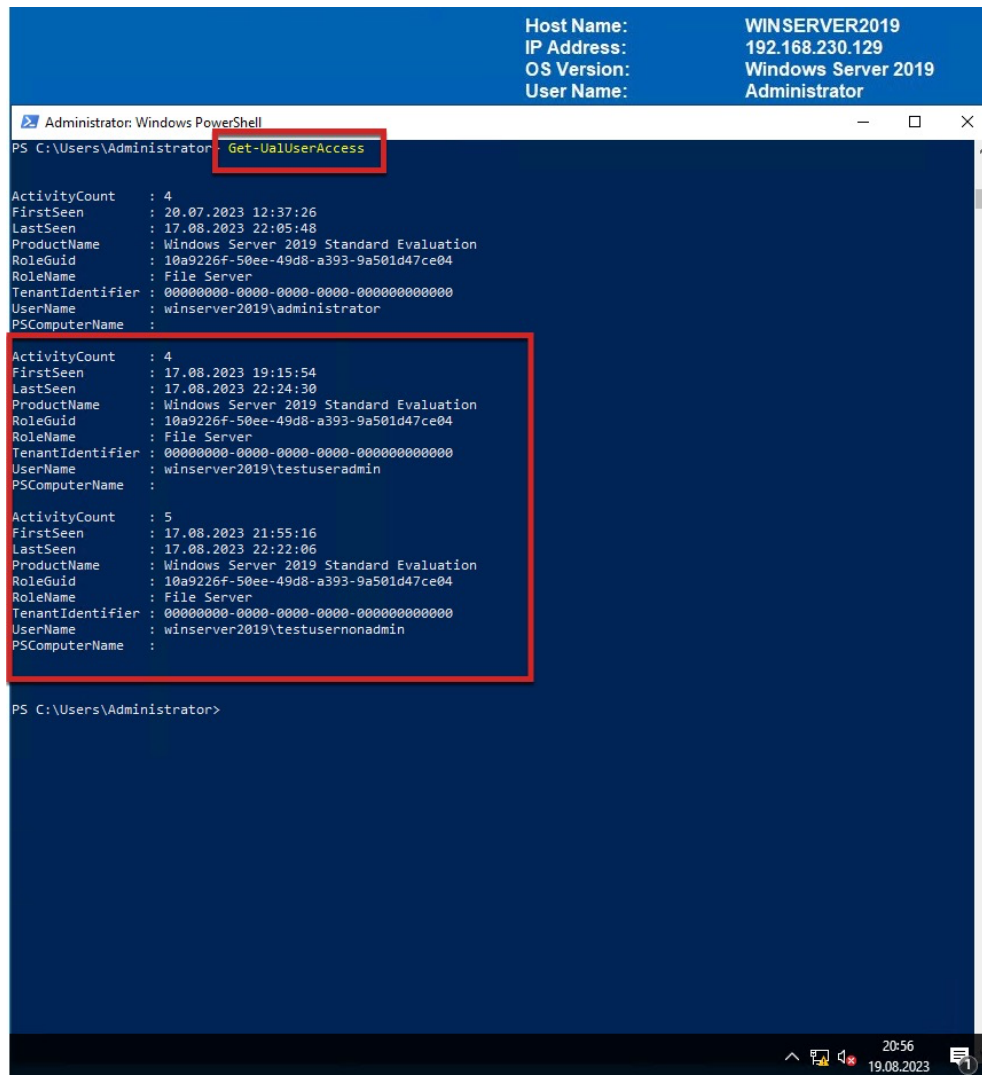
FirstSeen      :
GUID           : d8dclc8e-ea13-49ce-9a68-c9dca8db8b33
LastSeen       :
ProductName     : Windows Server 2019 Standard Evaluation
RoleName       : Windows Server Update Services
PSComputerName :

FirstSeen      : 15.07.2023 19:17:11
GUID           : 7fb09bd3-7fe6-435e-8348-7d8aefb6cea3
LastSeen       : 17.08.2023 22:02:05
ProductName     : Windows Server 2019 Standard Evaluation
RoleName       : Print and Document Services
PSComputerName :

```

Abbildung 16: Windows Server 2019 - Get-UalOverview

Durch das Verwenden des *PowerShell* Cmdlet *Get-UalUserAccess* können UAL-Informationen über Benutzerzugriffe auf spezifische Windows Services wie in unserem Fall den File Server, abgerufen werden. Die Ergebnisse zeigen die für die Tests erstellten Benutzer, *TestUserAdmin* sowie *TestUserNonAdmin*. Beide weisen die Einträge *FirstSeen* und *LastSeen* auf, somit wurden die Zugriffe und Aktionen erfasst und in Verbindung mit dem *File Server* gebracht.



```
Host Name: WINSERVER2019
IP Address: 192.168.230.129
OS Version: Windows Server 2019
User Name: Administrator

Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-UalUserAccess

ActivityCount : 4
FirstSeen : 20.07.2023 12:37:26
LastSeen : 17.08.2023 22:05:48
ProductName : Windows Server 2019 Standard Evaluation
RoleGuid : 10a9226f-50ee-49d8-a393-9a501d47ce04
RoleName : File Server
TenantIdentifier : 00000000-0000-0000-0000-000000000000
UserName : winserver2019\administrator
PSComputerName :

ActivityCount : 4
FirstSeen : 17.08.2023 19:15:54
LastSeen : 17.08.2023 22:24:30
ProductName : Windows Server 2019 Standard Evaluation
RoleGuid : 10a9226f-50ee-49d8-a393-9a501d47ce04
RoleName : File Server
TenantIdentifier : 00000000-0000-0000-0000-000000000000
UserName : winserver2019\testuseradmin
PSComputerName :

ActivityCount : 5
FirstSeen : 17.08.2023 21:55:16
LastSeen : 17.08.2023 22:22:06
ProductName : Windows Server 2019 Standard Evaluation
RoleGuid : 10a9226f-50ee-49d8-a393-9a501d47ce04
RoleName : File Server
TenantIdentifier : 00000000-0000-0000-0000-000000000000
UserName : winserver2019\testusernonadmin
PSComputerName :

PS C:\Users\Administrator>
```

Abbildung 17: Windows Server 2019 - Get-UalUserAccess

Durch das Verwenden des *PowerShell* Cmdlet *Get-UalDailyAccess* können UAL-Informationen über die Benutzer und die damit verbundenen Netzwerkinformationen abgerufen werden. Die Ergebnisse zeigen die Benutzernamen, *TestUserAdmin* sowie *TestUserNonAdmin* in Verbindung mit den Netzwerkinformationen (IP-Adresse). Eine Zuordnung der IP-Adresse zur Instanz 3 dem Windows 10 Client ist somit bestätigt.


```

Host Name: WINSERVER2019
IP Address: 192.168.230.129
OS Version: Windows Server 2019
User Name: Administrator

Administrator: Windows PowerShell

PS C:\Users\Administrator> Get-UalDailyAccess

AccessCount      : 1
AccessDate       : 20.07.2023
IPAddress        : ::1
Username         : winserver2019\administrator
TenantIdentifier : 00000000-0000-0000-0000-000000000000
ProductName      : Windows Server 2019 Standard Evaluation
RoleGuid        : 10a9226f-50ee-49d8-a393-9a501d47ce04
RoleName        : File Server
PSComputerName   :

AccessCount      : 1
AccessDate       : 10.08.2023
IPAddress        : fe80::4bda:a05d:fd8b:c3be
Username         : winserver2019\administrator
TenantIdentifier : 00000000-0000-0000-0000-000000000000
ProductName      : Windows Server 2019 Standard Evaluation
RoleGuid        : 10a9226f-50ee-49d8-a393-9a501d47ce04
RoleName        : File Server
PSComputerName   :

AccessCount      : 2
AccessDate       : 17.08.2023
IPAddress        : fe80::4bda:a05d:fd8b:c3be
Username         : winserver2019\administrator
TenantIdentifier : 00000000-0000-0000-0000-000000000000
ProductName      : Windows Server 2019 Standard Evaluation
RoleGuid        : 10a9226f-50ee-49d8-a393-9a501d47ce04
RoleName        : File Server
PSComputerName   :

AccessCount      : 4
AccessDate       : 17.08.2023
IPAddress        : fe80::6d77:b52d:1faf:d788
Username         : winserver2019\testuseradmin
TenantIdentifier : 00000000-0000-0000-0000-000000000000
ProductName      : Windows Server 2019 Standard Evaluation
RoleGuid        : 10a9226f-50ee-49d8-a393-9a501d47ce04
RoleName        : File Server
PSComputerName   :

AccessCount      : 5
AccessDate       : 17.08.2023
IPAddress        : fe80::6d77:b52d:1faf:d788
Username         : winserver2019\testuseradmin
TenantIdentifier : 00000000-0000-0000-0000-000000000000
ProductName      : Windows Server 2019 Standard Evaluation
RoleGuid        : 10a9226f-50ee-49d8-a393-9a501d47ce04
RoleName        : File Server
PSComputerName   :

```

Abbildung 18: Windows Server 2019 - Get-UalDailyAccess

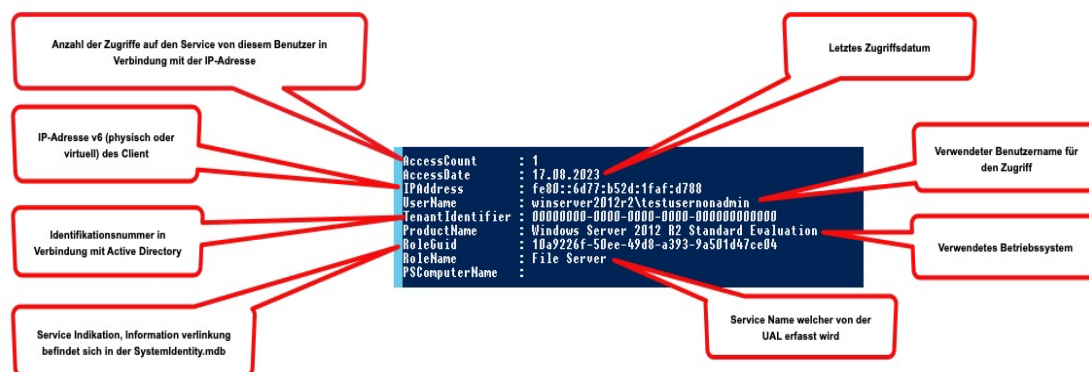


Abbildung 19: Beispiel - Informationsaufschlüsselung

Microsoft bietet keine weiteren für die vorliegende Untersuchung relevanten *PowerShell Cmdlets* an. Damit ist die Live-Untersuchung abgeschlossen und die von der UAL erfassten Daten wurden erfolgreich abgerufen.

4.4.2 Live-Untersuchung Windows Server 2012R2

Für die Live-Untersuchung werden die von Microsoft bereitgestellten *PowerShell Cmdlets*, Kapitel 6.3.5 – *Technische Grundlagen Windows User Access Logging (UAL)* genutzt. Mittels *PowerShell Cmdlet Get-UalOverview* wurde ein Überblick über UAL-Rollen, welche unterstützt werden, gewonnen. Dabei wurden insgesamt 13 Windows-Rollen identifiziert, die in direktem Zusammenhang mit der UAL stehen. Detaillierte Informationen sind in *Anlage 3* aufgeführt, lediglich die Einträge welche einen *FirstSeen* sowie einen *LastSeen* aufweisen, verarbeiten tatsächlich aktive Zugriffe von Clients. Insbesondere der Eintrag mit dem *Role Name, File Server* ist im Kontext dieser Arbeit von Bedeutung. Somit bestätigt die Übersicht, welche durch *Get-UalOverview* geliefert wurde, die Rolle des *File Server* sowie des *Print and Document Services*.

```

Host Name: WINSERVER2012R2
IP Address: 192.168.230.130
OS Version: Windows 2012 R2
User Name: Administrator

Administrator: Windows PowerShell

Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Get-UalOverview

FirstSeen      :
GUID           : 952285d9-edb7-4b6b-9d85-0c09e3da0bbd
LastSeen       :
Product Name   : Windows Server 2012 R2 Standard Evaluation
Role Name      : Remote Access
PSComputerName :

FirstSeen      :
GUID           : c50fcc83-bc8d-4df5-8a3d-89d7f80f074b
LastSeen       :
Product Name   : Windows Server 2012 R2 Standard Evaluation
Role Name      : Active Directory Certificate Services
PSComputerName :

FirstSeen      :
GUID           : c23f1c6a-30a8-41b6-bbf7-f266563dfcd6
LastSeen       :
Product Name   : Windows Server 2012 R2 Standard Evaluation
Role Name      : FTP Server
PSComputerName :

FirstSeen      :
GUID           : d6256cf7-98fb-4eb4-aa18-303f1da1f770
LastSeen       :
Product Name   : Windows Server 2012 R2 Standard Evaluation
Role Name      : Web Server
PSComputerName :

FirstSeen      : 30.07.2023 18:13:20
GUID           : 10a9226f-50ee-45d8-a393-9a501d47ce04
LastSeen       : 17.08.2023 22:28:19
Product Name   : Windows Server 2012 R2 Standard Evaluation
Role Name      : File Server
PSComputerName :

FirstSeen      :
GUID           : 910cbaf9-b612-4702-a21f-f7c75105434a
LastSeen       :
Product Name   : Windows Server 2012 R2 Standard Evaluation
Role Name      : BranchCache
PSComputerName :

FirstSeen      :
GUID           : d8dc1c8e-ea13-49ce-9a68-c9dca8db8b33
LastSeen       :
Product Name   : Windows Server 2012 R2 Standard Evaluation
Role Name      : Windows Server Update Services
PSComputerName :

FirstSeen      : 18.07.2023 17:57:28
GUID           : 7fb09bd3-7ee6-435e-8348-7d8aefb6cea3
LastSeen       : 17.08.2023 22:04:53
Product Name   : Windows Server 2012 R2 Standard Evaluation
Role Name      : Print and Document Services
PSComputerName :
  
```

Abbildung 20: Windows Server 2012 R2 - Get-UalOverview

Durch das Verwenden des *PowerShell Cmdlet Get-UalUserAccess* können UAL-Informationen über Benutzerzugriffe auf spezifische Windows Services wie in unserem Fall den File Server, abgerufen werden. Die Ergebnisse zeigen die für die Tests erstellten Benutzer, *TestUserAdmin* sowie *TestUserNonAdmin*.

Beide weisen die Einträge *FirstSeen* und *LastSeen* auf, somit wurden die Zugriffe und Aktionen erfasst und in Verbindung mit dem *File Server* gebracht.

```

Host Name: WINSERVER2012R2
IP Address: 192.168.230.130
OS Version: Windows 2012 R2
User Name: Administrator

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Get-UalUserAccess

ActivityCount : 7
FirstSeen : 30.07.2023 18:13:20
LastSeen : 17.08.2023 22:05:21
ProductName : Windows Server 2012 R2 Standard Evaluation
RoleGuid : 10a9226f-50ee-49d8-a393-9a501d47ce04
RoleName : File Server
TenantIdentifier : 00000000-0000-0000-0000-000000000000
UserName : winserver2012r2\administrator
PSComputerName :

ActivityCount : 1
FirstSeen : 17.08.2023 22:28:19
LastSeen : 17.08.2023 22:28:19
ProductName : Windows Server 2012 R2 Standard Evaluation
RoleGuid : 10a9226f-50ee-49d8-a393-9a501d47ce04
RoleName : File Server
TenantIdentifier : 00000000-0000-0000-0000-000000000000
UserName : winserver2012r2\testuseradmin
PSComputerName :

ActivityCount : 1
FirstSeen : 17.08.2023 22:26:06
LastSeen : 17.08.2023 22:26:06
ProductName : Windows Server 2012 R2 Standard Evaluation
RoleGuid : 10a9226f-50ee-49d8-a393-9a501d47ce04
RoleName : File Server
TenantIdentifier : 00000000-0000-0000-0000-000000000000
UserName : winserver2012r2\testusernonadmin
PSComputerName :

PS C:\Users\Administrator>
  
```

Abbildung 21: Windows Server 2012 R2 - Get-UalUserAccess

Durch das Verwenden des *PowerShell Cmdlet Get-UalDailyAccess* können UAL-Informationen über die Benutzer und die damit verbundenen Netzwerkinformationen abgerufen werden. Die Ergebnisse zeigen die Benutzernamen, *TestUserAdmin* sowie *TestUserNonAdmin* in Verbindung mit den Netzwerkinformationen (IP-Adresse). Eine Zuordnung der IP-Adresse zur Instanz 3 dem Windows 10 Client ist somit bestätigt.

```

Host Name: WINSERVER2012R2
IP Address: 192.168.230.130
OS Version: Windows 2012 R2
User Name: Administrator

Administrator: Windows PowerShell

PS C:\Users\Administrator> Get-UalDailyAccess

AccessCount : 1
AccessDate  : 30.07.2023
IPAddress   : ::1
UserName    : winserver2012r2\Administrator
TenantIdentifier : 00000000-0000-0000-0000-000000000000
ProductName : Windows Server 2012 R2 Standard Evaluation
RoleGuid    : 10a9226f-50ee-49d8-a393-9a501d47ce04
RoleName    : File Server
PSComputerName :

AccessCount : 1
AccessDate  : 17.08.2023
IPAddress   : fe80::6d77:b52d:1faf:d788
UserName    : winserver2012r2\testuseradmin
TenantIdentifier : 00000000-0000-0000-0000-000000000000
ProductName : Windows Server 2012 R2 Standard Evaluation
RoleGuid    : 10a9226f-50ee-49d8-a393-9a501d47ce04
RoleName    : File Server
PSComputerName :

AccessCount : 1
AccessDate  : 17.08.2023
IPAddress   : fe80::6d77:b52d:1faf:d788
UserName    : winserver2012r2\testusernonadmin
TenantIdentifier : 00000000-0000-0000-0000-000000000000
ProductName : Windows Server 2012 R2 Standard Evaluation
RoleGuid    : 10a9226f-50ee-49d8-a393-9a501d47ce04
RoleName    : File Server
PSComputerName :

AccessCount : 5
AccessDate  : 17.08.2023
IPAddress   : fe80::d5abcc9eb:ab92:c13
UserName    : winserver2012r2\Administrator
TenantIdentifier : 00000000-0000-0000-0000-000000000000
ProductName : Windows Server 2012 R2 Standard Evaluation
RoleGuid    : 10a9226f-50ee-49d8-a393-9a501d47ce04
RoleName    : File Server
PSComputerName :

```

Abbildung 22: Windows Server 2012 R2 - Get-UalDailyAccess

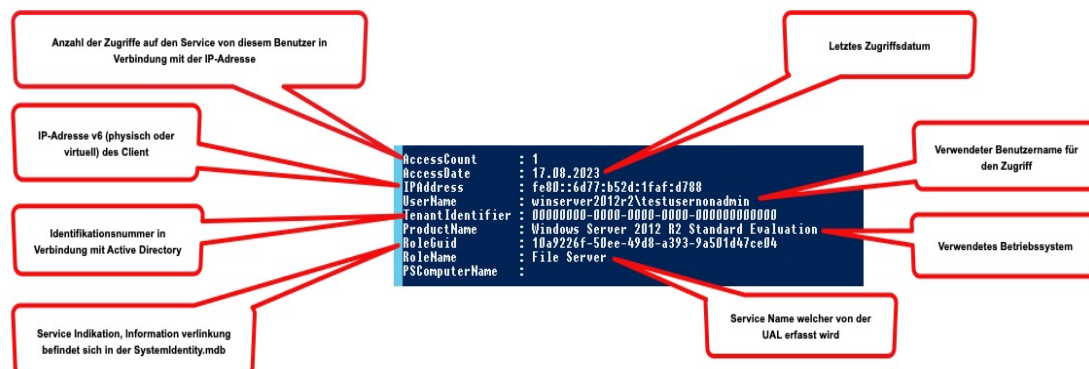


Abbildung 23: Kopie von Abb. 17 - Beispiel Informationsaufschlüsselung

Microsoft bietet keine weiteren für die vorliegende Untersuchung relevanten *PowerShell Cmdlets* an. Damit ist die Live-Untersuchung abgeschlossen und die von der UAL erfassten Daten wurden erfolgreich abgerufen.

4.4.3 Post-mortem-Untersuchung Windows Server 2019

Für eine Post-mortem-Untersuchung ist es erforderlich, Kopien sogenannte Abbilder der aktiven UAL-Datenbank(en) zu erstellen. Diese werden mittels *RawCopy* erstellt, *RawCopy* befindet sich bereits auf den Windows Server-Betriebssystem unter *C:\Windows\RawCopy*, wie im *Kapitel 7.1 – Testumgebung* bereits beschrieben.

Zum aktuellen Zeitpunkt der Untersuchung sind folgende UAL-Datenbank(en) unter *C:\Windows\System32\LogFiles\Sum* verfügbar welche mittels *RawCopy* kopiert werden müssen:

Datenbanken:

- Current.mdb
- {483D7CC6-AB32-4004-A9DB-22F08A1B3540}.mdb
- SystemIdentity.mdb

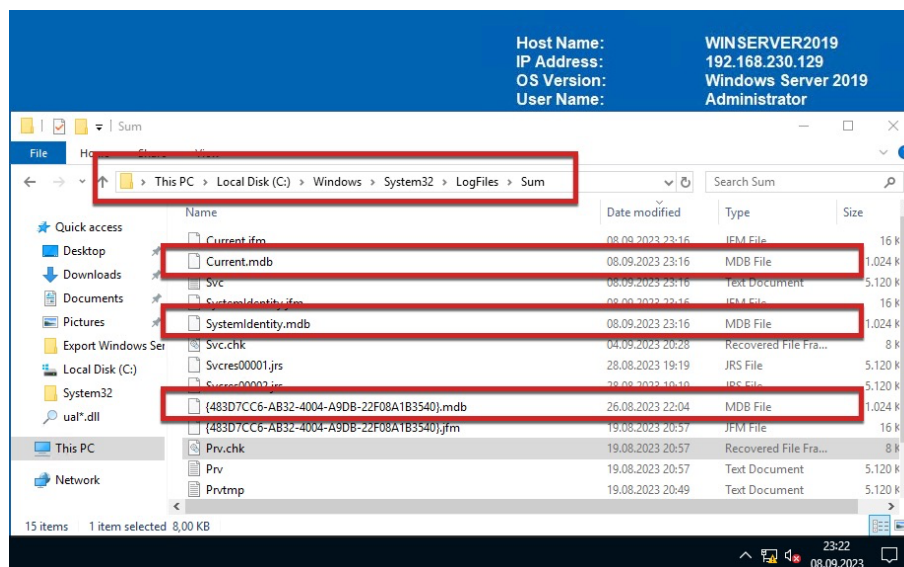


Abbildung 24: Windows Server 2019 - UAL-Datenbanken

RawCopy wird ausschließlich über die Befehlszeile (*Command Prompt (cmd)*) gestartet und gesteuert. Um eine Kopie der Datenbanken zu erstellen, werden die folgenden Befehle eingesetzt:

Current.mdb

*RawCopy.exe /FileNamePath:C:\Windows\System32\LogFiles\Sum\Current.mdb
/OutputPath:C:\RawCopyOutput\OutputName:Current_windowsserver2019.mdb*

{483D7CC6-AB32-4004-A9DB-22F08A1B3540}.mdb

RawCopy.exe /FileNamePath:C:\Windows\System32\LogFiles\Sum\{483D7CC6-AB32-4004-A9DB-22F08A1B3540}.mdb /OutputPath:C:\RawCopyOutput\ /OutputName:{483D7CC6-AB32-4004-A9DB-22F08A1B3540}_windowsserver2019.mdb

SystemIdentity.mdb

*RawCopy.exe /FileNamePath:C:\Windows\System32\LogFiles\Sum\SystemIdentity.mdb
/OutputPath:C:\RawCopyOutput\ /OutputName:SystemIdentity_windowsserver2019.mdb*

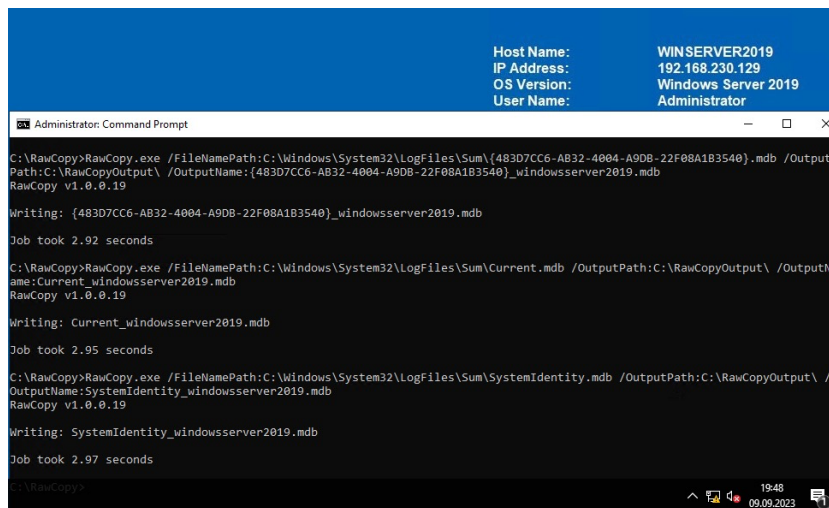


Abbildung 25: Windows Server 2019 - RawCopy

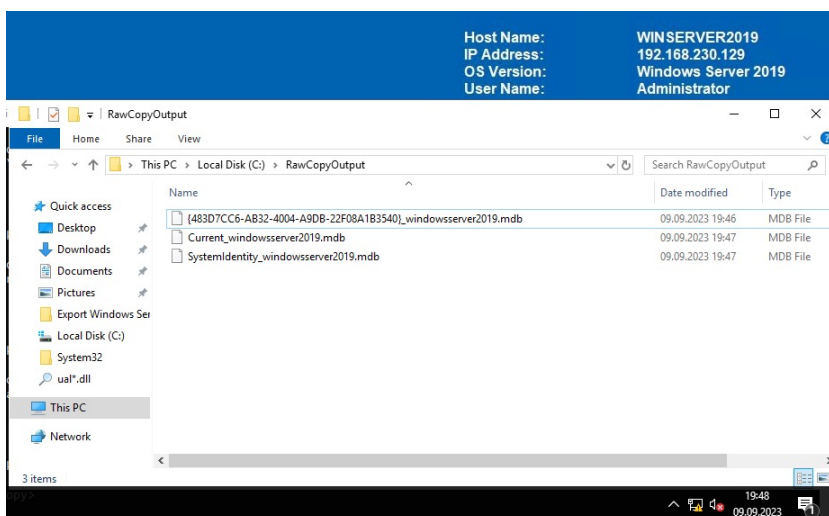


Abbildung 26: Windows Server 2019 - RawCopy Output

Nachdem die Datenbankkopien erfolgreich erstellt wurden, werden diese zur weiteren Untersuchung auf den Windows 10 Client (Instanz 4) übertragen:

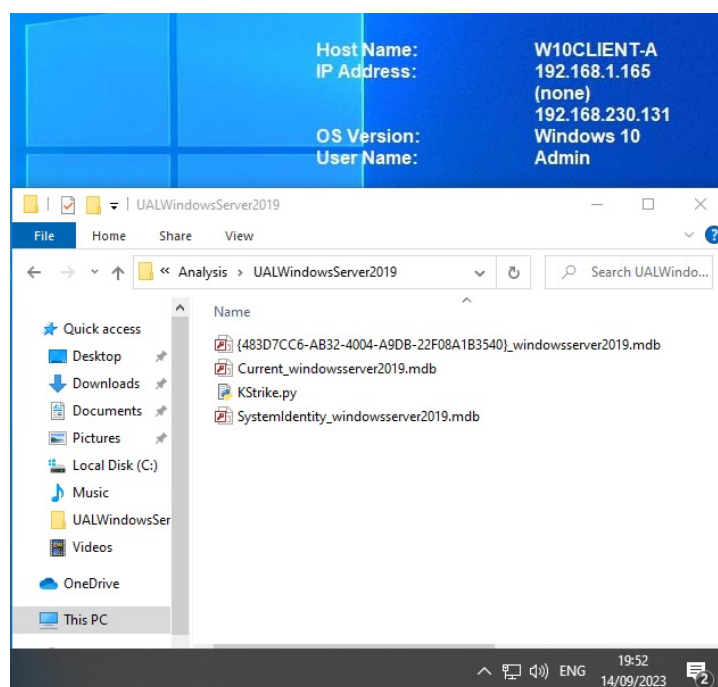


Abbildung 27: Windows 10 Client - UAL-Datenbanken Windows Server 2019

KStrike kann über die Befehlszeile (*Command Prompt (cmd)*) gestartet und gesteuert werden. Um *KStrike* zu starten wird *KStrike.py* aufgerufen:

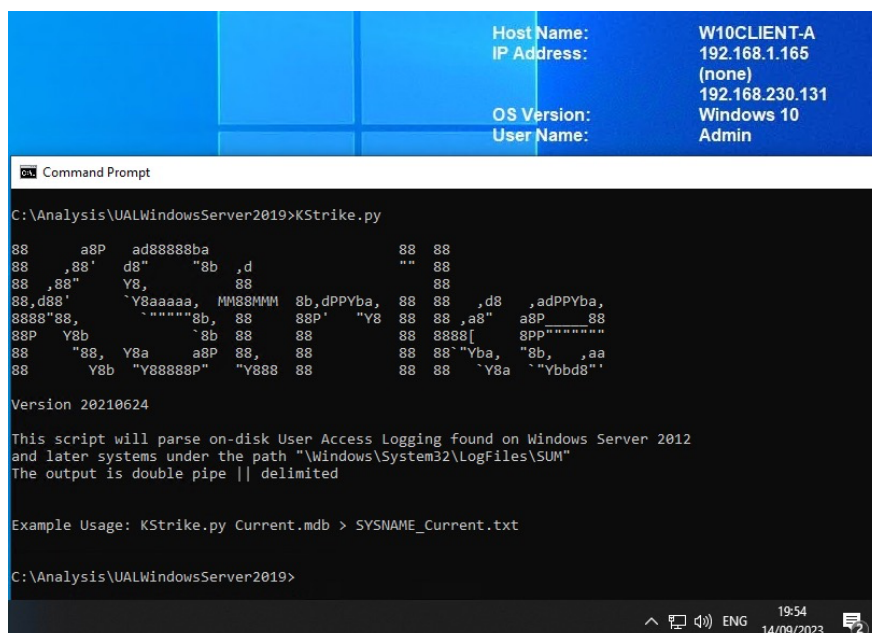
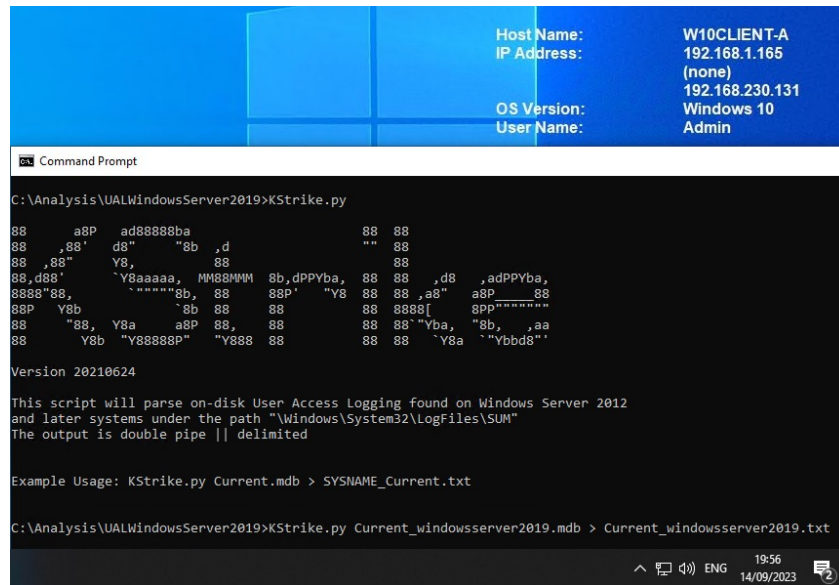


Abbildung 28: Windows 10 Client - KStrike

Um *KStrike* das Einlesen der Datenbankkopien zu ermöglichen, wird folgenden Befehle eingesetzt:

Current.mdb

Kstrike.py Current_windowsserver2019.mdb > Current_windowsserver2019.txt



```

Host Name: W10CLIENT-A
IP Address: 192.168.1.165
(none)
192.168.230.131
OS Version: Windows 10
User Name: Admin

C:\Analysis\UALWindowsServer2019>KStrike.py

88      a8P      ad88888ba      88      88
88      ,88'      d8"      "8b      ,d      ""      88
88      ,88"      Y8,      88      88      88
88      d88      `Y8aaaaa, MM88MMM      8b,dPPYba,      88      88      ,d8      ,adPPYba,
88888`88,      "-----8b,      88      88P'      "Y8      88      88      ,a8"      a8P      88
88P      Y8b      8b      88      88      88      8888[      8pp-----88
88      "88,      Y8a      a8P      88,      88      88      "Yba,      "8b,      ,aa
88      Y8b      "Y88888P"      "Y888      88      88      Y8a      "Yb88"

Version 20210624

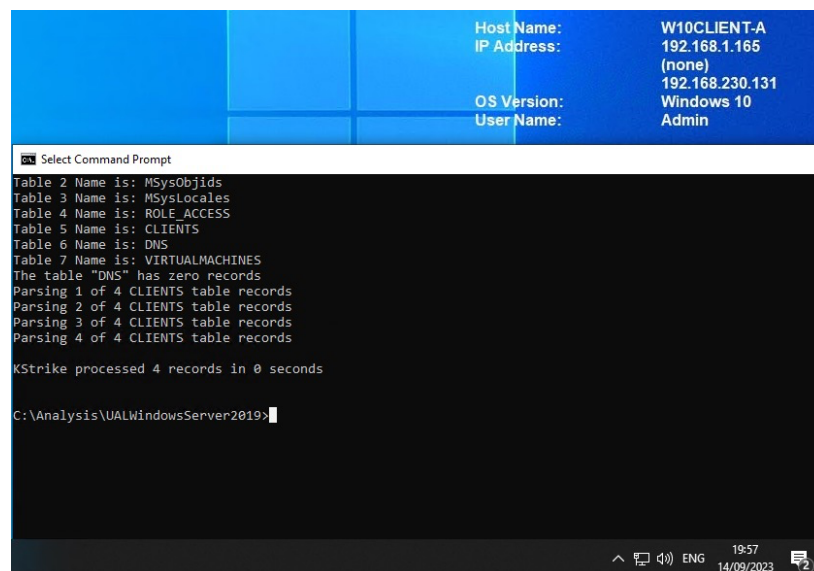
This script will parse on-disk User Access Logging found on Windows Server 2012
and later systems under the path "\\Windows\\System32\\LogFiles\\SUM"
The output is double pipe || delimited

Example Usage: KStrike.py Current.mdb > SYSNAME_Current.txt

C:\Analysis\UALWindowsServer2019>KStrike.py Current_windowsserver2019.mdb > Current_windowsserver2019.txt
  
```

Abbildung 29: Kstrike.py Current_windowsserver2019.mdb

KStrike liefert Informationen darüber, wie viele Einträge in der Datenbank verarbeitet und extrahiert wurden. Die abgerufenen Daten sind im *Current_windowsserver2019.txt* Text Dokument gespeichert worden.



```

Host Name: W10CLIENT-A
IP Address: 192.168.1.165
(none)
192.168.230.131
OS Version: Windows 10
User Name: Admin

Select Command Prompt

Table 2 Name is: MSysObjids
Table 3 Name is: MSysLocales
Table 4 Name is: ROLE_ACCESS
Table 5 Name is: CLIENTS
Table 6 Name is: DNS
Table 7 Name is: VIRTUALMACHINES
The table "DNS" has zero records
Parsing 1 of 4 CLIENTS table records
Parsing 2 of 4 CLIENTS table records
Parsing 3 of 4 CLIENTS table records
Parsing 4 of 4 CLIENTS table records

KStrike processed 4 records in 0 seconds

C:\Analysis\UALWindowsServer2019>
  
```

Abbildung 30: Kstrike.py Current_windowsserver2019.mdb, Verarbeitung

{483D7CC6-AB32-4004-A9DB-22F08A1B3540}.mdb

KStrike.py {483D7CC6-AB32-4004-A9DB-22F08A1B3540}_windowsserver2019.mdb >
{483D7CC6-AB32-4004-A9DB-22F08A1B3540}_windowsserver2019.txt

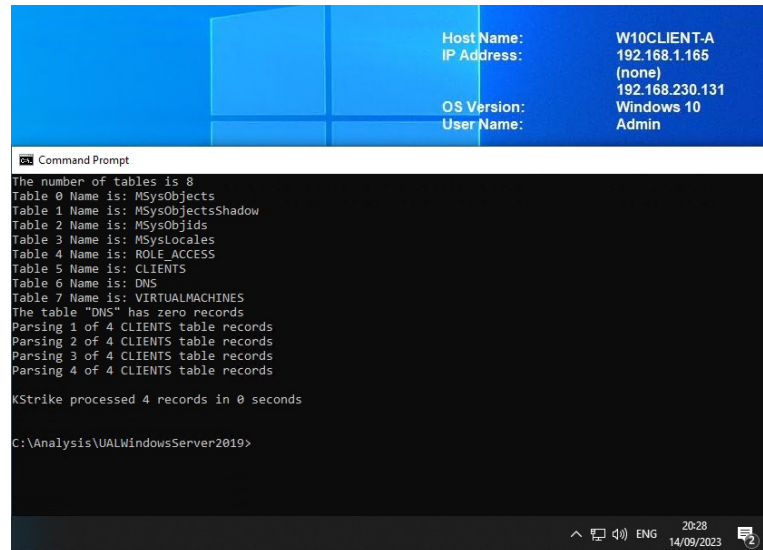


Abbildung 31: KStrike.py {483D7CC6-AB32-4004-A9DB-22F08A1B3540}_windowsserver2019.mdb

KStrike liefert Informationen darüber, wie viele Einträge in der Datenbank verarbeitet und extrahiert wurden. Die abgerufenen Daten sind im {483D7CC6-AB32-4004-A9DB-22F08A1B3540}_windowsserver2019.txt Text Dokument gespeichert worden.

SystemIdentity.mdb

Kstrike.py SystemIdentity_windowsserver2019.mdb > SystemIdentity_windowsserver2019.txt

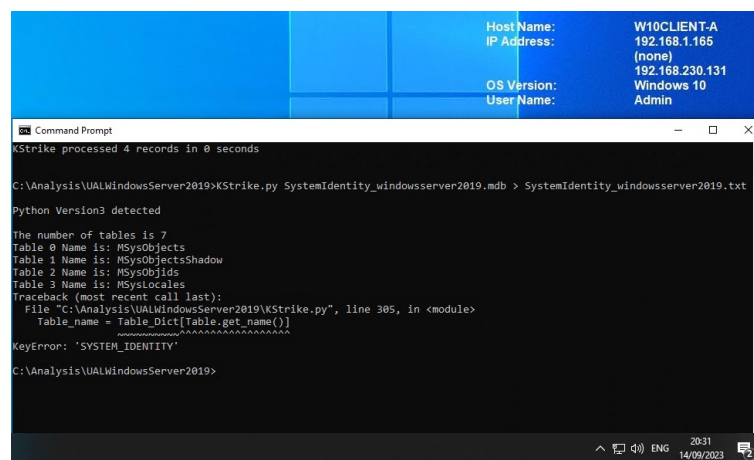


Abbildung 32: Kstrike.py SystemIdentity_windowsserver2019.mdb

SystemIdentity_windowsserver2019.mdb konnte nicht ausgelesen werden, der Grund hierfür ist unbekannt und liegt im Quellcode von *KStrike*. Die *SystemIdentity.mdb* enthält Informationen über Dateien, Verzeichnisse, Rollen, Dienste, GUIDs und andere Ressourcen des Servers, wie im *Kapitel 6.3.5 – Technische Grundlage Windows User Access Logging (UAL)*, beschrieben. Alle für diese Arbeit relevanten Informationen sollten sich in der *Current.mdb* sowie in der *{GUID}.mdb* befinden.

Die extrahierten Informationen wurden in den folgenden Text Dokumenten erfolgreich gespeichert:

- *Current_windowsserver2019.txt*
- *{483D7CC6-AB32-4004-A9DB-22F08A1B3540}_windowsserver2019.txt*

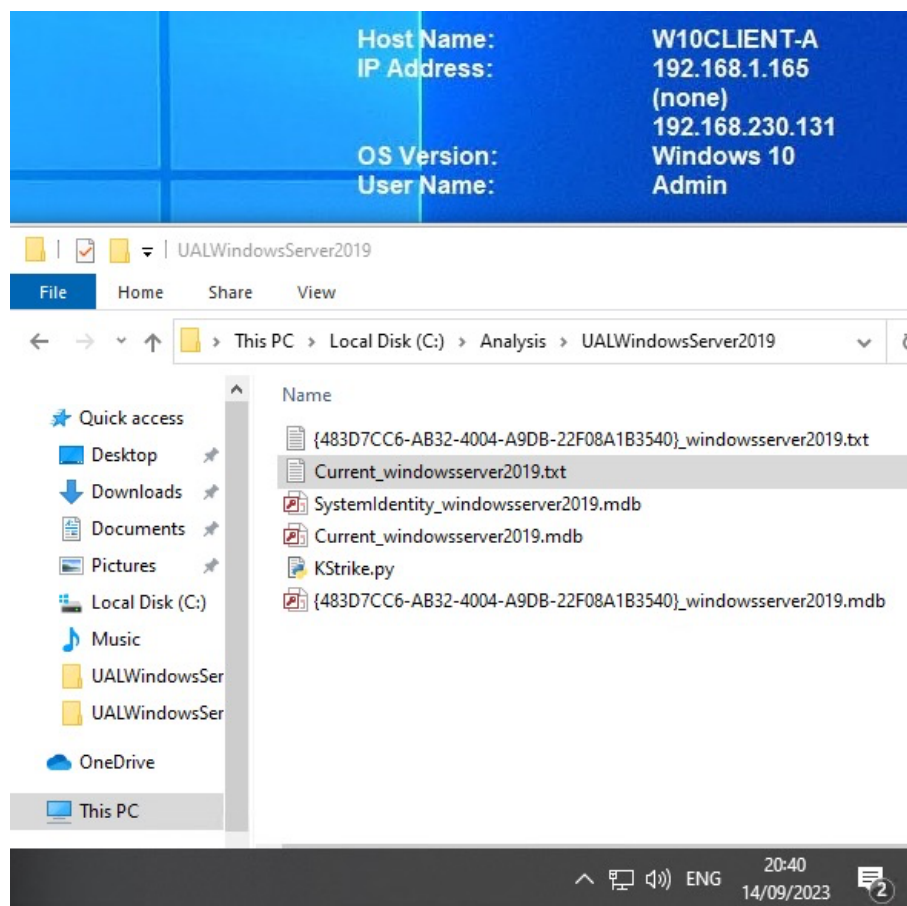


Abbildung 33: Speicherung *windowsserver2019.txt

Um den Inhalt der Text Dokumente benutzerfreundlicher darzustellen, wird das Text Dokument in *Microsoft Excel* importiert. Dies wird am Beispiel von *Current_windowsserver2019.txt* veranschaulicht.

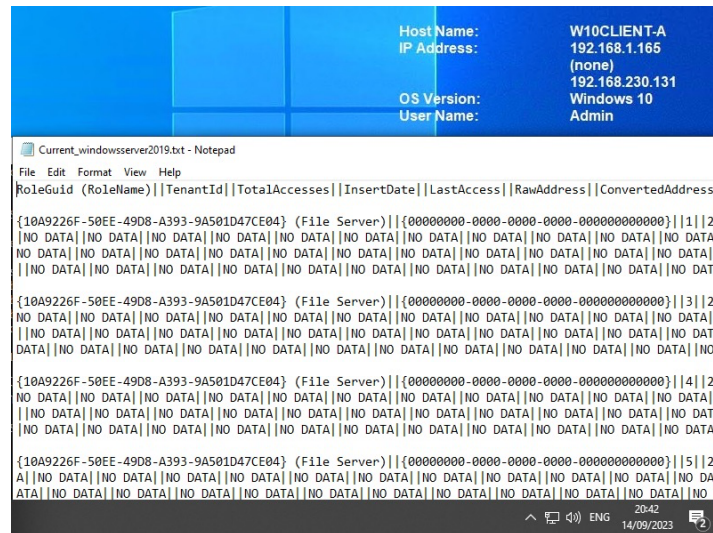


Abbildung 34: Current_windowsserver2019.txt

Die Importierung in Excel erfolgt über Data → From Text → Current_windowsserver2019.txt.

Mit folgenden Optionen: Delimited, File origin: 1251 : Cyrillic (Windows), Delimiters Other: |

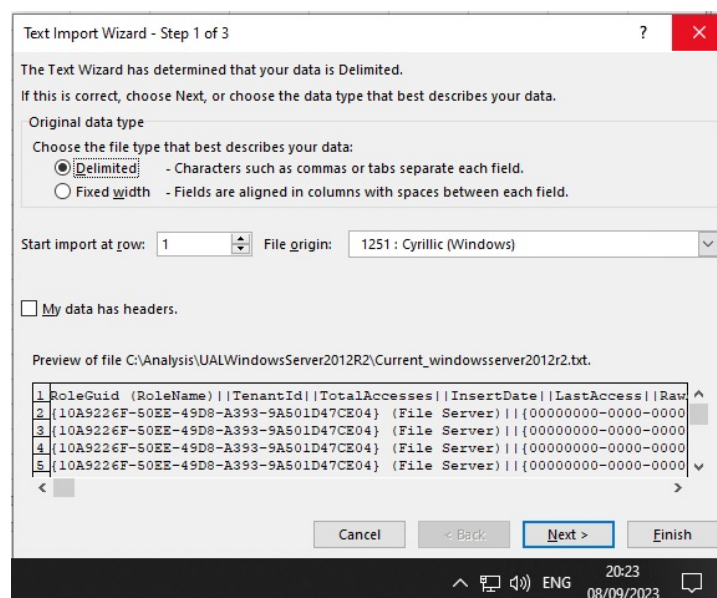


Abbildung 35: Text Import Wizard, Screenshot 1

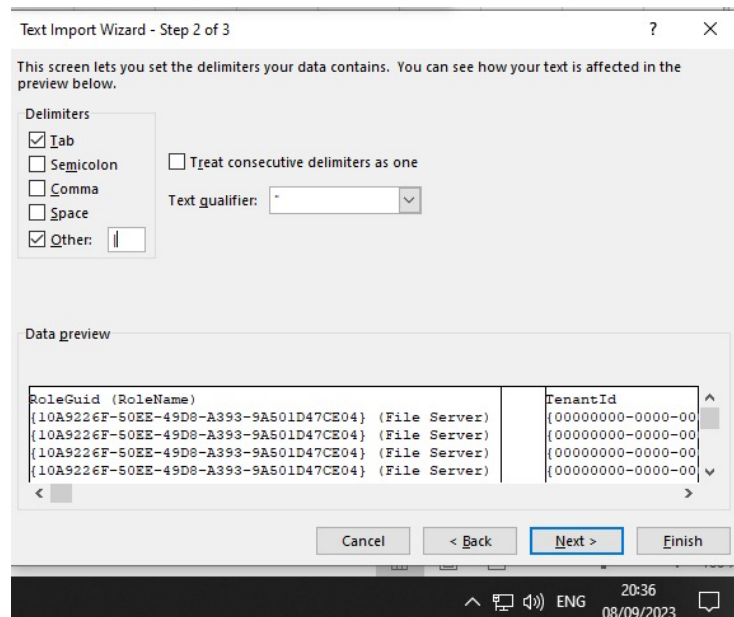


Abbildung 36: Text Import Wizard, Screenshot 2

Dies ermöglicht eine benutzerfreundlichere Darstellung der Ergebnisse:

RoleGuid (RoleName)	TenantId	TotalAccesses	InsertDate	LastAccess	ConvertedAddress (Correlated_HostName(s))	AuthenticatedUserName
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0000-0000-0000-000000000000}	1	2023-07-20 10:37:26.656626	2023-07-20 10:37:26.656626	Local Host ::1	winserver2019\administrator
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0000-0000-0000-000000000000}	3	2023-08-10 20:38:59.477108	2023-08-17 20:05:48.726180	fe80:0000:0000:0000:4bbd:a05d:fdb8:c3be IPv6 MAC: 49:BD:A0:88:C3:BE	winserver2019\administrator
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0000-0000-0000-000000000000}	4	2023-08-17 17:15:54.237136	2023-08-17 20:24:30.023822	fe80:0000:0000:0000:6d77:b52d:1faf:d788 IPv6 MAC: 6F:77:B5:AF:D7:88	winserver2019\testuseradmin
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0000-0000-0000-000000000000}	5	2023-08-17 19:55:16.974098	2023-08-17 20:22:06.633066	fe80:0000:0000:0000:6d77:b52d:1faf:d788 IPv6 MAC: 6F:77:B5:AF:D7:88	winserver2019\testusermonadmin

Abbildung 37: Current_windowsserver2019_txt_.xlsx

Inhalt - Current_windowsserver2019_txt_.xlsx:

RoleGuid (RoleName)	Tenant Id	Total Accesses	Insert Date	Last Access	Converted Address (Correlated _HostName(s)	Authenticated UserName
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0-0000-0000-0000-00000000}	1	2023-07-20 10:37:26.656626	2023-07-20 10:37:26.656626	Local Host ::1	winserver2019\administrator
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0-0000-0000-0000-00000000}	3	2023-08-10 20:38:59.477108	2023-08-17 20:05:48.726180	fe80:0000:0000:0000:4bbd:a05d:fd8b:c3be IPv6 MAC: 49:BD:A0:8B:C3:BE	winserver2019\administrator
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0-0000-0000-0000-00000000}	4	2023-08-17 17:15:54.237136	2023-08-17 20:24:30.023822	fe80:0000:0000:0000:6d77:b52d:1faf:d788 IPv6 MAC: 6F:77:B5:AF:D7:88	winserver2019\testuseradmin
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0-0000-0000-0000-00000000}	5	2023-08-17 19:55:16.974098	2023-08-17 20:22:06.633066	fe80:0000:0000:0000:6d77:b52d:1faf:d788 IPv6 MAC: 6F:77:B5:AF:D7:88	winserver2019\testusernonadmin

Tabelle 14: Current_windowsserver2019_txt_.xlsx

Die bereits genannte Vorgehensweise wurde bei {483D7CC6-AB32-4004-A9DB-22F08A1B3540}_windowsserver2019.txt ebenfalls angewendet:

RoleGuid (RoleName)	TenantId	TotalAccesses	InsertDate	LastAccess	ConvertedAddress (Correlated_HostName(s))	AuthenticatedUserName
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0000-0000-0000-000000000000}	1	2023-07-20 10:37:26.656626	2023-07-20 10:37:26.656626	Local Host ::1	winserver2019\administrator
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0000-0000-0000-000000000000}	3	2023-08-10 20:38:59.477108	2023-08-17 20:05:48.726180	fe80:0000:0000:0000:4bda05d:fd8b:c3be IPv6 MAC: 49:BD:A0:8B:C3:BE	winserver2019\administrator
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0000-0000-0000-000000000000}	4	2023-08-17 17:15:54.237136	2023-08-17 20:24:30.023822	fe80:0000:0000:0000:6d77:b52d:1faf:d788 IPv6 MAC: 6F:77:B5:AF:D7:88	winserver2019\testuseradmin
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0000-0000-0000-000000000000}	5	2023-08-17 19:55:16.974098	2023-08-17 20:22:06.433066	fe80:0000:0000:0000:6d77:b52d:1faf:d788 IPv6 MAC: 6F:77:B5:AF:D7:88	winserver2019\testusermonadmin

Abbildung 38: {483D7CC6-AB32-4004-A9DB-22F08A1B3540}_windowsserver2019

Inhalt - {483D7CC6-AB32-4004-A9DB-22F08A1B3540}_windowsserver2019
txt.xlsx:

RoleGuid (RoleName)	TenantId	Total Accesses	InsertDate	Last Access	ConvertedAddress (Correlated_HostName(s))	Authenticated UserName
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0000-0000-0000-000000000000}	1	2023-07-20 10:37:26.656626	2023-07-20 10:37:26.656626	Local Host ::1	winserver2019\administrator
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0000-0000-0000-000000000000}	3	2023-08-10 20:38:59.477108	2023-08-17 20:05:48.726180	fe80:0000:0000:0000:4bda05d:fd8b:c3be IPv6 MAC: 49:BD:A0:8B:C3:BE	winserver2019\administrator
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0000-0000-0000-000000000000}	4	2023-08-17 17:15:54.237136	2023-08-17 20:24:30.023822	fe80:0000:0000:0000:6d77:b52d:1faf:d788 IPv6 MAC: 6F:77:B5:AF:D7:88	winserver2019\testuseradmin

04} (File Server)	000000000 000}		4.2371 36		6F:77:B5:AF :D7:88	
-------------------	-------------------	--	--------------	--	-----------------------	--

Tabelle 15: {483D7CC6-AB32-4004-A9DB-22F08A1B3540}_windowsserver2019

Die Post-mortem-Untersuchung ist hiermit abgeschlossen und die von der UAL erfassten Informationen wurden erfolgreich ausgelesen.

4.4.4 Post-mortem-Untersuchung Windows Server 2012 R2

Für eine Post-mortem-Untersuchung ist es erforderlich, Kopien sogenannte Abbilder der aktiven UAL-Datenbank(en) zu erstellen. Diese werden mittels *RawCopy* erstellt, *RawCopy* befindet sich bereits auf den Windows Server-Betriebssystem unter *C:\Windows\RawCopy*, wie im *Kapitel 7.1 – Testumgebung* bereits beschrieben.

Zum aktuellen Zeitpunkt der Untersuchung sind folgende UAL-Datenbank(en) unter *C:\Windows\System32\LogFiles\Sum* verfügbar welche mittels *RawCopy* kopiert werden müssen:

Datenbanken:

- Current.mdb
- {0FE16C77-877A-4B7B-AFA1-24B2340644CB}.mdb
- SystemIdentity.mdb

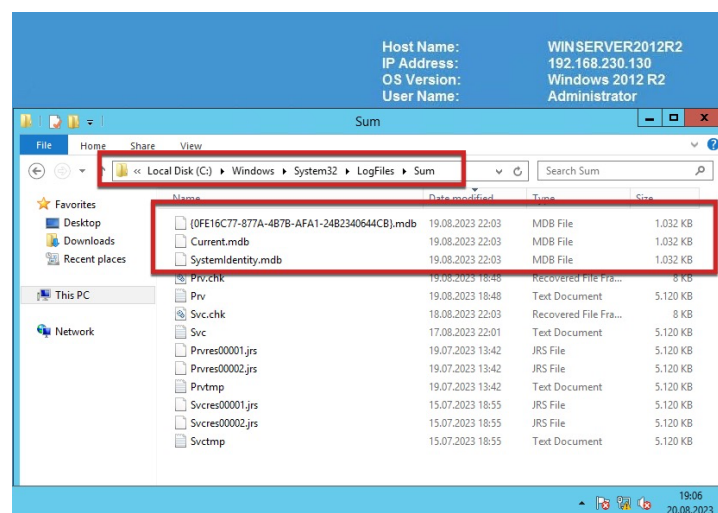


Abbildung 39: Windows Server 2012 R2 - UAL-Datenbanken

RawCopy wird ausschließlich über die Befehlszeile (*Command Prompt (cmd)*) gestartet und gesteuert. Um eine Kopie der Datenbanken zu erstellen, werden die folgenden Befehle eingesetzt:

Current.mdb

```
RawCopy.exe /FileNamePath:C:\Windows\System32\LogFiles\Sum\Current.mdb
/OutputPath:C:\RawCopyOutput\OutputName:Current_windowsserver2012r2.mdb
```

{0FE16C77-877A-4B7B-AFA1-24B2340644CB}.mdb

```
RawCopy.exe /FileNamePath:C:\Windows\System32\LogFiles\Sum\{0FE16C77-877A-4B7B-
AFA1-24B2340644CB}.mdb /OutputPath:C:\RawCopyOutput\ /OutputName:{40FE16C77-877A-
4B7B-AFA1-24B2340644CB}_windowsserver2012r2.mdb
```

SystemIdentity.mdb

```
RawCopy.exe /FileNamePath:C:\Windows\System32\LogFiles\Sum\SystemIdentity.mdb
/OutputPath:C:\RawCopyOutput\ /OutputName:SystemIdentity_windowsserver2012r2.mdb
```

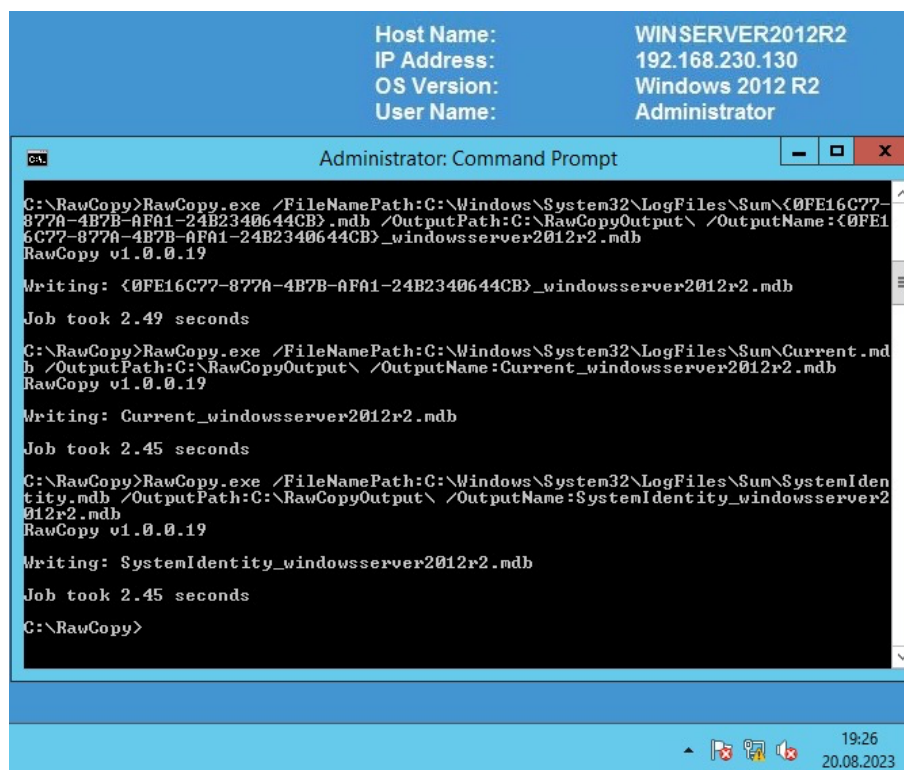


Abbildung 40: Windows Server 2012 R2 – RawCopy

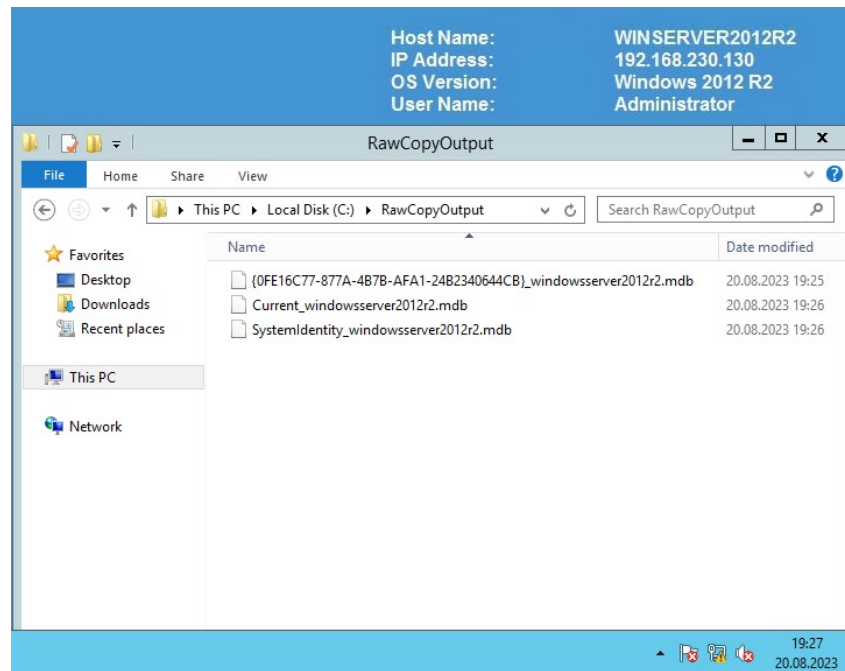


Abbildung 41: Windows Server 2012 R2 - RawCopy Output

Nachdem die Datenbankkopien erfolgreich erstellt wurden, werden diese zur weiteren Untersuchung auf den Windows 10 Client (Instanz 4) übertragen:

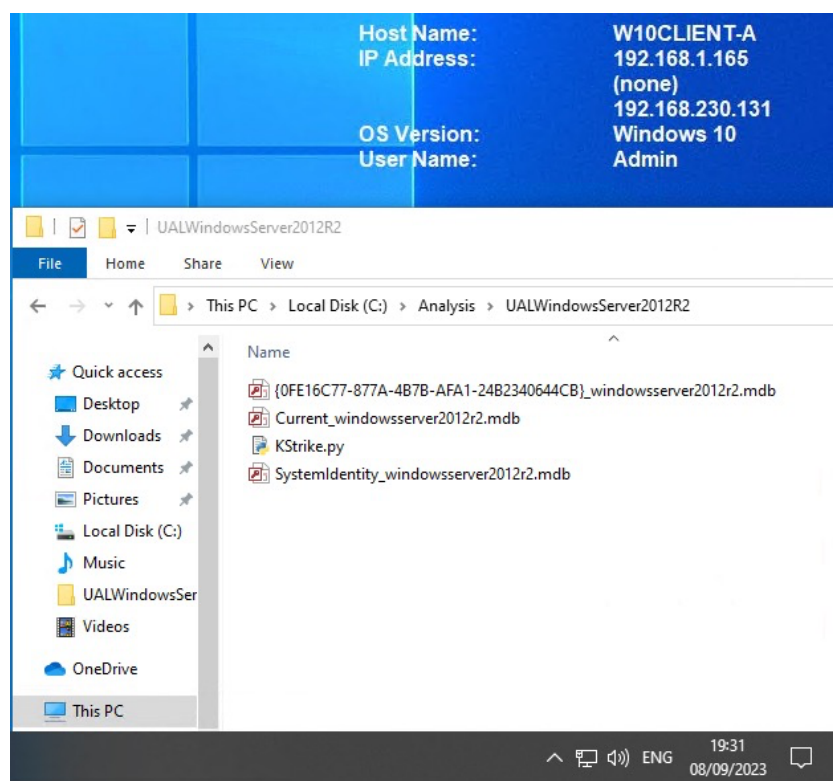


Abbildung 42: Windows 10 Client - UAL-Datenbanken Windows Server 2012 R2

KStrike kann über die Befehlszeile (*Command Prompt (cmd)*) gestartet und gesteuert werden. Um *KStrike* zu starten wird *KStrike.py* aufgerufen:

```

Host Name:      W10CLIENT-A
IP Address:     192.168.1.165
                (none)
                192.168.230.131
OS Version:    Windows 10
User Name:     Admin

Administrator: Command Prompt

C:\Analysis\UALWindowsServer2012R2>KStrike.py

88      a8P      ad88888ba      88      88
88      ,88"      d8"      "8b      ,d      88
88      ,88"      Y8,      88      88
88      d88"      `Y8aaaaa, MM88MMM      8b,dPPYba,      88      88      ,d8      ,adPPYba,
8888"88,      `*****8b,      88      88P"      "Y8      88      88      ,a8"      a8P      88
88P      Y8b      `8b      88      88      88      8888[      8pP      "*****
88      "88,      Y8a      a8P      88,      88      88      "Yba,      "8b,      ,aa
88      Y8b      "Y88888P"      "Y888      88      88      `Y8a      `~"Yb8d8"

Version 20210624

This script will parse on-disk User Access Logging found on Windows Server 2012
and later systems under the path "\Windows\System32\LogFiles\SUM"
The output is double pipe || delimited

Example Usage: KStrike.py Current.mdb > SYSNAME_Current.txt

C:\Analysis\UALWindowsServer2012R2>_

```

Abbildung 43: Windows 10 Client - KStrike

Um *KStrike* das Einlesen der Datenbankkopien zu ermöglichen, wird folgenden Befehle eingesetzt:

Current.mdb

Kstrike.py Current_windowsserver2012r2.mdb > Current_windowsserver2012r2.txt

```

Host Name:      W10CLIENT-A
IP Address:     192.168.1.165
                (none)
                192.168.230.131
OS Version:    Windows 10
User Name:     Admin

Administrator: Command Prompt

C:\Analysis\UALWindowsServer2012R2>KStrike.py

88      a8P      ad88888ba      88      88
88      ,88"      d8"      "8b      ,d      88
88      ,88"      Y8,      88      88
88      d88"      `Y8aaaaa, MM88MMM      8b,dPPYba,      88      88      ,d8      ,adPPYba,
8888"88,      `*****8b,      88      88P"      "Y8      88      88      ,a8"      a8P      88
88P      Y8b      `8b      88      88      88      8888[      8pP      "*****
88      "88,      Y8a      a8P      88,      88      88      "Yba,      "8b,      ,aa
88      Y8b      "Y88888P"      "Y888      88      88      `Y8a      `~"Yb8d8"

Version 20210624

This script will parse on-disk User Access Logging found on Windows Server 2012
and later systems under the path "\Windows\System32\LogFiles\SUM"
The output is double pipe || delimited

Example Usage: KStrike.py Current.mdb > SYSNAME_Current.txt

C:\Analysis\UALWindowsServer2012R2>KStrike.py Current_windowsserver2012r2.mdb > Current_windowsserver2012r2.txt

```

Abbildung 44: Kstrike.py Current_windowsserver2012r2.mdb

KStrike liefert Informationen darüber, wie viele Einträge in der Datenbank verarbeitet und extrahiert wurden. Die abgerufenen Daten sind im *Current_windowsserver2019.txt* Text Dokument gespeichert worden.

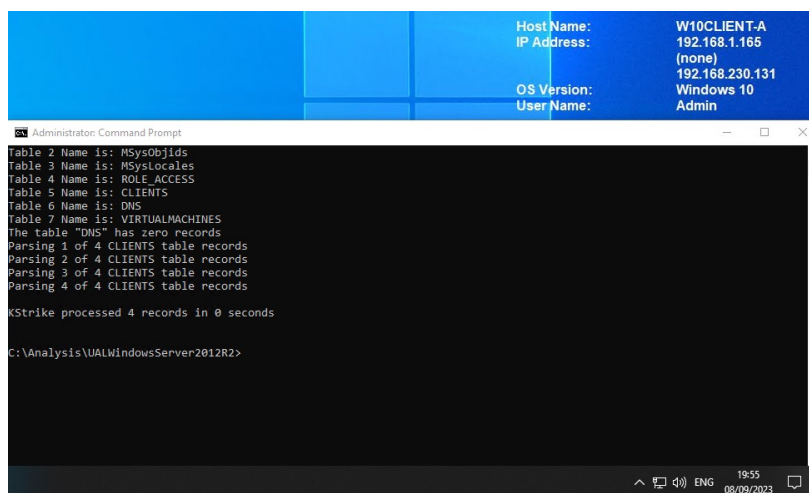


Abbildung 45: Kstrike.py Current_windowsserver2012r2.mdb, Verarbeitung

{0FE16C77-877A-4B7B-AFA1-24B2340644CB}.mdb

KStrike.py {0FE16C77-877A-4B7B-AFA1-24B2340644CB}_windowsserver2012r2.mdb >
 {0FE16C77-877A-4B7B-AFA1-24B2340644CB}_windowsserver2012r2.txt

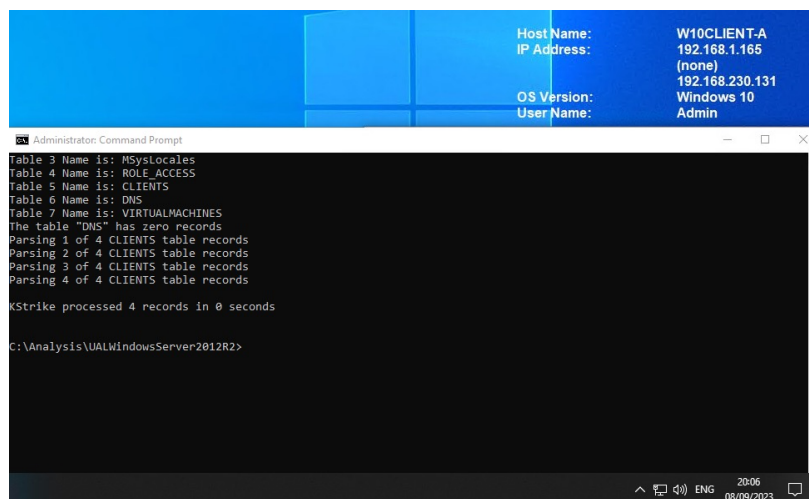


Abbildung 46: KStrike.py {0FE16C77-877A-4B7B-AFA1-24B2340644CB}_windowsserver2012r2.mdb

KStrike liefert Informationen darüber, wie viele Einträge in der Datenbank verarbeitet und extrahiert wurden. Die abgerufenen Daten sind im *{0FE16C77-877A-4B7B-AFA1-24B2340644CB}_windowsserver2012r2.txt* Text Dokument gespeichert worden.

SystemIdentity.mdb

Kstrike.py SystemIdentity_windowsserver2012r2.mdb > SystemIdentity_windowsserver2012r2.txt

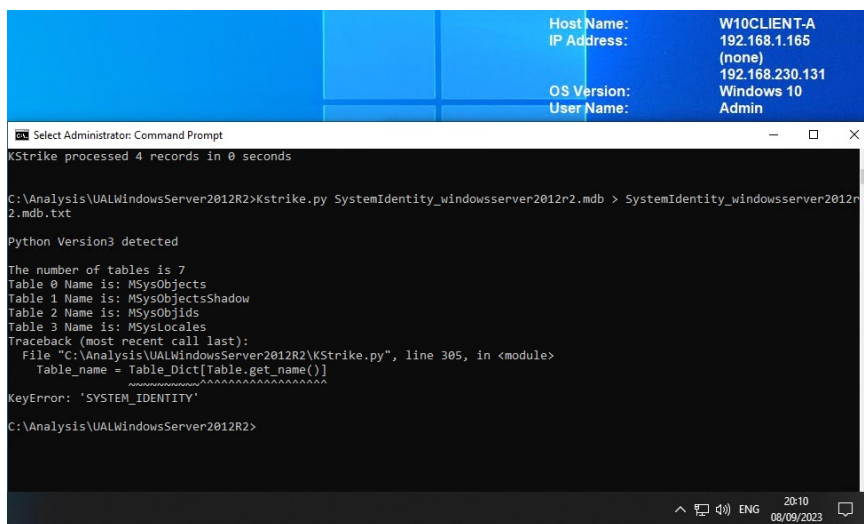


Abbildung 47: KStrike.py SystemIdentity_windowsserver2012r2.mdb

SystemIdentity_windowsserver2012r2.mdb konnte nicht ausgelesen werden, der Grund hierfür ist unbekannt und liegt im Quellcode von *KStrike*. Die *SystemIdentity.mdb* enthält Informationen über Dateien, Verzeichnisse, Rollen, Dienste, GUIDs und andere Ressourcen des Servers, wie im *Kapitel 6.3.5 – Technische Grundlage Windows User Access Loggin (UAL)*, beschrieben. Alle für diese Arbeit relevanten Informationen sollten sich in der *Current.mdb* sowie in der *{GUID}.mdb* befinden.

Die extrahierten Informationen wurden in den folgenden Text Dokumenten erfolgreich gespeichert:

- *Current_windowsserver2012r2.txt*
- *{0FE16C77-877A-4B7B-AFA1-24B2340644CB}_windowsserver2012r2.txt*

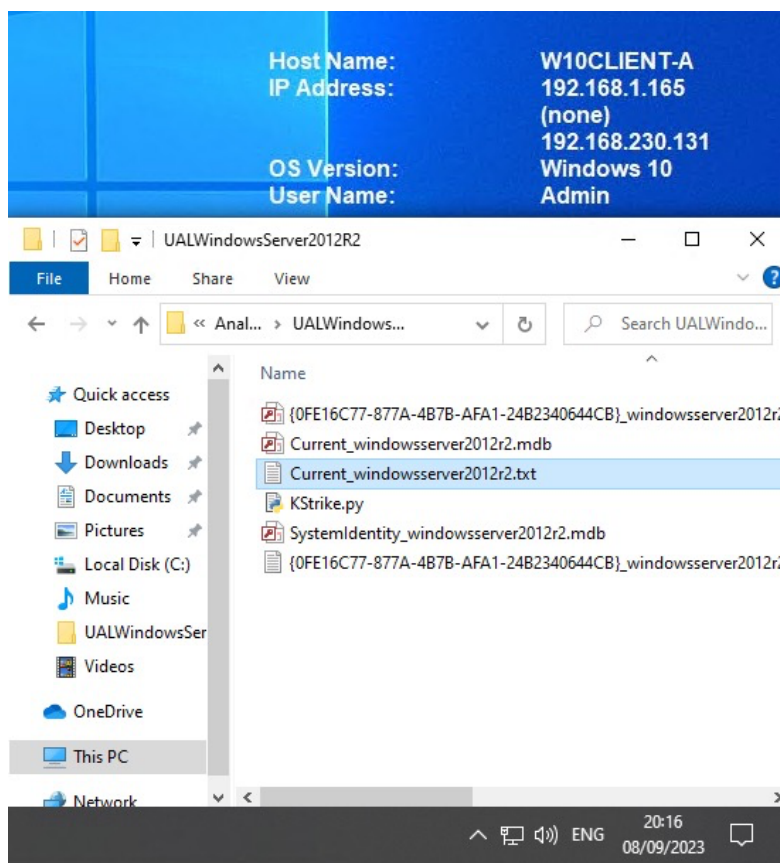


Abbildung 48: Speicherung *windowsserver2012r2.txt

Um den Inhalt der Text Dokumente benutzerfreundlicher darzustellen, wird das Text Dokument in *Microsoft Excel* importiert. Dies wird am Beispiel von *Current_windowsserver2012r2.txt* veranschaulicht.

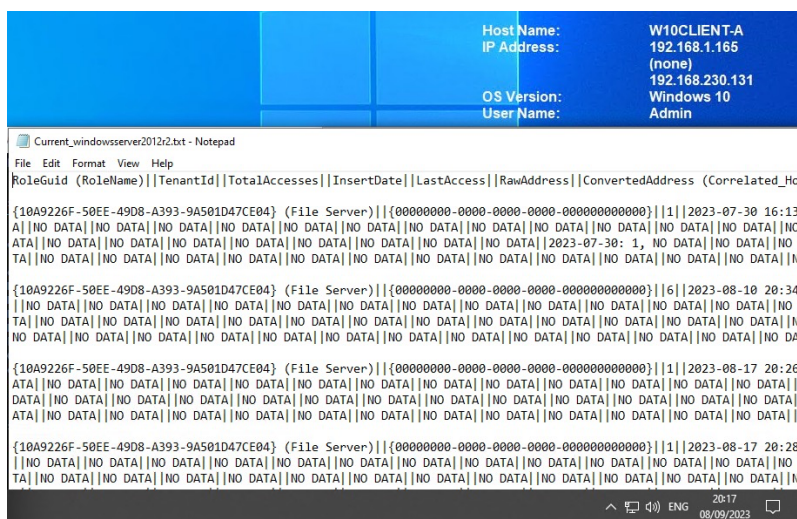


Abbildung 49: Current_windowsserver2012r2.txt

Die Importierung in Excel erfolgt über Data → From Text → Current_windowsserver2012r2.txt.

Mit folgenden Optionen: Delimited, File origin: 1251 : Cyrillic (Windows), Delimiters Other: |

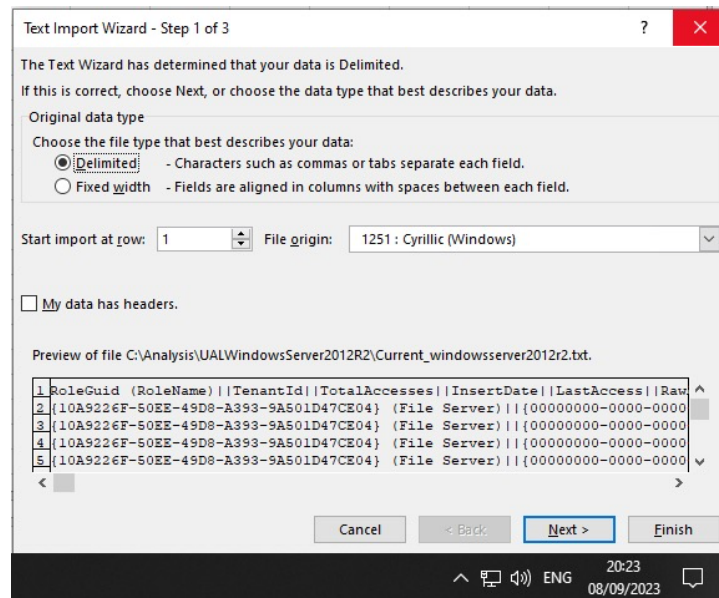


Abbildung 50: Text Import Wizard, Screenshot 1

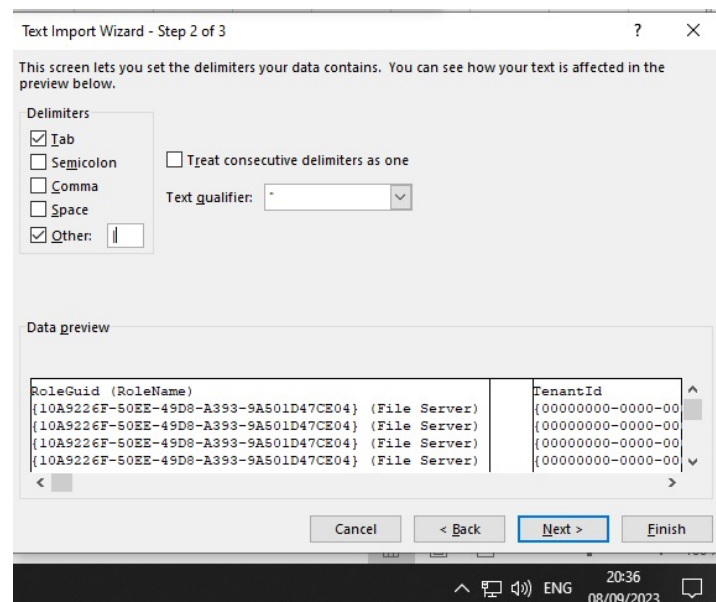


Abbildung 51: Text Import Wizard, Screenshot 2

Dies ermöglicht eine benutzerfreundlichere Darstellung der Ergebnisse:

RoleGuid (RoleName)	TenantId	TotalAccesses	InsertDate	LastAccess	ConvertedAddress (Correlated_HostName(s))	AuthenticatedUserName
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0000-0000-0000-000000000000}	1	2023-07-30 16:13:20.107030	2023-07-30 16:13:20.107030	Local Host ::1	winserver2012r2\administrator
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0000-0000-0000-000000000000}	6	2023-08-10 20:34:48.741282	2023-08-17 20:05:21.471334	fe80:0000:0000:0000:d5ab:c9eb:a92:0e13 IPv6 MAC: D7:AB:C9:92:0E;	winserver2012r2\administrator
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0000-0000-0000-000000000000}	1	2023-08-17 20:26:06.489462	2023-08-17 20:26:06.489462	fe80:0000:0000:0000:6d77:b52d:1faf:d788 IPv6 MAC: 6F:77:B5:AF:D7:88	winserver2012r2\testusermonadmin
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0000-0000-0000-000000000000}	1	2023-08-17 20:28:19.474306	2023-08-17 20:28:19.474306	fe80:0000:0000:0000:6d77:b52d:1faf:d788 IPv6 MAC: 6F:77:B5:AF:D7:88	winserver2012r2\testuseradmin

Abbildung 52: Current_windowsserver2012r2_txt_.xlsx

Inhalt - Current_windowsserver2012r2_txt_.xlsx:

RoleGuid (RoleName)	TenantId	Total Access es	Insert Date	Last Access	Converted Address (Correlate d _HostNam e(s))	Authenticated UserName
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0000-0000-0000-000000000000}	1	2023-07-30 16:13:20.107030	2023-07-30 16:13:20.107030	Local Host ::1	winserver2012r2\administrator
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0000-0000-0000-000000000000}	6	2023-08-10 20:34:48.741282	2023-08-17 20:05:21.471334	fe80:0000:0000:0000:d5ab:c9eb:a92:0e13 IPv6 MAC: D7:AB:C9:92:0E;	winserver2012r2\administrator
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0000-0000-0000-000000000000}	1	2023-08-17 20:26:06.489462	2023-08-17 20:26:06.489462	fe80:0000:0000:0000:6d77:b52d:1faf:d788 IPv6 MAC: 6F:77:B5:AF:D7:88	winserver2012r2\testusermonadmin
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0000-0000-0000-000000000000}	1	2023-08-17 20:28:19.474306	2023-08-17 20:28:19.474306	fe80:0000:0000:0000:6d77:b52d:1faf:d788 IPv6 MAC: 6F:77:B5:AF:D7:88	winserver2012r2\testuseradmin

9A501D47C E04} (File Server)	0000- 00000000 0000}		06.489 462		af:d788 IPv6 MAC: 6F:77:B5:A F:D7:88	
{10A9226F- 50EE-49D8- A393- 9A501D47C E04} (File Server)	{00000000 0-0000- 0000- 0000- 0000- 00000000 0000}	1	2023- 08-17 20:28: 19.474 306	2023-08-17 20:28:19.47 4306	fe80:0000:0 000:0000:6 d77:b52d:1f af:d788 IPv6 MAC: 6F:77:B5:A F:D7:88	winserver2012 r2\testuseradm in

Tabelle 16: Current_windowsserver2012r2_txt_.xlsx

Die bereits genannte Vorgehensweise wurde bei {0FE16C77-877A-4B7B-AFA1-24B2340644CB}_windowsserver2012r2.txt ebenfalls angewendet:

RoleGuid (RoleName)	TenantId	TotalAccesses	InsertDate	LastAccess	ConvertedAddress (Correlated_HostName(s))	AuthenticatedUserName
{10A9226F-50EE-49D8-A393-9A501D47CED4} (File Server)	{00000000-0000-0000-0000-000000000000}	1	2023-07-30 16:13:20.107030	2023-07-30 16:13:20.107030	Local Host ::1	winserver2012r2\administrator
{10A9226F-50EE-49D8-A393-9A501D47CED4} (File Server)	{00000000-0000-0000-0000-000000000000}	6	2023-08-10 20:34:48.741282	2023-08-17 20:05:21.471334	fe80:0000:0000:d5ab:c9eb:ab92:0e13 IPv6 MAC: D7-AB-C9-92-0E-13	winserver2012r2\administrator
{10A9226F-50EE-49D8-A393-9A501D47CED4} (File Server)	{00000000-0000-0000-0000-000000000000}	1	2023-08-17 20:26:06.489462	2023-08-17 20:26:06.489462	fe80:0000:0000:0000:6d77:b52d:1faf:d788 IPv6 MAC: 6F-77-B5-AF-D7-88	winserver2012r2\testusernonadmin
{10A9226F-50EE-49D8-A393-9A501D47CED4} (File Server)	{00000000-0000-0000-0000-000000000000}	1	2023-08-17 20:28:19.474306	2023-08-17 20:28:19.474306	fe80:0000:0000:0000:6d77:b52d:1faf:d788 IPv6 MAC: 6F-77-B5-AF-D7-88	winserver2012r2\testuseradmin

Abbildung 53: {0FE16C77-877A-4B7B-AFA1-24B2340644CB}_windowsserver2012

Inhalt - {0FE16C77-877A-4B7B-AFA1-24B2340644CB}_windowsserver2012

r2_txt_.xlsx:

RoleGuid (RoleName)	TenantId	Total Accesses	Insert Date	Last Access	ConvertedAddress (Correlated _HostName(s))	Authenticated UserName
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0000-0000-0000-000000000000}	1	2023-07-30 16:13:20.107030	2023-07-30 16:13:20.107030	Local Host ::1	winserver2012r2\administrator
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0000-0000-0000-000000000000}	6	2023-08-10 20:34:48.741282	2023-08-17 20:05:21.471334	fe80:0000:0000:0000:d5a b:c9eb:ab92:0e13 IPv6 MAC: D7:AB:C9:92:0E:13	winserver2012r2\administrator
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0000-0000-0000-000000000000}	1	2023-08-17 20:26:06.489462	2023-08-17 20:26:06.489462	fe80:0000:0000:0000:6d7 7:b52d:1faf:d788 IPv6 MAC: 6F:77:B5:AF:D7:88	winserver2012r2\testusernonadmin
{10A9226F-50EE-49D8-A393-9A501D47CE04} (File Server)	{00000000-0000-0000-0000-000000000000}	1	2023-08-17 20:28:19.474306	2023-08-17 20:28:19.474306	fe80:0000:0000:0000:6d7 7:b52d:1faf:d788 IPv6 MAC: 6F:77:B5:AF:D7:88	winserver2012r2\testuseradmin

Tabelle 17: {0FE16C77-877A-4B7B-AFA1-24B2340644CB}_windowsserver2012

Die Post-mortem-Untersuchung ist hiermit abgeschlossen und die von der UAL erfassten Informationen wurden erfolgreich ausgelesen.

5 Ergebnisse

5.1 Auswertung und Bewertung

In der nachstehenden Übersicht sind die UAL erfassten Aktivitäten aufgeführt, die im Zuge der Live-Analyse gesammelt wurden.

✓ Erkannt

-- Nicht Erkannt

TestszENARIO TC#	Windows Server 2019 TestUserAdmin	Windows Server 2019 TestUserNonAdmin	Windows Server 2012R2 TestUserAdmin	Windows Server 2012R2 TestUserNonAdmin
TC1	--	--	--	--
TC2	--	--	--	--
TC3	--	--	--	--
TC4	--	--	--	--
TC5	--	--	--	--
TC6	--	--	--	--
TC7	--	--	--	--
TC8	--	--	--	--
TC9	--	--	--	--
TC10	--	--	--	--
TC11	--	--	--	--
TC12	--	--	--	--
TC13	✓	✓		
TC14	--	--		

Testszenario TC#	Windows Server 2019	Windows Server 2019	Windows Server 2012R2	Windows Server 2012R2
	TestUserAdmin	TestUserNonAdmin	TestUserAdmin	TestUserNonAdmin
TC15	--	--		
TC16	--	--		
TC17			✓	✓
TC18			--	--
TC19			--	--
TC20			--	--
TC21			--	--

Tabelle 18: UAL erfassten Aktivitäten – Live-Untersuchung

In der nachstehenden Übersicht sind die UAL erfassten Aktivitäten aufgeführt, die im Zuge der Post-mortem-Untersuchung gesammelt wurden.

✓ Erkannt

-- Nicht Erkannt

Testszenario TC#	Windows Server 2019	Windows Server 2019	Windows Server 2012R2	Windows Server 2012R2
	TestUserAdmin	TestUserNonAdmin	TestUserAdmin	TestUserNonAdmin
TC1	--	--	--	--
TC2	--	--	--	--
TC3	--	--	--	--
TC4	--	--	--	--
TC5	--	--	--	--
TC6	--	--	--	--

TestszENARIO TC#	Windows Server 2019 TestUserAdmin	Windows Server 2019 TestUserNonAdmin	Windows Server 2012R2 TestUserAdmin	Windows Server 2012R2 TestUserNonAdmin
TC7	--	--	--	--
TC8	--	--	--	--
TC9	--	--	--	--
TC10	--	--	--	--
TC11	--	--	--	--
TC12	--	--	--	--
TC13	✓	✓		
TC14	--	--		
TC15	--	--		
TC16	--	--		
TC17			✓	✓
TC18			--	--
TC19			--	--
TC20			--	--
TC21			--	--

Tabelle 19: UAL erfassten Aktivitäten - Post-mortem-Untersuchung

Die UAL-Informationen, welche ausgelesen wurden über die von Microsoft bereitgestellten *PowerShell Cmdlets* sowie die UAL-Informationen, welche mit Hilfe von *KStrike* extrahiert worden sind, offenbaren eine klare Übereinstimmung der Informationen. Entgegen der anfänglichen Vermutung zu Beginn dieser Arbeit erfasst und speichert UAL nur spezifische Informationen, unter anderem:

- Angaben zum Service, welcher für eine Interaktion verwendet wurde.
- Anzahl der Zugriffe auf den Service durch einen Benutzer.
- Verwendete Netzwerkadresse.
- Verwendetes Betriebssystem.

Die zeitlichen Angaben der UAL-Erfassung decken sich mit den Daten der Durchführung und können daher als zeitlich präzise betrachtet werden. Damit wird auch die Funktionalität der Echtzeiterfassung bestätigt.

Trotz der anfänglichen Annahme aufgrund der minimalistischen Microsoft-Dokumentation, dass auch periphere Informationen von UAL erfasst werden, stellt sich heraus, dass Daten wie beispielsweise die Erfassung von mehrfach Login mit falschem Passwort (TC1), Login und Logout mit korrektem Passwort (TC2) bis und mit Testszenario 12 (TC12) nicht erfasst werden. Ursprünglich wurde vermutet, dass zumindest einige (auch wenn nicht vollständig) dieser Randinformationen erfasst werden, um bei einer Untersuchung ein umfassendes Bild zu liefern.

Die Testszenarien TC13 und TC17 liefern klare Erkenntnisse, die Testszenarien TC14 bis TC16 sowie TC18 bis TC21 hingegen können nur als teilweise erkannt betrachtet werden. Hierbei wurden zwar die spezifischen durchgeführten Aktionen nicht identifiziert, allerdings wurde das initiale Mapping auf das freigegebene Verzeichnis und damit der Zugriff auf den File Service erfasst.

5.1.1 W-Fragen

Im Allgemeinen zielt eine forensische Untersuchung darauf ab, die folgenden W-Fragen [48] zu beantworten:

- Was ist geschehen?
- Wo ist es passiert?
- Wann ist es passiert?
- Wie ist es passiert?

In der nachstehenden Übersicht soll kläre, ob und inwieweit eine UAL erfasst Aktivität auch Antworten auf die W-Fragen liefern kann.

Testszenario TC#	Was ist geschehen?	Wo ist es passiert?	Wann ist es passiert?	Wie ist es passiert?
TC1 bis TC12	Nicht erfasst	Nicht erfasst	Nicht erfasst	Nicht erfasst
TC13	Zugriff auf ein File Share wurde erfasst	Server Betriebssystem eindeutig identifizierbar	Erstmaliger Zugriff sowie letzter Zugriff erfasst	Zugriff mit einem Client System und einem Benutzer erfasst
TC14 bis TC16	Nicht erfasst	Nicht erfasst	Nicht erfasst	Nicht erfasst
TC17	Zugriff auf ein File Share wurde erfasst	Server Betriebssystem eindeutig identifizierbar	Erstmaliger Zugriff sowie letzter Zugriff erfasst	Zugriff mit einem Client System und einem Benutzer erfasst
TC18 bis TC21	Nicht erfasst	Nicht erfasst	Nicht erfasst	Nicht erfasst

Tabelle 20: UAL erfasst Aktivität - W-Fragen

Die Informationen aus der Übersicht und daraus folgend können die von der UAL erfassten Informationen als forensisch verwertbar betrachtet werden. Es ist besonders hervorzuheben, dass UAL-Artefakte die Fähigkeit haben, Informationen für einen Zeitraum von bis zu drei Jahren zu speichern, dieser Zeitraum bietet bei Untersuchungen eine unschätzbare Quelle von Informationen und Zuordnungsmöglichkeiten von Personen zu Netzwerkadressen und verwendeten Windows Services.

5.2 Grenzen und Möglichkeiten

5.2.1 Grenzen des UAL-Artefakts

Trotz der offensichtlichen Vorteile welche UAL-Artefakte über eine Dauer von bis zu drei Jahren bieten, gibt es Grenzen. Für Administratoren, Sicherheitsexperten und IT-Forensiker ist es daher wichtig die Grenzen zu verstehen. Die Grenzen in diesem Kontext können auch im Einzelfall als UAL-Schwachstellen betrachtet werden, basierend auf den Erkenntnissen dieser Arbeit lassen sich die folgenden Einschränkungen feststellen:

1. UAL protokolliert lediglich Aktivitäten, die in direktem Zusammenhang mit UAL unterstützten Windows Services stehen, daher werden nicht alle Aktivitäten auf Betriebssystemebene protokolliert.
2. Durch die fehlende Erfassung von allgemeinen und nicht unterstützten Aktivitäten durch UAL kann es in bestimmten Szenarien zu Interpretationsschwierigkeiten führen.
3. Der *ActiviyCount*, welcher die Anzahl der auf den Windows Service zugreifenden Zugriffe eines Clients anzeigt, ist limitiert auf 65`535 Zugriffe pro Tag [33].
4. Microsoft empfiehlt die UAL-Funktion für Server welchen einen direkten Internet-Zugriff haben zu deaktivieren, die Speicherbelastung der UAL-Datenbank würde die Systemleistung des Windows Servers zu stark beeinträchtigen [33].
5. Die Verwendung der von *PowerShell Cmdlets* bei der Auswertung einer großen Menge an UAL-Artefakten über einen längeren Zeitraum kann zu schwer interpretierbaren Ergebnissen führen.
6. Vor dem aktiven Betrieb von Windows Servern mit UAL sollte geprüft werden, ob die Nutzung im Einklang mit den Datenschutzbestimmungen steht.

5.2.2 Möglichkeiten des UAL-Artefakts

UAL bietet wichtige Einblicke in Bezug auf die Zugriffsaktivitäten eines Windows Server, diese Informationen sind für Administratoren, Sicherheitsexperten und IT-Forensiker hilfreich. UAL-Artefakte stellen unter anderem die folgenden Informationen über einen Zeitraum von bis zu drei Jahren zur Verfügung:

1. Eindeutige Identifikation des Benutzers durch den Benutzernamen
2. Eindeutige Identifikation des Zugriffsclients durch die Netzwerkadressinformationen
3. Echtzeit Erfassung des Zugriffzeitpunkts
4. Anzahl der Zugriffe

Die von UAL gespeicherten Informationen sind in den UAL-Datenbanken bis zu drei Jahre gespeichert. Es ist ein gängiges Vorgehen von Angreifern, ihre Spuren zu verwischen, indem sie Protokolle, einschließlich der Windows Event Logs, löschen oder manipulieren. Dies ist ein Versuch, ihre Aktionen zu verbergen und die Untersuchung ihrer Aktivitäten zu erschweren. Während der Ausarbeitung dieser Arbeit ist klar geworden, dass die UAL noch unbekannt ist und die UAL-Datenbanken leicht zu übersehen oder nicht sofort als potenzielle Artefakt Quelle erkannt werden. Dies könnte auf eine allgemeine Unkenntnis der über die UAL-Funktionen und -Fähigkeiten zurückzuführen sein. Für Administratoren, Sicherheitsexperten und IT-Forensiker können UAL-Artefakte jedoch einen entscheidenden Vorteil bei der Untersuchung und Aufklärung von Vorfällen liefern. Es ist jedoch wichtig zu betonen, dass die Sicherheit der UAL-Datenbanken nicht gewährleistet ist, mit den richtigen Administratorenrechten kann ein versierter Angreifer die UAL-Datenbanken löschen. Das bedeutet, dass alle darin gespeicherten UAL-Artefakte verloren gehen würden, ähnlich wie bei der Löschung von Windows Event Logs. Somit wird die Möglichkeit, diese Daten in einer Untersuchung zu nutzen, aufgelöst.

5.3 Beantwortung der Forschungsfragen

Forschungsfrage 1: Welche Informationen werden durch die UAL protokolliert (Informationsgehalt) und wie lange werden diese gespeichert?

Konkretisierung: Können mit Hilfe der UAL als forensisches Artefakt die W-Fragen [48] beantwortet werden (Was ist geschehen; Wo ist es passiert; Wann ist es passiert; Wie ist es passiert)?

UAL protokolliert unter anderem folgende Informationen zu entnehmen:

- Angaben zum Service, welcher für eine Interaktion verwendet wurde
- Anzahl der Zugriffe auf den Service durch einen Benutzer
- Verwendete Netzwerkadresse
- Verwendetes Betriebssystem

Die Ergebnisse sind dem *Kapitel 8.4 – Untersuchung*. Zudem beantwortet diese Arbeit die W-Fragen, vorausgesetzt, die UAL hat die betreffenden Interaktionen erfasst, die vollständigen Ergebnisse sind dem *Kapitel 9.1.1 – W-Fragen*, zu entnehmen.

Forschungsfrage 2: Wie können UAL-Artefakte ausgelesen und extrahiert werden?

Konkretisierung: Vorstellung der Methoden zum Auslesen sowie extrahieren von UAL-Artefakten.

Im Rahmen dieser Arbeit wurden zwei Methoden vorgestellt, welche es ermöglichen die UAL-Artefakte auszulesen und die Informationen zu extrahieren:

- Methode 1: Live-Analyse mittels *PowerShell Cmdlets*
- Methode 2: Post-mortem-Untersuchung mittels *KStrike*

Die vollständigen Ergebnisse sind dem *Kapitel 8.4 – Untersuchung*, zu entnehmen

Forschungsfrage 3: Unterscheidet sich die UAL-Funktion sowie die UAL-Artefakte von Windows Server 2012 R2 und Windows Server 2019?

Konkretisierung: Gibt es funktionelle Unterschiede der UAL-Funktion bei Windows Server 2012 R2 im Vergleich zu Windows Server 2019?

Konkretisierung: Gibt es Unterschiede der UAL-Artefakte bei Windows 2012 R2 im Vergleich zu Windows Server 2019?

Nach der durchgeführten Testszenarien und dem aktuellen Kenntnisstand gibt es keine funktionellen Unterschiede der UAL unabhängig auf welchem Windows Server-Betriebssystem. Ebenfalls wurden bei der Auswertung der Ergebnisse kein Unterschied der UAL-Artefakte auf verschiedenen Windows Server-Betriebssystem festgestellt. Die vollständigen Ergebnisse sind dem *Kapitel 9.1 – Auswertung und Bewertung*, zu entnehmen.

Forschungsfrage 4: Wie sind UAL-Artefakte zu interpretieren und kann den Anforderungen an die Erhebung von Daten gerecht werden (Robustheit)?

Konkretisierung: Wird UAL den Anforderungen gerecht in Bezug auf Akzeptanz, Glaubwürdigkeit, Wiederholbarkeit, Integrität, Ursache und Auswirkung sowie Dokumentation [20,21]?

- **Akzeptanz:** UAL bietet die Möglichkeit UAL-Artefakte bis zu drei Jahre zu speichern. Obwohl Microsoft die grundlegende UAL Funktionsweise offiziell dokumentiert, wird diese nicht ausdrücklich als forensisches Instrument innerhalb der Windows Server-Betriebssysteme beworben, sondern als technische Lösung für IT-Administratoren. Eine Auswertung von UAL-Artefakten kann daher auf allgemeine Akzeptanz treffen und als valide angesehen werden. Die in dieser Arbeit gelieferten Ergebnisse weisen zudem auf eine homogene UAL-Funktionsweise über verschiedene Windows Server-Betriebssysteme hinweg. Im Einzelfall muss eine Verteidigung dieser Methode vorbereitet werden, obgleich die Datenextraktion der UAL-Artefakte über die von Microsoft bereitgestellten *PowerShell Cmdlets* oder über verfügbare Werkzeuge wie *KStrike* erfolgt.
- **Glaubwürdigkeit:** UAL hat plausible Echtzeit-Ergebnisse geliefert, welche in einem forensischen Kontext interpretiert werden können, somit ist die Glaubwürdigkeit gewährleistet.
- **Wiederholbarkeit & Integrität:** Die Wiederholbarkeit ist gewährleistet da die UAL-Datenbank Informationen über einen Zeitraum von bis zu drei Jahren speichert und die Auslesung mehrfach ermöglicht. Die Post-mortem-Untersuchung einer Datenbankkopie ist zu bevorzugen, dieser Ansatz verhindert das unbeabsichtigte Hinzufügen weiterer UAL-Artefakte und schützt somit die Integrität der gespeicherten Informationen.
- **Ursache und Wirkung:** Ob die UAL-Artefakte zu einer Korrelation zwischen Ereignissen und Untersuchungsergebnissen führt, muss stets im individuellen Kontext betrachtet werden. Im Rahmen dieser Arbeit konnte jedoch eine Korrelation zwischen Ereignissen und Untersuchungsergebnissen hergestellt werden.
- **Dokumentation:** Die Schritte bei der Auswertung von UAL-Artefakten können angemessen, vollständig transparent und nachvollziehbar dokumentiert werden.

Forschungsfrage 5: Welche Grenzen gibt es bei der UAL als forensisches Artefakt?

Konkretisierung: Darstellung von technischen Grenzen.

<p>Es wurden mehrere Einschränkungen und Limitierungen bezüglich UAL identifiziert:</p> <ul style="list-style-type: none"> • UAL-Protokollierung ist nicht umfangreich genug um eine vollständige forensische Untersuchung zu vermeiden. • Interpretationsschwierigkeiten bei der Auswertung von UAL-Artefakten. • Es gibt Limitationen bei der UAL-Aktivitätserfassung. • UAL-Auswertungen können sich bei großen Informationsmengen problematisch gestalten. • Datenschutzbestimmungen sollten im Kontext UAL beachtet werden. <p>Die vollständigen Ergebnisse sind dem <i>Kapitel 9.2.1 – Grenzen des UAL-Artefakts</i>, zu entnehmen.</p>
<p>Forschungsfrage 6: Welche Möglichkeiten bietet die UAL als forensisches Artefakt?</p> <p><u>Konkretisierung:</u> Darstellung von technischen Möglichkeiten.</p> <p>Es wurden mehrere Möglichkeiten identifiziert, welche in Verbindung mit UAL stehen:</p> <ul style="list-style-type: none"> • Informationsspeicherung bis zu drei Jahre. • Eindeutige Identifikation des Benutzers durch den Benutzernamen. • Eindeutige Identifikation des Zugriffsclients durch die Netzwerkadressinformationen. <p>Die vollständigen Ergebnisse sind dem <i>Kapitel 9.2.2 – Möglichkeiten des UAL-Artefakts</i>, zu entnehmen.</p>

Tabelle 21: Beantwortung der Forschungsfragen

6 Zusammenfassung und Ausblick

In der vorliegenden Arbeit wurde User Access Logging als potenzielles IT-forensisches Artefakt untersucht insbesondere im Hinblick auf die Robustheit und den damit verbundenen Informationsgehalt mit dem Ziel die Grenzen und Möglichkeiten der UAL zu beleuchten. Digitale Informationen sind in unserer heutigen Gesellschaft bedeutsam für alle Bereiche unseres Lebens, somit besteht ein wachsender Bedarf an effizienten und robusten Methoden, Werkzeugen und Artefakten zur Aufklärung und Rekonstruktion digitaler Ereignisse um Untersuchungen effektiv zu unterstützen. In diesem Zusammenhang stellt UAL eine vielversprechende Ergänzung zu den bisherigen Artefakt Quellen der IT-Forensik dar.

Die Untersuchung ergab, dass UAL-Artefakte eine robuste und nützliche Quelle IT-Forensische Untersuchungen darstellen, insbesondere durch die Protokollierung von benutzerspezifischen Informationen, Zeitstempeln und gerätespezifischen Details von bis zu drei Jahren. Obwohl UAL nicht als Ersatz für eine vollständige Untersuchung dient, zeigt es das Potential, Wissenslücken zu schließen und bestehende Annahmen zu stärken.

Im direkten Zusammenhang mit dieser Arbeit gibt es Ansatzpunkte für die UAL-Erweiterbarkeit und -Verbesserung, künstliche Intelligenz könnte zur weiteren Analyse und Filterung der UAL-Artefakte eingesetzt werden, um somit eine homogene und zielgerichtete Auswertung zu ermöglichen. Eine Verbesserung bei der Visualisierung der UAL-Artefakt Informationen wäre wünschenswert, um einerseits die Darstellung jedoch auch die Interpretation der Informationen zu vereinfachen.

Zusammengefasst zeigt die Untersuchung in dieser Arbeit, dass UAL-Artefakte eine wertvolle Ergänzung darstellen. Es gibt eine Vielzahl an Möglichkeiten für zukünftige Forschungen und Anwendungen in den verschiedensten Bereichen, es bleibt jedoch unabdingbar sich mit Anforderungen und Problemstellungen auseinanderzusetzen, um für den digitalen Wandel gerüstet zu sein.

6.1 Konklusion

Ursprünglich wurde vermutet, dass UAL auch generelle Windows Server Aktivitäten erfasst, zumindest einige (auch wenn nicht vollständig) erfasst werden, um bei einer Untersuchung ein umfassendes Bild zu liefern und hierdurch eine alternative zu klassischen Artefakten bietet. User Access Logging stellt eine vielversprechende Ergänzung zu klassischen IT-Forensik dar, unabhängig der angewendeten Methode und Werkzeuge stellt die Untersuchung von UAL-Artefakten keinen Ersatz für eine vollständige Untersuchung dar. UAL-Artefakte bieten das Potential Wissenslücken zu schließen oder Annahmen während einer Untersuchung zu stützen. Vor allem die bis zu drei Jahre Informationsspeicherung bietet bei Untersuchung von Vorfällen welche länger in der Vergangenheit liegen im individuellen Fall nützliche Informationen. Die ursprüngliche Vermutung, dass das UAL die Aktivitäten von Windows Server erfasst, hat sich bestätigt. Selbst wenn es nicht alle generellen Windows Aktivitäten in ihrer Gesamtheit erfasst, liefert es ein bedeutendes Bild, das sich als eine wertvolle Ergänzung zu herkömmlichen forensischen Artefakten herausstellt. User Access Logging erweist sich als eine vielversprechende Ergänzung in der IT-Forensik. Jedoch sollte betont werden, dass trotz der Vielfalt an erfassten Daten und der wertvollen Einsichten, die UAL-Artefakte bieten können, sie nicht als Ersatz für eine vollumfängliche Untersuchung angesehen werden dürfen. Sie dienen eher dazu, Wissenslücken zu schließen und während einer Untersuchung bestehende Annahmen zu untermauern. Ein besonders bemerkenswertes Merkmal von UAL ist die Fähigkeit, Informationen für bis zu drei Jahre zu speichern. Dies kann von unschätzbarem Wert sein, besonders wenn Vorfälle untersucht werden, die weit in der Vergangenheit liegen, und liefert in solchen Fällen oft entscheidende Informationen.

6.2 Fazit

In einer Zeit, in der die Digitalisierung immer mehr an Fahrt aufnimmt und digitale Kriminalität immer präsenter wird, wächst die Bedeutung von neuartigen forensischen Artefakten, Instrumenten und Methoden. User Access Logging stellt sich in dieser Hinsicht als eine vielversprechende Artefakt Quelle dar, welche Untersuchungen und Auswertungen aktiv unterstützen kann. Aufgrund ihrer Robustheit und Zuverlässigkeit sollten UAL-Artefakte als potenziell bei Untersuchungen in Betracht gezogen werden. Abhängig der Fall-Komplexität können UAL-Artefakte eine wichtige Quelle für Informationen darstellen, UAL-Artefakte bieten eine signifikante Ergänzung bei Untersuchungen, indem es mögliche Wissenslücken schließt und bestehende Annahmen während der Untersuchung festigt. Insbesondere die UAL-Fähigkeit, Informationen bis zu drei Jahre zu speichern, kann bei der Aufklärung von Vorfällen, die länger zurückliegen, äußerst wertvoll sein.

Insgesamt liefert User Access Logging somit einen bedeutenden Beitrag zur IT-Forensik und IT-Sicherheit. Es hat das Potenzial bei der Rekonstruktion von Ereignissen zu unterstützen und somit zur Aufklärung von Vorfällen beitragen. Unabhängig davon bleibt abzuwarten, wie sich UAL-Artefakte weiterentwickeln und welche weiteren Möglichkeiten in der Zukunft geboten werden. Der aktuelle Stand der Dinge lässt jedoch darauf schließen, dass UAL-Informationen ein zentrales Artefakt in der nächsten Generation der IT-Forensik darstellen wird.

Literaturverzeichnis

- [1] VMware, VMware Workstation [Online]. Verfügbar unter: <https://docs.vmware.com/en/VMware-Workstation-Pro/17.0.2/rn/vmware-workstation-1702-pro-release-notes/index.html> [Zugriff am 01. Juli 2023].
- [2] VMware, VMware Docs [Online]. Verfügbar unter: <https://store-eu.vmware.com/vmware-workstation-17-pro-5710844200.html> [Zugriff am 01. Juli 2023]
- [3] Microsoft, Windows 10 release information [Online]. Verfügbar unter: <https://learn.microsoft.com/en-us/windows/release-health/release-information> [Zugriff am 01. Juli 2023].
- [4] Microsoft, Download Windows 10 [Online]. Verfügbar unter: <https://www.microsoft.com/en-us/software-download/windows10%20> [Zugriff am 01. Juli 2023].
- [5] Microsoft, Windows Server 2012 R2 [Online]. Verfügbar unter: <https://learn.microsoft.com/en-us/lifecycle/products/windows-server-2012-r2> [Zugriff am 01. Juli 2023].
- [6] Microsoft, Evaluation Center [Online]. Verfügbar unter: <https://www.microsoft.com/de-de/evalcenter> [Zugriff am 01. Juli 2023].
- [7] Microsoft, Windows Server 2019 [Online]. Verfügbar unter: <https://learn.microsoft.com/en-us/lifecycle/products/windows-server-2019> [Zugriff am 01. Juli 2023].
- [8] Microsoft, Microsoft Office 2016 [Online]. Verfügbar unter: <https://learn.microsoft.com/en-us/lifecycle/products/microsoft-office-2016> [Zugriff am 01. Juli 2023].
- [9] Microsoft, Download and install or reinstall Office 2019, Office 2016, or Office 2013 [Online]. Verfügbar unter: <https://support.microsoft.com/en-au/office/download-and-install-or-reinstall-office-2019-office-2016-or-office-2013-7c695b06-6d1a-4917-809c-98ce43f86479> [Zugriff am 01. Juli 2023].

- [10] Python, Python 3.11.4 [Online]. Verfügbar unter:
<https://www.python.org/downloads/release/python-3114/> [Zugriff am 01. Juli 2023].
- [11] Github, brimorlabs, KStrike [Online]. Verfügbar unter:
<https://github.com/brimorlabs/KStrike/tree/master> [Zugriff am 01. Juli 2023].
- [12] Github, Joakim Schicht, RawCopy [Online]. Verfügbar unter:
<https://github.com/jschicht/RawCopy> [Zugriff am 01. Juli 2023].
- [13] Wikipedia, Windows Server 2012 [Online]. Verfügbar unter:
https://en.wikipedia.org/wiki/Windows_Server_2012 [Zugriff am 02. Juli 2023].
- [14] SANS, DFIR Summit 2021, Where Have UAL Been [Online]. Verfügbar unter:
<https://sansorg.egnyte.com/dl/LFAJUFHnVB> [Zugriff am 02. Juli 2023].
- [15] Wikipedia, Forensik [Online]. Verfügbar unter: <https://de.wikipedia.org/wiki/Forensik>
[Zugriff am 24. Juli 2023].
- [16] BSI, "Leitfaden IT-Forensik", Version 1.0.1, 2011, S. 8 [Online]. Verfügbar unter:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf?__blob=publicationFile&v=1 [Zugriff am 24. Juli 2023].
- [17] Alexander Geschonneck, Computer Forensik: Computerstraftaten erkennen, ermitteln, aufklären, 6., aktualisierte und erweiterte Auflage, S. 66, dpunkt.verlag, Heidelberg, ISBN: PDF 978-3-86491-489-8. [Zugriff am 03. Juli 2023].
- [18] Alexander Geschonneck, Computer Forensik: Computerstraftaten erkennen, ermitteln, aufklären, 6., aktualisierte und erweiterte Auflage, S. 2, dpunkt.verlag, Heidelberg, ISBN: PDF 978-3-86491-489-8. [Zugriff am 03. Juli 2023].
- [19] Wikipedia, Artefakt [Online]. Verfügbar unter: <https://de.wikipedia.org/wiki/Artefakt>
[Zugriff am 24. Juli 2023].
- [20] BSI, "Leitfaden IT-Forensik", Version 1.0.1, 2011, S. 23 [Online]. Verfügbar unter:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf?__blob=publicationFile&v=1 [Zugriff am 24. Juli 2023].

- [21] Alexander Geschonneck, Computer Forensik: Computerstraftaten erkennen, ermitteln, aufklären, 6., aktualisierte und erweiterte Auflage, S. 66-67, dpunkt.verlag, Heidelberg, ISBN: PDF 978-3-86491-489-8. [Zugriff am 03. Juli 2023].
- [22] BSI, "Leitfaden IT-Forensik", Version 1.0.1, 2011, S. 24 [Online]. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf?__blob=publicationFile&v=1 [Zugriff am 24. Juli 2023].
- [23] Wikipedia, Post mortem [Online]. Verfügbar unter: https://de.wikipedia.org/wiki/Post_mortem [Zugriff am 25. Juli 2023].
- [24] Wikipedia, Live [Online]. Verfügbar unter: <https://de.wikipedia.org/wiki/live> [Zugriff am 25. Juli 2023]
- [25] Alexander Geschonneck, Computer Forensik: Computerstraftaten erkennen, ermitteln, aufklären, 6., aktualisierte und erweiterte Auflage, S. 107, dpunkt.verlag, Heidelberg, ISBN: PDF 978-3-86491-489-8. [Zugriff am 03. Juli 2023].
- [26] IT-Forensik Wiki, Post-Mortem-Analyse [Online]. Verfügbar unter: <https://it-forensik.fiw.hs-wismar.de/index.php/Post-Mortem-Analyse> [Zugriff am 25. Juli 2023]
- [27] Microsoft, Get Started with User Access Logging [Online]. Verfügbar unter: <https://learn.microsoft.com/en-us/windows-server/administration/user-access-logging/get-started-with-user-access-logging> [Zugriff am 03. Juli 2023].
- [28] Wikipedia, Client [Online]. Verfügbar unter: <https://de.wikipedia.org/wiki/client> [Zugriff am 27. Juli 2023]
- [29] Microsoft, Windows Server 2012 and 2012 R2 reaching end of support [Online]. Verfügbar unter: <https://learn.microsoft.com/en-us/lifecycle/announcements/windows-server-2012-r2-end-of-support> [Zugriff am 27. Juli 2023].
- [30] Microsoft, Microsoft Learn. Spark possibility [Online]. Verfügbar unter: <https://learn.microsoft.com/en-us/> [Zugriff am 27. Juli 2023].
- [31] Wikipedia, Dynamic Link Library [Online]. Verfügbar unter: https://de.wikipedia.org/wiki/Dynamic_Link_Library [Zugriff am 27. Juli 2023].

- [32] Wikipedia, Programmierschnittstelle [Online]. Verfügbar unter:
<https://de.wikipedia.org/wiki/Programmierschnittstelle> [Zugriff am 27. Juli 2023].
- [33] Microsoft, Manage User Access Logging [Online]. Verfügbar unter:
<https://learn.microsoft.com/en-us/windows-server/administration/user-access-logging/manage-user-access-logging> [Zugriff am 27. Juli 2023].
- [34] Wikipedia, Global Assembly Cache [Online]. Verfügbar unter:
https://de.wikipedia.org/wiki/Global_Assembly_Cache [Zugriff am 30. Juli 2023].
- [35] Ghidra, Homepage [Online]. Verfügbar unter: <https://ghidra-sre.org/> [Zugriff am 27. Juli 2023].
- [36] Wikipedia, Reverse Engineering [Online]. Verfügbar unter:
https://de.wikipedia.org/wiki/Reverse_Engineering [Zugriff am 27. Juli 2023].
- [37] HowToGeek, What is the System32 Directory? (and Why You Shouldn't Delete It) [Online]. Verfügbar unter: <https://www.howtogeek.com/346997/what-is-the-system32-directory-and-why-you-shouldnt-delete-it/> [Zugriff am 30. Juli 2023].
- [38] HELPDESKGEEK, What Is the WinSxS Folder, Why Is It Huge, and How to Cleanup [Online]. Verfügbar unter: <https://helpdeskgeek.com/windows-11/what-is-the-winsxs-folder-why-is-it-huge-and-how-to-cleanup/> [Zugriff am 30. Juli 2023].
- [39] AdvancedInstaller, What is the SysWOW64 folder and what is it used for? [Online]. Verfügbar unter: <https://www.advancedinstaller.com/what-is-syswow64-folder-and-its-role.html> [Zugriff am 30. Juli 2023].
- [40] Rapid, API Wrapper [Online]. Verfügbar unter: <https://rapidapi.com/blog/api-glossary/api-wrapper/> [Zugriff am 30. Juli 2023].
- [41] Wikipedia, Universally Unique Identifier [Online]. Verfügbar unter:
https://de.wikipedia.org/wiki/Universally_Unique_Identifier [Zugriff am 30. Juli 2023].
- [42] Microsoft, Extensible Storage Engine [Online]. Verfügbar unter:
<https://learn.microsoft.com/en-us/windows/win32/extensible-storage-engine/extensible-storage-engine> [Zugriff am 30. Juli 2023].

- [43] InfoSec Notes, User Access Logging (UAL) [Online]. Verfügbar unter:
https://notes.qazeer.io/dfir/windows/_artefacts_overview/user_access_logging [Zugriff am 30. Juli 2023].
- [44] Server World, Windows Server 2019 File Server: Install [Online]. Verfügbar unter:
https://www.server-world.info/en/note?os=Windows_Server_2019&p=smb&f=1 [Zugriff am 03. August 2023].
- [45] Microsoft, Installieren eines neuen Dateiservers [Online]. Verfügbar unter:
<https://learn.microsoft.com/de-de/windows-server/networking/branchcache/deploy/install-a-new-file-server-as-a-content-server> [Zugriff am 03. August 2023].
- [46] Server World, Windows Server 2012 R2 File Server: Install [Online]. Verfügbar unter:
https://www.server-world.info/en/note?os=Windows_Server_2012&p=smb&f=3 [Zugriff am 03. August 2023].
- [47] Microsoft, Installieren und Konfigurieren von Windows Server [Online]. Verfügbar unter:
<https://learn.microsoft.com/de-de/windows-server-essentials/install/install-and-configure-windows-server-essentials-or-windows-server-essentials-experience> [Zugriff am 03. August 2023].
- [48] BSI, "Leitfaden IT-Forensik", Version 1.0.1, 2011, S. 22 [Online]. Verfügbar unter:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf?__blob=publicationFile&v=1 [Zugriff am 24. Juli 2023].
- [49] Microsoft, Map a network drive in Windows [Online]. Verfügbar unter:
<https://support.microsoft.com/en-us/windows/map-a-network-drive-in-windows-29ce55d1-34e3-a7e2-4801-131475f9557d> [Zugriff am 11. August 2023].
- [50] Crowdstrike Blog, UAL Thank Us Later [Online]. Verfügbar unter:
<https://www.crowdstrike.com/blog/user-access-logging-ual-overview/> [Zugriff am 13. August 2023].
- [51] Autopsy, Official Homepage [Online]. Verfügbar unter: <https://www.autopsy.com/> [Zugriff am 13. August 2023].
- [52] Github, Autopsy Python Plugin [Online]. Verfügbar unter:
<https://github.com/markmckinnon/Autopsy-Plugins> [Zugriff am 13. August 2023].

- [53] Github, SumECmd [Online]. Verfügbar unter: <https://github.com/EricZimmerman/Sum>
[Zugriff am 13. August 2023].

Abbildungsverzeichnis

Abbildung 1: Windows Server 2019 - UAL Service	19
Abbildung 2: Windows Server 2012R2 - UAL Service	19
Abbildung 3: UAL*.DLL Dateien - Windows Server 2019	22
Abbildung 4: UAL*.DLL Dateien - Windows Server 2012 R2	23
Abbildung 5: UAL*.DLL Dateien - Export.....	24
Abbildung 6: UAL*.DLL Dateien - Import Ghidra	24
Abbildung 7: Ghirda - ualapi_2012_System32.dll exemplarisch	26
Abbildung 8: UAL-Service.....	27
Abbildung 9: UAL-Datenbanken	28
Abbildung 10: UAL-Architektur	30
Abbildung 11: Testumgebung.....	31
Abbildung 12: Share Windows Server 2019	33
Abbildung 13: Share Windows Server 2012 R2	33
Abbildung 14: Virtuelles Netzwerk	35
Abbildung 15: Netzwerkeigenschaften Virtuelle Instanzen	36
Abbildung 16: Windows Server 2019 - Get-UalOverview	43
Abbildung 17: Windows Server 2019 - Get-UalUserAccess	44
Abbildung 18: Windows Server 2019 - Get-UalDailyAccess	45
Abbildung 19: Beispiel - Informationsaufschlüsselung	45
Abbildung 20: Windows Server 2012 R2 - Get-UalOverview	46
Abbildung 21: Windows Server 2012 R2 - Get-UalUserAccess	47
Abbildung 22: Windows Server 2012 R2 - Get-UalDailyAccess	48
Abbildung 23: Kopie von Abb. 17 - Beispiel Informationsaufschlüsselung	48
Abbildung 24: Windows Server 2019 - UAL-Datenbanken.....	49
Abbildung 25: Windows Server 2019 - RawCopy.....	50
Abbildung 26: Windows Server 2019 - RawCopy Output	50
Abbildung 27: Windows 10 Client - UAL-Datenbanken Windows Server 2019	51
Abbildung 28: Windows 10 Client - KStrike	51

Abbildung 29: Kstrike.py Current_windowsserver2019.mdb	52
Abbildung 30: Kstrike.py Current_windowsserver2019.mdb, Verarbeitung.....	52
Abbildung 31: KStrike.py {483D7CC6-AB32-4004-A9DB- 22F08A1B3540}_windowsserver2019.mdb	53
Abbildung 32: Kstrike.py SystemIdentity_windowsserver2019.mdb.....	53
Abbildung 33: Speicherung *windowsserver2019.txt.....	54
Abbildung 34: Current_windowsserver2019.txt	55
Abbildung 35: Text Import Wizard, Screenshot 1	55
Abbildung 36: Text Import Wizard, Screenshot 2	56
Abbildung 37: Current_windowsserver2019_txt_.xlsx	56
Abbildung 38: {483D7CC6-AB32-4004-A9DB-22F08A1B3540}_windowsserver2019.....	58
Abbildung 39: Windows Server 2012 R2 - UAL-Datenbanken	59
Abbildung 40: Windows Server 2012 R2 – RawCopy	60
Abbildung 41: Windows Server 2012 R2 - RawCopy Output	61
Abbildung 42: Windows 10 Client - UAL-Datenbanken Windows Server 2012 R2	61
Abbildung 43: Windows 10 Client - KStrike	62
Abbildung 44: Kstrike.py Current_windowsserver2012r2.mdb	62
Abbildung 45: Kstrike.py Current_windowsserver2012r2.mdb, Verarbeitung	63
Abbildung 46: KStrike.py {0FE16C77-877A-4B7B-AFA1- 24B2340644CB}_windowsserver2012r2.mdb.....	63
Abbildung 47: Kstrike.py SystemIdentity_windowsserver2012r2.mdb	64
Abbildung 48: Speicherung *windowsserver2012r2.txt	65
Abbildung 49: Current_windowsserver2012r2.txt	65
Abbildung 50: Text Import Wizard, Screenshot 1	66
Abbildung 51: Text Import Wizard, Screenshot 2	66
Abbildung 52: Current_windowsserver2012r2_txt_.xlsx.....	67
Abbildung 53: {0FE16C77-877A-4B7B-AFA1-24B2340644CB}_windowsserver2012	68

Tabellenverzeichnis

Tabelle 1: Benutzerspezifischen Informationen [27]	17
Tabelle 2: Gerätespezifische Informationen [27]	18
Tabelle 3: UAL-Service - PowerShell	20
Tabelle 4: UAL*.DLL Dateien.....	21
Tabelle 5: Windows Verzeichnisse – Funktion	22
Tabelle 6: UAL*.DLL Dateien - Ergebnisse Ghidra.....	25
Tabelle 7: UAL-Datenbanken [43]	28
Tabelle 8: Microsoft, Collect UAL Data [33].....	29
Tabelle 9: Virtuelle Instanzen	32
Tabelle 10: Funktion / Zweck - File Server	33
Tabelle 11: Windows Server 2019 - Benutzerkonto	34
Tabelle 12: Windows Server 2012 R2 - Benutzerkonto.....	35
Tabelle 13: Konkretisierung der Forschungsfragen	41
Tabelle 14: Current_windowsserver2019_txt_.xlsx	57
Tabelle 15: {483D7CC6-AB32-4004-A9DB-22F08A1B3540}_windowsserver2019	59
Tabelle 16: Current_windowsserver2012r2_txt_.xlsx	68
Tabelle 17: {0FE16C77-877A-4B7B-AFA1-24B2340644CB}_windowsserver2012	69
Tabelle 18: UAL erfassten Aktivitäten – Live-Untersuchung	71
Tabelle 19: UAL erfassten Aktivitäten - Post-mortem-Untersuchung	72
Tabelle 20: UAL erfasst Aktivität - W-Fragen	74
Tabelle 21: Beantwortung der Forschungsfragen.....	79

Anlagenverzeichnis und Anlagen

[Anlage 1] Testzenarien

[Anlage 2] Get-UalOverview Windows Server 2019

[Anlage 3] Get-UalOverview Windows Server 2012 R2

Anlage 1 – Testszenarien

TC#	Testszenario	Ausführung (Datum, Zeit)
TC1	Login → TestUserAdmin & TestUserNonAdmin Aktion → Mehrfach Login mit falschem Password	Instanz 1: 17.08 ca. 20:05 Instanz 2: 17.08 ca. 20:06
TC2	Login → TestUserAdmin & TestUserNonAdmin Aktion → Login und Logout mit korrektem Password	Instanz 1: 17.08 ca. 20:08 Instanz 2: 17.08 ca. 20:10
TC3	Login → TestUserAdmin & TestUserNonAdmin Aktion → Änderung an Uhrzeit und Datum	Instanz 1: 17.08 ca. 20:14 Instanz 2: 17.08 ca. 20:18
TC4	Login → TestUserAdmin & TestUserNonAdmin Aktion → Neuen Benutzer erstellen/anlegen	Instanz 1: 17.08 ca. 20:25 Instanz 2: 17.08 ca. 20:28
TC5	Login → TestUserAdmin & TestUserNonAdmin Aktion → Benutzer deaktivieren	Instanz 1: 17.08 ca. 20:48 Instanz 2: 17.08 ca. 20:50
TC6	Login → TestUserAdmin & TestUserNonAdmin Aktion → Neuen Benutzer zur Gruppe Administrators hinzufügen	Instanz 1: 17.08 ca. 21:00 Instanz 2: 17.08 ca. 21:05
TC7	Login → TestUserAdmin & TestUserNonAdmin Aktion → Deaktivierung & Aktivierung Windows Firewall	Instanz 1: 17.08 ca. 21:15 Instanz 2: 17.08 ca. 21:18
TC8	Login → TestUserAdmin & TestUserNonAdmin Aktion → stoppen & starten des Windows Service: File Service	Instanz 1: 17.08 ca. 21:21 Instanz 2: 17.08 ca. 21:25
TC9	Login → TestUserAdmin & TestUserNonAdmin Aktion → Installation einer UAL-Relevanten Rolle → Web Server (ISS)	Instanz 1: 17.08 ca. 21:26 Instanz 2: 17.08 ca. 21:30
TC10	Login → TestUserAdmin & TestUserNonAdmin Aktion → Umbenennen der UAL-Datenbank-Datei Current.mdb	Instanz 1: 17.08 ca. 21:40 Instanz 2: 17.08 ca. 21:44
TC11	Login → TestUserAdmin & TestUserNonAdmin	Instanz 1: 17.08 ca. 21:47

TC#	Testszenario	Ausführung (Datum, Zeit)
	Aktion → Löschen der UAL-Datenbank-Datei	Instanz 2: 17.08 ca. 21:48
TC12	Login → TestUserAdmin & TestUserNonAdmin Aktion → Neustart Server	Instanz 1: 17.08 ca. 21:50 Instanz 2: 17.08 ca. 21:52
TC13	Login → TestUserAdmin & TestUserNonAdmin Aktion 1 → Verbinden zu \\WinServer2019\ShareUALWindowsServer2019 Aktion 2 → Erstellung neues Verzeichnis & Text Datei	Instanz 3: 17.08 ca. 22:20
TC14	Login → TestUserAdmin & TestUserNonAdmin Aktion 1 → Verbinden zu \\WinServer2019\ShareUALWindowsServer2019 Aktion 2 → Text Datei umbenennen	Instanz 3: 17.08 ca. 22:20
TC15	Login → TestUserAdmin & TestUserNonAdmin Aktion 1 → Verbinden zu \\WinServer2019\ShareUALWindowsServer2019 Aktion 2 → Inhalt Text Datei ändern und speichern	Instanz 3: 17.08 ca. 22:20
TC16	Login → TestUserAdmin & TestUserNonAdmin Aktion 1 → Verbinden zu \\WinServer2019\ShareUALWindowsServer2019 Aktion 2 → Löschen des Verzeichnisses	Instanz 3: 17.08 ca. 22:20
TC17	Login → TestUserAdmin & TestUserNonAdmin Aktion 1 → Verbinden zu \\WinServer2012R2\ShareUALWindowsServer2012R2 Aktion 2 → Erstellung neues Verzeichnis & Text Datei	Instanz 3: 17.08 ca. 22:25
TC18	Login → TestUserAdmin & TestUserNonAdmin	Instanz 3: 17.08 ca. 22:25

TC#	Testszenario	Ausführung (Datum, Zeit)
	Aktion 1 → Verbinden zu \\WinServer2012R2\ShareUALWindowsServer2012R2 Aktion 2 → Text Datei umbenennen	
TC19	Login → TestUserAdmin & TestUserNonAdmin Aktion 1 → Verbinden zu \\WinServer2012R2\ShareUALWindowsServer2012R2 Aktion 2 → Inhalt Text Datei ändern und speichern	Instanz 3: 17.08 ca. 22:25
TC20	Login → TestUserAdmin & TestUserNonAdmin Aktion 1 → Verbinden zu \\WinServer2012R2\ShareUALWindowsServer2012R2 Aktion 2 → Löschen des Verzeichnisses	Instanz 3: 17.08 ca. 22:25
TC21	Login → TestUserAdmin & TestUserNonAdmin Aktion → Installation Ledger Live	Instanz 1: 17.08 ca. 22:26 Instanz 2: 17.08 ca. 22:40

Anlage 2 – Get-UalOverview Windows Server 2019

FirstSeen :
GUID : 952285d9-edb7-4b6b-9d85-0c09e3da0bbd
LastSeen :
ProductName : Windows Server 2019 Standard Evaluation
RoleName : Remote Access
PSComputerName :

FirstSeen :
GUID : c50fcc83-bc8d-4df5-8a3d-89d7f80f074b
LastSeen :
ProductName : Windows Server 2019 Standard Evaluation
RoleName : Active Directory Certificate Services
PSComputerName :

FirstSeen :
GUID : c23f1c6a-30a8-41b6-bbf7-f266563dfcd6
LastSeen :
ProductName : Windows Server 2019 Standard Evaluation
RoleName : FTP Server
PSComputerName :

FirstSeen :
GUID : d6256cf7-98fb-4eb4-aa18-303f1da1f770
LastSeen :
ProductName : Windows Server 2019 Standard Evaluation
RoleName : Web Server
PSComputerName :

FirstSeen : 20.07.2023 12:37:26
GUID : 10a9226f-50ee-49d8-a393-9a501d47ce04
LastSeen : 17.08.2023 22:24:30
ProductName : Windows Server 2019 Standard Evaluation
RoleName : File Server
PSComputerName :

FirstSeen :
GUID : 910cbaf9-b612-4782-a21f-f7c75105434a
LastSeen :
ProductName : Windows Server 2019 Standard Evaluation
RoleName : BranchCache
PSComputerName :

FirstSeen :
GUID : d8dc1c8e-ea13-49ce-9a68-c9dca8db8b33
LastSeen :
ProductName : Windows Server 2019 Standard Evaluation
RoleName : Windows Server Update Services
PSComputerName :

FirstSeen : 15.07.2023 19:17:11
GUID : 7fb09bd3-7fe6-435e-8348-7d8aefb6cea3
LastSeen : 17.08.2023 22:02:05
ProductName : Windows Server 2019 Standard Evaluation
RoleName : Print and Document Services
PSComputerName :

FirstSeen :
GUID : bbd85b29-9dcc-4fd9-865d-3846dcb75c7
LastSeen :
ProductName : Windows Server 2019 Standard Evaluation
RoleName : Network Policy and Access Services
PSComputerName :

FirstSeen :
GUID : 4116a14d-3840-4f42-a67f-f2f9ff46eb4c
LastSeen :
ProductName : Windows Server 2019 Standard Evaluation
RoleName : Windows Deployment Services
PSComputerName :

FirstSeen :
GUID : 48eed6b2-9cdc-4358-b5a5-8dea3b2f3f6a
LastSeen :
ProductName : Windows Server 2019 Standard Evaluation
RoleName : DHCP Server
PSComputerName :

FirstSeen :
GUID : 7cc4b071-292c-4732-97a1-cf9a7301195d
LastSeen :
ProductName : Windows Server 2019 Standard Evaluation
RoleName : FAX Server
PSComputerName :

FirstSeen :
GUID : b4cdd739-089c-417e-878d-855f90081be7
LastSeen :
ProductName : Windows Server 2019 Standard Evaluation
RoleName : Active Directory Rights Management Service
PSComputerName :

Anlage 3 – Get-UalOverview Windows Server 2012 R2

FirstSeen :
GUID : 952285d9-edb7-4b6b-9d85-0c09e3da0bbd
LastSeen :
ProductName : Windows Server 2012 R2 Standard Evaluation
RoleName : Remote Access
PSComputerName :

FirstSeen :
GUID : c50fcc83-bc8d-4df5-8a3d-89d7f80f074b
LastSeen :
ProductName : Windows Server 2012 R2 Standard Evaluation
RoleName : Active Directory Certificate Services
PSComputerName :

FirstSeen :
GUID : c23f1c6a-30a8-41b6-bbf7-f266563dfcd6
LastSeen :
ProductName : Windows Server 2012 R2 Standard Evaluation
RoleName : FTP Server
PSComputerName :

FirstSeen :
GUID : d6256cf7-98fb-4eb4-aa18-303f1da1f770
LastSeen :
ProductName : Windows Server 2012 R2 Standard Evaluation
RoleName : Web Server
PSComputerName :

FirstSeen : 30.07.2023 18:13:20
GUID : 10a9226f-50ee-49d8-a393-9a501d47ce04
LastSeen : 17.08.2023 22:28:19
ProductName : Windows Server 2012 R2 Standard Evaluation
RoleName : File Server
PSComputerName :

FirstSeen :
GUID : 910cbaf9-b612-4782-a21f-f7c75105434a
LastSeen :
ProductName : Windows Server 2012 R2 Standard Evaluation
RoleName : BranchCache
PSComputerName :

FirstSeen :
GUID : d8dc1c8e-ea13-49ce-9a68-c9dca8db8b33
LastSeen :
ProductName : Windows Server 2012 R2 Standard Evaluation
RoleName : Windows Server Update Services
PSComputerName :

FirstSeen : 18.07.2023 17:57:28
GUID : 7fb09bd3-7fe6-435e-8348-7d8aefb6cea3
LastSeen : 17.08.2023 22:01:53
ProductName : Windows Server 2012 R2 Standard Evaluation
RoleName : Print and Document Services
PSComputerName :

FirstSeen :
GUID : bbd85b29-9dcc-4fd9-865d-3846dcba75c7
LastSeen :
ProductName : Windows Server 2012 R2 Standard Evaluation
RoleName : Network Policy and Access Services
PSComputerName :

FirstSeen :
GUID : 4116a14d-3840-4f42-a67f-f2f9ff46eb4c
LastSeen :
ProductName : Windows Server 2012 R2 Standard Evaluation
RoleName : Windows Deployment Services
PSComputerName :

FirstSeen :
GUID : 48eed6b2-9cdc-4358-b5a5-8dea3b2f3f6a
LastSeen :
ProductName : Windows Server 2012 R2 Standard Evaluation
RoleName : DHCP Server
PSComputerName :

FirstSeen :
GUID : 7cc4b071-292c-4732-97a1-cf9a7301195d
LastSeen :
ProductName : Windows Server 2012 R2 Standard Evaluation
RoleName : FAX Server
PSComputerName :

FirstSeen :
GUID : b4cdd739-089c-417e-878d-855f90081be7
LastSeen :
ProductName : Windows Server 2012 R2 Standard Evaluation
RoleName : Active Directory Rights Management Service
PSComputerName :

Verzeichnis der Abkürzungen

BSI	Bundesamt für Sicherheit in der Informationstechnik
CMD	Command Prompt
DFIR	Digital forensics and incident response
DLL	Dynamic Link Library
ESE	Extensible Storage Engine
SANS	SANS-Institute
TC	Test Case
UAL	User Access Logging

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-Plagiatsoftware zu ermöglichen.

Ort, Datum

Unterschrift