|  |  |  |
| --- | --- | --- |
|  |  | Logo_HSMW_blau_CMYK |
| **DOKUMENTATION**  **Programmierung I** |  |  |
|  |  |  |
| Herr Philipp Dellwo  Frau Melissa Futtig | * < |  |
| **Dokumentation Cisco Logdatei Analyse Programm** |  |  |
| Mittweida, 2025 |  |  |

|  |  |  |
| --- | --- | --- |
| Fakultät: Fakultät Angewandte Computer- und Biowissenschaften |  |  |
|  |
| **DOKUMENTATION**  **Programmierung I** |
|  |  |  |
| **Dokumentation Cisco Logdatei Analyse Programm** |  |  |
| Autoren: **Herr Philipp Dellwo**  **Frau Melissa Futtig** |  |  |
| Studiengang: **Bachelor of Science IT-Forensik/ Cybercrime** |  |  |
| Seminargruppe: **CC24w1-B** |  |  |
| Prüfer: **Herr Prof. Dirk Pawlaszczyk** |  |  |
| Einreichung: **Mittweida, 30.08.2025** |  |  |

Inhaltsverzeichnis

[1. Einleitung 4](#_Toc206147117)

[1.1 Zweck des Dokuments/ Aufgabenstellung 4](#_Toc206147118)

[1.2 Umfang des Programms 4](#_Toc206147119)

[1.3 Zielgruppe 5](#_Toc206147120)

[2. Grundlagen und Analyse 6](#_Toc206147121)

[2.1 SysLog-Protokoll 6](#_Toc206147122)

[2.2 Aufbau von Cisco Router-Logdateien 6](#_Toc206147123)

[3. Programmentwurf 7](#_Toc206147124)

[3.1 Diagramm/ Architektur des Programms 7](#_Toc206147125)

[3.2 Log-Einträge/ Filterkriterien 7](#_Toc206147126)

[3.3 Ausgabeformatierung 7](#_Toc206147127)

[4. Implementierung und Einrichtung 8](#_Toc206147128)

[4.1 Entwicklungsumgebung und Code-Struktur 8](#_Toc206147129)

[4.2 Installation, Kompilierung und Ausführung 8](#_Toc206147130)

[4.3 Bedienung 8](#_Toc206147131)

[5. Fazit 9](#_Toc206147132)

[5.1 Zusammenfassung 9](#_Toc206147133)

[5.2 Limitationen 9](#_Toc206147134)

# Einleitung

### Zweck des Dokuments/ Aufgabenstellung

Die Belegarbeit wird im Rahmen des Moduls „Programmierung I“ des Studiengang Bachelor of Science IT-Forensik/ Cybercrime erstellt.

Das Ziel ist die Erstellung, die erfolgreiche Implementierung und der Dokumentation eines Kommandozeilenprogramms, geschrieben in der Programmiersprache „C“. Dieses soll die Analyse von Cisco SysLog Router-Dateien ermöglichen.

Die Aufgabenstellung besteht darin, ein effizientes Tool zu entwickeln, das bestimmte Informationen, wie IP-Adressen, Zeitstempel und Ereignisbeschreibungen aus den Logdateien in eine separate Datei extrahiert und dem Nutzer Filteroptionen bietet, um eine zielgerichtete Auswertung zu erhalten.

### Umfang des Programms

In diesem Dokument wird sich mit einem Kommandozeilenprogramm befasst, das in der Sprache „C“ implementiert wurde und ohne grafische Benutzeroberfläche (GUI) auskommen soll.

Es ist darauf ausgelegt, Cisco SysLog Router-Dateien einzulesen und deren Inhalt zu parsen.

Das Programm enthält eine breite Palette an Filtermöglichkeiten, die es dem Nutzer ermöglicht, die Log-Einträge nach verschiedenen Kriterien zu durchsuchen und einzugrenzen.

Folgende Suchfunktionen sind implementiert:

* IP-Adresssuche (ipSuche(), ipFilterSucheEinfach())
* Zeitbereichsuche (zeitraum())
* Inhaltliche Suche (eigenerSuchbegriff())
* Benutzersuche (userSuche(), eigeneUserSuche())
* Severity Level Suche (severityLevel())
* Facility Suche (facilitySuche(), eigeneFacilitySuche())
* Mnemotics (mnemonicSuche(), eigeneMnemonicSuche())

### Zielgruppe

Zielgruppe dieses Projektes sind Personen, besonders jene mit einem praktischen Verständnis für die Programmierung von Analyse Tools und den effizienten Umgang mit großen Mengen an Logdaten. Weiterführend richtet sich das Programm an mögliche Netzwerkadministratoren und IT-Forensiker, die im Rahmen ihrer Tätigkeit Cisco Router SysLog-Dateien auswerten.

Im Zuge der Aufgabenstellung aus 1.1 richtet sich das Kommandozeilenprogramm an den Dozenten des Moduls Programmierung I und die Studierende des Studiengangs IT-Forensik/ Cybercrime der Hochschule Mittweida.

# Grundlagen und Analyse

### SysLog-Protokoll

Das Syslog-Protokoll ist ein Verfahren zur Übermittlung von System- und Ereignismeldungen in Rechnernetzen und wurde ursprünglich in den 1980er-Jahren im Rahmen des Sendmail-Projekts auf BSD-Unix entwickelt [1]. Es wird von einer Vielzahl an Betriebssystemen, Netzwerkkomponenten und Anwendungen unterstützt und ist im Bereich der Ereignisprotokollierung weit verbreitet [2].

Syslog wird in der Praxis vor allem für drei Aufgaben eingesetzt: Das zentrale Monitoring von Netzwerken und Systemen, die Fehlerdiagnose durch Sammlung und Auswertung von Ereignismeldungen und die IT-Sicherheitsüberwachung, etwa durch Korrelationsanalysen in Security Information and Event Management (SIEM)-Systemen [3].

Die Standardisierung des Protokolls erfolgt durch das Dokument RFC 5424 der Internet Engineering Task Force, das das ältere RFC 3164 ersetzt. Dieses RFC definiert den Nachrichtenaufbau, die zulässigen Felder sowie die Prioritäts- und Schweregrade [4].

Während RFC 5424 das Nachrichtenformat spezifiziert, beschreiben RFC 5426 (UDP) und RFC 5425 (TLS) die möglichen Transportvarianten [4] [5] [6].

Eine Syslog-Nachricht nach RFC 5424 setzt sich aus den vier folgenden logischen Komponenten zusammen: Die PRI (Priority) enthält die Priorität der Nachricht, gebildet aus der Kombination von Facility (Herkunft des Ereignisses, z. B. Kernel, Mail-System, Authentifizierung) und Severity-Level. Der Header enthält unter anderem Versionsnummer, Zeitstempel, Hostname, Applikationsname und Prozess-ID. Das Structured Data behinhaltet optionale strukturierte Zusatzinformationen in standardisiertem Format. In der letzten Komponente, MSG, steht der eigentliche Nachrichtentext.

Die Severity-Level reichen von 0 („Emergency“) bis 7 („Debug“) und dienen der Kategorisierung der Dringlichkeit. So können Ereignisse priorisiert und gefiltert werden [4].

Cisco-Router erzeugen Systemmeldungen im Syslog-kompatiblen Format und können diese an zentrale Syslog-Server weiterleiten [7]. Damit zeigen herstellerspezifische Implementierungen, dass sie auf dem Syslog-Standard aufsetzen und so eine einheitliche Ereignisprotokollierung ermöglichen.“

Auf den Aufbau von Cisco Router-Logdateien wird nachfolgend eingegangen.

### Aufbau von Cisco Router-Logdateien

Cisco SysLog-Dateien sind Protokolldateien, die in diesem Fall von Cisco Netzwerkgeräten, wie bspw. eines Routers oder Switches, automatisch erstellt werden. Diese enthalten, meist zeitlich geordnete Systemmeldungen, Ereignisse, Warnungen und Fehler, welche im Gesamten bestimmte Aktionen von Prozessen eines Computersystems mitschreiben.

Mit der Betrachtung einer beispielhaften Logging Nachricht aus einem Router Syslog, lässt sich folgendes Format aus Abbildung 1 betrachten:



Abbildung 1 Format Router SysLog-Datei

Eine Cisco IOS Syslog Nachricht teilt sich in grob fünf Bereiche auf: Zeitstempel, Facility, Severity Level, Mnemonic und der allgemeinen Beschreibung.

Der Zeitstempel, oft wie folgend aussehend, „\*Feb 14 09:40:10.326:“, gibt das Datum und die genaue Uhrzeit des jeweiligen Ereignisses an. Dabei kann es sein, dass die Nachricht anstatt mit eines „\*“, mit einer Nummer in Vergleichsoperatoren „<187>:“ beginnt. Das Beispiel hier bedeutet, dass am 14. Februar um 9:40 Uhr und 10.326 Sekunden ein Ereignis stattgefunden hat.

Das Facility, gibt die Subsystem- oder Prozessbezeichnung an, aus dem die Nachricht stammt. Es ist eine Art der internen Absendererkennung. In diesem Sinne zeigt „%LINEPROTO“ das momentane Line Protocol Subsystem an. Das Konzept der Facilities stammt ursprünglich aus UNIX-Systemen. Cisco hingegen verwendet eigene Bezeichnungen wie LINEPROTO, LINK, KERNEL usw., die auf die jeweiligen internen Module bzw. Prozesse verweisen.

# Programmentwurf

### Diagramm/ Architektur des Programms

### Ein Bild, das Entwurf, Zeichnung, Diagramm, Lineart enthält. KI-generierte Inhalte können fehlerhaft sein.

Abbildung 2 FlowChart Programmübersicht

Das in der Abbildung 2 dargestellte Diagramm stellt eine grobe Programmübersicht dar.

### Log-Einträge/ Filterkriterien

Nachfolgend werden die Log-Einträge/Filterkriterien erläutert. Zunächst ist zu erwähnen, dass durch den Benutzer ein beliebiger Suchbegriff eingegeben werden kann. Dabei durchsucht das Programm die gesamte Logdatei nach dem Vorkommen des eingegebenen Begriffs und gibt die entsprechenden Zeilen aus.

Weiter ist es möglich, mit dem Zeitraumfilter Logeinträge zeitlich einzugrenzen. Zur Verfügung stehen die Optionen, Meldungen ab einem bestimmten Zeitpunkt, bis zu einem Zeitpunkt oder innerhalb eines definierten Zeitintervalls auszugeben. Dies erleichtert die Analyse von Ereignissen, die zu einem konkreten Zeitpunkt auftraten.

Außerdem wurde eine IP-Adresssuche implementiert, die mehrere Varianten bietet: Der Benutzer kann eine bestimmte IPv4-Adresse manuell eingegeben oder automatisch nach privaten bzw. öffentlichen IP-Adressen filtern.

Über den Facility-Filter kann nach dem Subsystem gesucht werden, aus dem die Meldung stammt (z. B. LINK, STP, DHCP). Hier ist sowohl eine manuelle Eingabe eines Facility-Namens als auch die Auswahl aus allen in der entsprechenden Datei befindlichen Facilities möglich.

Es ist ebenfalls möglich nach Benutzernamen (User) zu filtern. Dabei unterstützt das Programm sowohl die direkte Eingabe eines Namens als auch die Anzeige aller im Log enthaltenen User mit anschließender Auswahl. Auf diese Weise lassen sich Aktivitäten bestimmter Benutzer nachvollziehen.

Das Mnemonic-Filterkriterium ermöglicht die Suche nach den Kennungen für Ereignisse (z. B. CONFIG\_I, UPDOWN). Analog zur Facility-Suche und der Suche nach Usern ist eine freie Eingabe und die Auswahl aus allen im Log enthaltenen Mnemonics möglich.

Letztlich erlaubt der Severity-Level-Filter die Eingrenzung nach Schweregrad einer Fehlermeldung, indem der entsprechende Schweregrad ausgewählt wird. So können besonders kritische Meldungen schnell isoliert betrachtet, während weniger wichtige Einträge ausgeblendet werden.

Damit deckt das Programm die wichtigsten Bestandteile zur Auswertung von Cisco-Syslogs ab.

### Ausgabeformatierung

Die Ausgabe der Ergebnisse erfolgt über die Konsole. Jeder gefundene Logeintrag wird in seiner ursprünglichen Form dargestellt und zusätzlich mit der entsprechenden Zeilennummer versehen. Dies ermöglicht eine Nachvollziehbarkeit innerhalb der ursprünglichen Logdatei.

Nach Abschluss einer Suche erfolgt eine zusammenfassende Darstellung. Dabei wird entweder die Gesamtanzahl der gefundenen Treffer angegeben oder es wird explizit darauf hingewiesen, dass keine passenden Logeinträge vorhanden sind. Auf diese Weise wird der Benutzer über das Ergebnis der jeweiligen Suche/Filterung informiert.

Außerdem wurde implementiert, dass bei einer fehlerhaften Eingabe entsprechende Meldungen an den Benutzer erfolgen. Zur besseren Lesbarkeit und Unterstreichung der Bedeutsamkeit dieser wird eine farbliche Hervorhebung eingesetzt. Kritische Meldungen und Fehlermeldungen werden rot markiert, während Warnungen in gelber Schrift erscheinen. Normale Meldungen verbleiben in der Standardfarbe. Diese farbliche Differenzierung erleichtert eine schnelle visuelle Einordnung und Bewertung der Ergebnisse.

Darüber hinaus besteht die Möglichkeit, die Ergebnisse in einer Ausgabedatei (*Suchergebnisse.txt*) zu speichern. Die gespeicherten Treffer werden dort im gleichen Format wie in der Konsole abgelegt.

Nach jeder Suche/Filterung wird der Benutzer zudem aufgefordert, über das weitere Vorgehen zu entscheiden. Dabei kann Suche wiederholt werden, ins Hauptmenü zurückgekehrt werden oder das Programm beendet werden.

# Implementierung und Einrichtung

### Entwicklungsumgebung und Code-Struktur

### Installation, Kompilierung und Ausführung

#### 4.2.1 Schritte zur Einrichtung

### Bedienung

# Fazit

### Zusammenfassung

### Limitationen

### Literaturverzeichnis

[1] C. Lonvick, "The BSD Syslog Protocol," RFC 3164, Internet Engineering Task Force, Aug. 2001. [Online]. Available: <https://datatracker.ietf.org/doc/html/rfc3164> [Accessed: 17-Aug-2025].

[2] J. Zhou, Y. Qian, Q. Zou, P. Liu and J. Xiang, "DeepSyslog: Deep Anomaly Detection on Syslog Using Sentence Embedding and Metadata," in *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 3051-3061, 2022, doi: 10.1109/TIFS.2022.3201379.

[3] K. Kent and M. Souppaya, Guide to Computer Security Log Management,

NIST Special Publication 800-92, Sep. 2006. [Online].

Available: <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-92.pdf> [Accessed: 17-Aug-2025].

[4] R. Gerhards, "The Syslog Protocol," RFC 5424, Internet Engineering Task Force, Mar. 2009. [Online]. Available: <https://datatracker.ietf.org/doc/html/rfc5424> [Accessed: 17-Aug-2025].

[5] A. Okmianski, "Transmission of Syslog Messages over UDP," RFC 5426, Internet Engineering Task Force, Mar. 2009. [Online]. Available: <https://datatracker.ietf.org/doc/html/rfc5426> [Accessed: 17-Aug-2025].

[6] M. Miao and Y. Ma, "Transport Layer Security (TLS) Transport Mapping for Syslog," RFC 5425, Internet Engineering Task Force, Mar. 2009. [Online]. Available: <https://datatracker.ietf.org/doc/html/rfc5425> [Accessed: 17-Aug-2025].

[7] Cisco Systems, “System Message Logging,” Cisco Documentation, Mar. 11, 2008. [Online]. Available: <https://www.cisco.com/c/en/us/td/docs/routers/access/wireless/software/guide/SysMsgLogging.html>. [Accessed: 17-Aug-2025].