

| TFTP

TFTP (Trivial File Transfer Protocol) ist ein einfaches Protokoll, das es Netzwerkgeräten ermöglicht, Dateien über das Netzwerk zu übertragen. Es ist eine schlanke Version des FTP (File Transfer Protocol) und wird häufig verwendet, um kleine Dateien wie Router-Konfigurationsdateien zu übertragen.

Es ist eine Client-Server-Anwendung, bei der Clients Anfragen an einen Server senden, um Dateien zu erhalten. Der Server überträgt dann die Datei über das Netzwerk an den Client. Es ist ein einfaches, leichtes Protokoll, das eine einfache und zuverlässige Dateiübertragung ermöglicht. TFTP wird häufig zum Herunterladen und Hochladen kleiner Dateien wie Router-Konfigurationsdateien, Firmware-Updates und Log-Dateien verwendet. Es ist auch eine beliebte Wahl für die Übertragung von Boot-Images und anderen Systemdateien auf Netzwerkgeräte.

Das Protokoll stösst aber an seine Grenzen, wenn es um große Dateien geht. Es kann zwar für große Dateien verwendet werden, aber da es langsam und ineffizient sein kann ist es nicht die beste Wahl hierfür. Für Netzwerkadministratoren hingegen ist TFTP ein leistungsstarkes Tool, um Systeme zu konfigurieren und zu administrieren und ist eine gute Wahl für die Übertragung kleiner Dateien. Es ist leicht zu implementieren und hat eine sehr geringe Netzerklastung.

In der Einfachheit von TFTP liegen auch einige Nachteile, so weiss das Protokoll beispielsweise keine Benutzerauthentifizierung auf. Somit können Dateien, welche von einem TFTP-Server zur Verfügung gestellt werden, von jedem TFTP-Client uneingeschränkt geladen werden. Auch kann mit TFTP nicht durch Verzeichnisse navigiert werden und es ist nicht möglich, die Dateien und Verzeichnisse mit speziellen Lese- und Schreibberechtigungen auszustatten.

Vorbereitung.

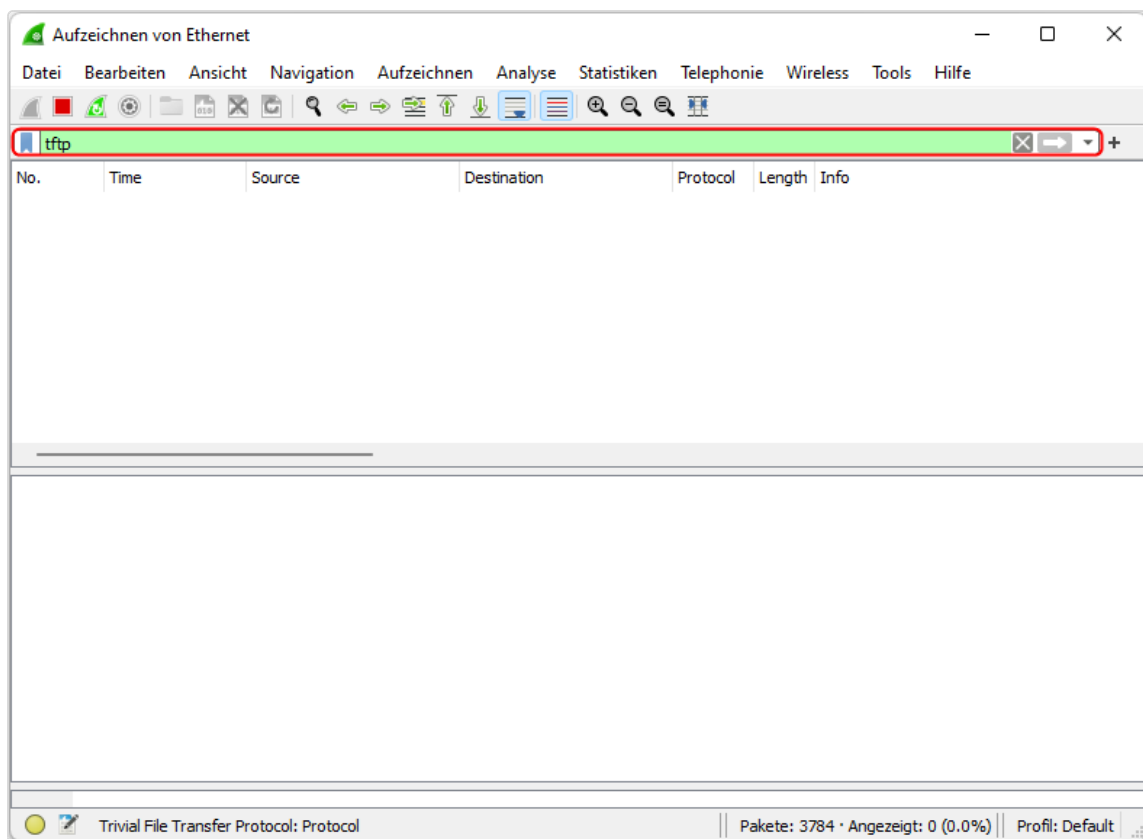
1. Laden Sie die Software Wireshark herunter: <https://www.wireshark.org/download.html>
(Windows Installer)
2. Installieren Sie Wireshark
3. Laden Sie die Software pumpKIN TFTP Client herunter: <https://kin.klever.net/pumpkin/binaries/>
(pumpkin-2.7.3.exe)
4. Installieren Sie die Software pumpKIN TFTP Client.

Download einer Datei

Machen Sie sich als erstes mit der Software Wireshark vertraut. Hierzu stehen folgende Ressourcen bereit:

- <https://www.youtube.com/watch?v=yn3yzFDub1E> (ca 10 Minuten)
- <https://de.wikipedia.org/wiki/Wireshark> (Grobe Übersicht)
- <https://www.computerbild.de/artikel/cb-Tipps-Software-Wireshark-Anleitung-um-Netzwerkverkehr-zu-analysieren-erste-Schritte-32362313.html>

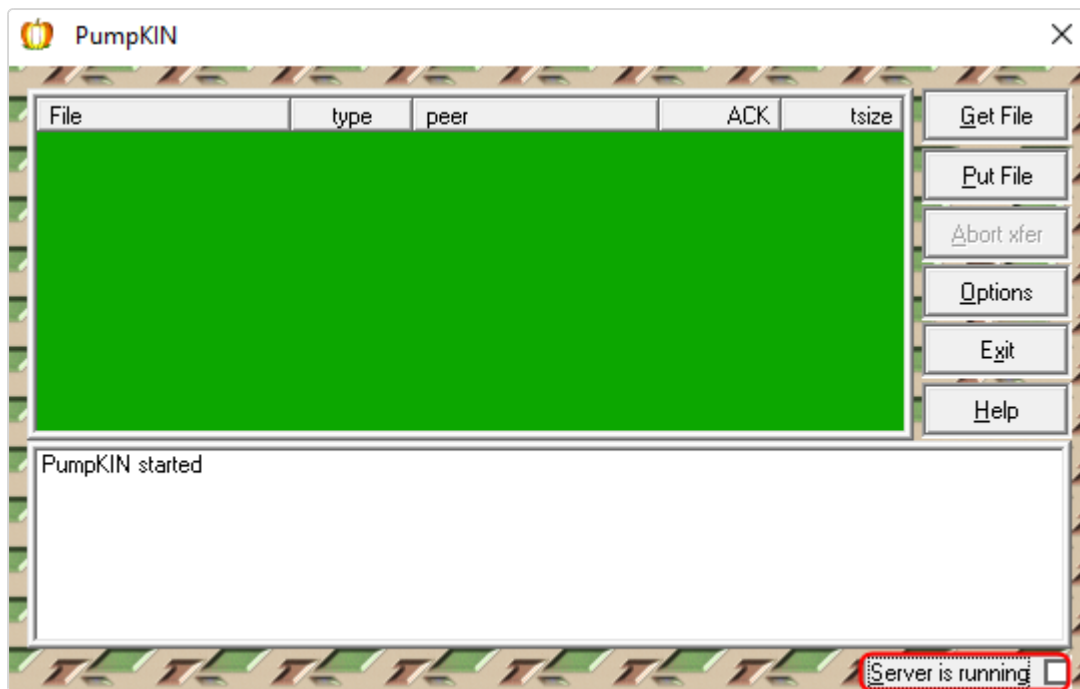
1. Starten Sie nun die Software Wireshark. Wählen Sie als Schnittstelle Ihr WLAN-Adapter aus.
2. Sie sehen nun den ganzen Traffic aller Datenpakete. Uns interessieren aber nur TFTP-Datenpakete. Aus diesem Grund setzen Sie als erstes einen Filter. Für TFTP-Pakete gibt es bereits einen vorgefertigten Filter **tftp**. Tragen Sie diesen in der Filtereingabe ein:



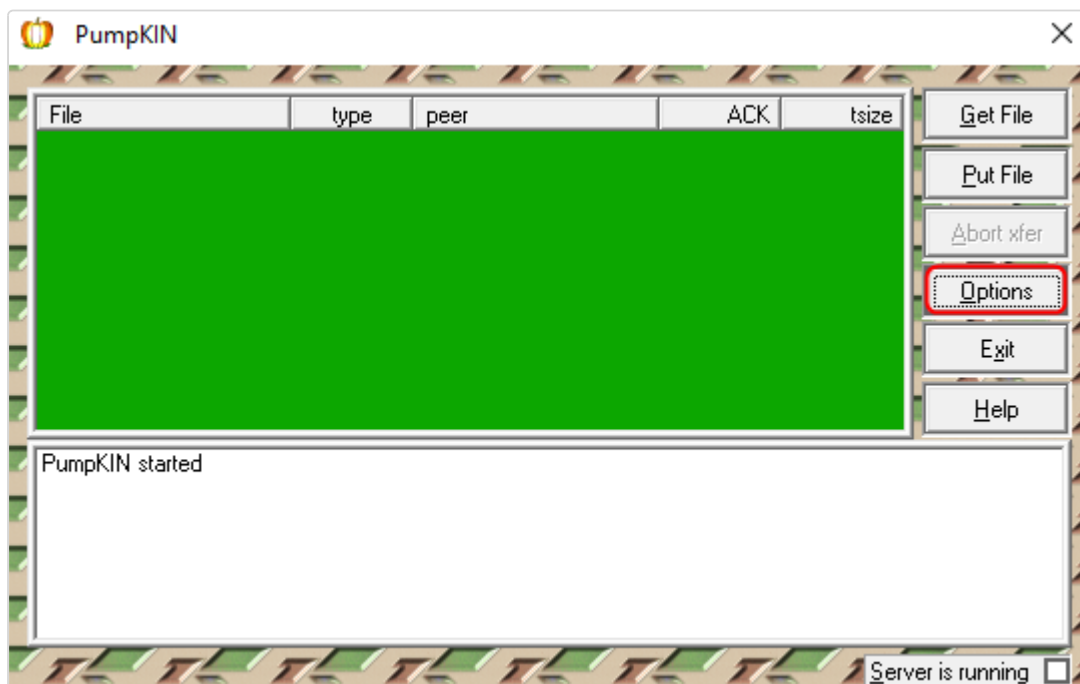
3. Nun sollten Sie keinen anderen Traffic mehr sehen, ausser TFTP-Pakete. Da noch keine versendet wurden, ist die Anzeige dementsprechend leer.
4. Starten Sie nun die Software pumpKIN. Hierbei handelt es sich um eine Software, welche gleichzeitig als TFTP-Server und TFTP-Client fungieren kann. Als erstes werden Sie die reine TFTP-Client Funktion untersuchen.

! Bei der ersten Verwendung müssen Sie die Windows Defender Meldung zulassen !

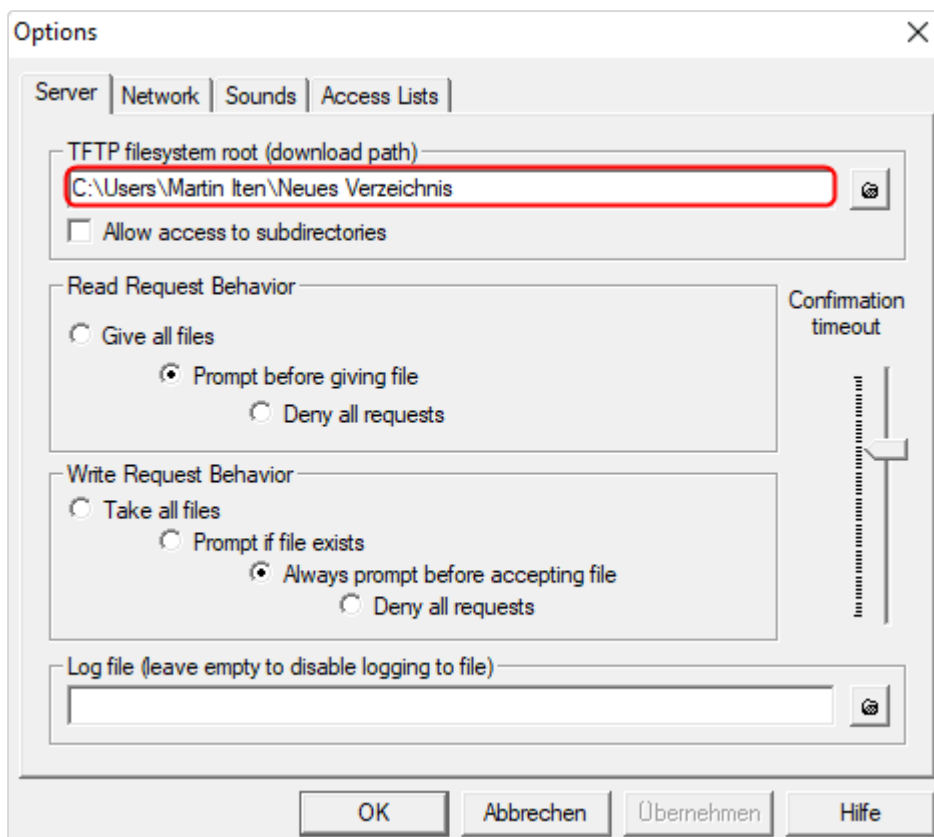
Stellen Sie hierzu sicher, dass die Option **Server is running** deaktiviert ist (Haken entfernen)



5. Nun setzen Sie das Arbeitsverzeichnis des Clients über **Options**:

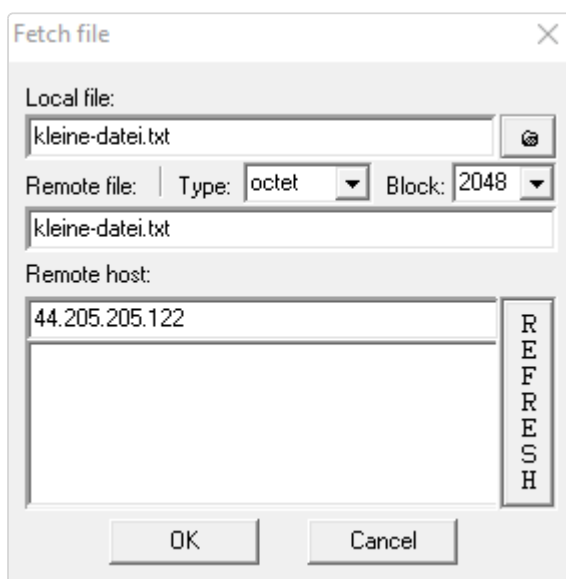


Und dann **TFTP filesystem root (download path)**. Erstellen Sie hier am besten ein neues Verzeichnis und wählen Sie dieses dann in der Einstellung aus:



Bestätigen Sie anschliessend mit **OK**.

6. Nun geht es darum, eine Datei von einem TFTP-Server herunterzuladen. Der TFTP-Client pumpKIN bietet hierzu die Option **GET File**. Verwenden Sie als TFTP-Server den Remote host **44.205.205.122** und als gewünschte Datei zum herunterladen unter **Remote file** die **kleine-datei.txt**



Bestätigen Sie mit **OK**.

7. Der Download sollte nun erfolgen. Prüfen Sie, ob Sie die Datei sehen.

Aufgabe 1: Prüfen Sie nun Wireshark. Es sollen jetzt Datenpakete ersichtlich sein. Jede Zeile entspricht hierbei einem Datenpaket. Erinnern Sie sich an die DHCP-Theorie. Dort gab es auch verschiedenen Datenpakete, welche zwischen Server und Client ausgetauscht wurden. Bei TFTP ist dies nicht anders.

Frage: Wie viele Datenpakete sind nun im Wireshark vorhanden?

Es sollten 5 Datenpakete vorhanden sein.

Aufgabe 2: Identifizieren Sie den Typ dieser TFTP-Datenpakete. Schauen Sie hierzu in welche Richtung das Paket versendet wurde (Source, Destination) und was dieses in etwa enthält (Info).

Datenpaket 1: Client -> Server, Read Request für die Datei kleine-datei.txt

Datenpaket 2: Server -> Client, Option Acknowledge

Datenpaket 3: Client -> Server, Acknowledgement für Block 0

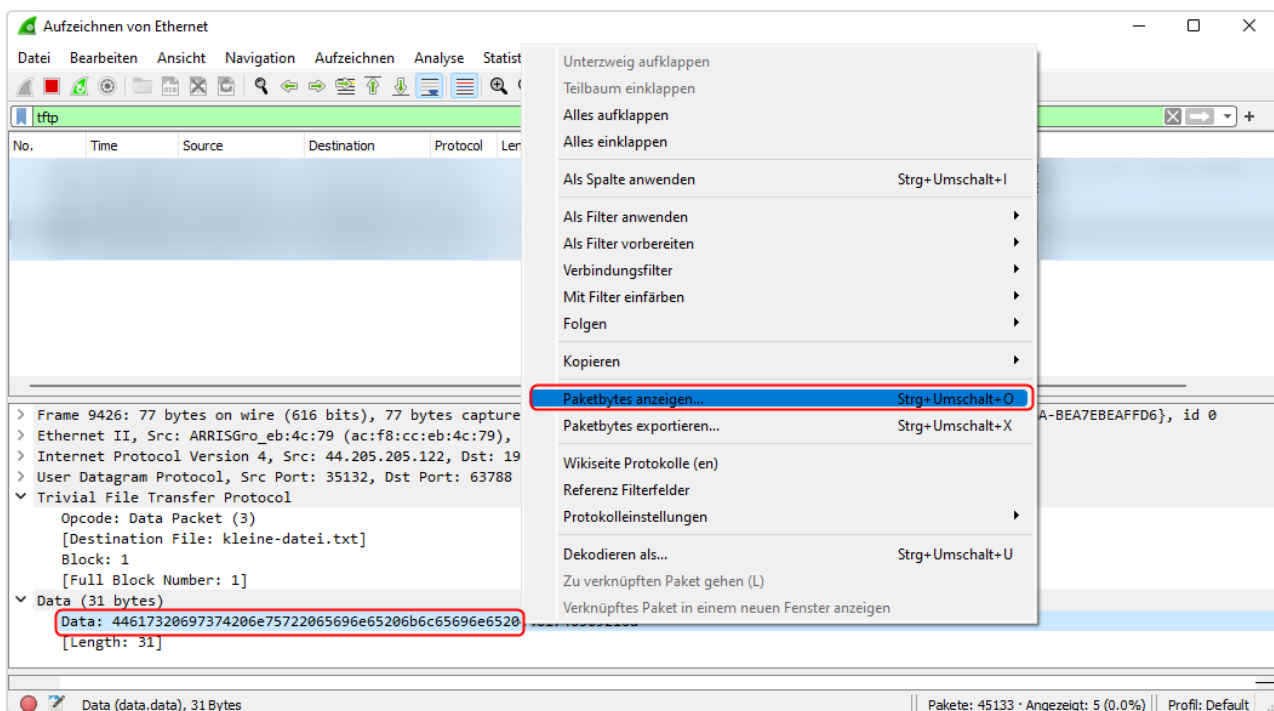
Datenpaket 4: Server -> Client, Data Packet Block 1

Datenpaket 5: Client -> Server, Acknowledgement Block 1

Frage: In welchem Datenpaket werden vermutlich die Daten übertragen?

Im 4. Datenpaket mit dem Typ Data Packet

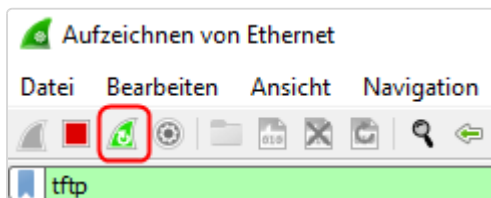
Klicken Sie nun auf das Datenpaket wo die Daten übertragen wurden. Klappen Sie im Baum das Feld Data aus und machen Sie einen Rechtsklick auf den Data-Wert (44617320.....). Wählen Sie hier die Option Paketbytes anzeigen:



Frage: Was zeigt Ihnen Wireshark nun an?

Es werden die übertragenen Daten angezeigt.

Auftrag: Leeren Sie nun die aufgezeichneten Datenpakete, indem Sie die Aufzeichnung neu starten:



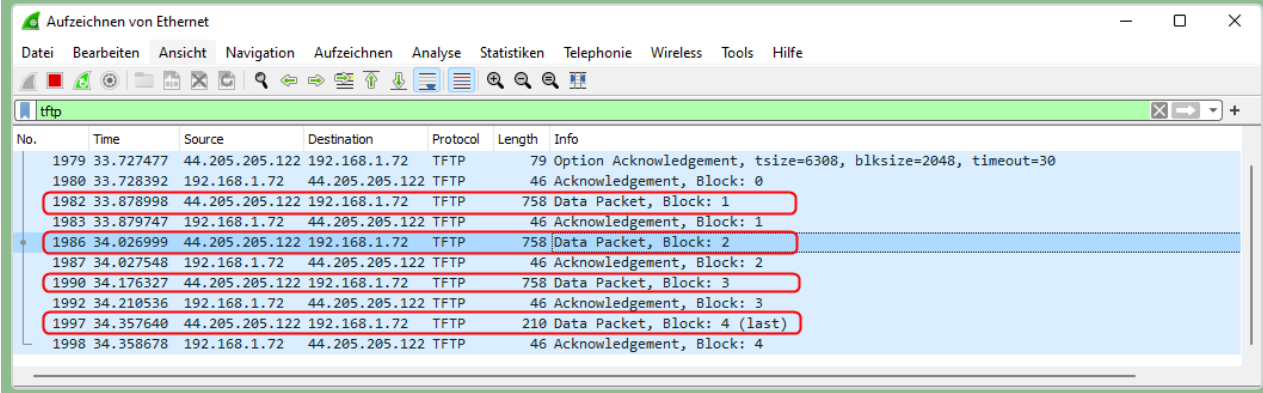
Speichern Sie die bisher aufgezeichneten Daten, so dass Sie diese später wieder finden.

Führen Sie nun vom selben TFTP-Server einen Download der Datei **grosse-datei.txt** durch. Prüfen Sie nun, ob sich etwas verändert hat im Vergleich zur kleineren Datei.

Tipp: Sie können nun die Aufgezeichnete Wireshark-Datei separat öffnen um beide Aufzeichnungen miteinander zu vergleichen. Setzen Sie wieder den Filter **tftp** um nur die relevanten Datenpakete zu sehen.

Frage: Was hat sich verändert?

Die Daten werden in vier Blöcken übertragen.



No.	Time	Source	Destination	Protocol	Length	Info
1979	33.727477	44.205.205.122	192.168.1.72	TFTP	79	Option Acknowledgement, tsize=6308, blksize=2048, timeout=30
1980	33.728392	192.168.1.72	44.205.205.122	TFTP	46	Acknowledgement, Block: 0
1982	33.878998	44.205.205.122	192.168.1.72	TFTP	758	Data Packet, Block: 1
1983	33.879747	192.168.1.72	44.205.205.122	TFTP	46	Acknowledgement, Block: 1
1986	34.026999	44.205.205.122	192.168.1.72	TFTP	758	Data Packet, Block: 2
1987	34.027548	192.168.1.72	44.205.205.122	TFTP	46	Acknowledgement, Block: 2
1990	34.176327	44.205.205.122	192.168.1.72	TFTP	758	Data Packet, Block: 3
1992	34.210536	192.168.1.72	44.205.205.122	TFTP	46	Acknowledgement, Block: 3
1997	34.357640	44.205.205.122	192.168.1.72	TFTP	210	Data Packet, Block: 4 (last)
1998	34.358678	192.168.1.72	44.205.205.122	TFTP	46	Acknowledgement, Block: 4

Frage: Was ist nun Ihre Schlussfolgerung daraus?

Grosse Dateien werden von TFTP in mehrere Blöcke aufgeteilt und übertragen.

Frage: Können Sie anhand der aufgezeichneten ableiten wie gross ein Block bei der Übertragung sein darf bevor er aufgeteilt wird?

Tipp: Vergleichen Sie die vier Blöcke. Die Grösse der Datei ist so gewählt, dass die Grösse des letzten Blocks nicht ausgeschöpft wird und somit kleiner als möglich übertragen wird.

Die Grösse beträgt 2048 Bytes. Dies wird ersichtlich wenn man in den Daten Packets den Wert **Length** vergleicht. Dieser ist überall auf 2048 Bytes gesetzt nur beim letzten Block ist dieser kleiner.

Zusatzinfo: Werden die Length aller 4 Datenpakete zusammengezählt, erhält man die Grösse der heruntergeladenen Datei.

Frage: Untersuchen Sie den TFTP-Client dahingehend ob es eine Möglichkeit gibt, zu prüfen was für Dateien auf dem TFTP-Server sonst noch abgelegt sind.

Nein. Es gibt keine weiteren Möglichkeiten.

Frage: Was bedeutet dies für Sie als TFTP-Anwender?

Es müssen alle Dateien vollständig bekannt sein, welche heruntergeladen werden möchten.

Revision #4

Created 20 December 2022 22:00:49 by Admin

Updated 12 January 2023 00:40:09 by Admin