Thema Internet of Things

Studiengang Digitale Forensik
Ausarbeitung im Rahmen des Modul 108

Markus Stoll

Datum 07.07.2017

Inhaltsverzeichnis

1 Theoretischer Teil 3
1.1 Internet of Things 3
1.1.1 SmartHome 3
1.1.1.1 Anwendungsbeispiele 4
1.1.1.2 Kommunikation per BUS-Kabel oder Funk 4
1.1.2 ZigBee 5
1.1.3 Z-Wave 5
1.1.4 HomeMatic 5
1.2 Funkprotokolle 6
1.2.1 Übersicht 6
1.2.2 Gemeinsamkeiten / Unterschiede 6
1.2.3 ZigBee Protokoll 7
1.2.3.1 Protokoll Stack 7
1.2.3.2 Protokoll Frame 8
1.2.3.3 Sicherheit 8
1.2.4 Z-Wave Protokoll 9
1.2.4.1 Protokoll Stack 9
1.2.4.2 Protokoll Frame 10
1.2.4.3 Sicherheit 10
1.2.5 HomeMotion (BidCos) Protokoll 10
1.3 Sicherheitsaspekte 11
1.3.1 ZigBee 11
1.3.1.1 Physical & MAC Layer 11
1.3.1.2 Übersicht der Profile 11
1.3.1.3 home automation profile 11
1.3.1.4 master key „ZigBeeAlliance09“ 11
1.3.1.5 installation code 11
1.3.1.6 application link key 12
1.3.1.7 rejoin mit dem Trust Center 12
1.3.2 Z-Wave 12
1.3.3 Herausforderungen für die Forensik 12
1.3.3.1 Hardware 12
1.3.3.2 Software 12
1.4 Exkurs - Gerätekommunikation mit den Herstellern 13
2 Praktischer Teil 14
2.1 Grundlegendes 14
2.1.1 Start des FHEM Server 14
2.1.2 Konfigurationsdatei fhem.cfg 15
2.1.2.1 Daten aus forensischer Sicht 15
2.1.2.2 Dateiname und Pfad 15
2.1.2.3 Verwendete Logdateien und SQL Datenbank 16
2.1.2.4 Verwendete Aktoren/Sensoren und Räume 18
2.1.2.5 Automatische Ereignisse zu bestimmten Zeitpunkten 18
2.1.2.6 Verwendete Benutzer und Zugangsarten 18
2.1.3 Inhalt der Logdateien 19
2.2 Forensische Auswertungen 20
2.2.1 Übersicht der Vorgehensweise 20
2.2.2 Sichern der Daten 21
2.2.2.1 Konfigurationsdatei 21
2.2.2.2 Logdateien und SQL Datenbank 22
2.2.3 Aussagen der Daten 23

1 Theoretischer Teil

1.1 Internet of Things

Das Internet of Things (IoT, Internet der Dinge) bezeichnet die zunehmende Vernetzung von Geräten und Sensoren. Unter Experten ist es unstrittig, dass das IoT unsere Art des Wirtschaftens, aber auch unser tägliches Leben - Stichwort: Smart City, Smart Home - revolutionieren wird. Eng mit IoT verbunden sind Themen wie ***connected cars*** oder ***wearables***.

Bereits im Jahr 1991 beschrieb der US-amerikanische Informatikwissenschaftler Mark Weiser in seinem Aufsatz "The Computer for the 21st Century" die Idee, dass zukünftig über das Internet verknüpfte Gegenstände quasi unmerklich und im Hintergrund den Menschen unterstützen, ohne selbst - wie etwa der Computer - Aufmerksamkeit auf sich zu lenken.

Erstmals 1999 wurde der Begriff “Internet of Things” von Kevin Ashton, einem britischen Technologie-Pionier, verwendet. Seitdem arbeiten Wissenschaftler an der Umsetzung seiner Vision eines “allgegenwärtigen Computereinsatzes”.

1.1.1 SmartHome

Bild: http://www.ebuyer.com/blog/2015/01/a-day-with-the-internet-of-things/

Smart Home dient als Oberbegriff für technische Verfahren und Systeme in Wohnräumen und -häusern, in deren Mittelpunkt eine Erhöhung von Wohn- und Lebensqualität, Sicherheit und effizienter Energienutzung auf Basis vernetzter und fernsteuerbarer Geräte und Installationen sowie automatisierbarer Abläufe steht

Smart Home hilft dabei, den Alltag komfortabler zu gestalten, indem es uns viele Steuer- und Überwachungstätigkeiten abnimmt. Gleichzeitig hilft ein klug vernetztes Zuhause dabei Strom zu sparen.

1.1.1.1 Anwendungsbeispiele

- **Heizungssteuerung**

Smarte Thermostate regeln die Wärme automatisch, basierend auf vordefinierten Programmen und lassen sich trotzdem jederzeit individuell regulieren.

- **Sicherheit**

Sensoren für Tür- und Fensterkontakte, Bewegungsmelder, Überwachungskameras, Feuermelder, Feuchtigkeits- und Wassersensoren.

1.1.1.2 Kommunikation per BUS-Kabel oder Funk

Damit ein Taster für eine Lichtszene oder ein Temperatursensor mit einem Aktor kommunizieren kann, benötigt man ein Medium für die Datenübertragung. Das kann in einem neuen Haus komplett mit der elektrischen Verdrahtung (BUS-Kabel, CAT 7 Kabel) übermittelt werden oder, vor allem für Nachrüster interessant, per Funk.

Die meisten Anbieter von Funksystemen für das SmartHome nutzen die Frequenzen im Bereich 434 MHz oder 868 MHz, weil die Nutzung lizenzkostenfrei ist. Dafür gibt es von Seiten der Bundesnetzagentur strenge Auflagen. Diese Frequenzbereiche sind Teil der sogenannten ISM-Bänder (Industrial, Scientific, Medical). Anwendungen aus der Industrie, der Wissenschaft, der Medizin und der Gebäudeautomation teilen sich die Bänder.

- **Proprietäre Funksysteme**

Sind geistiges Eigentum nur eines Anbieters. Als Kunde ist man darauf angewiesen, dass dieser Hersteller alles das bietet, was man möchte, und man muss das Vertrauen haben, dass dieser Hersteller seine Produkte auch noch in etlichen Jahren anbietet, falls man Ersatzteile benötigt oder ausbauen möchte.

Beispiel: HomeMatic (BidCoS)

- **Offene Funksysteme**

Für Funksysteme, die auf veröffentlichten Standards basieren, bieten viele Hersteller kompatible Produkte an. Das Angebot ist deshalb in der Regel breiter und die Langzeitliefersicherheit größer.

Beispiel: ZigBee

1.1.2 ZigBee

In der ZigBee Allianz haben sich namhafte Unternehmen zusammengeschlossen und die Industrie-Vernetzung, ebenso wie die Gebäudesteuerung und die Steuerung von Haushaltsgeräten zu vernetzen. Zu den Gründungsmitgliedern der ZigBee-Allianz gehören u.a. Atmel, Honeywell, Invensys, Mitsubishi, Motorola, NXP und Philips.

Daneben sind noch diverse Halbleiter-, Datenfunktechnik- und OEM-Hersteller als normale Mitglieder in der ZigBee-Allianz vertreten.

1.1.3 Z-Wave

Z-Wave ist ein internationaler Funkstandard, der von der Firma Sigma Designs und von der Z-Wave Alliance für die Hausautomatisierung entwickelt wurde. So können Produkte unterschiedlicher Hersteller miteinander vernetzt und gesteuert werden. Allerdings ist zu beachten, dass nicht jede Z-Wave funkende Zentrale auch alle Z-Wave funkenden Produkte einbinden kann. Die Kompatibilität hängt von den Herstellern ab. Zurzeit sind mehr als 1.300 Produkte aus allen Bereichen der Hausautomatisierung mit Z-Wave versehen.

Die verschiedenen Hersteller spezifizieren und entwickeln ihre Produkte auf Basis eines Z-Wave-System-on-a-Chip-ASICs (SOC). Dieser wird von der Firma Sigma Designs und als Lizenznehmer ebenfalls von der Firma Mitsumi angeboten.

Unter anderen sind die Unternehmen Deutsche Telekom, BOSCH, D-Link, Nokia und Samsung als „Full Member“ eingetragen.

1.1.4 HomeMatic

HomeMatic ist ein proprietäres System zur Hausautomation von der Firma eQ-3. Chronologisch kann man es als Nachfolgesystem von FS-20 sehen. Beide Systeme sind nicht direkt kompatibel, jedoch kann mittels Dritthersteller-Lösungen (IP-Symcon, homeputer) ein Mischbetrieb gewährleistet werden. Für die drahtlose Übertragung wird ein Funkprotokoll namens BidCos verwendet.

1.2 Funkprotokolle

1.2.1 Übersicht

Die Frequenzen sind Länderabhängig. Die untenstehenden sind für Europa.

	ZigBee	**Z-Wave**	**Homematic (BidCoS)**
offen	Ja	Nein	Nein
Frequenzbereich	868 MHz 2,4 Ghz	868 MHz	868 MHz
Verschlüsselung	AES-128	Nur Schließsysteme AES-128	Signatur AES-128
Mesh Network	Ja	Ja	Nein
Bidirektional	Nein	Nein	Ja
Batterielos	Ja	Nein	Nein
Brutto Datenrate	250 kb/s	9,6 – 40 kb/s	9,6 kb/s
Reichweite	75 m	150 m	200 m

1.2.2 Gemeinsamkeiten / Unterschiede

- **Frequenzbereich**

Alle drei Funkprotokolle verwenden den Frequenzbereich 868 MHz. Wobei ZigBee auch den Bereich 2,4 Ghz verwenden kann.

- **Verschlüsselung**

Die Verschlüsselung AES-128 Bit wird von allen drei Funkprotokollen verwendet. Ausschließlich im ZigBee Protokoll ist jede Nachricht komplett verschlüsselt.

Beim Homematic-Protokoll wird jedoch nur die Signatur mit AES-128 verschlüsselt, die Nutzinhalte sind XOR Codiert.

Das Z-Wave Protokoll verwendet die Verschlüsselung nur in Schließsystemen.

- **Mesh Network**

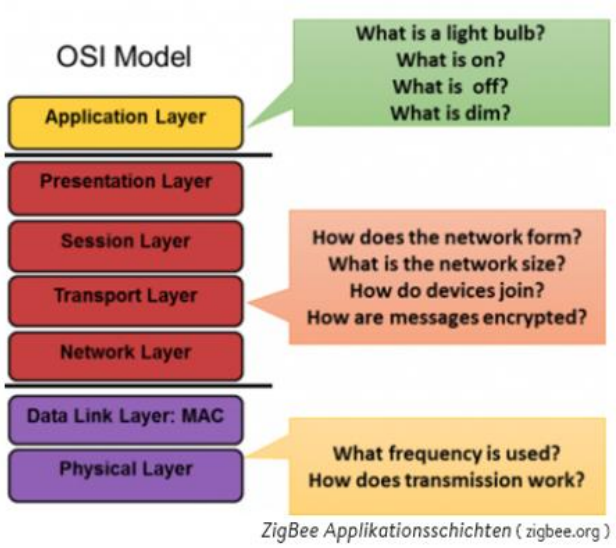
ZigBee und Z-Wave sind als Mesh Network implementiert. In einem Mesh Network ist jeder Netzwerkknoten mit einem oder mehreren anderen verbunden. Die Informationen werden von Knoten zu Knoten weitergereicht, bis sie das Ziel erreichen.

- **Bidirektional**

Eine bidirektionale Kommunikation zwischen Endgerät und Zentrale findet ausschließlich im Funkprotokoll Homematic statt.

1.2.3 ZigBee Protokoll

1.2.3.1 Protokoll Stack



ZigBee Applikationsschichten (zigbee.org)

Physical & MAC Layer (auf Basis dem Standard IEEE 802.15.4)

Die Basisschicht bestimmt Funktionen zum Funkablauf. Hier wird die Frequenz, mit der das Protokoll sendet, sowie die Übertragungsform der Datenpakete festgelegt.

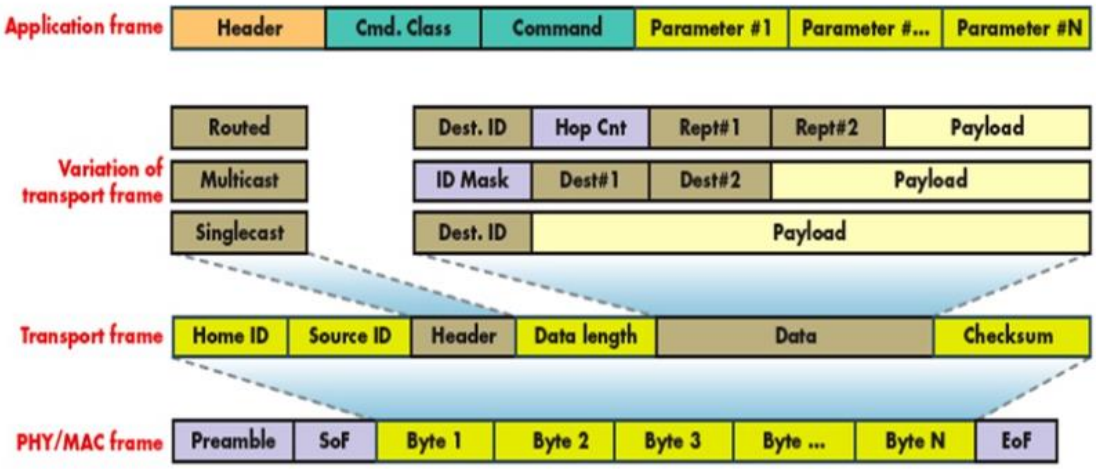
Networklayer bis Presentation Layer

Das Stack Feature Set enthält die Schichten vom Network bis zum Presentation Layer, die Form und Größe des Netzwerks definieren und regeln, wie Geräte beitreten können oder Daten verschlüsselt werden.

Application Layer

Die Applikationsprofile werden über Richtlinien und Arbeitsgruppen der ZigBee-Allianz (etwa Home Automation, Building Automation oder Energy Saving) je nach Einsatzzweck definiert. Für ein auf Lichtsteuerung ausgerichtetes Profil legt die Applikationsschicht spezifische Einstellungen wie An-/Aus-Status oder Dimmen verschiedener Empfänger fest.

1.2.3.2 Protokoll Frame



Der Transport Frame ist abhängig von dem Modus in dem der Teilnehmer betrieben wird.

1.2.3.3 Sicherheit

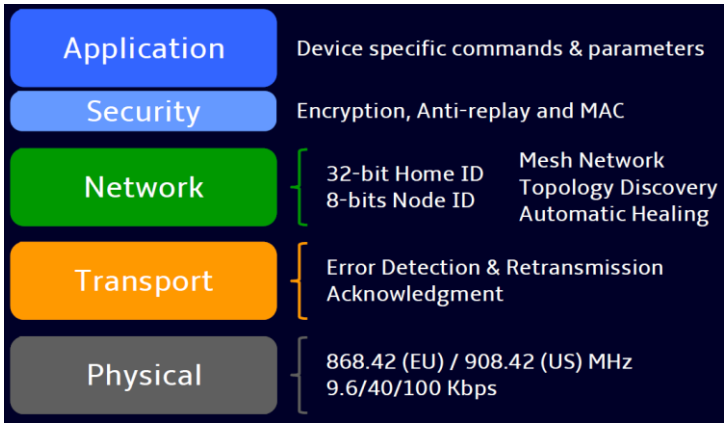
Das ZigBee Protocol setzt auf dem Standard IEEE 802.15.4 auf. Dieser Implementiert die beiden untersten Schichten im OSI-Modell, den Physical und Data Link Layer.

Der Standard IEEE 802.15.4 bietet Sicherheitsmaßnahmen auf MAC-Ebene durch Message-Integrity-Check und symmetrische Verschlüsselung. Es kann zwischen mehreren Verfahren gewählt werden, die auf CCM und AES basieren. Die Schlüssel werden durch die darüberliegende Schicht festgelegt und anschließend durch den MAC-Layer verwaltet. Die Verschlüsselung wird für jeden Kommunikationspartner separat festgelegt und automatisch vom MAC-Layer angewendet.

1.2.4 Z-Wave Protokoll

1.2.4.1 Protokoll Stack

Quelle: https://www.itu.int/rec/T-REC-G.9959-201202-S/en
https://cybergibbons.com/wp-content/uploads/2014/11/honeyimhome-131001042426-phpapp01.pdf



Physical & MAC Layer (auf Basis dem Standard ITU-T G.9959)

Wie beim ZigBee Protokoll bestimmt die Basisschicht Funktionen zum Funkablauf. Hier wird die Frequenz, mit der das Protokoll sendet, sowie die Übertragungsform der Datenpakete festgelegt.

Transport Layer

Fehlerbehandlung und Acknowledgment sind im Transport Layer implementiert.

Network Layer

Der network layer verwaltet die eindeutige 32-bit ID für den Home Controller und die 8 Bit große Teilnehmer ID.

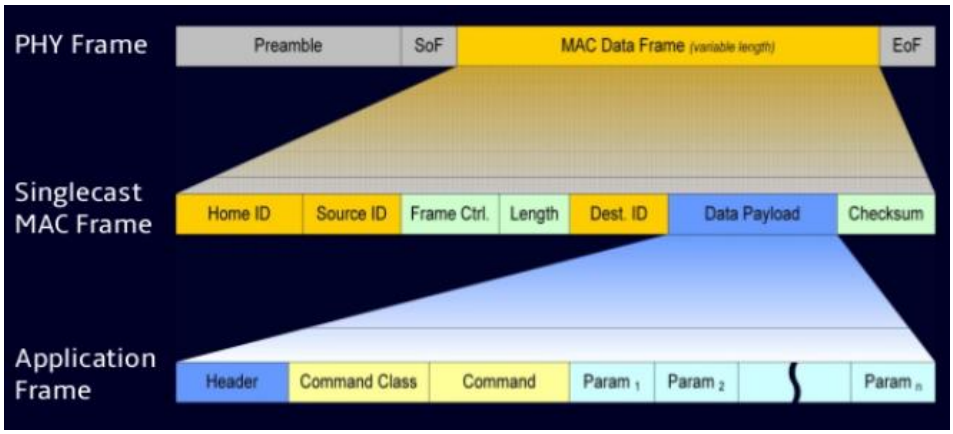
Security Layer

Implementierung der Verschlüsselung und Sicherheitsmechanismen. Werden von den einzelnen Herstellern selbst implementiert.

Application Layer

Im Application Layer sind Commands und Parameter abhängig vom Gerät und Hersteller implementiert.

1.2.4.2 Protokoll Frame



Das Protokoll ist nicht öffentlich zugänglich, wurde aber von Behrang Fouladi und Sahand Ghanoun durch Reverse Engineering ermittelt.

1.2.4.3 Sicherheit

Im Z-Wave Chip ist eine 128-bit AES Verschlüsselung implementiert. Diese wird jedoch nur bei Schließsystemen eingesetzt. Die Verschlüsselung muss in den oberen Schichten in einem Security Layer vom Hersteller selbst implementiert werden.

1.2.5 HomeMotion (BidCos) Protokoll

Das BidCos-Funkprotokoll ist proprietär und aufgrund dessen nicht frei zugänglich.

1.3 Sicherheitsaspekte

Quelle:
http://processors.wiki.ti.com/index.php/What%27s_New_in_ZigBee_3.0#Enhanced_security_for_Centralized_Networks_.28Networks_with_a_Coordinator.2FTrust_Center.29

1.3.1 ZigBee

1.3.1.1 Physical & MAC Layer

Wie in 1.2.4.2 beschrieben setzt ZigBee auf dem Standard IEEE 802.15.4 auf. Dadurch müssen die oberen Schichten die Kommunikation nicht selbst verschlüsseln, sondern ausschließlich Schlüssel verwalten.

1.3.1.2 Übersicht der Profile

In den ZigBee-Profilen sind Anwendungen als Application Profiles definiert. Neben den Anwendungsprofilen gibt es noch die Geräteprofile, die ZigBee Device Objects (ZDO). Während die Anwendungsprofile die Art der Kommunikation beschreiben, geht es bei den Geräteprofilen um den Aufbau der Geräte, deren Verhalten und die Interaktion mit anderen Geräten. Diese Geräteprofile definieren die ZigBee-Objekte und den Datenaustausch unter ZigBee-Objekten. Die nachfolgenden Sicherheitsaspekte beziehen sich auf das home automation profile.

1.3.1.3 home automation profile

ZigBee Home Automation (ZHA) ist ein ZigBee-Geräteprofil für Smart Homes mit dem Wohnungen und Häuser mit mehr Komfort und Sicherheit ausgestattet werden können. Die Übertragung in diesem Profil erfolgt verschlüsselt mit einem Netzwerkschlüssel.

1.3.1.4 master key „ZigBeeAlliance09“

Der Netzwerkschlüssel wird vom Teilnehmer, der in das Netzwerk eintritt, beim Trustcenter angefordert. Die Übertragung des Netzwerkschlüssels erfolgt dann verschlüsselt vom Trustcenter an den Teilnehmer. Bei dieser Übertragung wird der Netzwerkschlüssel durch den Master Key verschlüsselt. Mittlerweile ist der master key bekannt. Sprich dieser initiale Schlüsselaustausch kann mitgelesen werden.

1.3.1.5 installation code

Seit ZigBee HA 1.2.1 ist ein sogenannter Installation Code verpflichtend, der vom Hersteller auf das Gerät aufgebracht ist. Ein Trust Center kann anstelle des bekannten "ZigBeeAlliance09" Schlüssels diesen Geräteindividuellen Schlüssel verwenden, sodass der initiale Schlüsselaustausch bereits sicher ist.

Der Installation Code besteht aus 128 Bit random data und einem 16 Bit Hashcode. Dieser wird vom einzutretenden Teilnehmer an das Trustcenter gesendet. Aus dem Installation Code und der Hashsummer generiert dann das Trust Center den Netzwerkschlüssel.

1.3.1.6 application link key

Türschlösser müssen über eine weitere Verschlüsselung auf Anwendungsebene (APS Key oder auch application link key genannt) verfügen. Die Kenntnis des Netzwerkschlüssels reicht damit nicht aus, um dem Schloss Befehle wie "öffnen", "schließen" oder "neue PIN codes einlernen" zu senden.

1.3.1.7 rejoin mit dem Trust Center

Hochwertige Trust Center verweigert einen sogenannten „insecure rejoin“, d.h. einen Rejoin mit einem bekannten Schlüssel im laufenden Betrieb.

1.3.2 Z-Wave

Es werden ausschließlich Nachrichten der Schließsysteme verschlüsselt. Alle anderen Nachrichten werden nicht verschlüsselt. Für die Verschlüsselung sind die Hersteller in der Security Schicht selbst verantwortlich.

Das Z-Wave Protokoll ist proprietär und nicht öffentlich zugänglich. Durch dies sind Informationen die für einen Angriff auf ein Z-Wave Netzwerk erforderlich sind, schwer zugänglich.

1.3.3 Herausforderungen für die Forensik

1.3.3.1 Hardware

- Große Anzahl von Geräten auf dem Markt
- Große Anzahl von Geräten innerhalb eines Netzwerkes
- Geografische Verteilung der Geräte innerhalb eines Netzwerkes
- Schnell und leicht austauschbare Geräte innerhalb eines Netzwerkes

1.3.3.2 Software

- Proprietäre Protokolle
- Große Anzahl von Funkprotokollen
- Große Anzahl von Software und mobilen Anwendungen

1.4 Exkurs - Gerätekommunikation mit den Herstellern

http://www.spiegel.de/netzwelt/gadgets/was-die-daten-im-smart-home-verraten-a-1064107.html

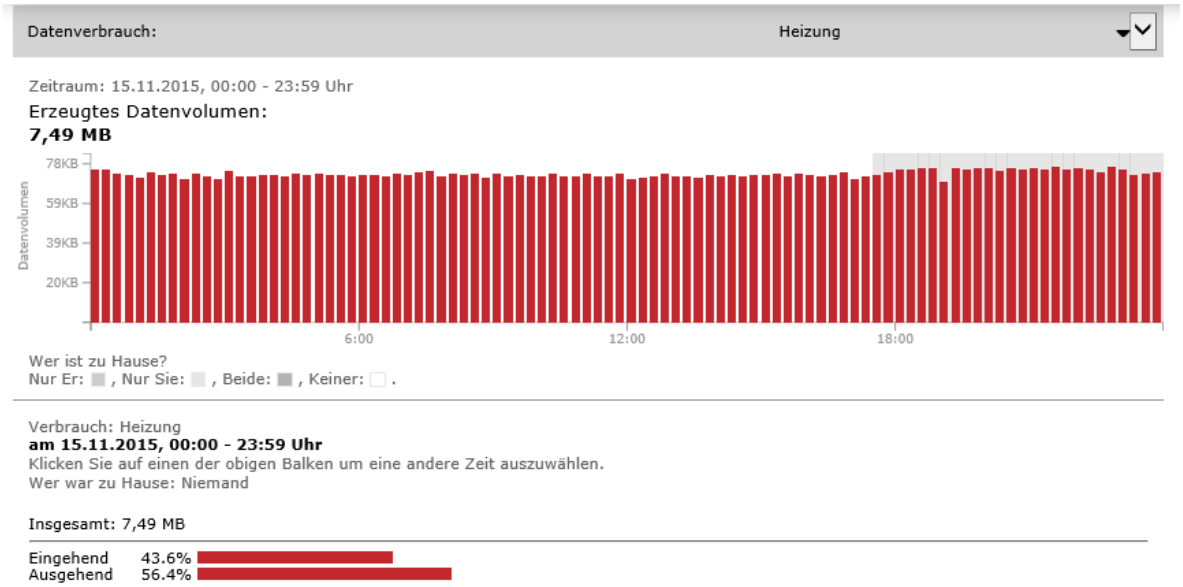
Die SmartHome Geräte melden die Daten auch über das Internet an ihre Hersteller. So sind diese über das Internet oder App auch von Unterwegs steuerbar.

Die Agentur OpenDataCity hat für Spiegel Online die Datenmengen von einer 65 Quadratmeter großen Wohnung festgehalten.

Wer ist wann zu Hause? Wann geht die Freundin ins Bett? Das Smart Home von meldet kleinste Details seines Privatlebens an die Gerätehersteller.

Der Heizungsthermostate von Honeywell meldet jede Sekunde seinem Hersteller, dass er noch da ist.

In der Grafik unten ist sichtbar, dass die Thermostate knapp 8 MB Internettrafic verursachten, obwohl bis 18 Uhr niemand zu Hause war.



2 Praktischer Teil

2.1 Grundlegendes

Zur Untersuchung im praktischen Teil wurden die folgenden Versionen verwendet. Die Installation und Untersuchung erfolgte in einer VM Windows 7 32 Bit.

- FHEM Version 5.8
- Strawberry Perl (32-bit) Portable Version 5.26.0.1-32bit

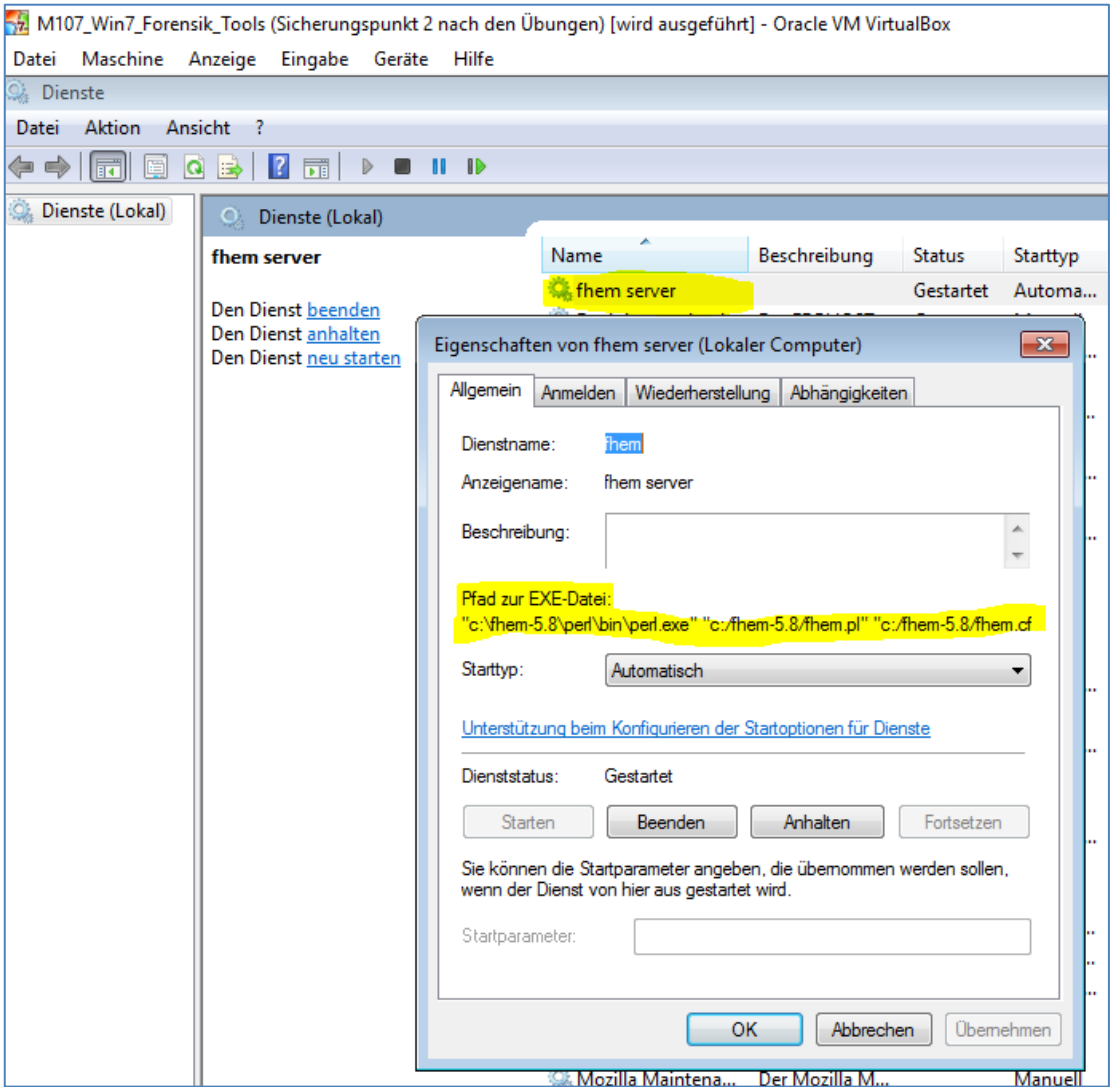
2.1.1 Start des FHEM Server

Der Start des Servers kann manuell über ein Batch-Skript oder als Windows-Dienst erfolgen. Dabei wird dem Server immer eine Konfigurationsdatei fhem.cfg angegeben.

- **Manuell**

D:\fhem-5.8\perl\bin\perl.exe D:\fhem-5.8\fhem.pl D:\fhem-5.8\fhem.cfg

- **Windows-Dienst**



2.1.2 Konfigurationsdatei fhem.cfg

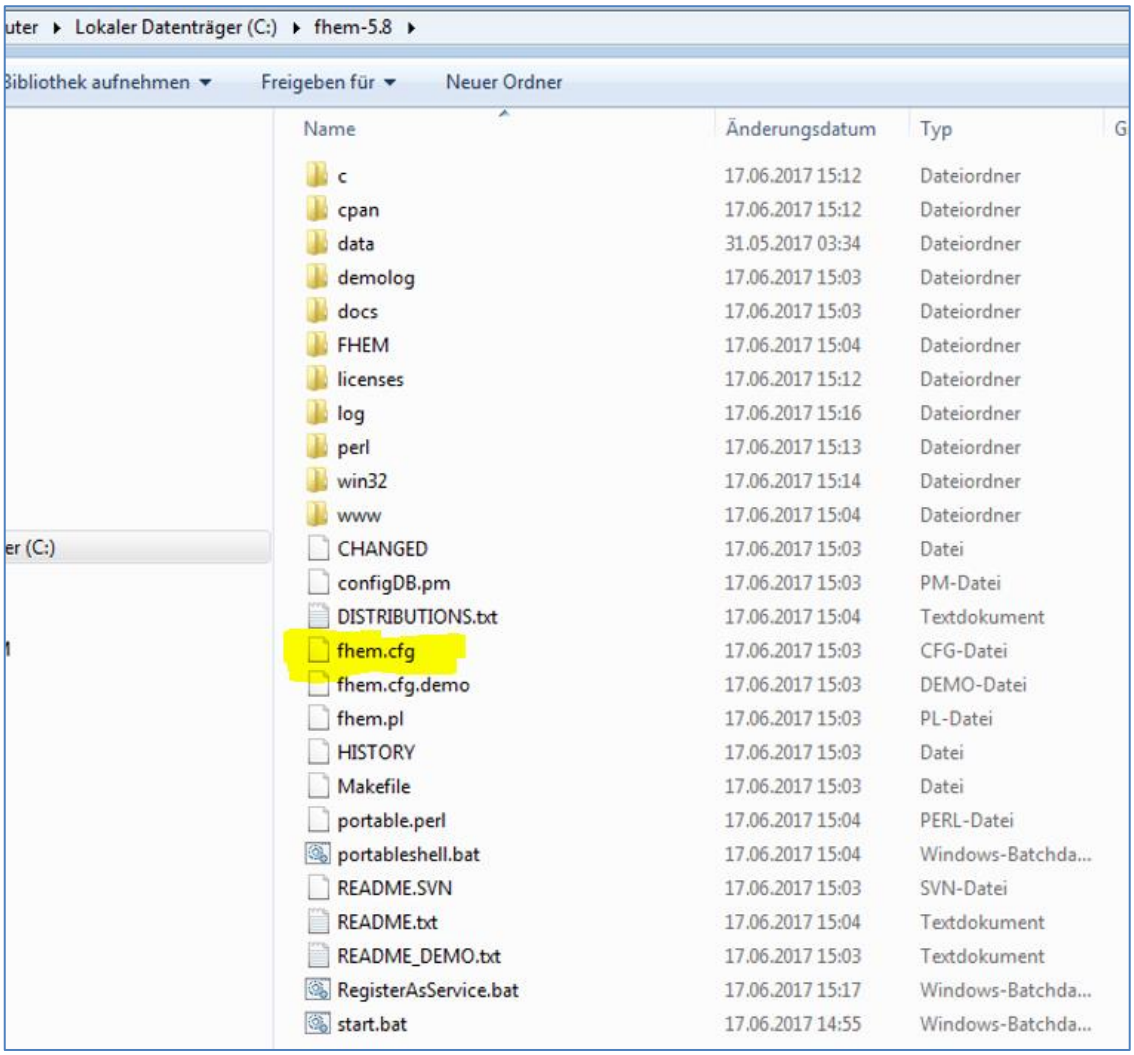
2.1.2.1 Daten aus forensischer Sicht

Über die Konfigurationsdatei können die verwendeten Logdateien oder die verwendete SQL Datenbank, Archive der Logdateien, Konfiguration der Aktoren/Sensoren und Benutzer sowie die verschiedenen Anmeldemöglichkeiten der Benutzer definiert werden.

Diese Dateien enthalten Informationen des FHEM Server die aus forensischer Sicht wichtig sind.

2.1.2.2 Dateiname und Pfad

Der FHEM Server wird über die Konfigurationsdatei fhem.cfg konfiguriert. Wobei der Dateiname und der Pfad beliebig geändert werden kann.



2.1.2.3 Verwendete Logdateien und SQL Datenbank

Der FHEM Server kann Logdateien im Textformat oder einen SQL Server mit SQL Datenbank verwenden.

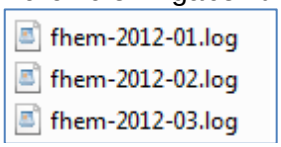
- **Globale Logdatei fhem.log**

Der FHEM Server verwendet eine globale Logdatei, in der die zentralen Ereignisse gespeichert werden. Über das Attribut ***attr global logfile*** wird die globale Logdatei konfiguriert.

Beispiel

attr global logfile c:\fhem\log\fhem-%Y-%m.log

Durch die Angabe %Y-%m wird eine separate Datei pro Monat pro Jahr angelegt.



- **Spezifische Logdateien**

Zusätzlich können beliebig viele spezifische Logdateien verwendet werden. In der Regel werden die spezifischen Logdateien für die einzelnen Geräte definiert. Über das Define ***define FileLog*** kann eine spezifische Logdatei definiert und einem Geräte zugeordnet werden.

Beispiel

define FileLog_Schalter_Buero FileLog c:\fhem\log\Schalter_Buero-%Y-%m.log

Im Beispiel werden die Logs der Komponente FileLog_Schalter_Buero gespeichert.

- **Archivierte Logdateien**

Zusätzlich können die Logdateien automatisch archiviert werden, wenn sie eine bestimmte Größe erreicht haben. Den Folder für die Archivierung kann mit dem Attribute ***attr achivedir*** konfiguriert werden.

Beispiel

attr FileLog_Schalter_Buero archivedir c:\fhem\log\

Im Beispiel werden die Logdateien der Komponente FileLog_Schalter_Buero in dem Folder c:\fhem\log\ archiviert.

- **Logdatei fhem.save**

In der Konfigurationsdatei fhem.save werden die Schaltzustände aller Geräte gespeichert. Nach einem Neustart des FHEM Servers werden die Geräte wieder mit ihrem letzten Schaltzustand angezeigt.

Über das Attribute ***attr global statefile*** kann die fhem.save konfiguriert werden.

Beispiel

attr global statefile c:\fhem\log\fhem.save

- **SQL Server**

Die Verbindung zur Datenbank (host, username, password, etc.) wird in der Datei db.conf hinterlegt. Über den Define ***define dbLog*** in der Konfigurationsdatei fhem.cfg wird der Pfad zur SQL Konfigurationsdatei konfiguriert.

define <name> DbLog <configfilename> <regexp>

<configfilename> ist der Pfad zur angelegten db.conf.

Beispiel:

define logdb DbLog ./db.conf .*:.*

2.1.2.4 Verwendete Aktoren/Sensoren und Räume

In der Konfigurationsdatei fhem.cfg werden die verwendeten Modelle der Aktoren und Sensoren konfiguriert. Ebenfalls die Zuordnung zwischen Raum/Location zu dem Aktor/Sensor.

Beispiel

attr Lampe model fs20-st
attr Lampe room Wohnzimmer

Im Beispiel wird eine Lampe vom Typ fs20-st im Raum Wohnzimmer definiert.

2.1.2.5 Automatische Ereignisse zu bestimmten Zeitpunkten

Automatische Ereignisse können ebenfalls über die Konfigurationsdatei fhem.cfg über den definiert werden.

Beispiel

define LampeAnUm1700 at 17:00:00 set lamp on

Im Beispiel wird das Einschalten einer Lampe um 17:00 Uhr definiert.

2.1.2.6 Verwendete Benutzer und Zugangsarten

Für die Benutzer können die folgenden Login Zugänge definiert werden

Zugangsdaten für das **Webinterface**
define WEB FHEMWEB 8083 global

Zugangsdaten für **Smartphone**
define WEBphone FHEMWEB 8084 global

Zugangsdaten für **Tablets**
define WEBtablet FHEMWEB 8085 global

Die Benutzerkennwörter sind in Textform oder verschlüsselt eingetragen.

Beispiel

Verschlüsseltes Kennwort, online Base64 Encoder wie www.base64online.com
attr WEB basicAuth <<verschlüsseltes Password>>
attr WEB basicAuth YmVudXR6ZXJuYW1lOnBhc3N3b3J0

Unverschlüsseltes Kennwort, mehrere Benutzer
attr WEB basicAuth { ("$user:$password" eq "user1:pwd1") || ("$u-ser:$password" eq "user2:pwd2") }

2.1.3 Inhalt der Logdateien

In den Logdateien sind die Zustände der Aktoren und Sensoren zu einem bestimmten Datum und Uhrzeit gespeichert.

Beispiel

2012.03.12 08:40:00 2: FS20 set sz_Leselampe dim100% 1280
2012.03.12 09:01:01 2: FS20 set sz_Rollo off
2012.03.12 09:20:01 2: FS20 set sz_Leselampe off
2012.03.12 09:20:01 2: FS20 set sz_Stehlampe off

2013-10-18 20:19:58 CUL_HM outTemperatur temperature: 12.4
2013-10-18 20:19:58 CUL_HM outTemperatur humidity: 88
2013-10-18 20:19:58 CUL_HM outTemperatur T: 12.4 H: 88

2.2 Forensische Auswertungen

2.2.1 Übersicht der Vorgehensweise

Die aus forensischer Sicht wichtigen Daten des FHEM Servers können wie folgt ermittelt werden.

- Ermitteln über welche Methode der FHEM Server gestartet wird.
- Ermitteln des Dateipfads und Dateiname der Konfigurationsdatei.
- Aus der Konfigurationsdatei die verwendeten Logdateien ermitteln.

  Globale Logdateien
  Gerätespezifische Logdateien
  Archivierte Logdateien
  Gespeicherte Schaltzustände aller Geräte

- Aus der Konfigurationsdatei die verwendete SQL Datenbank ermitteln.
- Aus der Konfigurationsdatei die Konfiguration der Räume / Teilnehmer ermitteln.
- Aus der Konfigurationsdatei die verwendeten Benutzer und Benutzerzugangsarten ermitteln.
- Aus den Logdateien oder SQL Datenbank die Zustände der einzelnen Aktoren und Sensoren ermitteln

2.2.2 Sichern der Daten

2.2.2.1 Konfigurationsdatei

Der Dateiname und Pfad der Konfigurationsdatei fhem.cfg muss zuerst ermittelt werden. Dies erfolgt je nach Startart des Servers unterschiedlich.

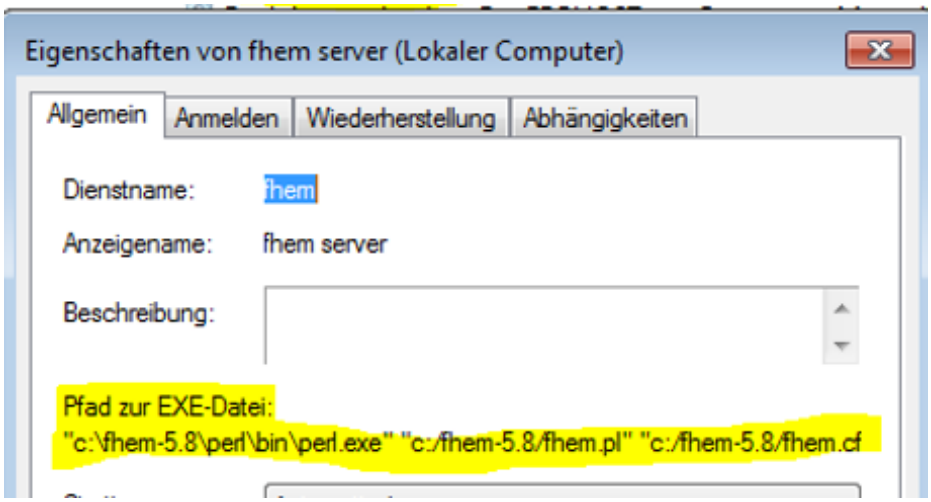
- **Manuell über die Kommandozeile oder Scriptdatei**

Wird der FHEM Server über ein Skript gestartet, dann wird die Konfigurationsdatei als Parameter beim Aufruf mitgegeben.

D:\fhem-5.8\perl\bin\perl.exe D:\fhem-5.8\fhem.pl D:\fhem-5.8\fhem.cfg

- **Windows-Dienst**

Der Dienstname des FHEM Servers ist FHEM. Über die Dienstkonfiguration kann der Pfad der Konfigurationsdatei ermittelt werden.



2.2.2.2 Logdateien und SQL Datenbank

Die Dateinamen und Pfade der einzelnen Logdateien können aus der Konfigurationsdatei fhem.cfg ermittelt werden.

- **Globale Logdatei**

attr global logfile c:\fhem\log\fhem-%Y-%m.log

- **Spezifische Logdateien**

define FileLog_Schalter_Buero FileLog c:\fhem\log\Schalter_Buero-%Y-%m.log
define …

- **Archivierte Logdateien**

attr FileLog_Schalter_Buero archivedir c:\fhem\log\
attr …

- **Gespeicherte Zustände**

attr global statefile c:\fhem\log\fhem.save

- **SQL Datenbank**

define <name> DbLog <configfilename> <regexp>

2.2.3 Aussagen der Daten

Über die gespeicherten Daten können folgende Aussagen getroffen werden:

- **Räumlich**

Wo sind welche Teilnehmer verbaut.

- **Zustände / Zustandswechsel**

Wann hatte ein Teilnehmer einen Zustandswechsel als Befehl erhalten, z.B. Tür öffnen und wann hatte ein Teilnehmer welchen Zustand, z.B. Raumtemperatur im Büro 22 Grad.

- **Personenbezogen**

Wann hat sich welcher Benutzer angemeldet, evtl. Systemänderungen vorgenommen.