Technische Berichte in Digitaler Forensik

Herausgegeben vom Lehrstuhl für Informatik 1 der Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU) in Kooperation mit dem Masterstudiengang Digitale Forensik (Hochschule Albstadt-Sigmaringen, FAU, Goethe-Universität Frankfurt am Main)

Forensische Untersuchung der Web-RTC Applikation „Circuit“ in der Version 1.1.4107 unter Microsoft Windows mit Google Chrome

Michael Kirchner

29.02.2016

Technischer Bericht Nr. 4

Zusammenfassung

In diesem Whitepaper wird die WebRTC basierte Collaboration Applikation Circuit forensisch untersucht. Neben browsertypsichen Spuren fallen hierbei vor allem Spuren in Form von Logdateien an, welche vornehmlich Metadaten zu Konversationen enthalten. Inhaltsdaten können teilweise aus dem Browsercache sowie aus dem RAM extrahiert werden.

Entstanden im Rahmen des Moduls Browser- und Anwendungsforensik des Studiengangs Digitale Forensik im Wintersemester 2015/2016 unter der Anleitung von Felix Freiling, Holger Morgenstern und Michael Gruhn.

Inhaltsverzeichnis

1 Einleitung

In dieser Hausarbeit wird die Anwendung Circuit[1] von Unify forensisch untersucht. Es sollen dabei Spuren der Anwendung identifiziert und charakterisiert werden.

1.1 Über Circuit

Bei der Anwendung „Circuit“ handelt es sich um eine WebRTC basierte Web-Anwendung, die derzeit als Cloud-Dienst angeboten wird. Aktuell ist die Webanwendung nur mit dem Browser *Chrome* nutzbar, weswegen sich die Untersuchung auch auf diesen beschränkt. Circuit ist ein Anwendung die einem geschlossenen Benutzerkreis *(In Circuit Tenant genannt)* Kommunikation über die Wege Text, Voice, Video sowie Bildschirmfreigabe ermöglicht, ohne hierfür eine zusätzliche Installation vorzunehmen.

Die Kommunikation erfolgt dabei in so genannten *Conversations* an denen mind. 2 Gesprächspartner beteiligt sind. Jede Conversation hat eine eindeutige ID (Diese ist bspw. in der Adresszeile in Abbildung 1 zu sehen.) Jeder Eintrag einer Conversation ist ebenfalls durch eine eindeutige Item ID gekennzeichnet, die jedoch für den Benutzer nicht sichtbar ist.

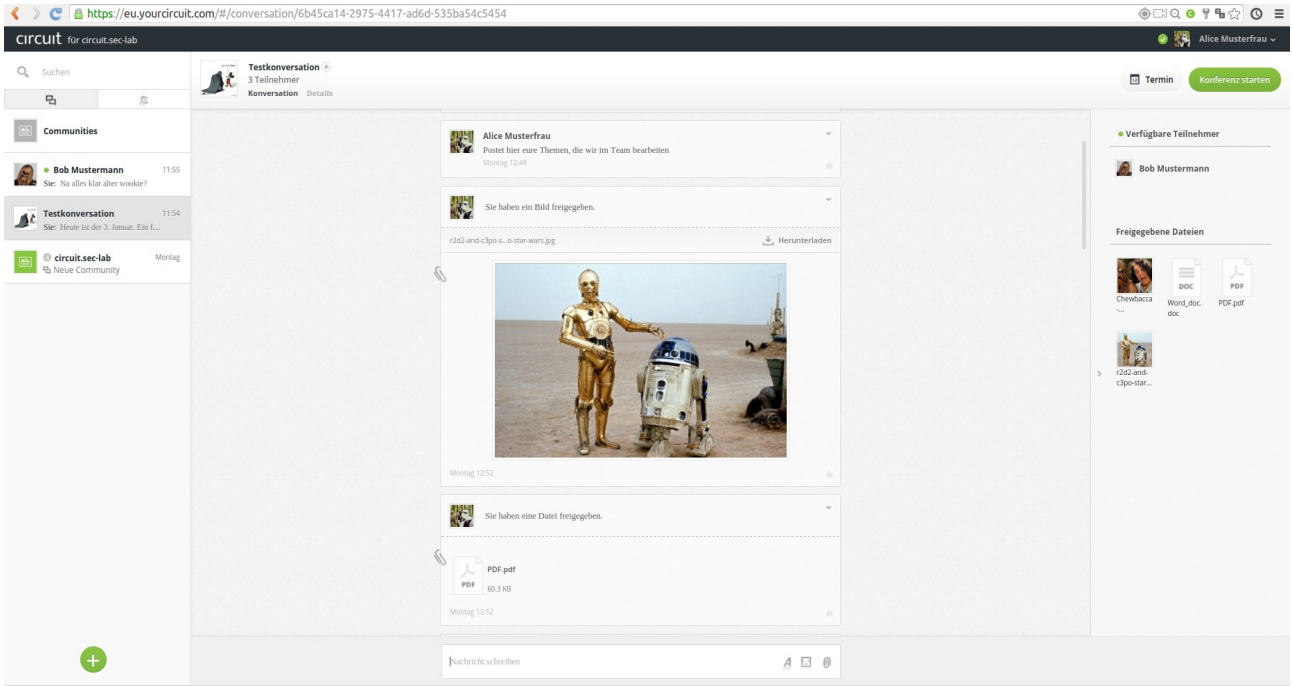


Abbildung 1: Oberfläche von Circuit

1.2 Motivation

Circuit ist ein neues Produkt und eines der ersten kommerziellen WebRTC Produkte. Durch die hohe Marktdurchdringung von Unify (ehemals Siemens) im Bereich von Kommunikationslösungen insbesondere im deutschen deutschen Markt, ist zu erwarten, dass zukünftig auch Circuit von einigen Unternehmen eingesetzt wird. Aus forensischer Sicht sind hierbei viele Spuren von Interesse, die sowohl Metadaten wie auch Nutzdaten umfassen.

1 https://www.circuit.com

2 Analyse

Die Analyse von Circuit unterteilt sich in die Bereiche der Festplatten- und Arbeitsspeicheruntersuchung. Die Erkenntnisse aus letzterer sind insbesondere bei Live Analysen verwendbar.

Testumgebung

Circuit

Version: 1.1.4107

Test-Tenant: circuit.acme.eu (Für Textnachrichten, Call, Desktopsharing)

Produktiv-Tenant: unify.com (Für Microsoft Exchange Kopplung)

Virtualisierungsumgebung:

Virtualbox Version 5.0.10_Ubuntu

Testsystem:

OS:	Windows XP SP3 x86
Updates:	keine
HD:	2,5 GB, FAT32
RAM:	512 MB
Software:	Google Chrome, Sync v2.2 und Procmon v3.2 aus der Sysinternals Suite

Analysesystem:

OS:	Ubuntu 15.04 x64
Software:	Volatility v2.4, The Sleuth Kit v4.1.3, wxHexEditor v0.23, DB Browser for SQLite v3.5.1, AESKeyFind v1.0, Wireshark v2.0.1

OS:	Ubuntu 14.04
Software:	idifference2

OS:	Windows XP SP3 x86
Updates:	keine
HD:	5 GB
RAM:	4 GB
Software	Google Chrome v47.0.2526.106 m, Chrome Cache View von Nirsoft v1.67

3 Spuren

Da Circuit über mehrere Funktionen verfügt besteht die Annahme, dass unterschiedliche Aktionen auch unterschiedliche Spuren hinterlässt. Es werden dabei folgende Aktionen unterschieden:

1) Installieren der Circuit Extension in Chrome (Wird für Desktopsharing benötigt)

2) Nachrichten Schreiben (Chat)

2) Circuit Call

3) Desktop Sharing

4) Herunterladen einer Datei

5) Microsoft Exchange Connector (Eingabe der Active Directory Zugangsdaten)

Darüber hinaus besteht bei Circuit die Möglichkeit bei der Anmeldung die Option zu aktivieren, dass es sich um einen privaten Computer handelt, die Anmeldung bestehen bleibt und der Cache aktiviert wird. In der Analyse hat sich gezeigt, dass dass diese Option keine Auswirkung auf die Spuren auf der Festplatte hat und wird somit nicht weiter beleuchtet.

Eine weitere Frage ist ob Circuit Spuren auf dem System hinterlässt, die auch nach dem Löschen der History bestehen bleiben. *(vgl. Origins Datei auf Seite 8)*

3.1 Festplatte

Die Spuren auf der Festplatte werden via idifference2 ermittelt. Hierfür werden die unterschiedlichen Aktionen jeweils 3-Mal wiederholt. Die Festplatte wird vor und nach der Ausführung gesichert. Anschließend wird die Differenzmenge gebildet. Die dafür verwendeten Skripte aus dem Digitale Forensik Modul M10 sind der Abgabe beigefügt.

Da Circuit als Web Applikation innerhalb von Google Chrome ausgeführt wird, fallen zum einen Chrome typische wie auch Circuit spezifische Spuren an. Interessante „Chrome-Spuren“ werden dabei aufgezeigt. Die anfallenden Spuren sind allesamt im Usaer Data Verzeichnis von Chrome zu finden. Die hier angegeben Pfade beziehen sich auf Windows XP. Andere Pfade sind im Forensicswiki[2] zu finden.

2 http://www.forensicswiki.org/wiki/Google_Chrome

3.1.1 Chrome Spuren

Cache:

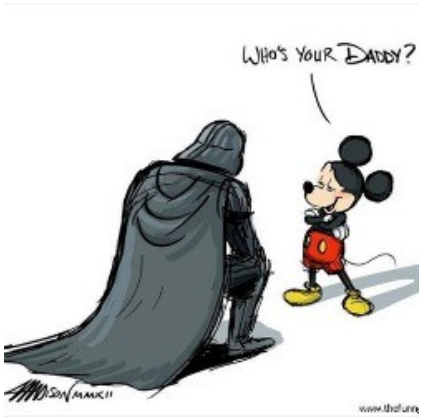
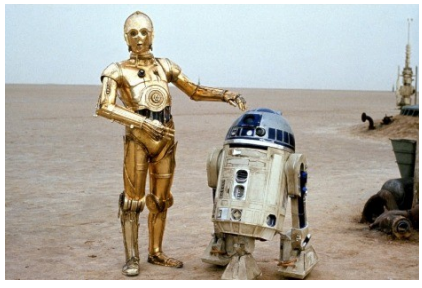
*%UserProfile%/Anwendungsdaten/Google/Chrome/User Data/%Profile%/ Application Cache/Cache/**

*%UserProfile%/Anwendungsdaten/Google/Chrome/User Data/%Profile%/Cache/**

Der Inhalt des Caches kann über das Programm *Chrome Cache View*[3] von Nirsoft einfach wiederhergestellt werden *(vgl.: Anhang Chrome Cache View (Nirsoft))*.

Im Chrome Cache finden sich unabhängig davon ob bei der Anmeldung an Circuit das Caching aktiviert wurde oder nicht, einige Spuren wie bspw. Bildmatrial aus Conversations.

Beispiele:

	Beispiel 1	Beispiel 2
User Avatar	 (Alice)	 (Bob)
Conversation Avatar	 (Teamkonversation)	 (Bob)
Bilder aus Conversations		

Dabei bleiben auch die originalen Dateinamen sowie die jeweilige URL nachvollziehbar.

3 http://www.nirsoft.net/utils/chrome_cache_view.html

Darüber hinaus legt Circuit nach der Anmeldung automatische einige Dateien im Cache an, selbst eine Datei, die diese Dateien auflistet: ansible.appcache. Der Inhalt letzterer ist im *Anhang Circuit Spuren in Chrome Cache ansible.appcache* dargestellt. Diese Spuren können insbesondere dafür verwendet werden um darzustellen, dass die Applikation Circuit verwendet wurde.

Cookies DB:

%UserProfile%/Anwendungsdaten/Google/Chrome/User Data/%Profile%/Cookies

SQLite DB enthält keine interessanten Spuren, da Circuit keine Cookies anlegt. Zur Vollständigkeit aufgeführt.

Favicons DB:

%UserProfile%/Anwendungsdaten/Google/Chrome/User Data/%Profile%/Favicons

SQLite DB enthält die einzelnen URL für die favicons gespeichert wurden. Darunter in der Tabelle „icon_mapping“ jede aufgerufene Circuit URL.

History DB:

%UserProfile%/Anwendungsdaten/Google/Chrome/User Data/%Profile%/History

SQLite DB enthält Informationen über heruntergeladene Dateien und die aufgerufene Circuit URLs inkl. Zeitstempeln.

Login Data DB:

%UserProfile%/Anwendungsdaten/Google/Chrome/User Data/%Profile%/Login Data

SQLite DB enthält (verschlüsselte) Zugangsdaten falls diese vom Benutzer gespeichert wurden.

Top Sites DB:

%UserProfile%/Anwendungsdaten/Google/Chrome/User Data/%Profile%/Top Sites

SQLite DB enthält die Seiten, die als „Most Viewed“ angezeigt werden. Zur Vollständigkeit aufgeführt.

Web Data DB:

%UserProfile%/Anwendungsdaten/Google/Chrome/User Data/%Profile%/Web Data

SQLite DB enthält Daten zur Autovervollständigung. Dies bezieht sich bei Circuit darauf, dass die Anmeldemaske bereits mit dem Usernamen vorausgefüllt wird. Es ist daher daran zu erkennen, welcher User zuletzt an Circuit angemeldet war.

WebRTCIdentityStore DB:

%UserProfile%/Anwendungsdaten/Google/Chrome/User Data/%Profile%/WebRTCIdentityStore

Enthält das Zertifikat und den (verschlüsselten) privaten Schlüssel für die DTLS Verbindung von WebRTC.

3.1.2 Circuit spezifische Spuren

Debug Datei:

%UserProfile%/Anwendungsdaten/Google/Chrome/User Data/%Profile%/
File System/000/t/00/0000000X

Bei der Ausführung von Circuit wird eine bzw. bei größeren Tenants mehrere Debugdateien angelegt *(Auszug: Anhang Auszug Circuit Debug Datei)*. Diese enthalten sehr viele Detaildaten zum Circuit Tenant, dem User sowie zur Session. Diese umfassen (jeweils mit Zeitstempel [Unix Zeitformat]):

- Informationen zum letzten eingeloggten User

  inkl. Browser, Version, Extension Version, Server Adresse, Username, TanantID, UserID, E-Mail Adresse

- Caching Status
- Überblick über die Conversations (Wann erstellt, wie viele Teilnehmer, zuletzt modifiziert)
- Auflistung der Metadaten zu einzelnen Conversation Items

  inkl. type {Text, RTC}, itemID, convID, creatinTime, modificationTime, creatorID

  keine Inhalte

- Details zu während der Session getätigten WebRTC Calls

  inkl. Teilnehmer, Dauer, IP Adressen (public wie lokal) von allen Teilnehmern verwendete UDP Ports

- Ausgabe aller (auch gelöschter) User (limitiert für ca. 1000 User, Limit konnte nicht exakt werden[4])

  inkl. der folgenden Attribute: UserID, LastName, firstName, displayName, Status (bspw. Available, Away, …), ImageURI (Avatar), emailAddress, userPrecenseStatus, timezone, tenantID, company, role, phoneNumbers, location, jobtitle, userstate {Active, Deleted}

- Getätigtes Suchen (auch vergangene)

Origins Datei:

%UserProfile%/Anwendungsdaten/Google/Chrome/User Data/%Profile%/
File System/Origins/000003.log

Die Dateien 000003.log unter Origins ist aus forensischer Sicht insofern interessant als das diese auch bei einem löschen des Browserverlaufs erhalten bleibt und in ihr Verweise auf die Domain https://eu.yourcircuit.com zu finden sind. Folglich kann bei Vorhandensein dieses Inhalts darauf geschlossen werden, dass die Website aufgerufen wurde, auch wenn in der Browserhistory davon

4 Im Test-Tenant mit 4 Usern wurden alle ausgegeben. Im Produktiv-Tenant mit ca. 7.000 Usern wurden etwa 1000 User aufgelistet.

nichts mehr zu erkennen ist.

Indexeddb:

%UserProfile%/Anwendungsdaten/Google/Chrome/User Data/%Profile%/IndexedDB/https_eu.yourcircuit.com_0.indexeddb.leveldb/…

In der Indexeddb sind die von Circuit gecachten Daten zu finden. Diese sind jedoch verschlüsselt und entziehen sich somit dem Zugriff.

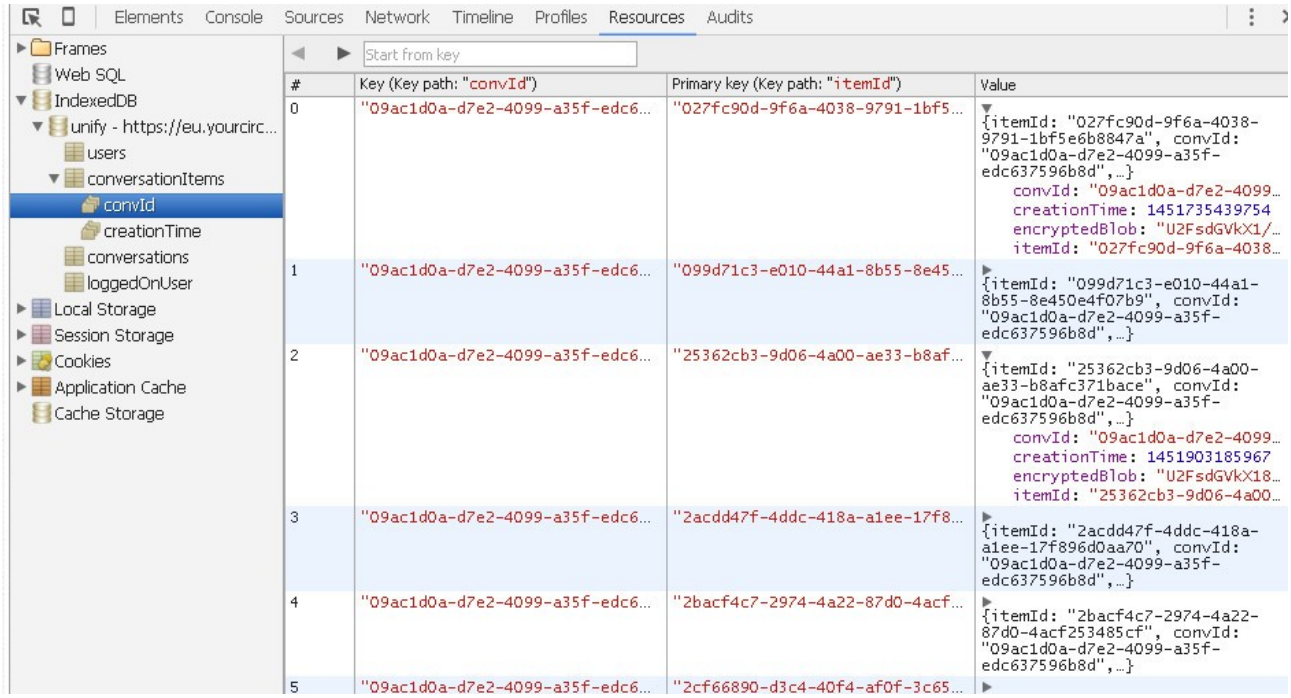


Abbildung 2: Indexeddb

Local Storage:

%UserProfile%/Anwendungsdaten/Google/Chrome/User Data/%Profile%/Local Storage/https_eu.yourcircuit.com_0.localstorage

In der SQLite DB ist vermerkt, in welcher Circuit Regin (z.B. Europe, Asia, America) die letzte Anmeldung stattgefunden hat und ob die Anmeldung gespeichert wurde.

Extension

%UserProfile%/Anwendungsdaten/Google/Chrome/User Data/%Profile%/Extensions/mhkbaognlahkdimlfcfhbeihldmjofgg/…

Circuit benötigt für das Desktopsharing und die Microsoft Exchange Kopplung eine eigene Extension. Die Nutzung dieser Extension weist auf eine der oben genannten Vorkommnisse hin.

3.2 Arbeitsspeicher

Der Arbeitsspeicher-Dump des virtualisierten Windows XP Testsystems wurde wie folgt erhoben. Die gefundenen Daten können u.U. auch in der pagefile.sys zu finden sein, wenn diese ausgelagert wurden.

```
# Erstellen des RAM Dumps
$ vboxmanage debugvm "testvm" dumpvmcore --filename ram_dump.elf

# Herausfinden von Offset und Größe des Dumps Hier: Offset 0x24a8 Größe: 20000000 Bytes =
512 MB
$ objdump -h ram_dump.elf|egrep -w "(Idx|load1)"
Idx Name          Größe      VMA               LMA               Datei-Off Ausr.
  1 load1         20000000  0000000000000000  0000000000000000  000024a8  2**0

# Erstellen des RAW Dumps
$ size=0x20000000;off=0x24a8;head -c $(($size+$off)) ram_dump.elf|tail -c +$(($off+1)) >
ram_dump.raw
```

Neben den im Folgenden dargestellten Erkenntnissen konnten mit dem Tool *AESKeyFind* einige AES Schlüssel sichergestellt werden. Diese stammen teilweise vermutlich von den getätigten Circuit Calls, die AES verschlüsselt stattfinden. Da eine Entschlüsselung der entsprechenden Netzwerktraces nicht erfolgreich durchgeführt werden konnten, werden diese hier nicht näher betrachtet.

3.2.1 Passwörter

Bei Circuit erfolgt die Anmeldung am System über Username/Passwort. Darüber hinaus kann innerhalb von Circuit eine Verbindung zum Microsoft Exchange Server des Unternehmens aufgebaut werden, wofür die entsprechenden Zugangsdaten angegeben werden müssen.

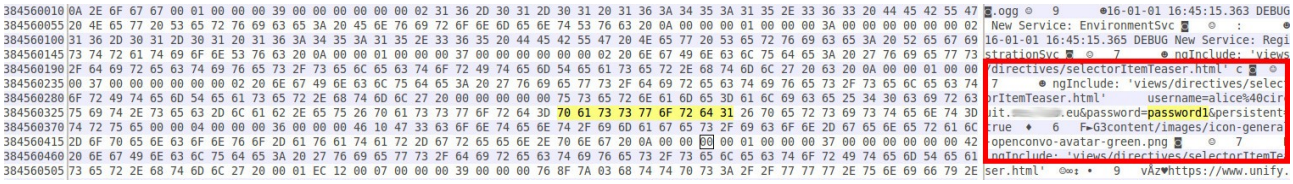


Abbildung 3: Circuit Zugangsdaten

Beide Zugangsdaten sind mittels eines HEX Editors im RAM zu finden.

Username: alice@circuit.acme.eu

Password: password1

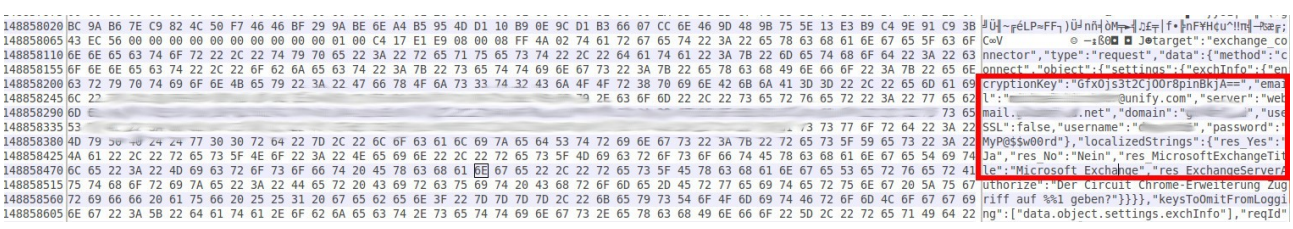


Abbildung 4: Exchange-Server bzw. Active Directory Zugangsdaten

Anmerkung: Die tatsächlichen Werte wurden, da es sich hierbei um Produktivdaten handelt, im Bild unkenntlich gemacht und im folgenden mit XXXXXX gekennzeichnet.

Email: XXXXXX@unify.com
Server: webmail.XXXXXX.net
AD Domain: XXXXXX
Username: XXXXXX
Password: MyP@$$w00rd

3.2.2 Conversation Items

Die Analyse des RAM Dumps mittels Strings offenbart Einblick in die Conversation Items. Diese umfassen hauptsächlich Metadaten und im Falle von Textnachrichten auch die Nutzdaten. Die Conversation Items sind im RAM fortlaufend sowie verteilt und damit schwer zu analysieren. Um die Conversation Items brauchbar zu analysieren wurde von mir ein Parser geschrieben, welcher die Conversation Items identifiziert und jeden einzeln in einer neuen Zeile in der Ausgabe ausgibt um diese von dort aus ggf. automatisiert weiterzuverarbeiten. *(vgl.: 5Anhang Circuit String Parser Programm)* Das Zeitformat ist das Unix Zeitformat in Millisekunden.

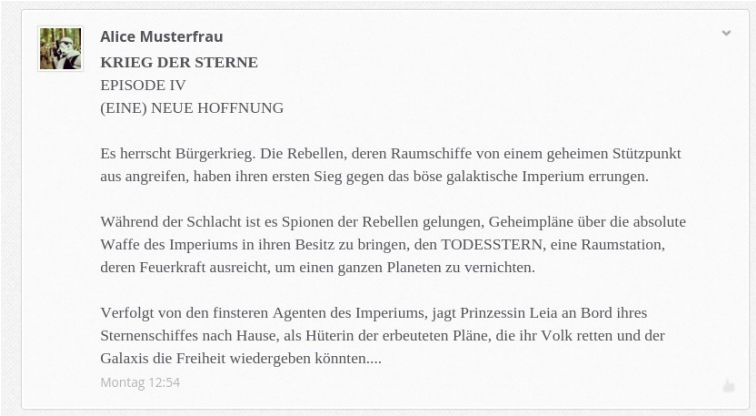


Abbildung 5: Conversation Item Text


```
{"type":"TEXT","itemId":"e0c93954-b55f-4efa-b6f0-37f927e28945","convId":"6b45ca14-2975-
4417-ad6d-535ba54c5454","text":
{"state":"CREATED","contentType":"RICH","content":"<b>KRIEG DER STERNE</b><br/>EPISODE
IV<br/>(EINE) NEUE HOFFNUNG<br/><br/>Es herrscht B&#252;rgerkrieg. Die Rebellen, deren
Raumschiffe von einem geheimen St&#252;tzpunkt aus angreifen, haben ihren ersten Sieg
gegen das b&#246;se galaktische Imperium errungen.<br/><br/>W&#228;hrend der Schlacht ist
es Spionen der Rebellen gelungen, Geheimpl&#228;ne &#252;ber die absolute Waffe des
Imperiums in ihren Besitz zu bringen, den TODESSTERN, eine Raumstation, deren Feuerkraft
ausreicht, um einen ganzen Planeten zu vernichten.<br/><br/>Verfolgt von den finsteren
Agenten des Imperiums, jagt Prinzessin Leia an Bord ihres Sternenschiffes nach Hause, als
H&#252;terin der erbeuteten Pl&#228;ne, die ihr Volk retten und der Galaxis die Freiheit
wiedergeben
k&#246;nnten....<br/>"},"creationTime":1451303647796,"modificationTime":1451303647796,"cr
eatorId":"b2d49d6d-fc8a-4487-9910-65e3b0b9a89d","includeInUnreadCount":true}
```

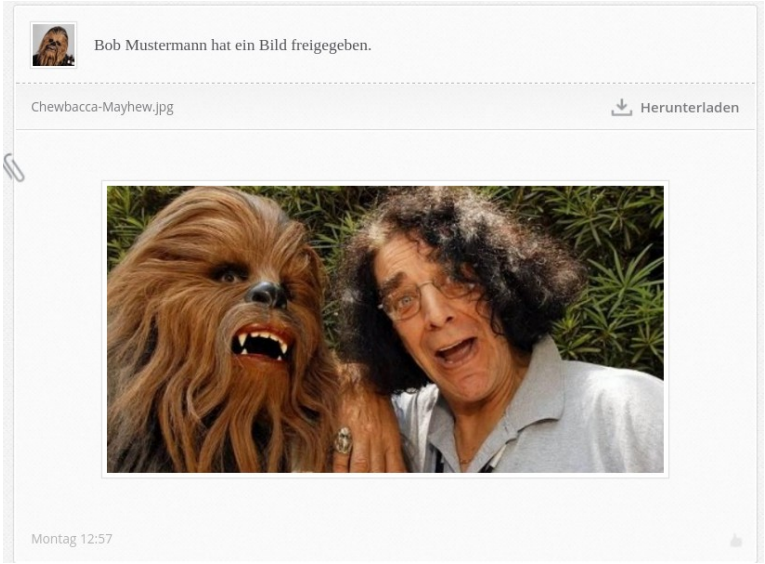


Abbildung 6: Conversation Item Bild


```
{"type":"TEXT","itemId":"43cd904e-269a-4e71-9913-8244b9a7f5fb","convId":"6b45ca14-2975-
4417-ad6d-535ba54c5454","attachments":[{"fileId":"219e8f02-3320-43e2-accf-
0354be37d997","fileName":"tHuMbNaIl___Chewbacca-
Mayhew.jpg","mimeType":"image/jpeg","size":54636,"itemId":"43cd904e-269a-4e71-9913-
8244b9a7f5fb","creationTime":1451303821046,"modificationTime":1451303821046,"creatorId":"
377fa6d0-6d8f-4675-8290-35a92a181d58"},{"fileId":"ebefb3c2-e157-4467-846b-
4a3298223260","fileName":"Chewbacca-
Mayhew.jpg","mimeType":"image/jpeg","size":54101,"itemId":"43cd904e-269a-4e71-9913-
8244b9a7f5fb","creationTime":1451303821046,"modificationTime":1451303821046,"creatorId":"
377fa6d0-6d8f-4675-8290-35a92a181d58"}],"text":
{"state":"CREATED","contentType":"RICH","content":""},"creationTime":1451303821046,"modif
icationTime":1451303821046,"creatorId":"377fa6d0-6d8f-4675-8290-
35a92a181d58","includeInUnreadCount":true}
```


4 Fazit

Die Applikation Circuit hinterlässt, da sie im Browser ausgeführt wird, Browser typsiche Spuren wie bspw. im Browsercache oder in der Browserhistory. Besonders interessant sind neben den browsertypischen, die Circuit spezifischen Spuren wie beispielweise die Debug Dateien, die sehr detailliert darlegen welche Aktionen von einem Benutzer ausgeführt wurden oder wer alles zu einer Circuit Gruppe dazugehört. Diese Metainformationen, wer hat sich wann mit wem wie ausgetauscht, können in einer forensischen Untersuchung sehr bedeutend sein. Das Wissen um die Tenant-, User- und Conversation-ID sind wichtige Informationen um bei einer polizeilichen Ermittlung beim Provider entsprechende Inhaltsdaten zu erhalten.

Die RAM Analyse bringt neben Zugangsdaten auch die Konversationsinhalte zutage sofern diese in Textform bestehen. Die These, dass durch im RAM gefundene AES Schlüssel ein via Netzwerktrace mitgeschnittenes WebRTC Gespräch zu entschlüsseln ist konnte noch nicht bewiesen werden.

Insgesamt fallen bei Circuit viele verwertbare Spuren an.

5 Anhang

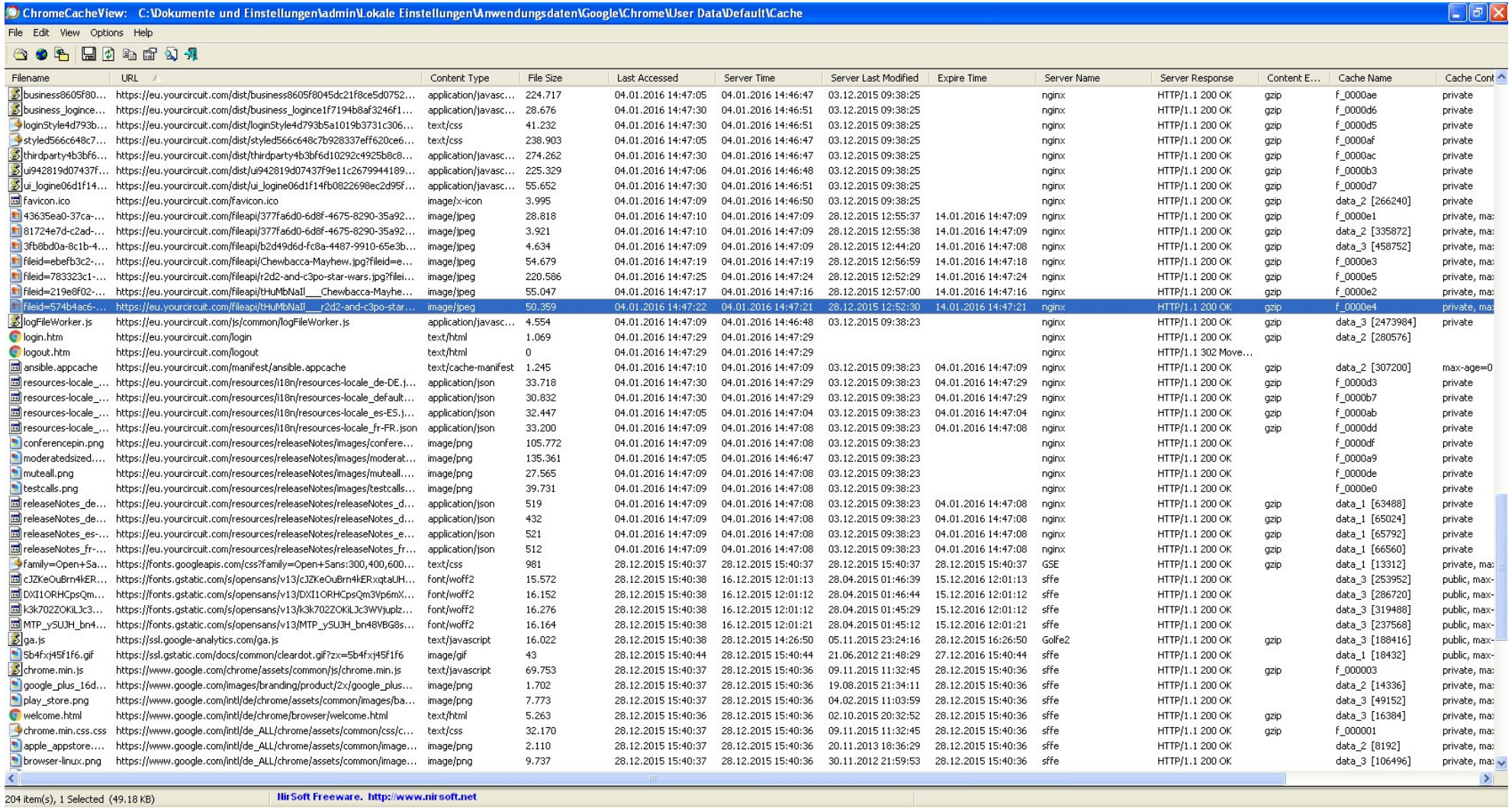
5.1 Circuit String Parser Programm

```
/**
 *
 * Author: Michael Kirchner
 * Masterstudiengang Digitale Forensik
 * M16
 */
package circuit.string.parser;

import java.io.IOException;

/**
 *
 * @author michael
 */
public class CircuitStringParser {

    /**
     * @param args the command line arguments
     */
    public static void main(String[] args) throws IOException {
        // TODO code application logic here
        String path = args[0];
        Parser p = new Parser((path));
        p.parseMyFile();
    }

}
/**
 *
 * Author: Michael Kirchner
 * Masterstudiengang Digitale Forensik
 * M16
 */
package circuit.string.parser;

import java.io.BufferedReader;
import java.io.FileNotFoundException;
import java.io.FileReader;
import java.io.IOException;
import java.util.Vector;


public class Parser {

    public Parser (String path)
    {
        this.path = path;
    }
    String path = null;
    Vector store = new Vector();

    public void parseMyFile() throws FileNotFoundException, IOException
    {
        if(path == null)
        {
            System.out.println("Error no path set");
            return;
        }

        FileReader fr = new FileReader(path);
        BufferedReader br = new BufferedReader(fr);
```

```
        String line = "";

        do
        {
          line = br.readLine();
          if(line!=null)
              parseLine(line);
        }
        while (line != null);


        br.close();
        printStorage();
    }
    protected void parseLine(String line)
    {
        int length = line.length();
        int start=0;
        int begin=0;
        for(int i = 0;i<length;i++)
        {
            //System.out.println("i: "+i+" Char: "+line.charAt(i));
            if(line.charAt(i) == '{')
            {
                if(validBegin(line.substring(i)))
                {
                    start=i;
                    begin=1;
                }
            }
            if(line.charAt(i) == '}')
            {
                if(validEnd(line.substring(start,i+1))&& begin!=0)
                {
                   // System.out.println("Gefunden start: "+start+" end: "+i);
                    begin=0;
                    addToStorage(line.substring(start,i+1));
                }
            }
        }

    }
    protected boolean validBegin(String begin)
    {
        if(begin.startsWith("{\"type\":\"RTC\",")||
begin.startsWith("{\"type\":\"TEXT\","))
        {

            return true;
        }
        else
            return false;
    }
    protected boolean validEnd(String end)
    {
        if(end.endsWith(",\"includeInUnreadCount\":false}")||
end.endsWith(",\"includeInUnreadCount\":true}"))
        {

            return true;

        }
        else
            return false;
    }
    protected void addToStorage(String conv)
    {
```

```
        if(!store.contains(conv))
            store.add(conv);
    }
    protected void printStorage()
    {
      //  System.out.println(store.size());
        while(!store.isEmpty())
        {
            String conv=(String) store.lastElement();
            store.remove(conv);
            System.out.println(conv);
        }
    }
}
```

5.2 Chrome Cache View (Nirsoft)



5.3 Circuit Spuren in Chrome Cache ansible.appcache

```
CACHE MANIFEST
# This manifest was generated by grunt-manifest HTML5 Cache Manifest Generator
# Time: Thu Dec 03 2015 10:36:27 GMT+0200 (EET)

CACHE:
/dist/styled566c648c7b928337eff620ce61117ba.css
/dist/business8605f8045dc21f8ce5d0752bf9842703.js
/dist/thirdparty4b3bf6d10292c4925b8c8958497b9a29.js
/dist/ui942819d07437f9e11c26799441893a47.js
/content/fonts/OpenSans-Bold.woff2
/content/fonts/OpenSans-Light.woff2
/content/fonts/OpenSans-Regular.woff2
/content/fonts/OpenSans-Semibold.woff2
/content/images/folder.png
/content/images/icon-ccb.png
/content/images/icon-file-box-folder.png
/content/images/icon-general-default-avatar-XL.png
/content/images/icon-general-default-avatar-blue-XL.png
/content/images/icon-general-default-avatar-blue.png
/content/images/icon-general-default-avatar-green-XL.png
/content/images/icon-general-default-avatar-green.png
/content/images/icon-general-default-avatar-orange-XL.png
/content/images/icon-general-default-avatar-orange.png
/content/images/icon-general-default-avatar-yellow-XL.png
/content/images/icon-general-default-avatar-yellow.png
/content/images/icon-general-default-avatar.png
/content/images/icon-general-default-room-XL.png
/content/images/icon-general-default-room-blue-XL.png
/content/images/icon-general-default-room-blue.png
/content/images/icon-general-default-room-green-XL.png
/content/images/icon-general-default-room-green.png
/content/images/icon-general-default-room-orange-XL.png
/content/images/icon-general-default-room-orange.png
/content/images/icon-general-default-room-yellow-XL.png
/content/images/icon-general-default-room-yellow.png
/content/images/icon-general-default-room.png
/content/images/icon-general-emptyconvo-avatar-XL.png
/content/images/icon-general-emptyconvo-avatar.png
/content/images/icon-general-hold-avatar-XL.png
/content/images/icon-general-hold-avatar.png
/content/images/icon-general-openconvo-avatar-blue-XL.png
/content/images/icon-general-openconvo-avatar-blue.png
/content/images/icon-general-openconvo-avatar-green-XL.png
/content/images/icon-general-openconvo-avatar-green.png
/content/images/icon-general-openconvo-avatar-grey-XL.png
/content/images/icon-general-openconvo-avatar-grey.png
/content/images/icon-general-openconvo-avatar-orange-XL.png
/content/images/icon-general-openconvo-avatar-orange.png
/content/images/icon-general-openconvo-avatar-yellow-XL.png
/content/images/icon-general-openconvo-avatar-yellow.png
/content/images/icon-general-phonecall-avatar-XL.png
/content/images/icon-general-phonecall-avatar.png
/content/images/icon-general-phonecall-disabled-avatar-XL.png
/content/images/icon-general-phonecall-disabled-avatar.png
/content/images/icon-general-plus-avatar-XL.png
/content/images/icon-general-recording-avatar.png
/content/images/icon-general-sessionguest-avatar-XL.png
/content/images/icon-general-support-avatar-XL.png
/content/images/icon-general-support-avatar.png
/content/images/logo-toast.png
/content/images/noimg.png
/content/images/nopic-large.png
/content/images/nopic.png
/content/sounds/sound-account-logging-in.ogg
/content/sounds/sound-account-logging-out.ogg
```

```
/content/sounds/sound-call-control-hanging-up.ogg
/content/sounds/sound-call-control-hung-up.ogg
/content/sounds/sound-call-control-mute.ogg
/content/sounds/sound-call-control-muted.ogg
/content/sounds/sound-call-control-unmute.ogg
/content/sounds/sound-call-control-unmuted.ogg
/content/sounds/sound-calling-accepting-call.ogg
/content/sounds/sound-calling-busy.ogg
/content/sounds/sound-calling-call-accepted.ogg
/content/sounds/sound-calling-call-error.ogg
/content/sounds/sound-calling-call-rejected.ogg
/content/sounds/sound-calling-incoming-call-during-call.ogg
/content/sounds/sound-calling-incoming-call.ogg
/content/sounds/sound-calling-initiating-call.ogg
/content/sounds/sound-calling-rejecting-call.ogg
/content/sounds/sound-calling-ringback-tone.ogg
/content/sounds/sound-conference-call-ended.ogg
/content/sounds/sound-conference-call-ending.ogg
/content/sounds/sound-conference-call-joined.ogg
/content/sounds/sound-conference-call-joining.ogg
/content/sounds/sound-conference-call-last-leaving.ogg
/content/sounds/sound-conference-call-leaving.ogg
/content/sounds/sound-conference-call-left.ogg
/content/sounds/sound-conference-call-removed.ogg
/content/sounds/sound-conference-call-started.ogg
/content/sounds/sound-conference-call-starting-call.ogg
/content/sounds/sound-group-call-incoming-call.ogg
/content/sounds/sound-messaging-incoming-direct-message.ogg
/content/sounds/sound-messaging-incoming-group-message.ogg
/content/sounds/sound-messaging-message-error.ogg
/content/sounds/sound-messaging-message-sent.ogg
/content/sounds/sound-new-conversation-created.ogg
/content/sounds/sound-new-conversation.ogg
/content/sounds/sound-presence-end-snooze-notifications.ogg
/content/sounds/sound-presence-start-snooze-notifications.ogg
/content/sounds/sound-screenshare-accepted.ogg
/content/sounds/sound-screenshare-accepting.ogg
/content/sounds/sound-screenshare-ended.ogg
/content/sounds/sound-screenshare-ending.ogg
/content/sounds/sound-screenshare-incoming.ogg
/content/sounds/sound-screenshare-initiating.ogg
/content/sounds/sound-screenshare-rejected.ogg
/content/sounds/sound-screenshare-rejecting.ogg
/content/styles/sprites/bg-3rd-column-texture.png
/content/styles/sprites/bg-conversation-feed-item-focus-texture.png
/content/styles/sprites/bg-conversation-feed-item-hover-texture.png
/content/styles/sprites/bg-conversation-feed-item-me-texture.png
/content/styles/sprites/bg-conversation-feed-item-texture.png
/content/styles/sprites/bg-conversation-feed-texture.png
/content/styles/sprites/bg-conversation-feed-tornstrip.png
/content/styles/sprites/bg-search-highlighter-focused.png
/content/styles/sprites/bg-search-highlighter-normal.png
/content/styles/sprites/bg-timestamp-scroll.png
/content/styles/sprites/emoticons-large-sprite1443011112.png
/content/styles/sprites/emoticons-large2-sprite1443011112.png
/content/styles/sprites/emoticons-small-sprite1443011111.png
/content/styles/sprites/logos-sprite1443011113.png
/content/styles/sprites/main-sprite1443011110.png
/content/styles/sprites/mobile-sprite1443011113.png
/content/styles/sprites/progress-loader-sprite1443011113.png
/content/styles/sprites/progress-spinner-sprite1443011113.png
/content/styles/sprites/writing-indicator-sprite1443011114.png
/js/common/logFileWorker.js
/resources/i18n/resources-locale_de-DE.json
/resources/i18n/resources-locale_default.json
/resources/i18n/resources-locale_es-ES.json
/resources/i18n/resources-locale_fr-FR.json
/resources/releaseNotes/releaseNotes_de-DE.json
```

```
/resources/releaseNotes/releaseNotes_default.json
/resources/releaseNotes/releaseNotes_es-ES.json
/resources/releaseNotes/releaseNotes_fr-FR.json
/resources/releaseNotes/images/conferencepin.png
/resources/releaseNotes/images/moderatedsized.png
/resources/releaseNotes/images/muteall.png
/resources/releaseNotes/images/testcalls.png
/favicon.ico
/

NETWORK:
*
```

5.4 Auszug Circuit Debug Datei

%UserProfile%/Anwendungsdaten/Google/Chrome/User Data/%Profile%/
File System/000/t/00/0000000X

```
Browser Type: chrome
Browser Version: 47.0.2526.106
Web Client Version: 1.1.4107
Chrome Extension Version: 1.1.4107
Server Address: eu.yourcircuit.com
User name: Alice Musterfrau
Tenant ID: c2d60240-9f59-48d2-a290-352786b75889
User ID: b2d49d6d-fc8a-4487-9910-65e3b0b9a89d
Account: alice@circuit.acme.eu
…
16-01-04 11:25:34.497 DEBUG [UserProfileSvc]: Successfully subscribed to my own presence
16-01-04 11:25:34.497 INFO RECV: [ConnectionHandler]: {
   "apiVersion": "1.9.3-14",
   "msgType": "RESPONSE",
   "clientId": "94d69775-dfeb-4ac2-97dc-f93d68cd05f8",
   "response": {
      "requestId": 6,
      "code": "OK",
      "appNodeName": "app-02-ams1prod-eu",
      "type": "ADMINISTRATION",
      "administration": {
         "type": "GET_TENANT",
         "getTenant": {
            "tenant": {
               "id": "c2d60240-9f59-48d2-a290-352786b75889",
               "company": "circuit.sec-lab",
               "country": "DE",
               "mainContactId": "3e98714b-3636-4a97-8856-fb1a08164b12",
               "tin": "9653",
               "state": "ACTIVE",
               "isTrial": false
            }
         }
      }
   }
}
…
16-01-04 11:25:34.741 INFO [ConversationSvc]: The client has received 3 new/modified
conversations
16-01-04 11:25:34.741 INFO [ConversationSvc]: Conversations summary - [
   {
      "type": "OPEN",
      "convId": "c0306722-5cdc-4481-a31c-419c1bf3bce7",
      "rtcSessionId": "null",
      "userData": {
         "lastReadTimestamp": 1451297093485,
         "unreadItems": 0
      },
      "numParticipants": 4,
      "numFormerParticipants": 0,
      "creationTime": 1451297093479,
      "modificationTime": 1451755465355,
      "lastItemModificationTime": 1451297093485,
      "topLevelItemCreationTime": 1451297093485,
      "topLevelItemModificationTime": 1451297093485
   },
   {
      "type": "DIRECT",
      "convId": "09ac1d0a-d7e2-4099-a35f-edc637596b8d",
      "rtcSessionId": "97b9ff3f-6e72-46b8-976e-76a4784925b6",
      "userData": {
```

```
         "lastReadTimestamp": 1451902814691,
         "unreadItems": 0
      },
      "numParticipants": 2,
      "numFormerParticipants": 0,
      "creationTime": 1451303088151,
      "modificationTime": 1451303088151,
      "lastItemModificationTime": 1451902814691,
      "topLevelItemCreationTime": 1451902814691,
      "topLevelItemModificationTime": 1451902814691
   },
   {
      "type": "GROUP",
      "convId": "6b45ca14-2975-4417-ad6d-535ba54c5454",
      "rtcSessionId": "0974e6f9-5143-469b-a65c-7aba37015db9",
      "userData": {
         "lastReadTimestamp": 1451902800211,
         "unreadItems": 0
      },
      "numParticipants": 3,
      "numFormerParticipants": 0,
      "creationTime": 1451303131339,
      "modificationTime": 1451303220141,
      "lastItemModificationTime": 1451902896391,
      "topLevelItemCreationTime": 1451902896391,
      "topLevelItemModificationTime": 1451902896391
   }
]
16-01-04 11:25:34.743 INFO [ConversationSvc]: The client received less conversations than
it asked for, which means no older conversations are available
…
16-01-04 11:25:35.716 INFO RECV: [ConnectionHandler]: {
   "apiVersion": "1.9.3-14",
   "msgType": "RESPONSE",
   "clientId": "94d69775-dfeb-4ac2-97dc-f93d68cd05f8",
   "response": {
      "requestId": 17,
      "code": "OK",
      "appNodeName": "app-02-ams1prod-eu",
      "type": "USER",
      "user": {
         "type": "GET_USERS_BY_IDS",
         "usersByIds": {
            "user": [
               {
                  "userId": "3e98714b-3636-4a97-8856-fb1a08164b12",
                  "lastName": "Kirchner",
                  "firstName": "Michael",
                  "displayName": "Michael Kirchner",
                  "state": "OFFLINE",
                  "emailAddress": "admin@circuit.acme.eu",
                  "userPresenceState": {
                     "userId": "3e98714b-3636-4a97-8856-fb1a08164b12",
                     "state": "OFFLINE",
                     "mobile": false,
                     "poor": false
                  },
                  "tenantId": "c2d60240-9f59-48d2-a290-352786b75889",
                  "roles": [
                     "USER",
                     "TENANT_ADMIN"
                  ],
                  "locale": "DE_DE",
                  "userState": "ACTIVE",
                  "isExternallyManaged": false
               },
               {
                  "userId": "d823e1f1-e21d-4135-b004-4791d0736cfe",
```

```
                  "lastName": "Eve",
                  "firstName": "Evil",
                  "displayName": "Evil Eve",
                  "state": "OFFLINE",
                  "emailAddress": "eve@circuit.acme.eu",
                  "userPresenceState": {
                     "userId": "d823e1f1-e21d-4135-b004-4791d0736cfe",
                     "state": "OFFLINE",
                     "mobile": false,
                     "poor": false
                  },
                  "tenantId": "c2d60240-9f59-48d2-a290-352786b75889",
                  "roles": [
                     "USER"
                  ],
                  "locale": "DE_DE",
                  "userState": "ACTIVE",
                  "isExternallyManaged": false
               },
               {
                  "userId": "377fa6d0-6d8f-4675-8290-35a92a181d58",
                  "lastName": "Mustermann",
                  "firstName": "Bob",
                  "displayName": "Bob Mustermann",
                  "state": "AVAILABLE",
                  "largeImageUri": "43635ea0-37ca-410e-b65d-be3583c82812",
                  "smallImageUri": "81724e7d-c2ad-4d94-b413-62386c61161f",
                  "emailAddress": "bob@circuit.acme.eu",
                  "userPresenceState": {
                     "userId": "377fa6d0-6d8f-4675-8290-35a92a181d58",
                     "state": "AVAILABLE",
                     "inTransit": false,
                     "longitude": "******",
                     "latitude": "******",
                     "locationText": "******",
                     "timeZoneOffset": -60,
                     "mobile": true,
                     "poor": false
                  },
                  "tenantId": "c2d60240-9f59-48d2-a290-352786b75889",
                  "roles": [
                     "USER"
                  ],
                  "locale": "DE_DE",
                  "userState": "ACTIVE",
                  "isExternallyManaged": false
               }
            ]
         }
      }
   }
}
…
16-01-04 11:25:35.856 INFO RECV: [ConnectionHandler]: {
   "apiVersion": "1.9.3-14",
   "msgType": "RESPONSE",
   "clientId": "94d69775-dfeb-4ac2-97dc-f93d68cd05f8",
   "response": {
      "requestId": 19,
      "code": "OK",
      "appNodeName": "app-02-ams1prod-eu",
      "type": "CONVERSATION",
      "conversation": {
         "type": "GET_ITEMS_BY_CONVERSATION",
         "getItemsByConversation": {
            "items": [
               {
                  "type": "TEXT",
```

```
                  "itemId": "606ede80-a117-4d43-b034-d474bbe0fb4a",
                  "convId": "09ac1d0a-d7e2-4099-a35f-edc637596b8d",
                  "text": "******",
                  "creationTime": 1451472366088,
                  "modificationTime": 1451472366088,
                  "creatorId": "b2d49d6d-fc8a-4487-9910-65e3b0b9a89d",
                  "includeInUnreadCount": true
               },
               {
                  "type": "TEXT",
                  "itemId": "36c4688f-fd11-4d00-83e2-86fb0a769735",
                  "convId": "09ac1d0a-d7e2-4099-a35f-edc637596b8d",
                  "text": "******",
                  "creationTime": 1451472702067,
                  "modificationTime": 1451472702067,
                  "creatorId": "b2d49d6d-fc8a-4487-9910-65e3b0b9a89d",
                  "includeInUnreadCount": true
               },
               {
                  "type": "RTC",
                  "itemId": "e3798fab-e80b-49dd-b37f-43e026b43f55",
                  "convId": "09ac1d0a-d7e2-4099-a35f-edc637596b8d",
                  "rtc": "******",
                  "creationTime": 1451473733500,
                  "modificationTime": 1451473733500,
                  "creatorId": "b2d49d6d-fc8a-4487-9910-65e3b0b9a89d",
                  "includeInUnreadCount": false
               }
            ]
         }
      }
   }
}
…
16-01-04 11:26:06.656 INFO RECV: [ConnectionHandler]: {
   "apiVersion": "1.9.3-14",
   "msgType": "EVENT",
   "clientId": "94d69775-dfeb-4ac2-97dc-f93d68cd05f8",
   "event": {
      "uuid": "16b96ba5-14c4-4b1c-bd85-3a301d98eda9",
      "serialNumber": 14,
      "type": "CONVERSATION",
      "conversation": {
         "type": "ADD_ITEM",
         "convId": "6b45ca14-2975-4417-ad6d-535ba54c5454",
         "addItem": {
            "item": {
               "type": "RTC",
               "itemId": "364e0f53-6472-4bd9-a336-7ddbab7ffa8a",
               "convId": "6b45ca14-2975-4417-ad6d-535ba54c5454",
               "rtc": {
                  "type": "ENDED",
                  "participants": [
                     {
                        "userId": "b2d49d6d-fc8a-4487-9910-65e3b0b9a89d"
                     },
                     {
                        "userId": "377fa6d0-6d8f-4675-8290-35a92a181d58"
                     }
                  ],
                  "ended": {
                     "duration": 14745
                  },
                  "rtcParticipants": [
                     {
                        "userId": "b2d49d6d-fc8a-4487-9910-65e3b0b9a89d",
                        "displayName": "Alice Musterfrau",
                        "type": "USER"
```

```
                    },
                    {
                       "userId": "377fa6d0-6d8f-4675-8290-35a92a181d58",
                       "displayName": "Bob Mustermann",
                       "type": "USER"
                    }
                 ],
                 "extendedType": "ENDED"
              },
              "creationTime": 1451903159423,
              "modificationTime": 1451903159423,
              "creatorId": "b2d49d6d-fc8a-4487-9910-65e3b0b9a89d",
              "includeInUnreadCount": false
           },
           "convId": "6b45ca14-2975-4417-ad6d-535ba54c5454"
        }
     }
  }
}
…
16-01-04 11:26:34.979 INFO RECV: [ConnectionHandler]: {
   "apiVersion": "1.9.3-14",
   "msgType": "EVENT",
   "clientId": "94d69775-dfeb-4ac2-97dc-f93d68cd05f8",
   "event": {
      "uuid": "8c1163fe-40b5-4c86-8d90-521c51fe11a8",
      "serialNumber": 32,
      "type": "RTC_CALL",
      "rtcCall": {
         "type": "SDP_ANSWER",
         "sessionId": "97b9ff3f-6e72-46b8-976e-76a4784925b6",
         "instanceId": "97b9ff3f-6e72-46b8-976e-76a4784925b6_1451903190149",
         "sdpAnswer": {
            "clientID": "94d69775-dfeb-4ac2-97dc-f93d68cd05f8",
            "sdp": {
               "type": "answer",
               "sdp": "v=0
o=- 1451903194667 2 IN IP4 127.0.0.1
s=-
t=0 0
a=msid-semantic: WMS stream_label
m=audio 63746 UDP/TLS/RTP/SAVPF 103 9 0 8 106 105 13 126
c=IN IP4 159.8.16.70
a=rtcp:9 IN IP4 0.0.0.0
a=candidate:3904714321 1 udp 2122260223 192.168.178.42 61490 typ host generation 0
a=candidate:607128002 1 udp 1686052607 62.158.132.251 61490 typ srflx raddr
192.168.178.42 rport 61490 generation 0
a=candidate:3418205964 1 udp 41885951 159.8.16.70 63746 typ relay raddr 62.158.132.251
rport 61490 generation 0
a=candidate:3418205964 1 udp 25108479 159.8.16.70 49755 typ relay raddr 62.158.132.251
rport 55188 generation 0
a=ice-ufrag:VSJfRTgxAJNVHhsT
a=ice-pwd:HIF74JDvWuWo1uarEe/otPnu
a=fingerprint:sha-256
C0:B1:2D:3D:E9:FA:85:91:04:C3:76:34:1B:86:03:04:CA:8D:68:4E:7F:74:CA:D4:11:BF:DC:F0:F5:70
:3C:4A
a=setup:active
a=mid:audio
a=extmap:3 http://www.webrtc.org/experiments/rtp-hdrext/abs-send-time
a=sendrecv
a=rtcp-mux
a=rtpmap:103 ISAC/16000
a=rtpmap:9 G722/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:106 CN/32000
a=rtpmap:105 CN/16000
a=rtpmap:13 CN/8000
```

```
a=rtpmap:126 telephone-event/8000
a=ssrc:301381721 cname:vmysbkJUFf3MEHkr
a=ssrc:301381721 msid:stream_label audio_label
a=ssrc:301381721 mslabel:stream_label
a=ssrc:301381721 label:audio_label
m=video 55940 UDP/TLS/RTP/SAVPF 100 116 117 96
c=IN IP4 159.8.16.70
a=rtcp:9 IN IP4 0.0.0.0
a=candidate:3904714321 1 udp 2122260223 192.168.178.42 51322 typ host generation 0
a=candidate:607128002 1 udp 1686052607 62.158.132.251 51322 typ srflx raddr
192.168.178.42 rport 51322 generation 0
a=candidate:3418205964 1 udp 41885951 159.8.16.70 55940 typ relay raddr 62.158.132.251
rport 51322 generation 0
a=candidate:3418205964 1 udp 25108479 159.8.16.70 62375 typ relay raddr 62.158.132.251
rport 55190 generation 0
a=ice-ufrag:2U4Rb9IJooBi9SIn
a=ice-pwd:ojFBqVzxuqkkNJMxksZjnYnV
a=fingerprint:sha-256
C0:B1:2D:3D:E9:FA:85:91:04:C3:76:34:1B:86:03:04:CA:8D:68:4E:7F:74:CA:D4:11:BF:DC:F0:F5:70
:3C:4A
a=setup:active
a=mid:video
a=extmap:2 urn:ietf:params:rtp-hdrext:toffset
a=extmap:3 http://www.webrtc.org/experiments/rtp-hdrext/abs-send-time
a=extmap:4 urn:3gpp:video-orientation
a=inactive
a=rtcp-mux
a=rtpmap:100 VP8/90000
a=rtcp-fb:100 ccm fir
a=rtcp-fb:100 nack
a=rtcp-fb:100 nack pli
a=rtcp-fb:100 goog-remb
a=rtpmap:116 red/90000
a=rtpmap:117 ulpfec/90000
a=rtpmap:96 rtx/90000
a=fmtp:96 apt=100
"
            },
            "transactionId": "21e06e1b-c076-4aee-3c56-23af19db99d3",
            "sessionId": "97b9ff3f-6e72-46b8-976e-76a4784925b6"
         }
      }
   }
}
```