

Test DFI Case #2

Digital Forensic Report

Prepared by:

Naif Hussain (naif.hussain0@gmail.com)

Abdullah Alhakami (aalhakami.26@gmail.com)

Mohammad Alattas (mohammed.Alattas@outlook.sa)

Jawad Fakiha (jawadfageha@gmail.com)

Specialist field:

Digital Forensics

Table of Contents

1	Introduction	3
	1.1 Summary of Case	
	1.2 Software Applications	
2	Content Relating to Offence	4
3	Identification	9
4	Intent	10
5	Quantity of Files	18
6	Installed Software	19

Digital Forensic Report

1 | Introduction

The purpose of this report is to provide a comprehensive analysis of a dump copy for the Samsung GSM SM-G973F DS Galaxy S10 device that was used to buy a ticket using a stolen credit card. The facts within this report are those within the preparer's own area of expertise and knowledge and do not extend to matters and knowledge outside such expertise.

Samsung	GSM	SM-G973F	DS
Brand Name	Global System for Mobile communications (GSM), If you travel in Europe GSM is the only type of cellular service available. GSM phones can be unlocked and switch carriers.	Refers to a Samsung Galaxy S10 smartphone 15.5 cm (6.1")	Dual SIM

Dump Name:	3_Samsung GSM_SM-G973F_DS Galaxy S10
SHA-256:	54877505f1b4eb26c4cb6b43fd6338424660c207e678b773044a4a79d6e374b7
Image Type	Dump
Notes	---
Acquired on OS	---
Acquired Using	---
Acquired Date	---
Unique Description	3_Samsung GSM_SM-G973F_DS Galaxy S10

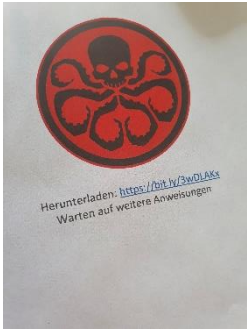
1.1 Summary of Case

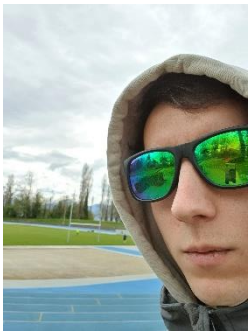
An individual on April 20th, 2021 at 18:30 tried to board a plane using a ticket bought with a stolen CC.

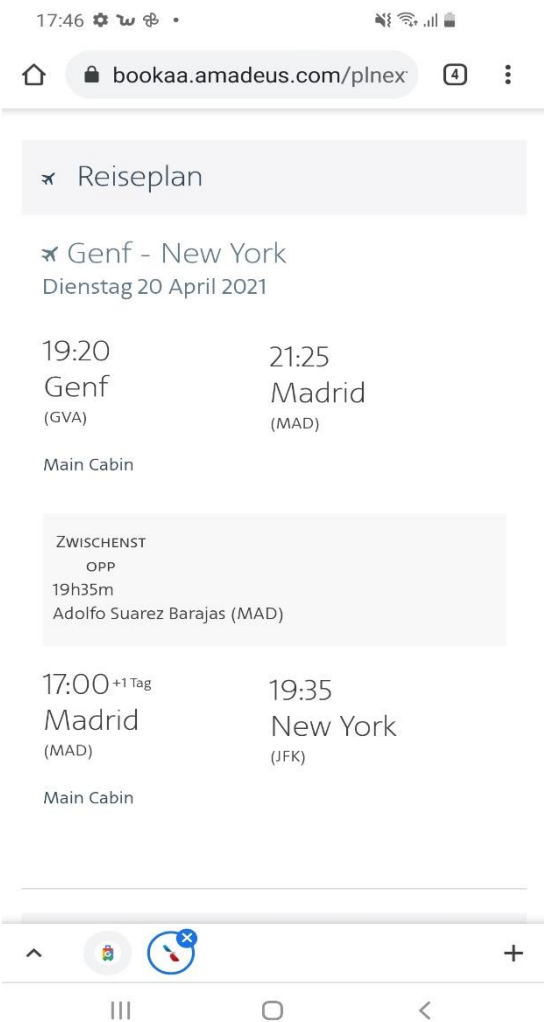
1.2 Software Application

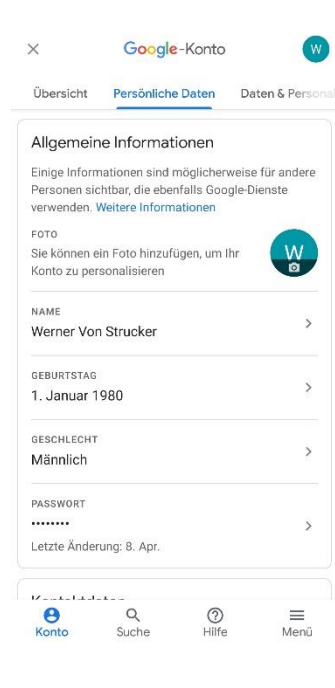
- Autopsy 4.19.3
- AccessData FTK Imager 4.2.0.13
- Audacity
- D2j-dex2jar
- Jadx
- ApkTool

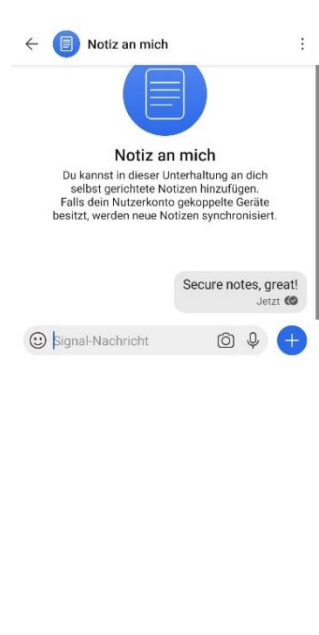
2 | Content Relating to Offence


	Filename	20210408_182133.jpg
	Location	/LogicalFileSet1/Dump/data/media/0/DCIM/Camera/20210408_182133.jpg
	MIME Type	image/jpeg
	Size	2322502
	Modified	-
	Accessed	-
	Created	2021/04/08 19:21:33
	MD5 Hash	5d23a808943d7a8715dcff1a0266b262
	Analysis	A picture taken that contains Hydra logo with a link that redirects to download a modified edition of OmniNote application.

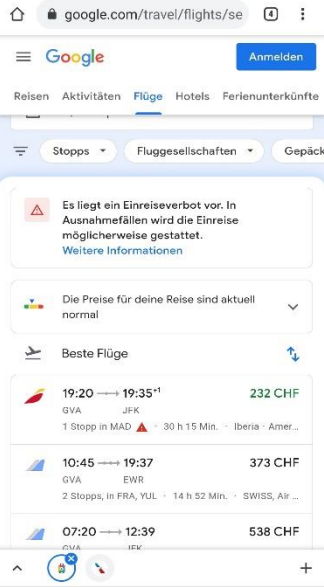
	Filename	IMG_20210411_144226.jpg
	Location	/LogicalFileSet1/Dump/data/media/0/DCIM/Camera/IMG_20210411_144226.jpg
	MIME Type	image/jpeg
	Size	1195948
	Modified	-
	Accessed	-
	Created	-
	MD5 Hash	933c06601d3ed61685132c4b1e52d4a6
	Analysis	Selfie for the owner of the phone, we indicate that he is Werner von Strucke


	Filename	Screenshot_20210418-174639_Chrome.jpg
	Location	/LogicalFileSet1/Dump/data/media/0/DCIM/Screenshots/Screenshot_20210418-174639_Chrome.jpg
	MIME Type	image/jpeg
	Size	228898
	Modified	-
	Accessed	-
	Created	-
	MD5 Hash	e954ed4e107dd668213715cb66eacbc4
	Analysis	A ticket for a transit flight from the airport of Geneva Madrid airport and then to John F. Kennedy International Airport in New York.

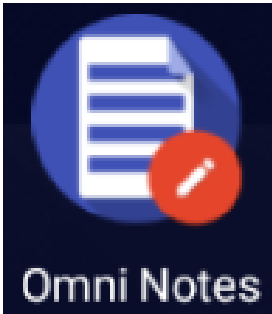
	Filename	f1459779.png
	Location	/LogicalFileSet1/Dump/data/system_ce/0/snapshots/141.jpg
	MIME Type	image/png
	Size	232822
	Modified	-
	Accessed	-
	Created	-
	MD5 Hash	-
	Analysis	A screenshot for Gmail information that contains personal information for Werner von Strucke.

	Filename	154.jpg
	Location	/LogicalFileSet1/Dump/data/system_ce/0/snapshots/154.jpg
	MIME Type	image/jpeg
	Size	152191
	Modified	-
	Accessed	-
	Created	-
	MD5 Hash	6247b810c1cdaf595371bf959c99b267
	Analysis	A screenshot from Signal that contains a suspicious note for self that mentions "Secure Notes", which mostly refers to the application that Hydra sent "OmniNote".

 <p>The screenshot shows a chat window with a blue header bar containing a red Hydra logo and a close button 'x'. The main area is titled 'Last Message Received' and contains a message from 'Dst # (Reserviert für RS)' that says: 'Btw Lay low, it seems your little fuckup with the Postomat had big consequences.' Below the message is a 'Send Message' section with a blue 'SEND' button and a text input field containing 'Dst # (Reserviert für RS)'. At the bottom, there is a greyed-out area with the text: 'will do. and again my apologies, will never happen again, i've installed the others much more carefully.'</p>	Filename	164.jpg
	Location	/LogicalFileSet1/Dump/data/system_ce/0/snapshots/164.jpg
	MIME Type	image/jpeg
	Size	150941
	Modified	-
	Accessed	-
	Created	-
	MD5 Hash	e8a5582f3f17a75e1b80c43e38be83e2
	Analysis	A screenshot from an application. We noticed that there is a similarity between the design of OmniNote and the application that used to communicate between Werner and Hydra. So we suspected that the application is modified, especially that there is a Hydra logo up left, that is not found on the application.

	Filename	175.jpg
	Location	/LogicalFileSet1/Dump/data/system_ce/0/snapshots/175.jpg
	MIME Type	image/jpeg
	Size	261705
	Modified	-
	Accessed	-
	Created	-
	MD5 Hash	86dfd4875e0a0630fe90d6ad3db976c9
	Analysis	Werner searched for a flight from the airport of Geneva to John F. Kennedy International Airport in New York.

	Filename	2021_04_09T1621.mp3
	Location	/LogicalFileSet1/Dump/data/media/0/Download/2021_04_09T1621.mp3
	MIME Type	audio/mpeg
	Size	1301392
	Modified	-
	Accessed	-
	Created	-
	MD5 Hash	066c187f3010f62a56c82298116ec3f8
	Analysis	The same audio of magnetic credit card information that we found in the skimmer_microSD_Physical case that led us to say it is the same credit card used to book the flight.

	Filename	OmniNotes-playRelease-6.1.0 Alpha 1.apk
	Location	/Dump/data/media/0/Download/OmniNotes-playRelease-6.1.0 Alpha 1.apk
	MIME Type	application/vnd.android.package-archive
	Size	7598422
	Modified	-
	Accessed	-
	Created	2021/04/08 , 19:42:48
	MD5 Hash	a995821e5cd6d63812a2be9669ae4211
	Analysis	A modified notes app, that has been modified and provided by Hydra to Werner to communicate in a secure encrypted way and has been download from the previous image 20210408_182133.jpg. (will be explained in Intention phase).

3 | Identification

Statements and evidence collected identified Hydra Organization is behind the incident and agent Werner von Strucke as a suspect of the skimming crime.

- Hydra logo with a link to download a special version of omninote for Werner von Strucke.
- A selfie found for Werner von Strucke.
- A screenshot for the profile of Werner von Strucke on google.
- Found the same credit card audio stolen from the skimming device used to book the flight.

4 | Intent

Is OmniNote malicious and why?

In the beginning, we found a collection of images that indicates that this phone belongs to Werner von Strucke and from the images, there is a suspicious image including the Hydra logo and a link to download a modified version of the OmniNote created for Werner von Strucke. After we reversed engineer and decompiled the modified version of the OmniNote application we found the following ...

While analyzing the apk file we found a class called MainActivity that define a counter variable and give it 5!

```
public class MainActivity extends BaseActivity implements SharedPreferences.OnSharedPreferenceChangeListener {  
    private static boolean isPasswordAccepted = false;  
    ActivityMainBinding binding;  
    private FragmentManager mFragmentManager;  
    private int open_comm_counter = 5;  
    boolean prefsChanged = false;  
    private Uri sketchUri;
```

This variable has been used in a function called openComm that has an if statement to make an object of CommActivity class if the condition was true, that means if the user clicks 5 time on a specific label it will appear a new frame.

```
    public void openComm(View view) {  
        String str = "Open Comm in -" + String.valueOf(this.open_comm_counter);  
        if (this.open_comm_counter == 0) {  
            this.open_comm_counter = 5;  
            startActivity(new Intent(this, CommActivity.class));  
        }  
        this.open_comm_counter--;  
    }
```

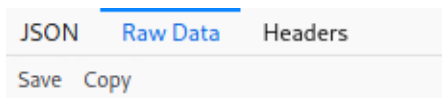
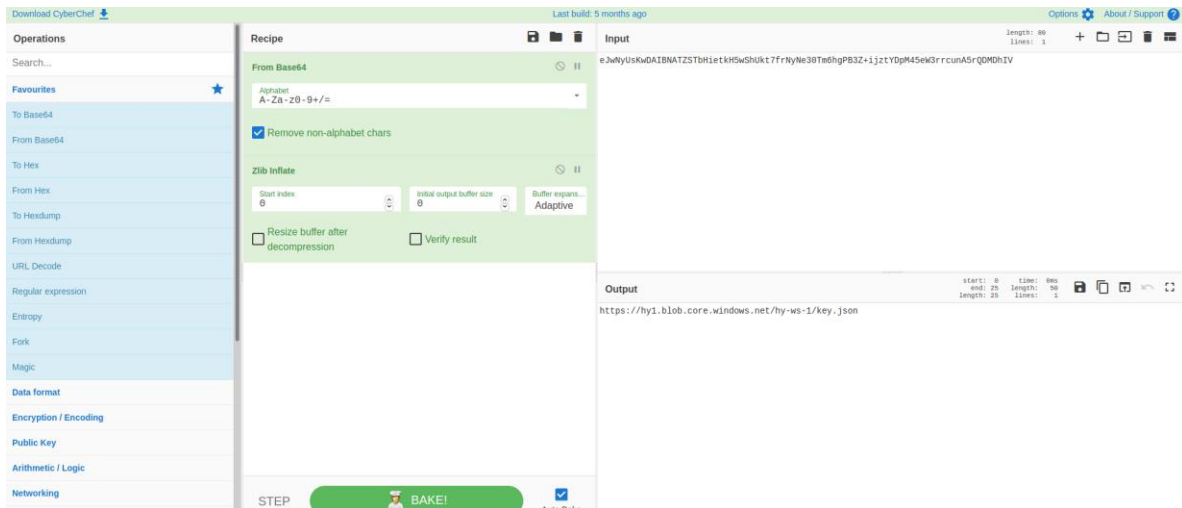
Therefore the CommActivity class has a function called putComm and it use SmsManager class to sends message via SMS . Also there is a variable put that deal with suspicious TextHelper class.

```
public void putComm(View view) {
    String put = new TextHelper(getResources()).put(((EditText) findViewById(R.id.text_multiline_msg_send)).getText().toString());
    if (put.length() > 160) {
        Toast.makeText(this, ZipHelper.decomp("eJwFQLEnWDAIe8UH5I1u6ZL2gQgs1AUPqEuR1eanI6bVTuIV8JUXsCi/OY832ED99UM+Q=="), 0).show();
    } else if (put.equals(BuildConfig.FLAVOR)) {
        Toast.makeText(this, ZipHelper.decomp("eJwFgLEJACAMBffJMpaCK6R4QhqV+/mLsOARb/Zkb8WnaUBZ9oIuA=="), 0).show();
    } else {
        Toast.makeText(this, ZipHelper.decomp("eJwFQLEJADAMESU7+kOmXlCoSBYX7x/kOn8tDJMhHhQ48AYI") + put + " to " + rsn(), 0).show();
        PendingIntent.getActivity(this, 0, new Intent(this, CommActivity.class), 0);
        SmsManager.getDefault().sendTextMessage(rsn(), null, put, null, null);
    }
}
```

Starting analyzing the suspicious TextHelper class we noticed that there is a function called get_data(), this function stores the key in decomp variables (The key in the URL provided but it is encoded using base64 and Zlib inflate). This function returns the KEY (Constant) + DATE (unstable depending on the date the message was received/sent)

```
private String get_data() throws IOException, JSONException {
    String decomp = ZipHelper.decomp("eJwFQLEnWDAIe8UH5I1u6ZL2gQgs1AUPqEuR1eanI6bVTuIV8JUXsCi/OY832ED99UM+Q==");
    HttpURLConnection httpsURLConnection = (HttpURLConnection) new URL(decomp + ZipHelper.decomp("eJwFwIEIAAAACC0/a10AEAAQ==") + ZipHelper.decomp(this.resources.getString(
    try {
        BufferedReader bufferedReader = new BufferedReader(new InputStreamReader(httpsURLConnection.getInputStream()));
        StringBuffer stringBuffer = new StringBuffer();
        while (true) {
            String readLine = bufferedReader.readLine();
            if (readLine != null) {
                stringBuffer.append(readLine);
            } else {
                String string = new JSONObject(stringBuffer.toString()).getString("key");
                String format = new SimpleDateFormat(ZipHelper.decomp("eJwFwIEIAAAACC0/a10AEAAQ=="), Locale.getDefault()).format(new Date());
                return string + format;
            }
        }
    } finally {
        httpsURLConnection.disconnect();
    }
}
```

When we decoded it we found URL that leads to a JSON file that includes the following KEY “rb5CuefkDLyb9T”



In this function we can notice that there are three characters “HHY” that will always be appended to the base64 encoded AES encrypted message.

```
private String open_msg(byte[] bArr) throws NoSuchPaddingException, NoSuchAlgorithmException, InvalidParameterSpecException, InvalidAlgorithmParameterException, InvalidKeyException, BadPaddingException {
    SecretKeySpec secretKeySpec = new SecretKeySpec(get_data().getBytes(), "AES");
    Cipher instance = Cipher.getInstance("AES/ECB/PKCS5Padding");
    instance.init(2, secretKeySpec);
    return new String(instance.doFinal(bArr), "UTF-8");
}

78 public String put(String str) {
79     try {
80         return "HHY" + Base64.encodeToString(save_msg(str), 2);
81     } catch (IOException | InvalidKeyException | NoSuchAlgorithmException | InvalidParameterSpecException | BadPaddingException | IllegalBlockSizeException | NoSuchPaddingException | JSONException | JSONException u
82     ) {
83         return BuildConfig.PLAYOFF;
84     }
85 }
```

Finally there is a function called OpenVMS(), This function basically takes a key from get_data() function and store it in secretKeySpec variable using AES algorithm/ECB mode, Then it uses Cipher class to use define the algorithm and the mode of encryption then use init method to decrypt and finally print the message decrypted.

```
private String open_msg(byte[] bArr) throws NoSuchPaddingException, NoSuchAlgorithmException,
    InvalidCipherTextException {
    SecretKeySpec secretKeySpec = new SecretKeySpec(get_data().getBytes(), "AES");
    Cipher instance = Cipher.getInstance("AES/ECB/PKCS5Padding");
    instance.init(2, secretKeySpec);
    return new String(instance.doFinal(bArr), "UTF-8");
}
```

Steps to decrypt the message :

- Message encrypted content after delete the first 3 characters "HHY"
- KEY+DATE(YYYY-MM-DD,date of the message receives)
- AES algorithm to decrypt the message
- Base64 decode
- Message is decrypted successfully (Plaintext).

The result of following the steps will be as shown in the following picture:

The screenshot shows a web-based AES Online Decryption tool. The interface is light gray with white input fields and blue buttons. At the top, the title 'AES Online Decryption' is in bold. Below it, the label 'Enter text to be Decrypted' is followed by a text input field containing 'ZEuQn5pAlhKmulAHVx55cA=='. The 'Input Text Format' section has two radio buttons: 'Base64' (selected) and 'Hex'. The 'Select Mode' dropdown menu is set to 'ECB'. The 'Key Size in Bits' dropdown menu is set to '192'. The 'Enter Secret Key' section has a text input field containing 'rb5CuefkDlyb9T2021-04-08'. A blue 'Decrypt' button is located below the key input. The output section is labeled 'AES Decrypted Output (Base64):' and features a text input field containing 'SGVpbCBleWRyYSE='. Below this, a blue 'Decode to Plain Text' button is present. At the bottom, a text input field displays the final result: 'Hell Hydra!'.

AES Online Decryption

Enter text to be Decrypted

ZEuQn5pAlhKmulAHVx55cA==

Input Text Format: ☒ Base64 ☐ Hex

Select Mode

ECB

Key Size in Bits

192

Enter Secret Key

rb5CuefkDlyb9T2021-04-08

Decrypt

AES Decrypted Output (Base64):

SGVpbCBleWRyYSE=

Decode to Plain Text

Hell Hydra!

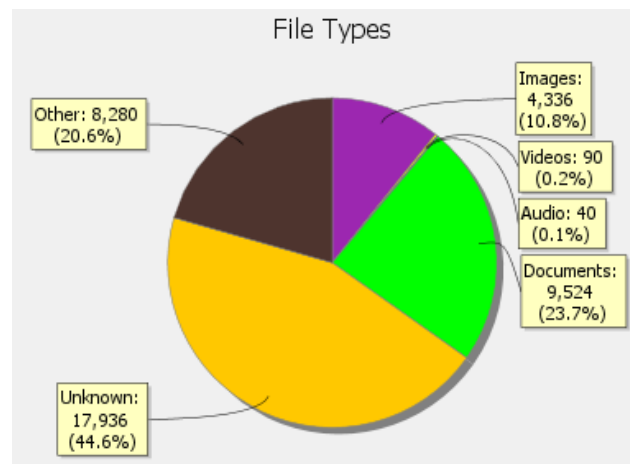
A table for all outgoing/ingoing messages in Werner's phone (the highlighted rows are the messages that was sent/received from OmniNote application to communicate between Hydra Organization and Werner):

Date/Time	Direction	Encrypted Message	Decrypted Message
2021-04-08 20:09:21 AST	Outgoing	HHY6cKEMFINU3NPs/bxhx PKQRyDXUrQK7a8tHtX5xB XdYQ=	Heil Hydra 🌀!
2021-04-08 20:10:33 AST	Incoming	HHYZEuQn5pA1hKmulAH Vx55cA==	Heil Hydra!
2021-04-08 20:11:08 AST	Outgoing	HHYU1+uAKNdKlj0YsLDm mJw3M2bFrI0/R5oPXCCfJ YqUwZ6z+usTidJxqnRJuW Eeiw8po5Hi1Gf6AaNdxUe qGBq+g==	Apologies for the email. Will never happen again.
2021-04-08 20:12:51 AST	Incoming	HHYKvEbze+wdEalheouf7 A2m98++suLv5Dv4GHZKF M4lpw=	Sure hope so for you.
2021-04-08 20:14:13 AST	Incoming	HHYsskk9VxsMQLIQ5jsWV GKu0cikDEZYDdgJOW//zK ch62LATxcR5WGFF6MtRtD WHJhLYMHxZ2TgngAqvsZr SsJKcHmTmIYAVR3P/U0un eLDbBbZkGDKzMjkb9349 ydCAT	Identify the best places for the items we sent you. Install them ASAP. I want Zola to proceed.
2021-04-08 20:16:54 AST	Outgoing	HHYbRTTaGxxLatLwNLMF 7ptPDTjpMnxkpy53B6M 6sPV9khvr0kKZpEK0zmG7 uAJa79	Will do. I've already some ideas.Hail Hydra!
2021-04-09 18:10:10 AST	Outgoing	HHYCIUGa/i7pLYjRGwzXrv pVg==	Hail Hydra!
2021-04-09 18:11:13 AST	Incoming	HHYCIUGa/i7pLYjRGwzXrv pVg==	Hail Hydra!
2021-04-09 18:13:53 AST	Outgoing	HHYBNsxyjLdeJ2KD5cKwn O1A81zVE6Xad+i+X0wojD 9jsFUumW48isXBeodD7cP CEAJ1r8fSw2D3FzsmCD5u 2Tavch2MC8acODGbE20i mqxTGhoeZC8UrJg5AThV C4McgpSfzlaRiuC77a6k2A 81IYd7A==	Installed second device today but something went wrong. Lots of policemen on place 15min after. I'm worried.

2021-04-09 18:15:16 AST	Incoming	HHYoD/v/R9xC1A8TqJ/U WCf/pdR9nO4f85nxcgE3G KZBwJspL7YqyD5PtqGT8p TXlhlcJHuQXIn4Gro+BYU2 FxiI5ingKEy6BHoYedEMSG Wdj0=	Proceed as planned, Ward will take care of that if it escalates.
2021-04-15 09:49:43 AST	Incoming	HHY2NToA10DeweA+V3m utF9QA==	Hail Hydra!
2021-04-15 09:50:11 AST	Outgoing	HHY2NToA10DeweA+V3m utF9QA==	Hail Hydra!
2021-04-15 09:51:05 AST	Incoming	HHYHiiOyvP7s0llu5N2ta9y /Qsk5FeloFJOXZvQpzDR7p 9XBQHyYuhfdel6g3OUs4cj	What's the status on the devices?
2021-04-15 09:52:48 AST	Outgoing	HHYOeHfDhFU8pIFmx7J5 qXltG1XGwpcbrBtUjNSeR OwGZ95dNIEMUGQFJdO7 n3U3m6PaSjcUUKMY9yQZ kdmuluV6UhxQ+j33/Vyjc +z2+hAVo=	Installed two more in the scouted locations. still have a couple available.
2021-04-15 10:02:17 AST	Incoming	HHYiNf68BXbaolSBtAav5y YU7WHDHaADyWmtazUb SOTFTukKKj2wv4zRTpjf+l9 n3sb/YUXpRbOjQmos4+Ql 8Np1Q==	Good... everything is still calm despite Friday incident.
2021-04-15 10:03:13 AST	Incoming	HHYbm0jyH9MsbIM1Dsyt NU9iDm63RQa9/1FxfRs/A 75m3wAM04VwDGphJ4m 9IUTjPQ//3qbJmQkxQQu 50WmK0zLHj93BiByuFEHs vHwzcfHsl=	We need to meet you. Get to geneva asap, further instructions will follow.
2021-04-15 10:05:00 AST	Outgoing	HHYS6+p9IajgCnkXlm0tou uBzw/c5dSk4ZVzCEeA7BZ mnR7+J5ybgmhLeXCypw ovM8yFaK1NQtfAJXHKwH nMGIxg==	understood, was headed to geneva anyway, already on a train.
2021-04-15 10:13:37 AST	Incoming	HHYcdZD5nSpEbiNiPHaM n/eJR3qfnG1bBjxHLgN2Q9 1Jjx+DaAtq15BuatyPqSSH 0ZOqLPbis211525r4RIkum QSF1p8xjb7tbOHzWN250 Sqmoh9v+9kcE6lnWMOcY Ho4ub	Good. Meet us at our base. Below the Turkish consulate. Delete this message once read!
2021-04-15 10:16:19 AST	Outgoing	HHY9frkML1o7eM6Ri32ER hNUEnmIbDg1syRQ+CP5z cYWYQ=	wilco hail hydra!
2021-04-15 10:17:08 AST	Incoming	HHY2NToA10DeweA+V3m utF9QA==	Hail Hydra!

2021-04-15 12:54:54 AST	Outgoing	HHY6JGyTGtI0Ij8PgtU2T/ w5YPNCw1PhZ/Lagr4Mhn CQhX+q36vX3TeUBZ6r/od TJU	Installed device at airport as discussed
2021-04-18 18:00:47 AST	Incoming	HHYj6DtE+EQdYzoKjUoVP 8DQw==	Hail Hydra!
2021-04-18 18:01:08 AST	Outgoing	HHYj6DtE+EQdYzoKjUoVP 8DQw==	Hail Hydra!
2021-04-18 18:01:27 AST	Incoming	Cher client, votre crédit disponible est inférieur à CHF 10.00. Meilleures salutations, votre équipe Coop Mobile	
2021-04-18 18:02:10 AST	Incoming	HHYqDAJ2HSbMahjfWcjFc L8H41ALcW17JkzdXUV02 H4eHGTt+6mU+twizvAsvd MU6FkiUHHrPcLzbiBsCV99 j/skyID1A6fR7cocoqjOb61 DM8=	We sent you the payment to the address you provided us. confirm reception.
2021-04-18 18:02:56 AST	Outgoing	HHYRvZdXk+/U616OwdSp 1fk350QysrJXGGJ9XkQkDI gFI0sMmxZm8fbD0SYK5O N8zcc	Understood, Payement receiced successfully.
2021-04-18 18:05:14 AST	Incoming	HHY97NA5dDGdqomydjZt 0GGycKgRS2T2vltp40yuO Ao9azlfHzaNR3r2Fw78GX BuVC4YIifClzf+VKxxK13O2 MgHwKDeGxIGva+uFj7wL +YnpKhdeGdwLiZ2/wszZN 9dKlx	Btw Lay low, it seems your little fuckup with the Postomat had big consequences.
2021-04-18 18:06:46 AST	Outgoing	HHYgSQ2GGQd5ZEvKdOk 5qRrWfoEH0baqjRkTwacp wgxp02qqrNOueQ0z31KEi L65EZCnHrjYy+7qbqFiVcCJ CBnXnQdMC1MI64+dyXku K6e/9I/ebQM3ZaAhqNLbl HNPOkTv35Hz1VseDqLE1 YpOPI4YQ==	will do. and again my apologies, will never happen again, i've installed the others much more carefully.
2021-04-18 18:30:22 AST	Outgoing	Hey Jackie! Hope you alright! Thanks for the coffee money! Sent you back the money for the pizza on BRD!	

5 | Quantity of Files



File Type	Quantity
xml	155
json	1417
vnd.android.package-archive	609
x-matroska	30
x-sh	50
x-sqlite3	881
x-gzip	226
related	4
appledouble	3
css	123
x-jsp	6
x-matlab	30
x-pascal	3
x-python	298
x-vcard	1
x-java-properties	43
x-web-markdown	2
plain	4416
xml	2747
html	171
x-ini	3
x-log	71
mp4 (video)	17
quicktime	73

File Type	Quantity
vnd.microsoft.icon	4
gif	116
png	1614
jpeg	1757
svg / xml	26
vnd.zbrush.pcx	274
webp	845
mp4 (audio)	39
mpeg	33
vnd.wave	7
vorbis	127
x-xz	3
zip	93
x-executable	1
x-gtar	2
octet-stream	17936
java-archive	123
xmd-dtd	1
javascript	423
x-dex	3
x-object	3
pdf	1
x-font-ttf	256
x-sharedlib	5140

6 | Installed Software

Software	Software Purpose
OmniNotes-playRelease-6.1.0 Alpha 1.apk	A special version of a tricky software provided by Hydra to Werner von Strucke to create a secure communication channel that sends and receives SMS messages between the organization and the agent, which has a hidden page that encrypts the messages by using AES/ECB/PKCS5PADDING encryption and Base64 encode with padding techniques that pads "HHY" characters to achieve strong encryption for the messages.
Signal	A software that was used for Werner himself to remind himself that the Secure Notes app which is OmniNote is the app he use to communicate with his affiliation.