A Forensic Analysis of an Emotionally Intelligent Device: The EmoSPARK

Will Perry
wperry@stu.norwich.edu
PO Box 517
East Barre, VT 05649
Faculty Advisor: Prof. Huw Read

May 1, 2016

1 Abstract

Considerable effort has been spent exploring potential repositories of information on devices commonly recovered in the course of an investigation. These devices present investigators with a wealth of information about an individuals relationship and activity patterns. However, these devices are often limited in terms of providing insight into a users state of mind. The next generation of intelligent devices will more fully be aware of a users state of mind and thus provide another view to investigators. The availability of emotional evidence could prove crucial to a variety of investigations such as domestic abuse or home invasion where there are traditionally few witnesses. The recent release of EmoShapes emotion detecting EmoSPARK highlights the importance of preparing for the eventuality of these devices. This study aims to discover methods of data recovery on the EmoSPARK.

Contents

2 Introduction

Todays investigators are presented with a plethora of data sources from which to piece a crimes story together. From mobile devices to social media accounts, and even gaming profiles like those on Xbox Live or Playstation Network, forensic investigators have a massive amount of data to comb through. This data will often illuminate connections in the evidence or create new leads that would otherwise have remained hidden from view. However, in several types of crimes these data points do not provide a complete picture of the events that led to the crime in question.

Crimes such as domestic violence or home invasion often have few witnesses and involve either close interpersonal relationships in the case of domestic violence or complete strangers in the case of home invasion. As such, they are difficult to investigate and combing through the usual data sources provide few clues to investigators as to the cause or other contributing factors of the crime. In both cases, some form of emotional and verbal record just prior to or during the crime could prove extremely valuable to investigators. In the case of domestic violence, this type of record could highlight a history of violence in the house or an elevated emotional response, such as a fight, that would provide the context necessary to connect evidence together. In a home invasion the record would provide a view into the relationship between the victims and the perpetrators and make it possible to more easily evaluate the contributing factors to any violent crimes. The current trend of mobile devices and software make it likely that an omnipresent device or service will be developed in the near future that will have some form of emotional detection.

As of writing there are several devices and services that use a variety of contextual information to anticipate the needs or wants of a user. Examples of these include the Google Now service provided with all Google accounts and Amazons practice of anticipatory shipping to move products closer to consumers even before they order. While these services use a data points, such as commonly travel destinations or purchase history, to make incredibly accurate predictions, they do not make any judgements based on a persons emotions.The recent arrival on the market of Emoshape Ltd.s EmoSPARK provides a glimpse into the future of the industry and a possible source of an emotional record.

The EmoSpark is advertised as being able to detect and interpret eight primary emotions: Joy, Sadness, Trust, Disgust, Fear, Anger, Surprise and Anticipation[5]. While a great deal of the processing is accomplished by a remote server it is our hope that there will remain some record of a users emotions on the devices memory. This project aims to discover and document a method of data acquisition that a forensic investigator may follow should the EmoSpark be encountered in the course of an investigation.

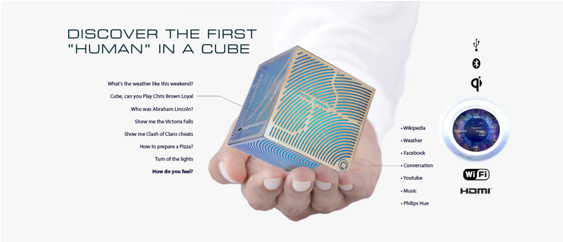


Figure 1: Features of the EmoSpark as listed on www.emospark.com

[5]

3 Literature Review

There exists a great deal of existing work documenting data acquisition with common devices. Due to the innovative nature of the EmoSpark and its relatively recent release there has been no work done to examine it or similar devices such as the Amazon Echo. However, after reviewing product material available on the EmoSpark website it was ascertained that the device is, in its most basic form, an Android tablet. The software that makes EmoSpark unique runs as an Android application in much the same way as applications from the Google Play Store do. As a result we focused our review of existing techniques on Android and embedded system acquisition methods.

While a great deal of material was reviewed in the interest of being thorough several works stood out as being especially relevant. The first of these was Android Forensics: A Physical Approach[2]. This article provided a brief overview of the Android operating system and how different pieces of the operating system work together. The authors also described in detail a common method of acquisition using ADB (Android Debugging Bridge) to push a variety of utilities onto the device in question.

The next article, Forensic analysis of the android file system YAFFS2[1], provided an in depth description of how the flash-based YAFFS2 file system used on Android devices differs from traditionally used memory formats. This information would be invaluable to an investigator dealing with a sophisticated user who had manipulated the file system in order to hide information. Additionally, the article described in their method a workaround to the root access problems that were described in Android Forensics: A Physical Approach. That is, the authors described using a known Android exploitation tool, called SuperOneClick, to gain root access to a device. The authors then used ADB and yaffs2utils to retrieve the devices data.

New acquisition methods based on firmware update protocols for Android smartphones[14] provided an overview of an alternative, albeit riskier, approach to performing a memory dump. The authors described how they had reverse engineered the firmware update protocols on three devices, of different manufacturer origin, so that they could then load their own, custom-made firmware onto the devices. In this way, they could have access to the memory through the firmware as opposed of through the operating system. This has the advantage of not needing any sort of traditional access to the phone in order to retrieve data. However, there is some risk involved with replacing the firmware on a device as it could render the device inoperable.

Amazon Kindle Fire HD Forensics[7] was reviewed because of Amazons extensive work on altering the Android OS. While the methods of extraction described in the article were nearly identical to those described in previously mentioned articles, the authors described using a modified active power cable in order to load a custom boot loader onto the device. This boot loader would allow an investigator direct access to the memory in a similar manner to custom firmware.

Andrew Hoogs Android Forensics[6] provided a great deal of background information that made it possible to understand the rest of the literature described. The book went into detail about the design of the Dalvik Virtual Machine (DVM) which all Android apps run inside and the boot process of the operating system. This provided a general understanding of the critical components of any Android device. Most importantly for this experiment was Hoogs identification of potential locations of user data. By default the Android OS stores user data in a /data/data directory. Within this directory there are subdirectories labelled by app name. However, it was noted that apps are increasingly choosing to store user data on an internal SD card, be that virtual or physical, where an app may choose what directory format to use.

Lastly, one of the most potent sources of information about the EmoSpark came from the devices community forums[12]. It was here that we were able to not only find a great deal of device specific information from individuals attempting to find novel uses for the EmoSpark but also to contact two individuals who had done minor backwards engineering on the device itself. These individuals, usernames of Drago2308 and DarkSpartan, provided details on how they had used Google Play Store apps to extract the EmoSpark APK and transfer those files over a wireless network to a computer for analysis. This proved to be the method through which the majority of information was later identified.

4 Experiment Definition

Given the limited time frame of this experiment, all features of the device were not able to be extensively tested. The team was most concerned with the device as a possible repository for personal information and as a record of events. As such the experiment was designed to explore the features of the device that would most likely yield those results.

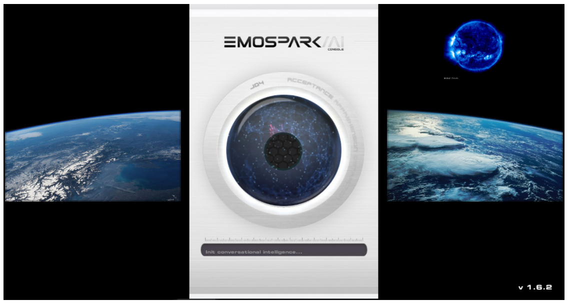


Figure 2: EmoSpark app running on a TV [12]

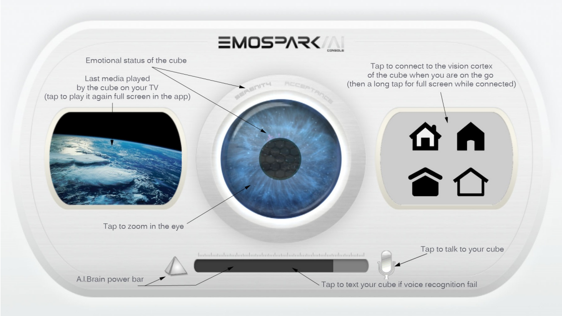

EMOSPARK AI
CONSOLE
Emotional status of the cube
Last media played
by the cube on your TV
(tap to play it again full screen in the app)
SERENITY
ACCEPTANCE
Tap to connect to the vision cortex
of the cube when you are on the go
(then a long tap for full screen while connected)
Tap to zoom in the eye
Tap to talk to your cube
A.I.Brain power bar
Tap to text your cube if voice recognition fail

Figure 3: EmoSpark companion app [5]

4.1 Device Features

The EmoSpark has been advertised having the ability to integrate with a users Facebook, query Google Search, Youtube and Wikipedia and connect to an external IP camera. Most importantly to this research, the device reportedly detects and interprets the eight primary emotions of Joy, Sadness, Trust, Disgust, Fear, Anger, Surprise and Anticipation. The device is still very primitive and requires the user to install and use a companion app on a tablet or phone to interact with the device. The rest of the interaction and results take place through the TV that the EmoSpark is plugged into via an HDMI cable. An IP camera is available for facial recognition but was not used for the purposes of this project because of our focus on user data stored on the device.

The EmoSpark is, in its simplest form, an android tablet. It is possible to plug USB peripherals into the open USB port on the outside of the device or associate other bluetooth devices after in order to navigate through settings menus. The manufacturer also left applications typical of an Android tablet installed such as the Google Play Store, a Gmail client and Google Maps. It was discovered through the user community forums that the device is rooted by default. The availability of the Play Store and root access allow a curious individual complete access to the device through standard forms such as the settings page or through third party applications from the Play Store.

4.2 Experimental Goal

As stated above, the goals of this experiment is to discover a method through which forensic professionals could acquire data from the EmoSpark if such a device were recovered during the course of an investigation. Most importantly, we hope to identify the location of personal data such as query requests and entries into some form of emotional record. Additionally, our secondary goal is to capture a process that forensic professionals may follow in order to recreate our results. It is our hope that this will prove valuable for future investigations.

5 Design and Development

The experiment was designed to most closely mimic an average user. Thus, when presented with any menu or form of choice we defaulted to pressing the most obvious selection and entered information only when absolutely necessary. That being said, a great deal of preparation was done in order to capture both the data fed into the device and also any signals given off by the device that were transient in nature. These transient signals included network captures and the Android system buffer logs.

5.1 Forensic Integrity

Forensic integrity was an important aspect of all activities during the course of the experiment. All activities were initially conducted with special attention paid to conform as closely as possible to the current standards of a forensic investigation. However, as methods of acquisition were tried and ruled out as viable, riskier methods were attempted in hopes that some data could be extracted.

5.2 Planned Methodology

5.2.1 Input Methods

The primary means of data input consisted of a spoken or written query through the companion app on a tablet. Several tablets were attempted before finding one that consistently worked with EmoSpark. The first tablets attempted were an Asus Nexus 7 running Android 6.0.1 (Marshmallow) and a Samsung GT-N8013 (Galaxy Note 10.1) running Android 4.1.2 (Jelly Bean). While it was never clear to the authors why the first pair of tablets did not function correctly, it is believed that an incompatibility between the Android version and the companion app was the culprit. A Samsung SM-T230NU (Galaxy Tab 4) running Android 4.4.2 (KitKat) was found to consistently function correctly. Queries were performed entirely by one individual so as to maintain a consistent emotional profile. Queries were created to cover the majority of the features advertised:

- Facebook integration
- Audio/video media functionality
- Ability to serve Google Search results
- Conversational voice comprehension
- Emotions processing

It is the opinion of the authors that these handful of features would most frequently be used and thus be the largest source of information to investigators. Sample queries:

> Who was Abraham Lincoln?
>
> Check the weather for tomorrow?
>
> Play world's largest rope swing from YouTube.
>
> How do you feel?

5.2.2 Emotional Variance

Testing the full range of emotions was the chief concern of the project. The experimenter attempted to mimic emotions that the device would encounter through regular use by altering the tone of voice, type of language used in each queries, direct interaction with the device through questions and answers and content requested. The full range was not tested in each session with the device but instead the device was used over a period of several weeks to facilitate this. The longer test period was also considered to have the inherent benefit of testing the ability of the device to recall previous interactions.

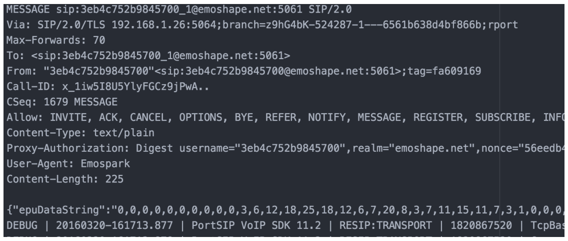
5.2.3 Extraction Methods

A variety of methods were to be used to capture data from the device. Tools such as Wireshark and tcpdump were used to capture network traffic. These tools would be employed throughout the entirety of the experiment. In the early stages of the project the nmap network scanning tool was used to detect any ports that might be open and responsive on the device.

Our initial steps in system forensics was to perform a complete a non-invasive physical image of the device. From there we believed that we could perform any operation on the device and be able to restore it original conditions. The next step in our process was to capture a logical image of the device before and after some use to get a better idea of the systems structure. After data locations were identified in this simpler image, the device would be used and successive images would be taken with data analysis occurring in the interim between use sessions. Finally, as a last resort, an invasive physical extraction would be performed using JTAG or chip-off methods.

6 Experiment

Performing a forensic analysis of the EmoSpark proved to be much more difficult than anticipated. Many of the planned extraction methods were more time intensive or impossible to execute than originally planned. As a result, there was a great deal of deviance from the planned steps described in the section above. However, the general thrust of locating potential repositories of user data and a form of record on the device was maintained.



```
MESSAGE sip:3eb4c752b9845700_1@emoshape.net:5061 SIP/2.0
Via: SIP/2.0/TLS 192.168.1.26:5064;branch=z9hG4bK-524287-1---6561b638d4bf866b;rport
Max-Forwards: 70
To: <sip:3eb4c752b9845700_1@emoshape.net:5061>
From: "3eb4c752b9845700"<sip:3eb4c752b9845700@emoshape.net:5061>;tag=fa609169
Call-ID: x_1iw5I8U5YlyFGCz9jPwA..
CSeq: 1679 MESSAGE
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, REGISTER, SUBSCRIBE, INF
Content-Type: text/plain
Proxy-Authorization: Digest username="3eb4c752b9845700",realm="emoshape.net",nonce="56eedb4
User-Agent: Emospark
Content-Length: 225

{"epuDataString":"0,0,0,0,0,0,0,0,0,0,3,6,12,18,25,18,12,6,7,20,8,3,7,11,15,11,7,3,1,0,0,0,
DEBUG | 20160320-161713.877 | PortSIP VoIP SDK 11.2 | RESIP:TRANSPORT | 1820867520 | TcpBas
```

Figure 4: SIP error log

6.1 Procedure

6.1.1 File System Forensics

Our investigation began by investigating the structure of the EmoSpark file system prior to inputting any data into the device. Many of the procedures described above were impossible to carry out on the device. Using common Android acquisition methods, such as ADB and professional tools like FTK imager, were not possible with the EmoSpark. The EmoSparks developers or manufacturers have disabled the resources necessary to use these tools. ADB access was attempted over a variety of cable media including USB-to-USB, micro USB-to-USB, a powered USB hub, and an active USB cable to ensure there was not a fault with the cable. In all instances, the EmoSpark was not visible on the attached computer under ADB or as an attached USB device.

The initial file system investigation was carried out through an attached USB mouse and a root file system viewer app pre-installed on the EmoSpark. The file system did not exhibit any unusual directories or permissions compared to that of a normal Android file system. The EmoSpark app directory contained files that would be expected to be present in any Android app. After the file system was thoroughly investigated and recorded, the next step was to input data into the EmoSpark and reexamine the file system to detect any changes.

Data input was much more difficult than portrayed in the EmoSparks advertising. Advertising displayed an omnipresence similar to the way the Amazon Echo functions. Instead, a user had to be within range of a second device running the companion app in order to send commands and queries to the EmoSpark. Additionally, the companion app was not always listening for a user to speak. A button press would start the device listening for vocal commands. While this made recording what was input into the device much simpler, it made normal use irritating and troublesome. This was especially true when the speech recognition function did not interpret commands correctly and phrases had to be repeated or manually typed into the app.

Complicating these input issues was the availability of compatible Android tablets and phones to use. A limited number of devices were available for use because of the devices reliance on a companion app available only to Android devices. Furthermore, the compatibility issues described between the companion app and the Android versions running on the devices limited which devices could be used for this purpose. These devices are described in more detail in the Input Methods section above.

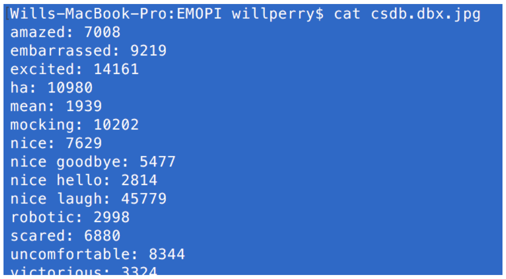
Once a suitable match was made between a tablet and the EmoSpark, we proceeded to send a number of simple queries to the device. The EmoSparks responses were recorded in addition to the content of the queries. These initial queries were meant to test basic features such as the ability to play music, stream videos from YouTube and detect emotions. Additionally, this provided the opportunity for the research team to observe the sophistication of the speech recognition software. As mentioned above, at times the speech recognition failed even after phrases were repeated. These queries had to be manually typed into the app.

Next, we attempted to perform a second file system analysis. When the results of the first and second analyses was compared there was little change. Those changes that had occurred were of minor value and comprised almost entirely of error logs concerning the failure of the Session Initiation Protocol (SIP)[8]. This is quickly shown to be related to the EmoSpark app because the contents of the log had Emospark listed as the agent and because, in the FAQ section of EmoSpark.com, there is a mention of the importance of leaving network ports 5060 and 5061 open when traveling. However, these logs revealed little information regarding any queries that were fed into the device. Even the presence of data structures with, what appeared to be, emotions values could not be deciphered without access to software documentation.

After reviewing the first two analyses, we concluded that there was little information that could be gained through our current course of investigation. It was at this point that we scoured the user forums of the EmoSpark website in hopes of finding a clue to analyzing the device. The majority of the user forums contained question and answer threads for troubleshooting basic functionality. However, two users repeatedly appeared in a number of threads solving more advanced problems and as the originators of threads concerning topics such as requesting developer options be opened or upgrading the memory of the EmoSpark.

As mentioned above, these users were Drago2308 and DarkSpartan. DarkSpartan had posted the tutorial[10] on expanding the memory of the device through a micro-SD card slot hidden inside the case of the EmoSpark. In our last attempt to acquire a full system image, we followed DarkSpartans directions to expand the memory with a micro-SD card and then attempted to perform a backup to the SD card in order to bypass the USB port problems discussed earlier. However the system would not allow the system to be backed up to anything other than a computer that had previously been associated to the device. This was not possible because the only way to associate a computer was via a USB cable.

In emails exchanged with Drago2308[4], he described the process that DarkSpartan and himself had followed in their attempt to reverse engineer the app. The process he described involved the use of an APK extractor, and an HTTP server; both of which were installed from the Google Play Store. The APK extractor was used to break the EmoSpark app into its obfuscated component files and databases. It was then possible to transfer these files to a computer using the HTTP server for easier analysis.

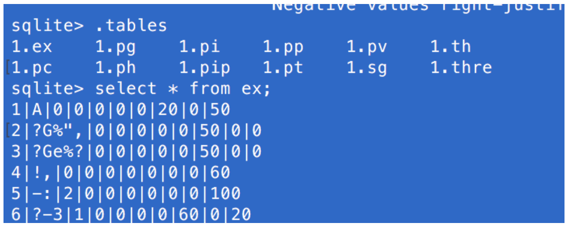


```
Wills-MacBook-Pro:EMOPI willperry$ cat csdb.dbx.jpg
amazed: 7008
embarrassed: 9219
excited: 14161
ha: 10980
mean: 1939
mocking: 10202
nice: 7629
nice goodbye: 5477
nice hello: 2814
nice laugh: 45779
robotic: 2998
scared: 6880
uncomfortable: 8344
victorious: 3324
```

Figure 5: EmoSpark APK: csdb.dbx.jpg contents

This method proved to be extremely useful as the HTTP server allowed the use of a web browser to navigate through the file system of the EmoSpark much more quickly. We were able to do a more thorough check of all directories as a result of the ease of use. Very little was discovered outside of the extracted APK. The extracted APK mainly consisted of binaries and image files but also three SQLite3 databases. Only two of the three databases provided any additional information.

One database, csdb.dbx.jpg, was a plain text file containing a list of emotions and their corresponding values and the other, csdb.db.jpg, was an unencrypted SQLite3 database. While the csdb.db.jpg database most likely contained pertinent information, there very little could be inferred because the table and column names were obfuscated into strings of digits and letters 2-3 characters in length. The row entries did little to shed light on the purpose of any of the data for the same reason.



```
                             Negative values right-justif
sqlite> .tables
1.ex    1.pg    1.pi    1.pp    1.pv    1.th
1.pc    1.ph    1.pip   1.pt    1.sg    1.thre
sqlite> select * from ex;
1|A|0|0|0|0|0|20|0|50
2|?G%",|0|0|0|0|0|50|0|0
3|?Ge%?|0|0|0|0|0|50|0|0
4|!,|0|0|0|0|0|0|0|60
5|-:|2|0|0|0|0|0|0|100
6|?-3|1|0|0|0|0|60|0|20
```

Figure 6: EmoSpark APK: csdb.db.jpg table names and table 'ex' contents.

Finally, the Android system logs were checked, using a Google Play Store app, for any information. Unfortunately, the logs only contained records of the memory utilization and system level events. One consideration when investigating Android system logs is their temporary nature. Android uses a buffer log, therefore, no data would be present for an investigator to view unless the device was kept plugged in. At this point in the project there was very little time for additional techniques to be used.

6.1.2 Network Forensics

Network packet captures were performed in conjunction with the methods described above because the EmoSpark is advertised as being connected to a remote server. A spare laptop running Ubuntu 14.04 LTS was configured as a wireless router and used as the capturing device. This ensured that the entirety of the transmissions were captured and also, at the same time, removed any encryption on the local network. Several packet captures were performed in order to minimize the effects of errors in any individual capture. Wireshark was used as both the capture method and the analysis tool.

Little was discovered from the captures because the EmoSpark uses SSL/TLS to encrypt any sensitive information sent to the remote server. The only data that was captured in plain was NASA images of the sun[9] that are used in the EmoSpark apps dashboard and session dependent Google Video requests. The addresses of the Google Video requests were hashed,therefore, no identifying information was present that an investigator could use to recreate the request or identify the videos or other media requested.

6.2 Results

No decipherable information was extracted from the EmoSpark using a wide variety of techniques. However, the technique used to extract the APK reveals an alternative method of data extraction that was previously little used by forensic professionals in a device investigation. By extracting the APK some of the inner workings of the application were exposed that would allow, with a different app, an investigator to better understand the type of data that was collected by the device. A great deal of work reverse engineering the EmoSpark app would have to be done in order for this level of understanding to be reached with the EmoSpark.

7 Conclusions

We were surprised to discover the level of privacy implemented given the lack of functionality and the bugginess experienced when using the EmoSpark. The levels of obfuscation and encryption would make it extremely difficult or impossible for an investigator to determine any information of value. For these reasons, the authors would recommend any investigator who encounters this device in the course of an investigation to focus efforts on more readily accessible data sources where possible. However, the rising popularity of increasingly intelligent devices highlights the need for continued investigation of devices like the EmoSpark. This will be especially important if investigating similar devices are similarly difficult. It is our hope that the methods exposed may aid future studies of similar devices.

List of Figures

References

[1] M. Alzaabi and D. Quick. Forensic analysis of the android file system yaffs2. In *Proceedings of the 9th Australian Digital Forensics Conference*, pages 100–109, December 2011.

[2] L. M. Aouad and T. M. Kechadi. Android forensics: a physical approach. In *Proceedings of the World Congress in Computer Science, Computer Engineering and Applied Computing*, pages 311–315, July 2012.

[3] M. Davies, H. Read, K. Xynos, and I. Sutherland. Forensic analysis of a sony playstation 4: A first look. *Digital Investigation*, 12, Supplement 1:S81 – S89, 2015. {DFRWS} 2015 EuropeProceedings of the Second Annual {DFRWS} Europe.

[4] Drago2308 and W. Perry. Emails: Emospark documentation, February 2016. [Private Emails; accessed 28-February-2015].

[5] Emospark ai console, November 2015.

[6] A. Hoog. *Android Forensics: Investigation, Analysis and Mobile Security for Google Android*. Syngress Publishing, 1st edition, 2011.

[7] A. Iqbal, H. Alobaidli, A. Marrington, and I. Baggili. Amazon kindle fire hd forensics. In P. Gladyshev, A. Marrington, and I. Baggili, editors, *Digital Forensics and Cyber Crime*, volume 132 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pages 39–50. Springer International Publishing, 2014.

[8] G. C. e. a. J. Rosenberg, H. Schulzrinne. Sip: Session initiation protocol. `https://www.ietf.org/rfc/rfc3261.txt`, June 2002. [Online; accessed 16-April-2016].

[9] N. S. D. Observatory. Sdo-the sun now. `http://www.nasa.gov/mission_pages/sdo/the-sun-now/index.html`, 2016. [Online; accessed 12-April-2016].

[10] L. Summers. Emospark dissection & upgrading the memory. `http://www.filearchivehaven.com/2015/07/15/emospark-dissection-upgrading-the-memory/`, July 2015. [Online; accessed 23-February-2016].

[11] I. Sutherland, H. Read, and K. Xynos. Forensic analysis of smart tv: A current issue and call to arms. *Digital Investigation*, 11(3):175 – 178, 2014. Special Issue: Embedded Forensics.

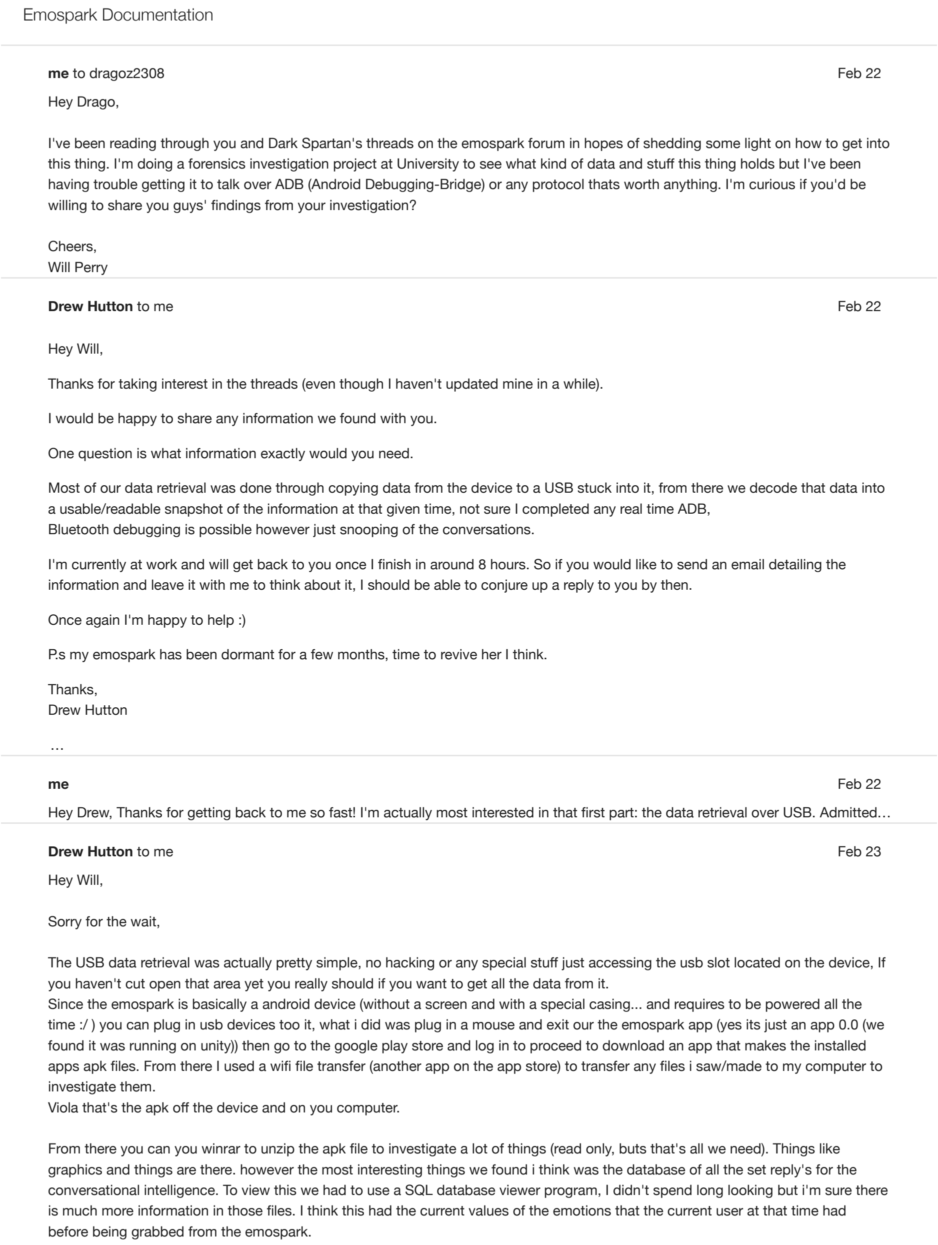
[12] Various. Emospark forums, February 2016. [Online: accessed 28-February-2016].

[13] Wikipedia. Android (operating system) — Wikipedia, the free encyclopedia. `http://en.wikipedia.org/w/index.php?title=Android%20(operating%20system)&oldid=690441893`, 2015. [Online; accessed 13-November-2015].

[14] S. J. Yang, J. H. Choi, K. B. Kim, and T. Chang. New acquisition method based on firmware update protocols for android smartphones. *Digital Investigation*, 14, Supplement 1:S68 – S76, 2015. The Proceedings of the Fifteenth Annual {DFRWS} Conference.

8 Appendix: Drago2308 Emails

The following emails are between one of the authors, William Perry, and Drew Hutton, Drago2308.[4]



Emospark Documentation

me to dragoz2308 Feb 22

Hey Drago,

I've been reading through you and Dark Spartan's threads on the emospark forum in hopes of shedding some light on how to get into this thing. I'm doing a forensics investigation project at University to see what kind of data and stuff this thing holds but I've been having trouble getting it to talk over ADB (Android Debugging-Bridge) or any protocol thats worth anything. I'm curious if you'd be willing to share you guys' findings from your investigation?

Cheers,
Will Perry

Drew Hutton to me Feb 22

Hey Will,

Thanks for taking interest in the threads (even though I haven't updated mine in a while).

I would be happy to share any information we found with you.

One question is what information exactly would you need.

Most of our data retrieval was done through copying data from the device to a USB stuck into it, from there we decode that data into a usable/readable snapshot of the information at that given time, not sure I completed any real time ADB,
Bluetooth debugging is possible however just snooping of the conversations.

I'm currently at work and will get back to you once I finish in around 8 hours. So if you would like to send an email detailing the information and leave it with me to think about it, I should be able to conjure up a reply to you by then.

Once again I'm happy to help :)

P.s my emospark has been dormant for a few months, time to revive her I think.

Thanks,
Drew Hutton

...

me Feb 22

Hey Drew, Thanks for getting back to me so fast! I'm actually most interested in that first part: the data retrieval over USB. Admitted...

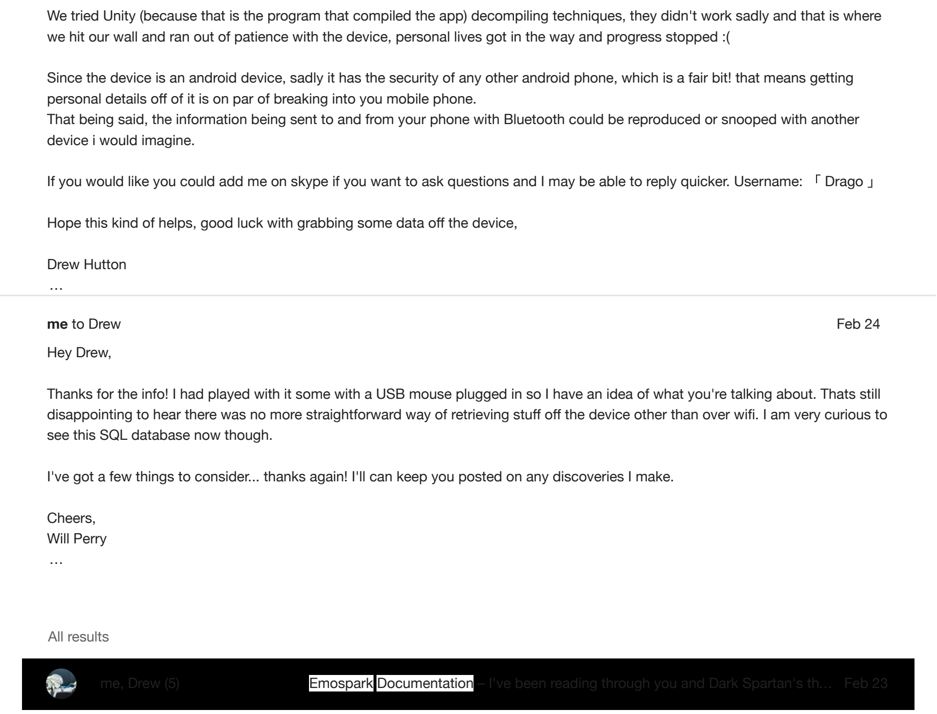
Drew Hutton to me Feb 23

Hey Will,

Sorry for the wait,

The USB data retrieval was actually pretty simple, no hacking or any special stuff just accessing the usb slot located on the device, If you haven't cut open that area yet you really should if you want to get all the data from it.
Since the emospark is basically a android device (without a screen and with a special casing... and requires to be powered all the time :/) you can plug in usb devices too it, what i did was plug in a mouse and exit our the emospark app (yes its just an app 0.0 (we found it was running on unity)) then go to the google play store and log in to proceed to download an app that makes the installed apps apk files. From there I used a wifi file transfer (another app on the app store) to transfer any files i saw/made to my computer to investigate them.
Viola that's the apk off the device and on you computer.

From there you can you winrar to unzip the apk file to investigate a lot of things (read only, buts that's all we need). Things like graphics and things are there. however the most interesting things we found i think was the database of all the set reply's for the conversational intelligence. To view this we had to use a SQL database viewer program, I didn't spend long looking but i'm sure there is much more information in those files. I think this had the current values of the emotions that the current user at that time had before being grabbed from the emospark.



We tried Unity (because that is the program that compiled the app) decompiling techniques, they didn't work sadly and that is where we hit our wall and ran out of patience with the device, personal lives got in the way and progress stopped :(

Since the device is an android device, sadly it has the security of any other android phone, which is a fair bit! that means getting personal details off of it is on par of breaking into you mobile phone.
That being said, the information being sent to and from your phone with Bluetooth could be reproduced or snooped with another device i would imagine.

If you would like you could add me on skype if you want to ask questions and I may be able to reply quicker. Username: 「Drago」

Hope this kind of helps, good luck with grabbing some data off the device,

Drew Hutton
…

me to Drew Feb 24

Hey Drew,

Thanks for the info! I had played with it some with a USB mouse plugged in so I have an idea of what you're talking about. Thats still disappointing to hear there was no more straightforward way of retrieving stuff off the device other than over wifi. I am very curious to see this SQL database now though.

I've got a few things to consider... thanks again! I'll can keep you posted on any discoveries I make.

Cheers,
Will Perry
…

All results

me, Drew (5) Emospark Documentation – I've been reading through you and Dark Spartan's th... Feb 23