FORENSIC REPORT

Submitted to:

Dr. Darren R. Hayes.

Professor, Department of Information Technology

Seidenberg School of Computer Science and Information Systems

Pace University

Submitted by

Jithukrishnan Venu

Student, Pace university

Introduction

In this report, we utilize FTK Imager, a widely respected digital forensics tool, to analyze two AD1 image files: LG-vx9100(en V2)_0 and Cingular_Sim_0. AD1 files are commonly used in digital investigations as they contain bit-by-bit copies of data extracted from digital devices, preserving the exact state of the evidence. The primary objective of this analysis is to extract and interpret relevant data from these files to understand the stored information, which may include messages, contacts, call logs, network configurations, and other digital artifacts. This comprehensive approach involves examining the structure of the files, identifying key data points, and analyzing their relevance in a forensic context to reconstruct activities on the devices. By doing so, we aim to demonstrate the powerful capabilities of FTK Imager in handling mobile device data, its efficiency in extracting crucial evidence, and its role in ensuring the integrity of the digital investigation process.

Overview of FTK Imager

FTK Imager is a digital forensic imaging tool widely used by investigators to acquire and analyze digital evidence. It is designed to capture an exact bit-by-bit copy of storage devices, preserving the integrity of the original data without altering it. FTK Imager supports various file formats and can create forensic images in a format that is usable by other forensic software. It has powerful capabilities for previewing files and extracting data, making it a crucial tool for examining file structures, content, and metadata. Its primary importance lies in its ability to preserve the chain of custody by ensuring that the evidence remains unchanged during the entire investigation process.

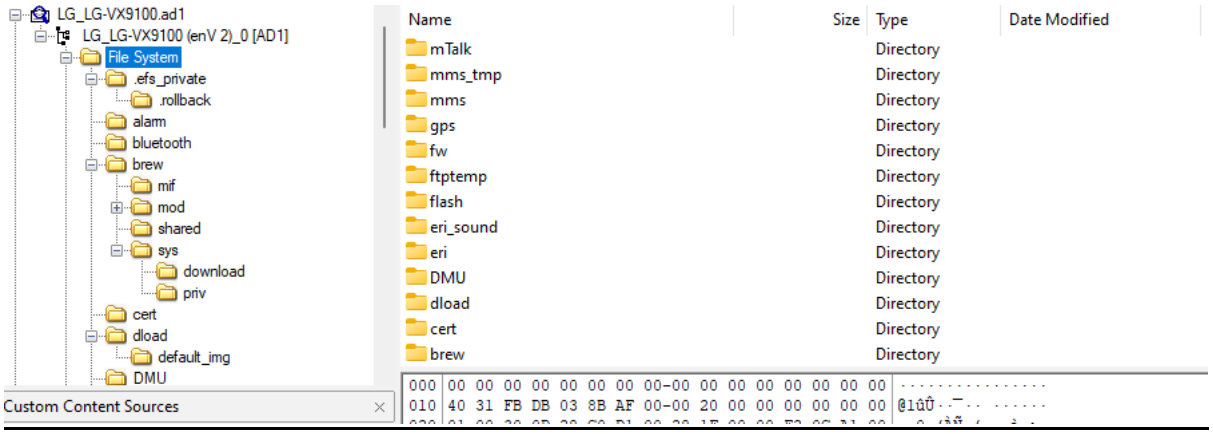
Importance of AD1 Files

AD1 files are a proprietary forensic image format used by AccessData's FTK Imager to store digital evidence. These files act as a container, holding multiple files and data extracted from various sources such as hard drives, mobile devices, or memory cards. AD1 files are essential in digital forensics because they maintain the integrity of the evidence by preserving both the data and its metadata in a secure and unalterable format. They are often chosen for forensic analysis because they allow investigators to efficiently manage and analyze large volumes of data, ensuring that no critical information is lost or compromised during the investigation process.

Analysis of LG-VX9100.ad1

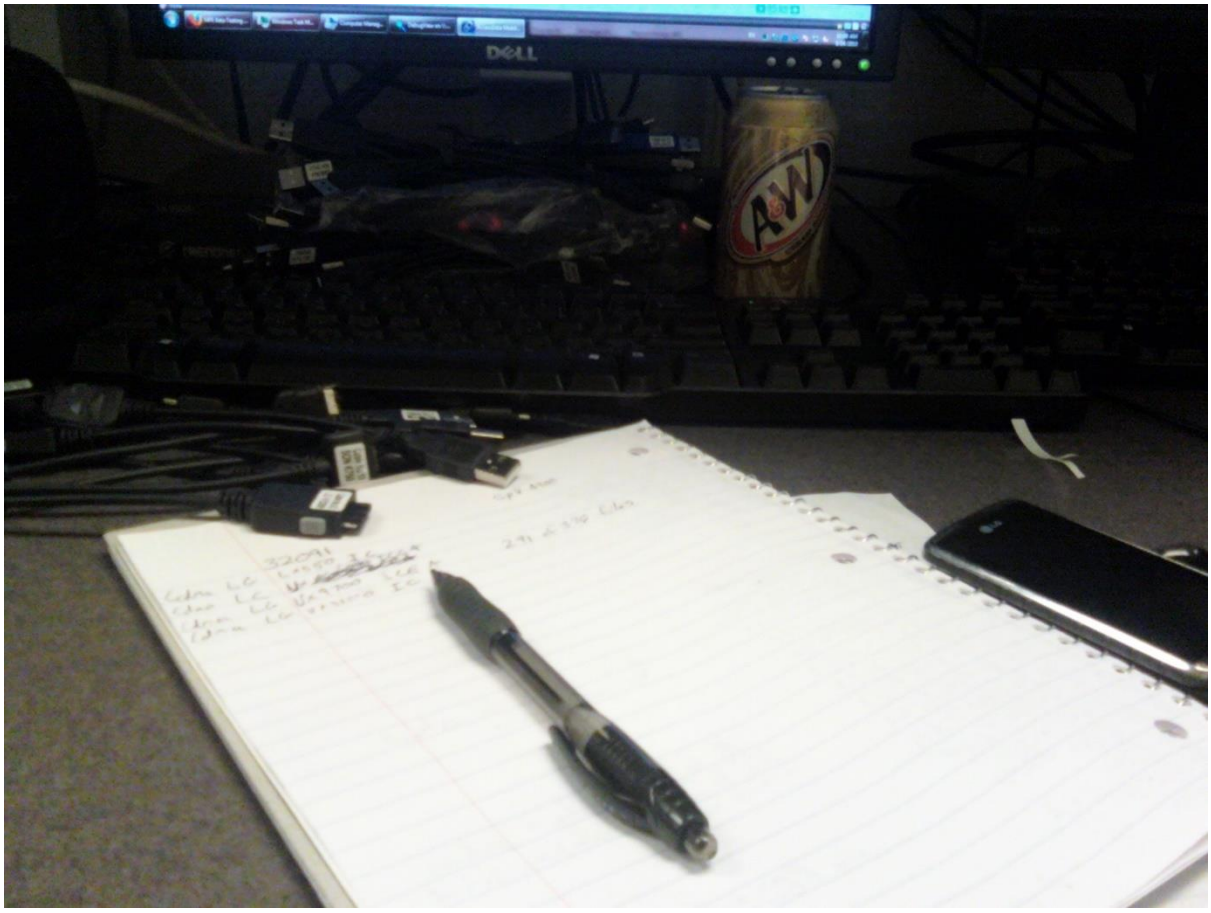
First we will analyze the LG-vx9100(en V2)_0. AD1 file

The LG enV2 was a Verizon Wireless digital messaging feature phone manufactured by LG. The AD1 image is from this device particularly. Let's dive in.

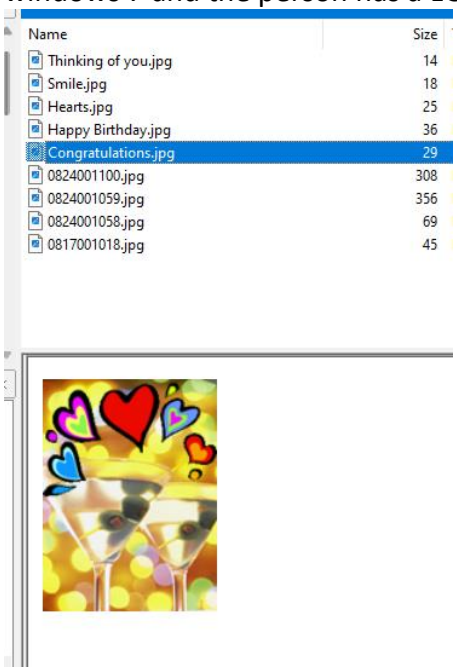


After we load the ad1 file as evidence, we can see all the directories, files including images. We will be analyzing important files in it.

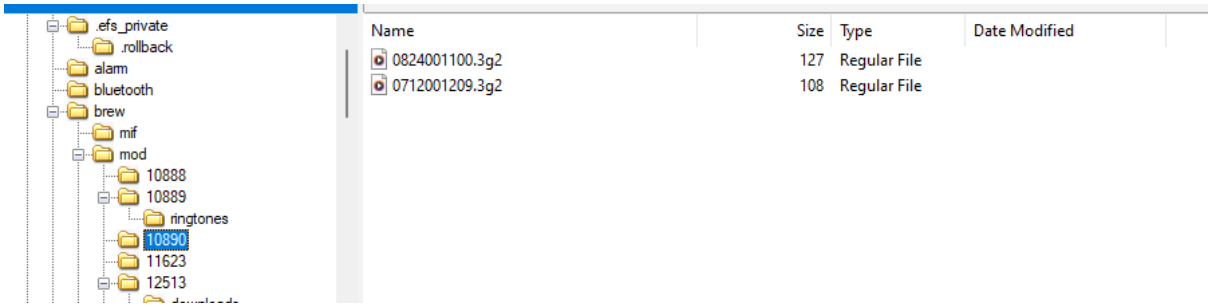
As you can see in the image, the image contains the standard directories of a handset which includes alarm, Bluetooth, user data which includes phone, messages and much more.



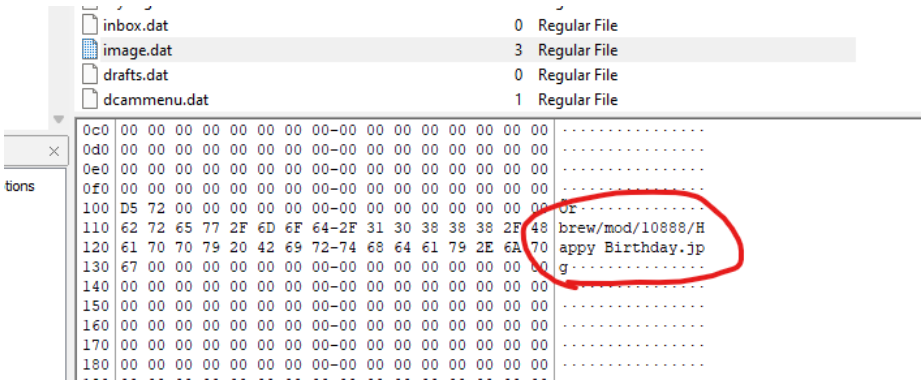
When you analyze this image, we can understand that the user is using a Dell Monitor with windows 7 and the person has a LG handset, which looks like LG Premier **LTE – LGL62VL.**



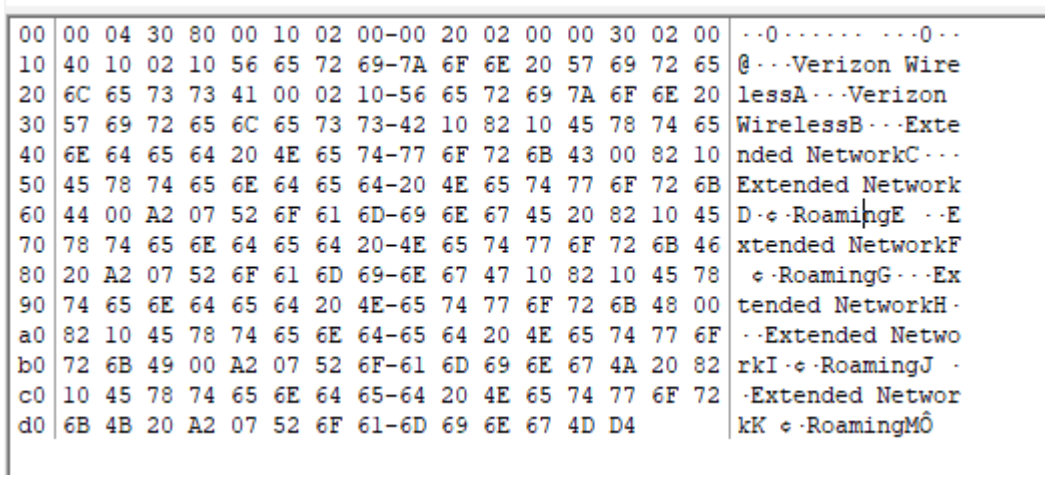
And there are other photos as well, which has congratulations, happy birthday, hearts. Etc.



The image also includes audio files.



This dat file has a reference to the image which can lead to further finding if we dwell up on this particular file.

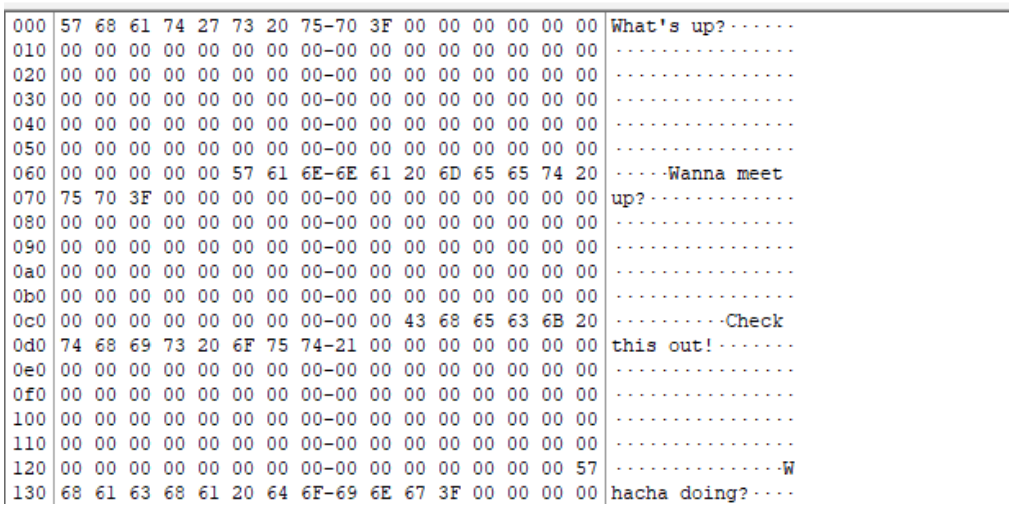


the data appears to include information about network statuses or codes, potentially related to a mobile or wireless network. The terms like "Extended Network" and "Roaming" suggest that this data might be describing the connectivity state of a mobile device or service.

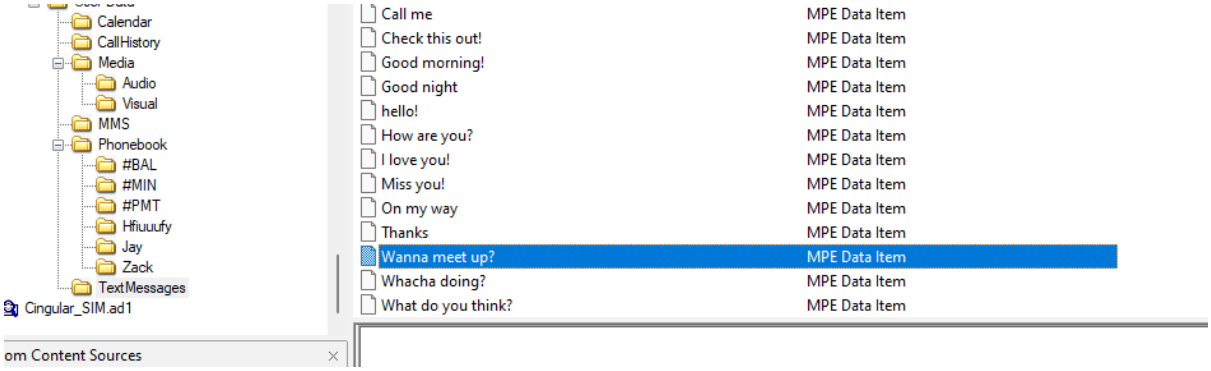
Extended Network: This typically indicates that the device is connected to a network that is not its primary home network but is still within its service area.

Roaming: This usually signifies that the device is connected to a network outside its home area, often incurring additional charges

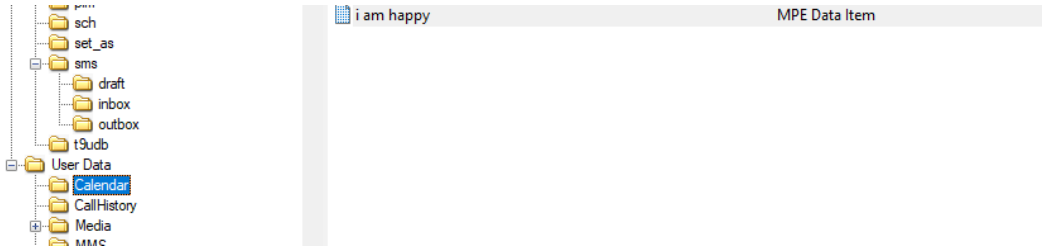
Now lets analyze text message:



This dat file is having text messages , which can be very crucial in forensic investigations.



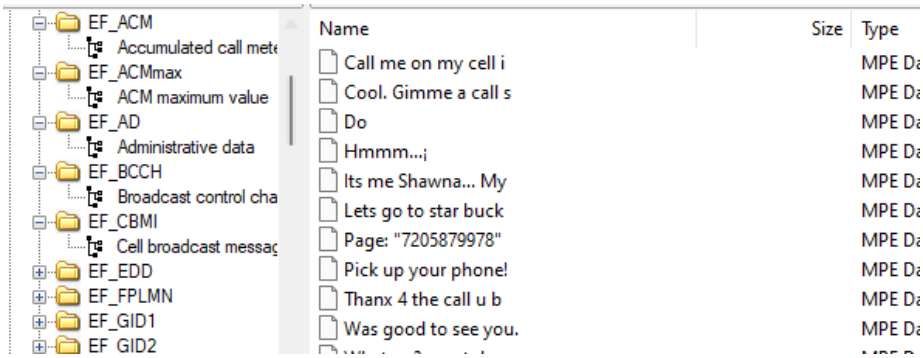
And we can also see other text messages in it.



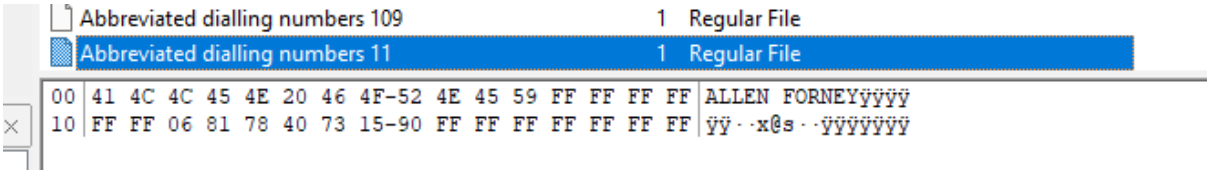
This is part of a calendar event, The MPE data item might have data related to schedules or events.

Let’s analyze the second one, which is Cingular_Sim_0[AD1]:

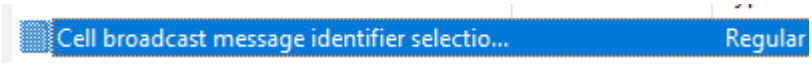
Cingular Wireless was a mobile phone company from the United States. Cingular Wireless was created in 2000 resulting from a joint venture of SBC Communications Inc. and the BellSouth Corporation. AT&T Mobility LLC bought Cingular in 2006, subsequently causing Cingular to adopt the AT&T Wireless name.



This Image also got some text messages, and the data can be used for further investigation



The image shows a hexadecimal representation of an abbreviated dialing number. The image shows a hexadecimal representation of an abbreviated dialing number. The ASCII translation reveals the name "ALLEN FORNEY." The trailing FF FF FF FF might be padding or a separator. ALLEN FORNEY" appears to be associated with this entry, indicating that this is the contact’s name stored.




```
CB_Message_Identifier 1 : FFFF
CB_Message_Identifier 2 : FFFF
CB_Message_Identifier 3 : FFFF
CB_Message_Identifier 4 : FFFF
CB_Message_Identifier 5 : FFFF
CB_Message_Identifier 6 : FFFF
CB_Message_Identifier 7 : FFFF
CB_Message_Identifier 8 : FFFF
CB_Message_Identifier 9 : FFFF
CB_Message_Identifier 10 : FFFF
```

The term **CB_Message_Identifier** likely refers to **Cell Broadcast Message Identifier**, which is used in mobile telecommunications. Cell Broadcast (CB) messages are a way of delivering messages to multiple users in a specific geographic area simultaneously. This technology is commonly used for emergency alerts, weather warnings, or other types of mass notifications. **CB_Message_Identifier** set to **FFFF**, it often indicates that no specific message type has been assigned or that the broadcast channel is not currently being utilized.

Conclusion

The analysis conducted using FTK Imager provided a clear demonstration of its effectiveness in handling AD1 files and extracting valuable digital evidence. Throughout the investigation, we uncovered a variety of critical data points, including contact information, text messages, network statuses, and other device-related artifacts, all of which are essential for constructing a detailed view of the device's activities. These findings underscore the importance of FTK Imager in the field of digital forensics, as it enables investigators to accurately recover and interpret data from mobile devices, ensuring that no critical information is overlooked. Furthermore, the ability of FTK Imager to maintain the integrity of the data during the extraction process reaffirms its credibility and reliability as a forensic tool. This analysis highlights the indispensable role of FTK Imager in uncovering digital evidence, supporting forensic conclusions, and providing a robust foundation for legal proceedings and investigative reports.