2007

Mood 300 IPTV decoder forensics

An Hilven
Edith Cowan University

DOI: 10.4225/75/57ad67437ff39
Originally published in the Proceedings of the 5th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, December 3rd 2007.

Mood 300 IPTV decoder forensics

An Hilven
School of Computer and Information Science
Edith Cowan University
ahilven@student.ecu.edu.au

Abstract

Since June 2005, viewers in Belgium can get access digital TV or IPTV available via ADSL through Belgacom, the largest telecommunications provider in the country. The decoders used to enjoy these services are the Mood 300 series from Tilgin (formerly i3 Micro Technology). As of the Mood 337, the decoders contain a hard disk to enable the viewer to record and pause TV programs. Although it is publicly known that the Mood's hard disk is used to save recorded and paused TV programs, it was still unknown if it contains any data that could be of interest during a forensic investigation. Interesting data ranges from which TV programs where watched, over discovery of unauthorized data storage, to criminal profiling and alibi verification. This paper will research the possibilities, especially with regards to which TV programs were watched and alternate data storage, as criminal profiling and alibi verification is not merely a task the forensic investigator can do alone.

Just like game consoles that use a hard disk, the Mood 337 can easily be disassembled and attached to a PC for forensic analysis. The reason why analysis of this system is necessary is simply because it contains a hard disk. Anyone with a screwdriver can remove, replace or modify it not only for experimenting purposes but also for illegitimate uses. Analysis shows that most of the 80 Gb of disk space on the disk is not even in use, and can easily have data being written on it without interfering with the system's primary function of providing IPTV services. It was also found that the Mood runs on a Linux base system with a 2.4 kernel, using XML file for the configuration of IPTV functions and services. Analysis reveals that even the (billable) 'pause' function is nothing more but a 'yes' or 'no' flag in an XML file. Other files that would be expected on a Linux system, such as /etc/fstab or /etc/passwd, were not found, while these might have been proven useful in this analysis. Further examination of the hard disk indicates the use of certificates for protection against piracy. However, it was proven to be a trivial task to simply copy recorded data to a PC and play it with a media player.

The most important discovery of this research is that correctness of time and date appears to be of lesser value for the creators and/or distributors of the Mood 337. Throughout the system, various different time stamps and time zones were used, and more importantly time and date were changed several times. Even though two NTP servers are configured for time synchronisation, neither one of them seems to be correct. In order for data recovered from this hard disk to be acceptable before a court of law, fixing the time and date should be one of the highest priority changes that are needed.

Keywords

Belgacom, IPTV, Mood 300, forensics

INTRODUCTION

It has a hard disk…

It has a network connection…

It does not have any "warranty void if removed" stickers on the sides…

These three facts together make the Mood 337 decoder, used for IPTV in Belgian homes, motivate a curious forensic investigator-to-be to disassemble it and see if any forensically interesting information can be dissected from its hard drive.

What started out as mere curiosity about the contents of the little black box grew into actual forensic analysis of the Mood 337. In the end it was clear that analysis of its hard disk was not just fun, but can also prove helpful during real digital investigations. Probably the most obvious reason for performing forensic analysis is to discover if it was used as a hidden data storage device. The hard disk of a Mood 337 is not likely to be the most obvious place for law enforcement to search for evidence of illegitimate use and illegal data storage. Furthermore, the fact whether or not non-IPTV-related data is found can indicate that the suspect is technically savvy. Another reason to forensically analyse the decoder is that it could be used in criminal profiling. Because

traces of watched TV programs can be recovered, comparisons can be made between them. A decoder containing mostly traces of horror movies probably has an owner with a completely different personality than one containing nothing but Disney cartoons. The last reason for Mood 337 forensics is that the traces of watched TV programs can help identify when the owner was watching TV, and might help in verifying alibis. A suspect could claim he watched soccer all evening yesterday, and may be able to answer questions such as "which team won" and "who made the goals", but he may as well have heard that on the radio later on. The Mood 337's hard disk may well contain traces of last night's soccer match. However, for this data to actually stand before a court of law an effort should be made by the designers and/or distributors of the device to ensure correct timestamps are used throughout the system.

Forensic analysis on alternate data storage devices is nothing new. It was already done before by for example, Schroader and Cohen in their recently published book "Alternate data storage forensics", and by Burke and Craiger (2006) in their paper about forensics on Microsoft's Xbox gaming console. In their paper, Burke and Craiger explain that the Xbox can quite easily be modified to support multiple operating systems, and thereby making it possible to store non-game-related data on the device. The same is true for data storage on the Mood 337.

Although it was not tested during this research to run additional operating systems, the Mood's hard disk holds plenty of disk space that can be experimented with, even if only for data storage. It has been tested, however, by a user (Dreamweaver, 2006) of an unofficial Belgacom ADSL forum, that the IPTV signal can be captured by a regular PC and played, posted that he was able to use GeeXbox Linux to get the IPTV signal on his PC, being able to swap channels and watch TV in high quality video using just Mplayer. Additionally, Dreamweaver created an image he created of a working system and made it publicly available (Dreamweaver, 2006). The fact that the IPTV signal can be replayed on a regular PC proves that no specific hardware or operating system is required, and thus it should be possible as well to run another or additional operating systems on the Mood 337.

Burke and Craiger (2006) were also able to set up a network connection to the Xbox system and perform their analysis via a simple SSH connection. For the analysis of the Mood 337, however, a different approach was used, namely physically removing the hard disk from the casing and attaching it to a PC. As it is not known beforehand whether or not a network connection would change data on the Mood's hard disk, this risk was not taken. The reason for this is that the system used in this analysis was not a test device, but is in fact still used by the owner. Siglio, a user on the Userbase.be forums, was in fact able to set up a network connection to the Mood and could set up a CGI script that allowed him to make changes to the system directly from the Mood's internal web server he was connected to (Siglio, 2007).

In an article on Linuxdevices.com (2002), i3 GM for Streaming Products Chris Chalkitis revealed that the Mood's kernel is merely a 2.4.x kernel retrieved from kernel.org and then modified for IPTV use. Other publicly available Linux tools were used as well, and because most of these are GPL licensed, i3 decided to make their changes to the source code publicly available as well on their FTP server. These sources were not immediately made public, yet after requests from an end user (Siglo, 2006) they were made available in June 2006 on ftp://ftp.opensource.tilgin.com/MOOD/.

It may be clear that quite some research was already done on the Mood decoder, but most of this research was merely either out of curiosity or experimentation with the IPTV signal. It appears that no (publicly available) research has yet been performed from a forensic angle. This paper will analyse the contents of the Mood's internal hard disk, and will discuss the findings that came forth from it..

HARDWARE INFORMATION

All research is performed on is the Mood 337 V2 BE from Tilgin AB, manufactured in August 2006. Detailed information on all components used in this device can be found in its product sheet (Tilgin, 2006). This paper will focus on the Mood 337's hard disk, which in this case is of the type WD Caviar (WD800BB-55JKC0) from Western Digital with manufacturing date 8 May 2006. This is an IDE hard disk running at 7200 rpm. Although analysis of other sources of data such as the NOR and NAND flash chips may reveal interesting information, it is outside of the scope of this paper and saved for possible future work.

FORENSIC PROCESS

Preparation

The hard disk was removed from the Mood 337 hardware and attached as a regular IDE disk to a PC. The 'cable select' jumper setting was left in place during this process. The power connector was left attached to the original Mood 337 casing instead of hooking it up to the PCs power supply, because it was uncertain how the Mood 337 fed power to the hard disk.

Acquisition

The acquisition of the hard disk was done from a Debian Etch system, using *dd* to create a bitwise copy of each partition. A total of 3 partitions were found, namely hda1, hda2 and hda3.

Analysis

To retrieve some initial general information about the partitions, each of the images was loaded into *FTK* (under Windows XP Professional) and *Autopsy* (under Helix). Both came up with the same information, confirming the outcome is likely to be correct.

NAME	SIZE	FORMATTING
hda1	1 Gb	raw, unformatted
hda2	1 Gb	ext3
hda3	72 Gb	ext2

Fig. 1 – Size and formatting of the Mood 337 hard disk

On each partition, a large amount of free space was found. This was 100% for hda1, 80% for hda2, and 91% for hda3:

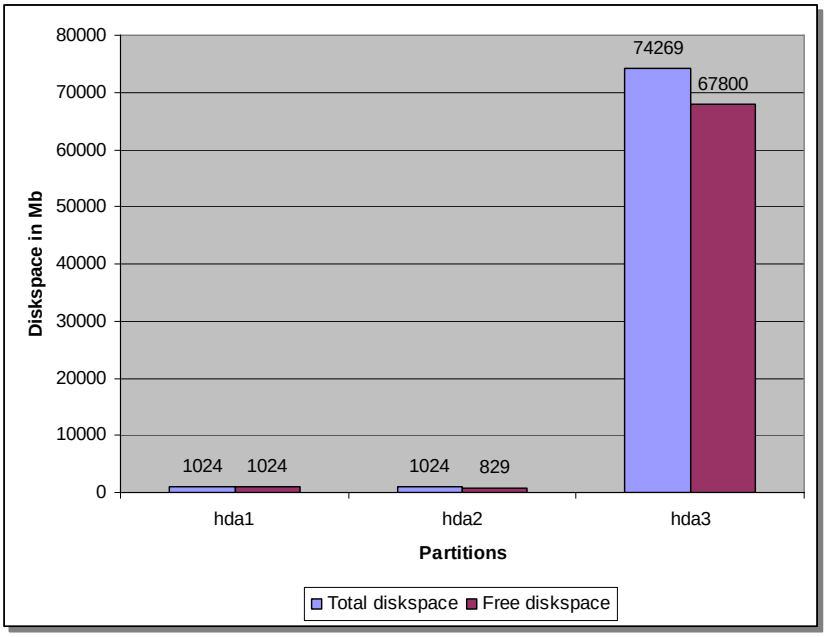

Fig. 2 – Amount of free disk space compared to the total partition size for a Mood 337 decoder

More detailed analysis was done with a three applications. For general analysis *FTK* and *Autopsy* were used. However, because these tools are not sufficient for more advanced file carving, *Scalpel* was used for this purpose instead.

For each partition, first the directory structure is analysed and interesting files are listed and discussed. Next, manual analysis of the free space areas is done. And to conclude, file carving is done on the free space, and the outcome is discussed.

PARTITION 1 (HDA1)

Directory structure

FTK and *Autopsy* found that this is a raw, unformatted, partition containing nothing more than free space. Manually analysing this partition in hexadecimal format reveals that it is indeed completely clean, and does not appear to have ever been written to at all.

File carving

To ensure nothing was overlooked, the image was sent through *Scalpel*, with a configuration file edited to search for all known file types. The result confirmed the initial findings, as no files were found.

PARTITION 2 (HDA2)

This section describes the findings of examination of each of the directories (see below) and their contents with both *FTK* and *Autopsy* For each of the directories listed, a brief explanation is also given as to whether or not and in which cases its contents can be of evidentiary value during a forensic investigation.

Directory structure

This partition is formatted with the ext3 file system, and its directory structure looks quite similar to a normal Linux system, especially when looking at the structure of the */root* directory. Besides the directories normally expected on a Linux system, two directories appear to be the odd ones out, being */persist* and */localexec/conf*.

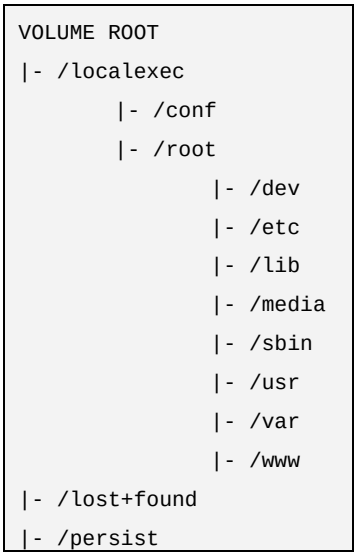

Fig. 3 – High-level directory structure of the hda2 partition on a Mood 337 system

/localexec/conf

This directory holds an XML file that seems to be the configuration of where the firmware (*netimage-myrioi-3.7.2-bel-137.tar.gz*) was copied or downloaded from, and that it is/was encrypted with AES.

Note that the statement regarding copy or download locations is merely speculation, based on the fact that the path in the “from” line does not exist on the hard disk, and such it might be an (incomplete) web or network location.

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<addonlist count="1">
   <version>
      <type>Mood300</type>
   </version>
   <addon-key type="AES">59EC1A5B172E119D558CA3B93FD62E4B</addon-key>
   <file>
      <revision>myrioi-3.7.2-bel-137</revision>
      <from>myrioi-3.7.2-bel-137/netimage/netimage-myrioi-3.7.2-bel-
           137.tar.gz</from>
      <to>netimage-myrioi-3.7.2-bel-137</to>
      <size>15899140</size>
      <crc>30873</crc>
      <md5>83bf45d9d2b0d5a7d149dab7245e5346</md5>
      <moddate>2007-06-23 00:56:26</moddate>
   </file>
</addonlist>
```

Fig. 4 – Myrioi firmware information for the Mood 337

The other three files in this directory appear to be related to the XML file. The first file, *netimage-myrioi-3.7.2-bel-137.tar.gz.md5* contains the same MD5 sum as found in the XML file. The second file, *netimage-myrioi-3.7.2-bel-137.tar.gz.dirlist*, contains a listing of directories likely to be included in the firmware package or the locations it should be extracted to. The last file, *netimage-myrioi-3.7.2-bel-137.tar.gz.nodelist*, contains a list of symbolic links likely to be created during installation of the firmware.

The "moddate" line appears to contain the date and time when the firmware was installed or updated. The last firmware update was indeed done around 23 June 2007, and the same firmware version is visible in the decoder's menu (Belgacom, n.d.). However, the fact that other timestamps and time zones used in the system are inconsistent may raise doubts to the reliability of this information. An example of this inconsistency is that the MAC times of these files are all 1 January 2000, instead of the date of the firmware update.

/localexec/root/dev

This directory does not contain any devices. It merely holds two symbolic links, one for the internal web browser (*myriohandler.fifo*) and one for a mouse driver (*gpmdata.fifo*). The symbolic links reference to files in this same directory, yet these files do not exist.

/localexec/root/etc

In contrast with a regular Linux system, this directory does not contain the files that are usually of interest during investigations, such as *fstab*, *mtab*, *passwd*, etcetera. However, it does contain other interesting data such as files listing the hardware and software version.

```
VER_HARDWARE=i3-mood-HD
BASEMODEL=I3MICRO-MOOD
DISKTYPE=COMPACTFLASH
CD=NOCD
NETCARD=NATSEMI
```

Fig. 5 –Mood 337 hardware information as discovered in configuration files

```
VER_SOFTWARE=3.7.2-137
CLIENT_VARIANT=bel
BUILD_STAMP="build@build-vm on Fri Jun 22 15:51:45 PDT 2007"
```

Fig. 6 –Mood 337 software information as discovered in configuration files

This confirms, as stated earlier, that time and dates are used inconsistently on this system. For example the previously discussed XML file used CET, while the software information file uses PDT. Note that in June there was a time difference of 7 hours between CET and PDT, and thus the timestamps do not even match when converting the time zones.

Further interesting information is found in the *rc2.d* subdirectory, as this will show which processes are started at system boot time. Although expected processes such as syslogd and klogd are missing, DHCP configuration and swap file creation do initiate at system boot. Various other processes are started; all of which seem to be not (or less) used on regular Linux systems. These processes are: *zapper*, *dvrd*, *ipmd*, *moodplayer*, *movie*, *recorders*, *hwversion*, *mpersist*, *savemoodconf*, *loadkeys*, *myriohandle*, *setkeycodes*, *myriodispd*, *startapp*, *security_engine*.

In the *X11* subdirectory, an *X Windows* configuration file is found. Even though it was found already that time and date seem to be an issue on this system, it does appear that *X Windows* is synchronized with a time server (although it does not seem to be configured in an officially supported manner).

```
# TODO - FIXME - temp hacks - BEGIN
# force sync with server time
DOMAIN=nat.myrio.net
. /etc/dhcpc/dhcpcd-eth0.info
if [ "$DOMAIN" = "nat.myrio.net" ]
then
        rdate time.nat.myrio.net
fi

# TODO - FIXME - temp hacks - END
```

Fig. 7 –Temporary hacks for the Mood's time synchronisation in X11

One last piece of interesting information found in this directory is a configuration file, *movie.conf*, which seems to be used to configure where media streams should be sent to. However, this location, */media/hdd/PVR*, does not exist on the hard disk.

/localexec/root/lib

This directory only contains two symbolic links, one to *../usr/lib/dspimage.out* and one to *../usr/lib/dspimage.ver*. Analysis of *dspimage.ver* shows that it contains nothing more than two numbers (4 and 34), which is likely a version number of some kind. Examination of *dspimage.out* indicates that this could be a library used to decode media streams, as it contains many references to media such as mpeg3, mp3, ac3, aacdec, mpeg2, as well as various uses of the words 'dec' and 'decode'.

/localexec/root/media

A subdirectory named *persist* is the only data found in this directory. It holds files nearly identical to the ones in */persist*, with the only difference that the MAC times are off by 2 minutes. The contents of these files will be discussed in the */persist* section below.

/localexec/root/sbin

Just one file, named *zapper*, resides in this directory. *Zapper* was sent through strings in order to get an idea what this file is used for. The results indicate that it has something to do with IGMP, as it contains strings related to this subject. Some further investigation (Juniper Networks, 2007) to the relationship between IGMP and IPTV teaches that IGMP is used as the method for changing TV channels in IPTV environments.

/localexec/root/usr

This directory mainly contains two types of files: Java APIs and kernel modules.

The JAVA APIs reveal a little more information with regards to which software runs on the decoder. The most eye-catching ones are: *Bouncycastle* (used for crypto), *Apache Crimson* (used for XML parsing), *Apache Ant* (a build tool), *Apache Jakarta ORO* (used for regex processing), *Apache Log4j* (used for logging), *Myrio Escape* (a web browser)

Besides minimal kernel modules needed for the system to actually run, a few other interesting modules were found in this directory. For example, there are modules for IGMP processing, MTS file processing (MTS files will be discussed later). One kernel module, *cas_verimatrix.so*, is the first indication discovered that this system was set up with security in mind, as this module seems to be responsible for the handling of SSL, TLS, RSA keys, etcetera.

/localexec/root/var

Yet again, this is one more directory which's contents are nothing like what would be found on a regular Linux system. It was expected that logging would be found here, but instead two symbolic links were found, one to the *../media/persist* directory and one to the *../media/persist/myrio/persist* directory.

/localexec/root/www

This directory contains various GIF files that do not appear to be used anywhere. Furthermore there are symbolic links named *zapper.cgi* and *playtv.cgi*, both linked to a non-existing file *cgi.cgi*. A live search with *FTK* for any references to .cgi files did not result in any possible related files.

/lost+found

This directory is empty.

/persist

The */persist* directory holds all files and information used to configure the decoder, such as the locale, cache size, buffer size, video standard, logging settings and enabling or disabling the 'pause' option. It is remarkable, however, that although Apache Log4j is configured in *mclient_log4j.properties*, the file all logging should be written to (*var/data/log/mclient.log*) does not exist.

```
#### Second appender writes to a file
log4j.appender.R=org.apache.log4j.RollingFileAppender
log4j.appender.R.File=/var/data/log/mclient.log

# Control the maximum log file size
log4j.appender.R.MaxFileSize=2000KB
# Archive log files (one backup file here)

log4j.appender.R.MaxBackupIndex=2
```

Fig. 8 – Snippet of Apache Log4j configuration on the Mood 337

In this same directory a root certificate was found as well, revealing that Verimatrix is used as the Certificate Authority. More research teaches that this is a company that incorporates security features in Pay TV systems with the goal of enhancing revenue and verifying the legitimacy of streaming content to protect against piracy. Verimatrix does this through a PKI infrastructure and the use of X.509 digital certificates.

Further the directory contains a list of all hardware related error message the end-user might see, such as hard disk maintenance start and completion, and warnings that the temperature is too high.

On a side note; the option to pause live programs (mentioned above) is only enabled if paid for on a monthly basis. Testing and experimenting with editing configuration files may be interesting for future work.

Swap file

Analysis of the swap files in the root of the decoder revealed a few things that could not be deduced from configuration files. Something that may be very important during an investigation is that a trace of the device's IP address can be found. Because the swap file is overwritten every time the system restarts, it is likely that only the last IP address can be found here (if at all).

```
Lease of 10.131.27.19 obtained, lease time 604800
```

Fig. 9 –The Mood's last IP address and lease time was found in the swap file

Another interesting piece of information is which NTP server is used and how often it is polled. Strange enough, this is a different server than the one that was found in a configuration file earlier.

```
NTPSERVER="ntp.nat.myrio.net"
NTP_INTERVAL="172800"
```

Fig. 10 – Another NTP server configuration extracted from the swap file

The swap file also revealed what the management IP addresses are that are allowed to make a network connection to the decoder. This might prove very valuable during an investigation (if the investigator's PC can be configured with one of these addresses), and interesting for future research.

```
CONTROL_IP="10.48.18.122,195.238.8.137,195.238.8.78,81.245.3.187"
```

Fig. 11 – IP addresses the Mood 337 can be managed from

Besides the above findings, no information was discovered in the swap file that could not have been found by analysing configuration files.

Free Space

First, the boot record was analysed. Even though a boot record exists, it is empty and looks like it has never been written too.

Next, *FTK* was used to extract all free disk space of this partition in the form of 33 files with an average size of 25 Mb. Each of these files was analysed manually through *FTK*'s capability of viewing files in hexadecimal form, in order to get an idea whether or not any forensically interesting information could be found.

At the beginning of the free space, mostly gibberish was found. However, once in a while text appears indicating start and completion of hard disk maintenance and temperature warnings.

At around three quarters of the free space, contents of configuration and Java class files were visible, but did not contain any information that could not already be found in the configuration files and class files themselves.

At the very end, contents of the online TV guide were found from mid-December 2004 and January 1971. This indicates another issue with the usage of time and date on this system. For example, a description (in Dutch) of the final episode of the TV series 'Heroes' was found. This episode was broadcasted in Belgium on 4 June 2007. However, the time stamp indicates that it was aired 17 December 2004.

```
1103287700|0|Heroes|5||||||2|||110||FI|C.Serie||||0||us||1|De
ontknoping nadert... De helden zijn in New York voor de
belangrijkste dag van hun leven. Zij zijn uitverkoren om de
wereld te redden van een naderende ondergang. Hun missie is
om te voorkomen dat Mendez' afbeelding van de ontploffende
man realiteit wordt. Kunnen de helden de vernietiging van New
York en de wereld voorkomen? Kan de ontploffende man
tegenhouden worden?|6|Hayden Panettiere|Masi Oka|Ali
Larter||||false|false|false|false|false|false|false|false||||
```

Fig. 12 – Heroes goes back in time

Another description was recognized, this time of 'Big Cat Diary'. This was aired on 14 October 2007, while the time stamp indicates this was 18 December 1970. It may be worth to note that the firmware upgrade which was discussed earlier falls between the two 'real' dates. It appears very likely that during this upgrade the time and date was changed or reset.

File Carving

To see if any further interesting data could be found, all free space files extracted by *FTK* were fed to *Scalpel* with a configuration file edited to search for all known file types (identical to the configuration used for analysis of hda1)

This resulted in various GIF and JPG files. The GIF files contained all kinds of logos of for example i3 and Espial, but also MGM and Disney. Looking through the user interface on TV, these logos do not seem to be used anywhere. The JPG files are images for movies as they would appear in the online movie catalogue for rental movies. However, this only contains relatively old movies, none of which are currently available in the online catalogue. It is assumed that either these movies were available a long time ago, or they were left behind during the initial installation of the system.

PARTITION 3 (HDA3)

This partition uses the ext2 file system. It does not contain much data, other than various files that appear to belong to three groups if grouped by MAC time (23 June 2007, 5 October 2007 and 19 October 2007). Each group consists of four files with identical filenames but different extensions. These extensions are .idx, .info, .time and .mts.

The .idx files do not appear to contain any information, except for repeated sequences of same hexadecimal values over and over again.

```
00 00 00 00 ec 84 00 00 00 00 00 00 04 f6 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 bc 00 bc 00 00 00 00 00 ec 84 00 00
00 00 00 00 04 f6 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 bc 00 bc 00
```

Fig. 13 – Example of repeating sequence in an .idx file found on the Mood 337's hda3 partition

The .info files contain XML data. Although information such as title and description are not available, these files indicate when a recording was started and stopped.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<tv><channel id="-1">
<display-name></display-name>
<url></url>
<icon src="" />
</channel>
<programme start="20071005201000 -0000" channel="">
<title>title not set</title>
<desc></desc>
<desc lang="">STOPPED</desc>
<length units="seconds">3</length>
<task>RECORDING</task>
</programme>
</tv>
```

Fig. 14 – Example of start and stop times in an .info file found on the Mood 337's hda3 partition

No interesting information was found in the .time files. It is however notable that these files always appear to be 1.92 Mb in size.

The .mts files are the largest files. The ones found here were 4 Mb, 1.8 Gb and 3.7 Gb in size respectively. Due to these file sizes; it is thought that these files might contain the actual recorded TV stream. To test this, the largest file was exported from *FTK* and played with *Windows Mediaplayer*. *Windows Mediaplayer* did appear to recognize the file as a media file, but threw an error indicating the required codec was not available. More research regarding the .mts file extension revealed that this type of files can be played with the *VLC media player*. This application was downloaded, and playback of the .mts file showed the movie 'King Arthur', recorded from TV on 23 June 2007, in excellent mpeg4 quality. Also note that the other files, with extensions .idx, .info and .time were not required during playback of the movie.

Due to the fact that up to 74 Gb of recorded data can be stored on this partition, it may be possible to profile the owner of the decoder, because it is possible to know which TV programs he or she likes.

Free space

Again first, the boot record was analysed. As with hda2 a boot record exists, but it is empty and looks like it has never been written too.

Similar to hda2, *FTK* was used to extract all free disk space of this partition in the form of 2712 files with an average size of 25 Mb. Although a tedious work, each of these files was analysed manually in the same manner the free space files on hda2 were analysed (i.e. through hexadecimal viewing).

The only data that was found was in free space files 1 through 69. After free space file 70, only zeroes exist. However, the files that do contain data do not hold any interesting information such as configuration files or logging. To analyse this further, file carving is needed.

File Carving

Similarly to processing hda1 and hda2, all free space files of hda3 extracted by *FTK* were fed to *Scalpel* with a configuration file edited to search for all known file types (again identical to the configuration used for analysis of hda1 and hda2).

Scalpel carved hundreds of small MPEG files. When playing these files consecutively in the order they were carved, fragments of TV programs that had been watched could be seen. In some cases, several of these MPEG files together formed a complete TV program, while for other TV programs only 1 or 2 minutes were found. It appears that the more recently the TV program was watched, the more fragments of it can still be found in free space. The oldest recognizable fragments were from a program broadcasted over 2 months ago. With a little help from the TV station (which can easily be identified by its logo in one of the corners), the exact date and time a specific fragment was broadcasted can be determined. With this information, it would be possible to prove that someone was watching a specific program on a certain date and time (or at least that the TV was on during that timeframe). This might help in verifying alibis and the like.

WRITING TO DISK

Because the decoder used for this research is in fact still in use, no major testing was done with writing data to the disk, or editing configuration files. For future work, a decoder should be used that is no longer active, so that this can be experimented with as well. It would be interesting to see what happens when for example the 'pause' setting is changed, or what the logging would contain if it were properly enabled. And especially whether or not the decoder would continue to work as normal, as well as seeing if the configuration files are overwritten at a next reboot.

What was tested, however, is that it possible to copy files to hda3 without having any impact on the working of the device. It was also possible to delete the files, again without impacting the device's working. Therefore the hard disk of a Mood 337 makes an excellent choice for storing data that is intended to be kept secret.

CONCLUSION

Due to inconsistent use of time, date and time zones, using evidence retrieved from a Mood 337 set top box used for Belgacom customers would be likely to be rejected before a court of law. However, fragments of TV programs and help from TV stations may result in information of higher evidentiary value, as they could help in believing or rejecting alibis. Furthermore, with an analysis of the recorded TV programs it might even be possible to profile the owner of the decoder.

Forensic analysis of these decoders may also prove valuable in cases of copyright infringement, because it was found that it is really easy to just copy recorded programs and watch them on PC. A next step of editing the file to cut out commercial breaks, and burning it to a DVD is not a large one to take.

Because a simple, unprotected, hard drive is used for saving configurations and recorded data, two possible issues raise. First, one may be able to edit configurations and making paid services free (which was not tested in this paper, and is saved for future work). And second, any other data can be written to this hard disk. So if someone really wants to hide data, but is afraid that it will be revealed when his or her PC is forensically examined, why not write it to a hard disk that has less chance to be spotted by law enforcement?

REFERENCES

Belgacom (n.d.). How can I verify the firmware version of my decoder. Retrieved on October 8, 2007, from http://selfcare.belgacom.net/index.html?l=private:search&a=default&r=613671&p_faqid=9028&p_created=1140432120&p_sid=ZS6tGoPi&p_lva=&p_sp=cF9zcmNoPTEmcF9zb3J0X2J5PSZwX2dyaWRzb3J0PSZwX3Jvd19jbnQ9MSZwX3Byb2RzPTU2LDYwJnBfY2F0cz0mcF9wdj0yLjYwJnBfY3Y9JnBfcGFnZT0xJnBfc2VhcmNoX3RleHQ9ZmlybXdhcmU*&p_li=&p_topview=1 (Dutch)

Burke, P. K., Craiger, Ph. (2006). Xbox Forensics, Journal of Digital Forensic Practice, 1:4, 275 – 282, Retrieved on November 23, 2007, from http://dx.doi.org/10.1080/15567280701417991

Dreamweaver (2006. BGTV on GeeXboX. Retrieved on November 26, 2007, from http://forum.adsl-bc.org/viewtopic.php?t=35357 (French)

Juniper Networks (October 2007). Introduction to IGMP for IPTV networks. Retrieved on October 22, 2007, from http://www.juniper.net/solutions/literature/white_papers/200188.pdf

Lehrbaum, R. (July 2002). Device profile: i3 micro Mood Box. Retrieved on November 26, 2007, from http://linuxdevices.com/articles/AT9483972214.html

Schroader, A., Cohen, T. (November 2007). Alternate data storage forensics. Syngress. ISBN 1-59749-163-2.

Siglio (2006). Does Belgacom/Tilgin violate GPL? Retrieved on November 26, 2007, from http://forum.adsl-bc.org/viewtopic.php?t=30063 (Dutch/French)

Siglio (2007). Belgacom Mood hacking. Retrieved on November 26, 2007, from http://www.userbase.be/forum/viewtopic.php?t=13104 (Dutch)

Tilgin (2006). Mood 300 Series. Retrieved on September 18, 2007, from http://www.tilgin.com/Documents/Product%20sheets/Mood%20300_PAL_ProductSheet.pdf

COPYRIGHT