A Preliminary Approach to the Forensic Analysis of an Ultraportable ASUS Eee PC

Trupti Shiralkar[1], Michael Lavine[1], and Benjamin Turnbull[2]

[1] Johns Hopkins University Information Security Institute
4th Floor, Wyman Park Building, 3400 North Charles Street
Baltimore, Maryland, USA 21218
{tshiral1,mlavine}@jhu.edu
[2] Defence and Systems Institute, University of South Australia
University Blvd, Mawson Lakes, South Australia, 5095
Benjamin.Turnbull@unisa.edu.au

Abstract. Subnotebooks, or 'netbooks, are a relatively new consumer market but one that continues to grow significantly worldwide. The aim of this paper is to analyse one of the leading subnotebooks, the 'ASUS Eee PC' from a forensics perspective. Specifically, the work investigates current image creation methods for making image of Eee PCs Solid State Drive and it analyses forensically important artefacts.

1 Introduction and Background

The current generation of subnotebook PCs, epitomised by the Aspire One, Asus Eee PC, One Laptop Per Child OLPC XO-1 and HP 2133 Mini-Note, is eclipsing traditional consumer computers in growth due to their low cost, ease of use and light weight. These ultraportable devices offer fast Internet connectivity with a user-friendly means of performing basic computing tasks. Given this growth, the likelihood that these devices will be misused cannot be ignored. As more criminal investigations include a computer forensic component we can expect that investigators in both the public and private sectors will encounter these and similar devices. Therefore, this work seeks to understand the forensic implications of the subnotebook class of devices through analysis of an Asus Eee PC.

The main purpose of this research is to identify data extraction methods suitable to the Eee PC and seek for forensically interesting features of this device that will benefit to the investigator. Specifically, this work seeks to understand what information can be obtained from the pre-installed applications of the Eee PC that can be used as digital evidence.

2 Technical Overview

The Eee PC 701 is representative of the subnotebook class, with a 7-inch screen and weighing approximately 2 pounds (900g.). Although this device does not offer

M. Sorell (Ed.): e-Forensics 2009, LNICST 8, pp. 116 – 121, 2009.

support for all applications, it offers a customised set of frequently used applications related to word processing and the Internet. The Eee PC 701 has three USB ports, one SD card slot and a VGA port, but no onboard DVD or floppy drive. The ASUS Eee PC comes in three popular series viz. 700, 900 and 1000 with a range of configurations depending on a user's preference for OS, microprocessor speed, RAM, storage and other specifications. The offerings in this range of products are comparable to competitive products in the marketplace, which have similar specifications in the processor, memory and storage [3][4].

Officially, the ASUS Eee PC officially supports two operating systems: a customized version of Xandros and Microsoft Windows XP. The default Xandros OS comes with two modes: *Easy* and *Advanced*. The Easy Mode uses IceWM window manager and a six tab structured interface. The full desktop mode is the Advanced Mode that uses the KDE Desktop Environment. Both use Debian GNU/Linux 4.0, kernel 2.6.22. The start menu of the Advanced Mode provides an option for switching to the Easy Mode. The Easy mode also provides a special tab to switch to advanced mode. The default file system is ext2. A user can also install various distributions of Linux, such as Ubuntu, Kubuntu, Xubuntu, and EeeBuntu, from a USB connected peripheral. However, the Eee PC driver support for these operating systems is not guaranteed.

With the Eee PC, a traditional hard drive is replaced by solid-state drive (SSD) based on non-volatile NAND flash memory [5]. The Eee PC has options for SSD sizes ranging from 2GB through to 16GB.

3 Forensic Considerations and Research Plan

This work has identified three primary areas for consideration in subnotebook forensic collection and analysis, and these issues will be explored independently. The first issue is related to the on-board SSD. The Eee PC uses solid-state memory instead of a hard drive that soldered directly on to the motherboard. Given this, mechanisms used to forensically copy hard disks from notebooks and other systems are not applicable to subnotebooks, and therefore a process of cloning the SSD without altering data must be developed. The second forensic issue with subnotebooks is the lack of onboard CD or floppy disk drive. The third forensic consideration with these devices is that, by default, the underlying system is abstracted from the user. It is possible that many forensics examiners do not have an in-depth technical knowledge of this unique system. The Eee PC also supports different flavours of Linux operating systems, as previously discussed. Each of these OS' may have a different file system, structure and default storage location. Hence, a forensics investigator should know the suitable forensics tools required for each of these OS and file systems. However, for the purposes of this work, analysis was conducted on an Eee PC with its default Operating System.

3.1 Research Design and Scope

This work was divided into two major phases, *Image Acquisition* and *Analysis*. As the first phase, image acquisition involved an exploration and determination of a reliable method to create a forensically sound image of the SSD. In the second phase, we focused on examining the image with Encase v 6.11 to identify the evidence and the default locations where it may be contained.

As has been noted, it is difficult to physically remove the SSD from an Eee PC. An unsuccessful attempt to remove the SSD could easily damage the SSD, which may irrecoverably destroy forensic evidence as well as the machine itself. Hardware-based data recovery from flash memory is beyond the scope of this paper [6]. Similarly, the process for removing electronics from onboard, soldered systems for forensic purposes has known potential side effects [7]. Therefore, this is not the preferred method for acquisition.

3.2 Image Acquisition

Given the lack of direct access to the SSD that would enable disk imaging through write-blocking hardware, live forensic environments become the only option for access. The lack of CD/DVD drive on these systems initially posed an issue, but the system booted both from USB memory drives and USB-connected DVD drives.

As discussed, not all live environments will boot on an Eee PC. Possibly the best-known live forensic environment is Helix. *Helix version 2*, based on the Knoppix environment, was unable to successfully boot the Eee PC into a live forensic environment. However, *Helix 3* (released September 2008), based on the Ubuntu live environment, did boot the system successfully. Researchers also used *BackTrack 3* to boot the system directly from a USB drive. Although Backtrack contains digital forensics imaging utilities, the environment itself is not considered forensically sound.

Once booted successfully and in a forensically sound manner, it is a relatively simple and well documented process of making a forensic copy of the Eee PC drives. Mounting an external USB disk with read/write permissions, there are several applications that provide forensic copying ability. At a basic level there is *DD*, *DCFLDD* and *DD_Rescue*. However, researchers used *Adepto 2.1*imaging software and Guidance Software's *Linen* to create images of the SSD.

From this point, it was possible to either create a raw image of the entire SSD (**/dev/sda** of 4 GB in size) or create forensic copies of individual partitions. The partitions are as follows:

- /dev/sda1 – system (EXT2, 2.3GB).
- /dev/sda2 – user data (EXT3, 1.4GB).
- /dev/sda3 – BIOS (VFAT, 7.9MB).
- /dev/sda4 – Hidden (boot partition) (FAT, 7.9MB).

The first partition, **/dev/sda1**, contains the variant of *Xandros* operating system. The second partition is mounted as top of first partition. The third and fourth partitions are comparatively small Windows FAT partitions and are less relevant in the analysis of user-created data.

3.3 Forensic Analysis

Acquisition of forensic data provides the framework on which to analyse, and the EeePC (and small scale devices as a class), has considerations associated with it. The use of a custom operating system potentially changes the default storage locations for stored information, and the small size of the SSD potentially limits the possible system files and user-created data saved on the system.

The Easy Mode of an Eee PC environment, which is the default purchased state, provides an application set aimed at a casual user (e.g. word processing, communication and Internet related). The following list summarises the information used by the pre-installed applications and information of potential interest to forensics investigators. Each of these areas is discussed independently.

- **Web browser (Mozilla Firefox) -** Web Browser History, Cookies, iGoogle Settings, Bookmarks and Cache Files.
- **Email (Hotmail, Yahoo, and AOL) -** Email IDs, Chat IDs, Email Archive, History Files, Cache Files, URLs.
- **Instant Messenger: Skype and Pidgin -** Chat IDs, Chat History Logs, Contact Lists, and Phone Numbers. Pidgin Chat program supports: AIM, Google Talk, ICQ, IRC, MSN, QQ, SIMPLE, Sametime, XMPP, and Yahoo.
- **Personal Information Manager (PIM) -** Contacts (Address Book), Journal, To-Do List, Notes and Email.
- **File Manager** (Stores file generated by the following applications) - OpenOffice.org, Notes, Mail, PDF Reader, Digital Camera, Screen Capture application - Word Processing Documents, Spreadsheets, Presentations, Images, and Videos.

Other considerations - Peripheral device connections (e.g. USB, MMC.SD, and Portable Hard Drive), Command Line History, recently accessed documents, installed software, nstalled

- Xandros Anti-Virus Logs, and other application and system Logs

Easy web browsing is one of most attractive features of this computer and could likely be one of the main reasons that a suspect will make use of Eee PC for accessing the Internet. Hence, it is crucial for the forensics investigator to analyse Internet usage. The Eee PC uses *Mozilla Firefox* as the default, pre-installed web browser. The forensic examiner should look at the **/home/user/mozilla/ firefox/** folder to analyse: web browser history, cookies, *iGoogle* Settings, browser cache and bookmarks.

Similarly, Net Books are advertised as internet-capable devices, and the idea that these devices will be used for email and instant messaging is a logical extension. The Web Mail tab provides direct links to the *Hotmail*, *Yahoo Mail* and *AOL* mail programs. For instance, using Encase, Email-IDs can be retrieved from the browser cache even if the IDs are not stored in the web browser. *Skype* and *Pidgin* are the two messengers available for chatting and instant messaging, and between them, can be used for dialling a phone number, voice chatting, and instant messaging. This work was able to identify Chat IDs, Chat history, phone numbers and contact list to be of interest. For example, our work found that an individual's Skype ID is stored at **/home/User/.Skype/ID/chatsync**.

The Eee PC also makes use of a *Personal Information Manager* (PIM). The PIM merges applications like *KOrganizer*, *Kmail* and *KAddressBook* to provide easy access to check e-mails, appointments, and stored contacts. The forensics investigator will be able to obtain To Do List, contact list (Address-book), notes, and journal information which is stored at **/home/user/.kde/share/apps/kabc** which can then be analysed with a number of forensic tools.

By default all documents, spreadsheets, presentations, audio files, video files and images are stored in File Manager. The default location for user-created files is **/home/user/My Documents/**, which stores all Open office, PDF docs and other files. This folder has the sub-folders **/My Pictures/** and **/My Videos/** which store images and videos created using the digital camera and screen capture application respectively.

The files deleted from My Documents are moved to the **/home/user/Trash** folder. If the data stored in these folders is erased, an investigator can still retrieve the names of files recently accessed from **/home/user/.kde/share/apps/Recent Documents**. The information about images including deleted images can be retrieved from the **/home/user/.thumbnail/normal/** folder. It is noted that in its default form, these folders are invisible to the user.

A forensic investigator may also retrieve the list of peripherals (e.g. USB, portable hard drive, external DVD rewriter) attached to the Eee PC at the **/media** and **/disk/removable** folders. From the list provided it will be clear which peripherals where used, all of which can be further examined onsite or in a forensics laboratory.

The **/var/log** folder contains the application logs. For example: *Xandros Antivirus* logs are stored at **/home/user/.XandrosAntivirus/logs/scan.log**. List of all newly installed software can be disclosed at **/var/cache/apt/archives** and at **/usr/bin**. Upon analysing **/dev/shm/resolveconf/interface** folder using EnCase 6.11, the investigator will be able to obtain the IP address(es) of the network(s) to which an Eee PC was connected.

Another forensically interesting item is the command line history. This is stored at **/home/user/.bash_history** and contains a list of all the commands entered and/or executed. The forensics investigator can get information about all the malicious operations performed, such as; installation of anti-forensics tools, downloading root-kits, secure deletion of files and metadata, and disk wiping etc. It is quite possible that an attacker may forget to delete the contents of the bash_history [11]. Hence, the bash_history can play a vital role in understanding the sequence of command line activities and help develop an effective timeline analysis.

4 Conclusion and Future Research

The use and subsequent misuse of new technologies is a known fact, and there is consequently a need for forensics examiners to adapt. Whilst many of the specifics discussed in this paper are unique to the Asus Eee PC, the lessons can be generalised to similar devices. The analysis of small-scale, ultra-portable personal computers will continue to grow as this class of device becomes more popular. Considering the growing market of notebooks and subnotebooks, a comprehensive study of these types of devices should be done and a common investigative framework should be developed to help the forensic investigator's work in this emerging area.

This work has identified a number of areas for future research. One of the areas of research should address how to extract data from an Eee PC that is not operational. Further research is needed to recover data from an intact SSD or one that has been tampered with.

Since this work focussed only on the Eee PC 4G 700 Series model, additional work can verify the outcomes discussed on both the more recent 900 and 1000 series devices within the Eee PC line-up, and also consider the specific analysis issues associated with other, similar devices. Furthermore, since this work was restricted to analyse only one of the default Xandros OS; the second default operating system, Windows XP should be investigated in order to develop an equally important preliminary approach for forensic analysis.

References

1. ASUSTek Pty Ltd, Eee PC, News Release, ASUS Eee PC is America's Most Wanted Christmas Gift, November 21 (2007), http://eeepc.asus.com/global/news11212007.htm
2. Eee PU USA News Release, ASUS Introduces All-New Eee PC for Complete Mobile Internet Enjoyment (October 16, 2007), http://eeepc.asus.com/us/news101612007.htm
3. ASUSTek Pty Ltd., Eee PC Specifications (August 19, 2008), http://eeepc.asus.com/us/product.htm
4. Smith, T.: Subnotebooks and Mini-Laptops (September 18, 2008), http://www.reghardware.co.uk/2008/09/12/rh_bg_subnotebooks/
5. Eee wiki, eeeuser.com, Asus Eee PC, http://wiki.eeeuser.com/eee_pc_701
6. Breeuwsma, M., Jongh, M., Klaver, C., Van der Knijff, R., Roeloffs, M.: Forensic Data Recovery from Flash Memory. Small Scale Digital Device Forensics Journal 1(1) (June 2007)
7. Willassen, S.Y.: Forensic Analysis of Mobile Phone Internal Memory. Presented at the 1st IFIP WG 11.9 Workshop on Digital Evidence, Orlando, Florida (2005)
8. Fogie, S.: PC Forensics Tools, Security Reference Guide (March 18, 2004), http://www.informit.com/guides/content.aspx?g=security&seqNum=106
9. Rude, T.: DD and Computer Forensics (August 2000), http://www.crazytrain.com/dd.html
10. Bezroukov, T.: Unix DD Command and Image Creation (June 05, 2008), http://www.softpanorama.org/Tools/dd.shtml
11. Belshaw, G.: Forgetting to lock the back door: A break-in analysis on a Red Hat Linux 6.2 machine (August 04, 2002), http://www.sans.org/reading_room/whitepapers/incident/654.php