Methods to find digital footprints on a personal computer

K Yu Zhigalov¹, E V Volkova², M S-U Khaliev³

¹V.A. Trapeznikov Institute of Control Sciences of RAS, 65, Profsoyuznaya Street, Moscow, 117997
²Irkutsk National Research Technical University, 83, Lermontov str., Irkutsk, 664074, Russian Federation
³Chechen State University, 17а, Dudaev Boulevard, Groznyy, 364015, Russia

E-mail: kshakalov@mail.ru;

Abstract. Digital footprints remain on a personal computer no matter how hard PC users try to wipe them. This paper can be useful both as an instruction to find such footprints and as an instruction for their destruction. The paper is devoted to the overview of specific examples of the use of modern hardware and hardware-software systems to find digital footprints of activity directly on a personal computer. The options to obtain information from random access memory (RAM), hard drives and SSD devices are described in detail. For example, the following information can be obtained from a dump of the RAM of a PC: running processes, network connections, passwords, various encryption keys, clipboard, etc.

1. Introduction
Nowadays it is difficult to imagine our life without the use of digital data in certain areas of our activity and life. At the same time, each of us has a certain amount of digital data that we try to hide. It can be both passwords from mail and digital cryptoassets. However, almost all the data we use leaves some kind of footprints on our devices. These footprints can be further used by both operational services and intruders or malicious users.

2. Types of digital footprints
To begin with, storage media can be divided into non-volatile and volatile. Nonvolatile storage media can store recorded data for a long time without the need to connect to a power source. A volatile storage medium can not store data for a long time after being disconnected from the power source.

Here it is necessary to clearly understand that digital footprints can be located not only on hard drives, but also in RAM and network traffic dumps. At the same time, most of the malicious programs work just in RAM, which allows them to leave no footprints on the computer upon the finish of work.

At the same time, the following are often stored in the RAM of PC:

- list of running processes;
- information on network connections;
- used passwords for access;
- currently decrypted files;
- encryption keys;
- clipboard;
• user’s correspondence.

Of course, if we turn off the computer, this data will be irretrievably lost.

Let us take a look at what can be learned from network traffic as an example. In network traffic, we can try to find IP addresses of the remote server on which we either work (RDP connection with username/password) or store information (FTP server). At the same time, if these IP addresses are changed several times a day, then this significantly minimizes the possible damage from the loss of this kind of data.

In order to collect data from volatile storage media, the following software systems are usually used: Windows operating system: Mandiant “Memoryze”, AccessData “FTK Imager”. For Linux operating system LiME, Fmem are used. For OS X we use Mac Memory Reader. These programs are shareware and are in free access.

3. Digital footprints in RAM

In order to conduct an experiment of making a copy of the contents of RAM, we can use the Memoryze utility. Using the command line, we need to run the following file from the directory of the Memoryze program:

`MemoryDD.bat –output <out_dir>`

As a result of the operation of this utility, an image of the RAM is saved in the form of a file with the *.img extension.

As it is mentioned earlier, during the study of RAM, we can get a list of running processes and services. If we are talking about the study of memory in order to protect the system, then the appearance of an unknown (new) process in this list should alert us (Figure 1).

```
>tasklist /SVC >tasklist.txt
```

![Figure 1. List of running processes and services](image)

During the study of the list of drivers installed in the system, we can learn which external devices were connected to a computer and in what state they were at the time of their removal from RAM. This will allow a PC to be monitored for unauthorized use of additional means of removing and transmitting information.

In addition to the studies described above, we can get a log of the sites visited by a user. In Figure 2, we can see their names and real IP addresses. Thus, for example, the site www.openrce.org has an IP address 96.126.125.53.
Figure 2. Log of visited sites

The list of running open connections allows determining which network resources a computer was connected to when RAM was removed and with which resources it interacted. There is a double benefit here. On the one hand, it is possible to track an intruder if he used the network to transfer stolen data or control computers. On the other hand, we can use this memory feature to spy on the end user.

4. **Study of HDD**

Without special devices, it is impossible to create a copy of the item we are interested in from a disk on a working computer. Any operation of copying data changes the attributes of the studied files. For that work you can use programs:

- Memoryze,
- AccessData “FTK Imager”,
- LiME, Fmem,
- Mac Memory Reader.

Usually, as a result of the data copying you will have a snapshot file with *.img Mac extension (Figure 3). This allows controlling unauthorized copying of data on a working computer.
Of course, there are software products on the market that allow copying the contents of discs without making changes to them, but for this a computer must be restarted and an external drive must be connected to it, which significantly complicates copying without a user.

To carry out computer expert analysis, the following hardware and software systems are most often used:

- Paraben's P2C,
- EnCase Forensic
- Belkasoft Evidence Center.

These complexes can recover deleted information, carry out contextual search according to various criteria within files, sort information in an easy-to-read form and automatically generate a report that can be used in applications to an expert opinion. It is also possible to view the contents of all the main Internet chats, using which we can identify interlocutors and read their messages. In addition, viewing the history of browsers, we can get the chronology of visits to sites by a user.

5. Conclusion

In recent times the game in the direction of information struggle has been conducted in two directions: as a defense (by a user) and as an attack (by intruders, malicious users, relevant authorities, etc.). The result of this struggle if an intruder wins may be the loss of reputation, money and other things by an end user or a company as a whole. This paper does not cover mobile devices, but they also need to be protected because sometimes they store more confidential information than a personal computer. At the same time, in fact, they are not very different from computers.

References

[1] Bhardwaja A, Samb L, Martín-Torresa F J, Kumarb R 2016 UAVs as remote sensing platform in glaciology: Present applications and future prospects. Remote Sensing of Environment 175 196–204
[2] Zhigalov K 2016 USAGE OF THE GAME TECHNOLOGIES ENGINES FOR THE PURPOSE OF MODERN GEOGRAPHIC INFORMATION SYSTEMS CREATION. ITM Web of Conferences 6 03018
[3] In-Ae Yeoa, Jurng-Jae Yee 2016 Development of an automated modeler of environment and energy geographic information (E-GIS) for ecofriendly city planning. Automation in Construction. 71 398–413
[4] Zhigalov K, Avetisyan K, Konyukhov V Y, Osmaev A D 2020 Hierarchical approach to artificial intelligence. Journal of Physics: Conference Series 1661 012094
[5] Karlina A I, Kondrat'ev V V, Kolosov A D, Balanovskiy A E, Ivanov N A 2019 Production of new nanostructures for modification of steels and cast irons. IOP Conference Series: Materials Science and Engineering 560(1) 012183
[6] Bulatov Y N, Cherepanov A V, Kryukov A V, Suslov K 2020 Distributed Generation in Railroad Power Supply Systems. *Proceedings of 2020 3rd International Colloquium on Intelligent Grid Metrology, SMAGRIMET 2020*, pp. 54–60, 9264013

[7] Voropai N, Ukolova E, Gerasimov D, Suslov K, Lombardi P, Komarnicki P 2019 A Study on Cost-Effectiveness of Energy Supply Based on the Energy Hub Concept. *Proceedings of 2019 IEEE PES Innovative Smart Grid Technologies Europe, ISGT-Europe 2019*, 8905736