Professional paper / Stručni rad
Manuscript received: 2017-06-23
Revised: 2017-09-07
Accepted: 2017-09-12
Pages: 27 - 36

Remote digital forensics practices

Damir Delija

Insig2 d.o.o
Zagreb, Croatia

damir.delija@gmail.com

Abstract: In this paper, the idea of remote digital forensics is introduced, its benefits and possible drawbacks are presented. It is important to understand it is more a recognition of existing state of the affairs than introducing a new concept. Various aspects of forensically sound remote approach are described with references to tools and practices. Relations to other digital forensic fields are presented and highlighted with aim to recognize distributed work and parallelism in modern digital forensic as existing practice close to remote forensics.

Keywords: remote digital forensics, enterprise forensics tools, enterprise forensics

INTRODUCTION

Capacity and behavior of computers changed since the early days of digital forensics in 1990. It is not only change in huge performance increase, but also in being constantly in power-on and using resources over network. These three conceptual changes are the main drive for remote access to data and machines, or better to say for the using of remote digital forensics approach.

Whole remote forensics process more evolved than being suddenly introduced, it is now in order with current forensic practices, especially for new and emerging areas like e-discovery, enterprise forensics, preventive forensics or forensic system state analyses. It is important to understand that introducing remote access does not violate any forensic principles or requirements.

Since digital forensics is heavily influenced by technology cycle, remote access to media and systems containing possible digital evidence will be more and more important as the number of interconnected system and services grows. Also, the volume of data which possibly contains relevant digital evidence can be so big that traditional „dead box“ (e.g. access to not working system) approach simply cannot be used, in such situation remote access to live systems are the only option available.

With remote access, there are always issues of legal authority, for what we at this moment does not have a universal and acceptable solution. Each legal system handles this situation in a different way.

DIGITAL FORENSICS AND REMOTE DIGITAL FORENSICS

What is a remote forensics and what exactly remote forensics means for the digital forensics? To answer these questions best is to start with definitions. Digital forensics [1] is simply the application of computer investigation and analysis techniques in the interest of determining potential legal (digital) evidence. Digital forensics retrieve digital evidence, where digital evidence or electronic evidence is any probative information stored or transmitted in digital form that a party to a court case may use at trial [15]. This definition covers a wide range of possibilities and does not require that target system must be shut down or directly physically accessible during forensic process.

Starting from these commonly known definitions we can define remote digital forensics as the application of digital forensics at remote device or remote location. In practice, it mostly means we don’t have physical access to the media which contains digital evidence. From digital evidence viewpoint, it is acquiring digital evidence on remote device or location. Remote forensics are often understood only as live forensics, in fact, live forensics can overlap with remote forensics. Live forensics is application of digital forensics on systems which cannot be stopped. Basic requirements for data and system integrity can be easily fulfilled for the live forensics and for the remote forensic approach if we follow acquisition rules and known best practices. Not to forget, in some situa-

tion live forensic approach is more effective and less harmful to the system than the traditional dead box approach, better to say working with power-off system. In some situations, live approach is the only nondestructive approach. Such example is mobile forensics or acquisition of some types of computers which cannot be dismantled. Same situation is for the acquiring network traffic, a situation where we only have an original copy of the data, not the data on the media itself.

Forensics tools for the live access over network is the first idea about live forensics, but also there are examples where it is not a live forensics, but it is still a remote forensics. Possible example, maybe the oldest one, is booting computer from forensic Linux distribution and then accessing it remotely. Well known example is old *Helix 2* Linux distribution or more recent *Linen* boot CD for *EnCase* [18]. For *Linen*, this is remote access, but not live access since machine we are examining is not working under its own native operating system but under forensic Linux distribution. The more recent situation is using Tableau *TD3* or *TX1* [3] forensic remote write blocker and duplicator to access data over iSCSI protocol [13] in physical access, or over the web and cifs [2] in logical access (Figure 1).

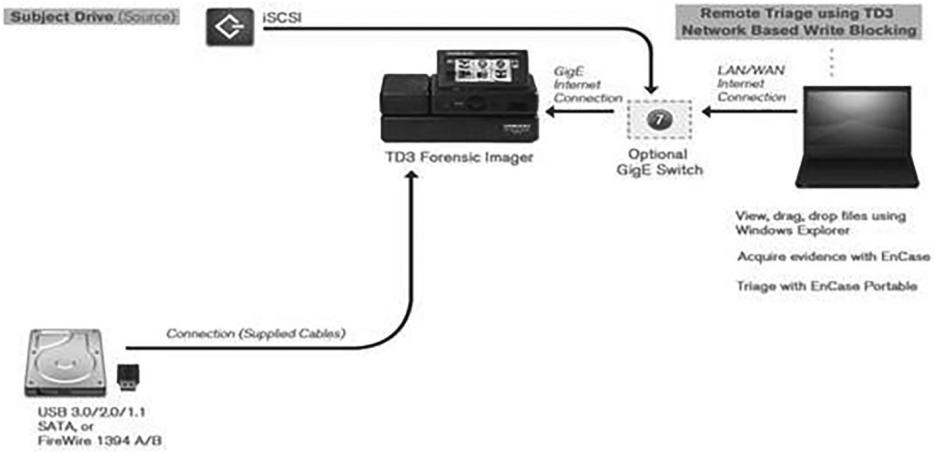

Figure 1: *TD3* or *TX1* device Triage/Collect action [23], operating in a role of the network write blocker, picture is provided by courtesy of GuidanceSoftware.

Forensic imager is connected to network over gigabit Ethernet. Hard drive with evidence is connected directly to the write blocker device and is accessible over TCP/IP trough iscsi, cifs, https. Any accredited forensic workstation can mount remote device and work with it as with any local device.

To be forensically safe forensic tools which are designed for full remote access use strong authentication and access right protection. Such tools have low level access to

remote data, capable of getting to all data levels even to the best protected operating system memory ranges strict protection of data integrity must be provided.

Remote access to data depends on the tool used and its capabilities and also on legal authority. There are various access possibilities depending on many factors:

- • Low level/raw access: kernel/system level tool capable of accessing raw data on disks or in memory
- • Agent level: agent is an independent process which can access data on target system where it is installed in forensically acceptable way
- • Service level access: implemented service which can access data on target system where it is installed in forensically acceptable way
- • API level access / Communication protocol
    - Standard https, iscsi, ssh
    - Proprietary *EnCase*, fidelis cybersecurity

Table 1: Levels of remote access for different types of forensic tools

Tool	**Access level**	**Data type accessible**
TD3 preview (logical) mode e-discovery tool, Forensic tool	Cloud SaaS Web access API access	web service, database
TD3 in preview mode Forensic tool, eDiscovery tool	Cloud PaaS File system level access	files, database, file systems, virtual machine images
Forensic tool *TD3* in acquisition (physical) mode	Cloud iaaS Raw data access	Iscsi protocol, proprietary protocol (*EnCase*, *FTK* [20])

Different types of forensic tools can be used for remote access depending which level of access it is available. For example, eDiscovery tool can access remote data trough web server as html documents or in a file system level if it has cifs access to target system.

There are different remote forensics fields depending on the goals, tools and methods used, roughly we can recognize:

- eDiscovery
- forensic system state analyses or preventive forensic
- digital forensic in the incident response
- enterprise forensic
- network forensics
- dark web forensics
- cloud forensic as newest established and
- remote forensics of mobile devices as just emerging

Maybe most used in legal actions is eDiscovery [19] or electronic discovery, which refers to discovery in legal proceedings such as litigation, government investigations, or Freedom of Information Act requests, where the information sought is in electronic format, often referred to as electronically stored information or ESI what is well defined in "New Federal Rule of Evidence to Directly Impact Computer Forensics and eDiscovery Preservation Best Practices" [21]. From system investigation point of view ESI can be external and internal documents which must be found, collected and preserved for further usage. Digital forensic tools are exceptionally good in such scenarios since it guaranties all requirements on ESI collecting satisfied. Tools can vary depending on the level of access to ESI and ownership of system IT infrastructure (Table 1).

Preventive forensics or system state analyses is part of incident response where forensics is used over the live system to define the state of the system, prepare it for incident control or to find and investigate an incident. In such role, a preventive forensic is a subset of an earlier term "enterprise forensic", which was created about 10 years ago in the effort of mayor forensic vendors to expand their existing forensic solution to the live networked systems. Maybe best-known tools with such concept and still existing are *EnCase* [18],[11],[4] from Guidance Software and *FTK* [5],[20] from Access Data. There are many other tools fully in this field or just providing part of functionality required. Among such tools are very old *CFEngine* [6], not a forensic tool, but tool whose ideas are in the core or all enterprise forensic and security systems. There is also new *GRR Rapid Response* [7], an incident response framework focused on remote live forensics, it is from Google, a free open source implementation aimed at systems with many end nodes.

Traditional network forensics can also be part of remote forensics if traffic dump, metadata or flows are collected on the fleet of probes around the network and analyzed centrally like in *xplico* tool [8] or *Fidelis Cybersecurity* [9]. Various tools can offer different versions and features of remote forensic access, so it is important to do detailed homework and preparations to choose the right tool and the right option to fulfill the forensic task acceptably. Usually there are many possibilities of approach, some possibilities are presented in more detail in the *EnCase* examples and in *EnCase* direct servlet acess [4] or *EnCase* basic file collection [11].

For the dark web, specialized forensic browsers and collecting tools exists [22], it is like for the cloud solutions. Tools like *Faw* [16] or "*X1 Social Discovery*" [17] enables reliable data collecting from web sites from web spider level [22] to sophisticated api access to service data on various social networks like LinkedIn, Facebook, Twitter. For the cloud forensics, it is more application of exiting tools in cloud context, depending on the type of cloud and level of access to cloud layers from SaaS to lowest iaaS level [10] as it is shown in Table 1. Since the surge of the cloud services, it is very important to have developed procedures how to do forensically acceptable digital forensics of remote cloud devices. One interesting sidetrack is the current trend of introduction parallelism in digital forensic tools and laboratories. Basically, it is important ground for using remote

forensic approach in accessing and processing evidence in the lab with aim to speed up process.

Enterprise level forensic tools and remote forensic are not used much in Europe, most of the usage is in the US. European law enforcement is not using it, there are different reasons, but it is not "classic forensic". There are earlier mentioned legal reasons, budget limitations to buy "remote version" of already in inventory commercial tools, lack of knowledge and lack of Standard Operating Procedures (SOP). Finally a reason for lacking remote practices in the most European countries is predominant type of investigations, a traditional "dead system" investigations.

Better situation is with the government organizations. US State Department is one of the causes for development of *EnCase* Enterprise or adding remote capabilities and access controls to existing *EnCase* frameworks. In the other way, FBI is responsible for *TD3* or adding remote capabilities to forensic imaging/writeblocking device.

Some business, mostly big companies are also doing remote forensics but internally. Even with obvious advantages for speeding up incident response there are problems. International business is a very complex environment, with usually very hostile organizational structure and legal concerns which blocks effective usage of remote forensic tools. In fact, even in the big business main reasons for not using is lack of resources needed for implementation and everyday usage of remote enterprise forensic tools.

HOW TO DO REMOTE FORENSIC

Accessing remote data in a forensically sound manner is usually a complex task which requires detailed preparations, right tools and reliable step by step logging with result verification. It is important to plan it in detail, with all necessary paperwork and testing. Among preparations it is important to do estimates on the volume and type of data which will be browsed and collected, also to analyze the impact of data collecting to IT infrastructure trough which data will flow. It is a good idea to certify IT infrastructure based on some well-known standards like "RFC 2544 Testing of Ethernet Services in Telecom Networks" or another relevant standard. Certifying the infrastructure will prevent a lot of problems later, but still it will not exclude doing tests. When requirements are defined appropriate tool and method should be selected, unfortunately even if there is a choice, in most cases there is only one option available for implementation.

To a measure real impact, a test case should be done, as close as possible to real situation, testing results should be analyzed in detail and applied back in basic work plan and SOP. After testing and with appropriate legal authority remote forensic operation can be done, all aspects should be documented, especially any problems, errors, retries or installation of agents or other additional tools. Fortunately, remote forensic tools create automated logs for practically every activity, still a proper paper documentation is required as with any other investigation or scientific process. After the remote

forensic job is finished it is important to remove any additional tools or agents used in the process. Removal of installed tools is crucial, but often forgotten step were proper documentation helps to locate and remove all such leftovers. Very often among these leftovers are temporary copies of collected data, which should be forensically soundly erased. All other activities should be done in order with plan and legal best practices.

EXAMPLE *ENCASE* ENTERPRISE BASIC IMPLEMENTATION

EnCase is used an example to present remote access capabilities since is one of the best commercial general purpose forensic tools available. Its various options and flexibility trough programming provides well known platform with a long history of improvements. *EnCase* development history shows how remote access was gradually implemented in the standard host forensic framework.

In this example [11], the basic *EnCase* Enterprise system is presented (Figure 2), with its components. Components are SAFE, examiner, servlet, concurrent connections and snapshot technology. On each remote machine (end nodes), small agent is installed (a servlet). Servlets are controlled by SAFE server and forensically used by examiner workstations (examiners).

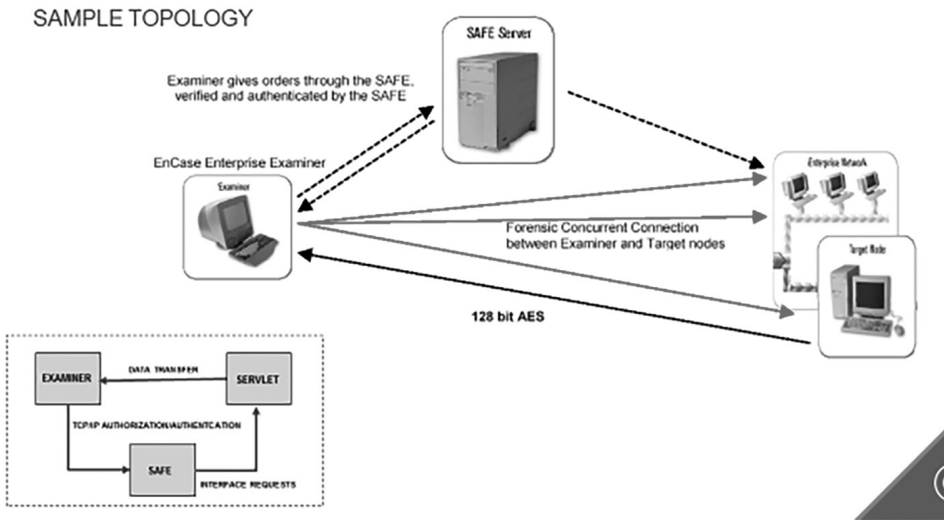

Figure 2: *EnCase* Enterprise implementation, picture is provided by courtesy of GuidanceSoftware.

System can include more than one SAFE machine, more than one examiner stations, where organization depends on the network spread, geographical issues, legal issues and many other factors. If it is properly implemented digital evidence can be collected

and analyzed all over the remote location in very short time utilizing network connections.

The SAFE [11](Secure Authentication for *EnCase*®) is the security core of the system. It authenticates users, administers access rights, retain logs of *EnCase* transactions, brokers communications and provides secure data transmission. The SAFE communicates with examiners and end nodes using encrypted data streams, ensuring no information can be intercepted and interpreted

The examiner [11] is a forensic examiner workstation. It is installed on a computer where authorized investigators perform examinations and audits. The user interface is identical as for the forensic version of *EnCase*.

The servlet [11] is a small, passive software agent that gets installed on network workstations and servers, on the end nodes. Connectivity is established between the SAFE, servlet, and the *EnCase* enterprise examiner to identify, preview, and acquire local and networked devices. Enterprise concurrent connections are secure parallel connections established between the examiner & servers, desktops or laptops that are being searched or investigated snapshot. The "Snapshot" [11] is a technology that enables the forensic examiners to scan thousands of end nodes to detect, collect, preserve and remediate any network intrusion on an enterprise-wide scale.

In this version *EnCase* is basic level remote access tool capable of various tasks on the end nodes, an example of eDiscovery task execution can be seen in "*EnCase* Enterprise Basic File Collection" [11]. Current forensic version of *EnCase* also provides a lightweight version of remote access without SAFE called "direct servlet access" for small remote access tasks [12].

Other general forensic tools have same feature set and capabilities as *EnCase*, but because of lack of standardization naming is widely different what makes comparation hard. Each of the vendors has influenced other vendors, but without keeping compatibility what makes remote forensic tasks very complicated, hard to automate and validate. This is even true for comparation with open source tools like *GRR* [7].

CONCLUSION

Remote forensics is a very useful idea, it is extension of best forensic practices and tools with aim to expand into networked environment. It is essential for future survival, unfortunately at them moment it is not much in use or in favor, but in future, with Internet of Things (IOT) it will be unavoidable and maybe only possible way do execute digital forensic tasks.

For the future use and practice, we expect eDiscovery arriving in Europe and the rest of the world. On the global scale, we expect automation and standardization for remote forensic because of increasing security problems and incident response requirements. Good example of the trend is introduction of the Open Command and Control (OpenC2)

language trough OpenC2 forum "The OpenC2 Forum defines a language at a level of abstraction that will enable unambiguous command and control of cyber defense technologies" [14].

REFERENCES

[1] John Sammons: "The Basics of Digital Forensics, 2nd Edition, Chapter 1: What is Digital Forensics", Syngress 2014

[2] (20.6.2017) https://technet.microsoft.com/en-us/library/cc939973.aspx,

[3] (20.6.2017) https://www.guidancesoftware.com/tableau/hardware/*TD3*,

[4] (20.6.2017)https://www.slideshare.net/DamirDelijadamirdeli/ecase-direct-servlet-acess-v1,

[5] (20.6.2017) http://accessdata.com/products-services/forensic-toolkit-ftk

[6] (20.6.2017) https://cfengine.com/product/what-is-cfengine/

[7] (20.6.2017) https://github.com/google/*GRR*

[8] (20.6.2017) http://www.xplico.org/

[9] (20.6.2017) https://www.fidelissecurity.com/

[10] (20.6.2017)https://www.ibm.com/blogs/cloud-computing/2014/02/what-is-platform-as-a-service-paas/

[11] (20.6.2017)https://www.slideshare.net/DamirDelijadamirdeli/e-ev7ediscovery-1?next_slideshow=1

[12] (20.6.2017) https://www.slideshare.net/DamirDelijadamirdeli/ecase-direct-servlet-acess-v1

[13] John L. Hufferd: "iSCSI: The Universal Storage Connection", Addison-Wesley Professional 2002

[14] (20.6.2017) http://openc2.org/

[15] John Sammons: "The Basics of Digital Forensics, 2nd Edition, Chapter 2: Key Technical Concepts", Syngress 2014

[16] (20.6.2017) http://www.fawproject.com/en/default.aspx

[17] (20.6.2017) http://www.x1.com/

[18] (20.6.2017) https://www.guidancesoftware.com/*EnCase*-forensic

[19] John Sammons: "The Basics of Digital Forensics, 2nd Edition, Chapter 7: Electronic Discovery, Chapter 1: Deep Web vs. Surface Web", Syngress 2014

[20] (20.6.2017) http://accessdata.com/solutions/digital-forensics/forensic-toolkit-*FTK*

[21] (20.6.2017)https://articles.forensicfocus.com/2016/12/19/new-federal-rule-of-evidence-to-directly-impact-computer-forensics-and-ediscovery-preservation-best-practices/

[22] Eduard C. Dragut; Weiyi Ming; Clement T. Yu: “Deep Web Query Interface Understanding and Integration”, Morgan & Claypool Publishers 2012

[23] (20.6.2017) https://www.slideshare.net/DamirDelijadamirdeli/olaf-extension-*TD3*-inisg2-2