Technical and legal aspects of security

e-Discovery or digging for (digital) evidence

Antoine Puissant

Teachers : Mrs. Carla XXX and M. Arnim XXX

2014 - 2015

Résumé

Ceci est le résumé

Table des matières

1 Introduction incident investigation

1.1 Fundamentals

1.1.1 EDRM

EDRM [1] is about finding a international model for investigations.
There are 9 stages in the all model :

1. Information management (T0)
2. Identification (T1)
3. Preservation (T2)
4. Collection (T2)
5. Processing (T3)
6. Review (T3)
7. Analysis (T3)
8. Production (T4)
9. Presentation (T5)

Sometimes, you can find some pieces of material that forces you to go back on the model. This is why there is some arrows going down and back.
The fourth part is the volume (yellow). It express the need of reducing the size of the volume (huge at the beginning, small at the end).
The fifth element is the relevance of the data. At the end you must have few data but relevant data.
The beginning of the investigation doesn't start at the first stage. This first stage is about knowing where are the files, what system is running, etc...They start when « *shit appends* ».
This often start when there is litigation (suing). In the USA, when someone says « I'm going to sue you », the target have the obligation to freeze all his data. This is called litigation hold.
In Europe, I can't have the right to demand some data to the other to prove the case (like in the USA). In Europe, you have to find your proofs all by yourself and present them to a judge.

Information management (T0)
To manage all sources of Information, including ESI. It does that by defining and implementing for all sources of Information, especially for ESI.
Data can be in rest, idle, in the cloud, out of used (archived, tapes, special hard disks, etc...) but you legally obliged to keep them for legal obligations.
Then, you need some retention policies : how the data will be stored, what data can be destroy (then you need a legal department to know what data you can destroy. If you destroy wrong data, you can be sued), how long the data should be stored...
You can also have some e-Discovery-processes ready when something wrong happen.
But most of the time, it is not so great, is most of the time a mess for every process. This is a lot about documentation. This part is often skipped because of lack of time or laziness.

1. Electronic discovery reference model

Identification (T1)
This stage is about determining what should be preserved and collected, the data that should be kept. You should also determine the scope, the breadth and depth of needed ESI.
So you're simply making a list of what you want.

Preserve

Collect
In this part you want to get the information you have identified. You want this data exactly the same.

Process
You need to extract the data, convert it to make it more readable, remove non-relevant data, scan the papers to make some faster searches on it, get rid of the duplicates, remove data out of the time scope you selected, etc...

Review (T5)
Then, you need some tools to get through the data really faster. This is not only about finding some specific words, it can be to check the relevancy of the data too.
You also have to get rid of the privileged information (lawyer - client, doctor - client, priest - believer, etc...). You can't look at those information as an investigator or you will surely loose the case.
The data given to the judge are only non-privileged ones.

Analysis (T6)
Here, you are trying to build the picture of what happened.
To do so, you need to build some relation diagrams, some activities lists, etc...
You also need to determine some specific vocabulary, specific keywords that are signals for the scheme of malicious people.
This part is more about mind work, putting all the pieces together.

Production (T7)
Now that you know what happened, how did it happened, you can produce some responsive documents for the client. You need to know how the client wants the information (reports, excel spreadsheet, pdf, raw data, etc...).

Presentation (T8)
Then, you also need to make a presentation. This can be only for the client or as an expert witness in court (in front of the jury).

1.2 The trigger

A trigger can be an unexpected event that differs from the normal business operation and has caused/causes/might cause harm or damages.
The incident is something from the past. The signal/warning is the present. And the uncertainty is for the future.

If there is a trigger, there is an assignment. This assignment differs between the different triggers.

Incident	Past	Reconstruction
Signal/Warning	Present	Audit/Inspection
Uncertainty	Future	Exploration

TABLE 1 – Assignments for specific triggers

Depending on the type of assignment, you have to answer to different questions :

Reconstruction	What happened ? How did it happened ?
Signal/Warning	What is happening ? How is it happening ?
Uncertainty	What might happen ? How might this happen ?

TABLE 2 – Question for specific assignments

1.2.1 The investigation : ...

For an investigation, you have to be able to ask 8 ≪ w ≫ questions :

What	Intelligent data Analysis
Who	Business investigator
Where	Location
When	Time period
With what	Means
Which way	Approach
Why	(Re)Construction
What for	Story

TABLE 3 – Eight question you must ask during an investigation

1.2.2 The investigation : the model

You can use some tools to make some mind mapping such as the one after. An investigator doesn't have any authority regarding the data he can use. He also have to be independent and impartial. Even if the result doesn't please the client.
The first thing you have to do when you have an assignment is asking questions about the goal of the client, about the data that was given to us, or even about the assignment itself.

1.2.3 The investigation : Digging for...

An investigator is here to find some facts, not truth or anything else.

1.3 The job

1.3.1 investigation is like archeology

There are 5 phases :

1. Preliminary research : Where to dig ?
2. Field work : The digging and the findings
3. Lab work : Process the findings
4. Desk work : (Re)Construction the issue
5. Closing : Present the results

The investigator find some things like artefact's and traces. Since those things don't talk, it is the investigator duty to tell their story. He has to reconstruct the past and present or construct the future.

1.4 The process

1.4.1 Phase 1 : Preliminary researches

The first case analysis is about searching for background information on the case using given documents and public sources about all persons, places, times involved.
Here, we're giving a scope. We don't have to get out of this scope for the case. « I found very likely that... »
You cannot make any conclusion while writing some reports. You must present only facts. You can't say you're sure 100% sure about something. « There is someone on the camera feed looking like person A. It's very likely that this person took some supplies at this moment ». You can only give your thought about a fact if this is something the client ask about it.

2 Incident response : Legal and documentation aspects

2.1 Important stuff

e-Discovery is not about technical stuff, more on static forensic, live forensic, order of volatility, etc...
It's always better to write things down before making any action. It helps organizing your mind and stay legal.
No matter how sure you are about a legal thing, you must always call your lawyer first.

2.2 Civil law

Basicaly, it's about « A against B for some reason ». What is asked is a compensation (usually, money). Both of the parties collect their proofs (documents (any kind of documents, papers, digital records, etc...)). Then, a court of law decide. Civil law is a balance of probabilities.
To get some stuff from the other party, you can't get it by betting on the will of B. To get the evidence, you have the Anton Piller Order and the Norwich Pharmacal Order. Those are both court orders. So you have to convince a judge to give one to you.

2.2.1 Anton Piller Order

Search an seizure without prior warning.

2.2.2 Norwich Pharmacal Order

A and B goes at the court and a third party to get A's requirement against B. In France, C, the third party, is Hadopi. This order is under the European Convention of Human Rights - Article 8 [2]. Since this is a privacy violation, you must have the court authorization.

2.3 Criminal laws

Here, it's society (people, states, etc...) against « bad guys ». It is about murder, theft (financial, identity, shoplifting, etc...).
Since this is the state and not M. A, they have other rights :

- They can arrest suspects
- They can collect some evidence (interogation, search and seizure, etc...) usually overseen by the police

The difference between Civil law and Criminal law is that criminal law is about punishing people and not about compensation.

Since we can't know at the beginning if this is going to be a criminal or an civil case, we always assume that it's a criminal one. Then, to be able to prove

it's really a criminal case (to involved the police force), you have to document everything you do.

2.4 Documentation aspects

You can read the ACPO [2] guideline to get some ideas about taking some data :

— Every time you can, copy the data, don't work on the originals.
— ...
— Don't be an idiot
— The person in charged of this investigation is responsible that the law and these principles are respected.

2. Association Chief Police Officer

3 Acquisition in computer forensic

3.1 Introduction

Acquisition is about preservation and collection. Preservation is about safely securing important information (without damaging data). Collection is about safely collecting potentially important data.
If you want to make an investigation, you have to seize every devices. Now, this means lots of devices like computers, mobile phones, drives, etc...
To gain some crucial information, you have to look for meta-data. This data of data is something really critical. They are created automatically so the user doesn't have full control of it. To trust meta-data, they must be sure about the veracity of this data. For example, for remote logging, you can correlate the information and be sure of it veracity. Since remote logging can prove something since they are from multiple devices (for example, logging from a camera feed plus phone location, etc...).
The problem with a computer is the volatility of data. This problem is called OOV [3]. The volatile componants in a computer come in the following order :

1. CPU : register and cache
2. RAM
3. Networking information (traffic and connection status)
4. Processes (running operating system and program used)

3.2 Static forensic

This is the « old way » of analysis. For example, they would seize a computer, make an image of the hard disk and start investigate right there. But this is really dangerous. You don't start a computer on the place. It can be rigged with explosives. When you are on site, you just have to collect it and start the analyze it later, in a lab.
The information can be find on multiple types of devices : HDD, USB-keys, mobile phones, etc...
When you have copy your data, you have to prove the copy didn't made a error and alter the one on the source. To do so, you hash the data so you can check the hashes (MD5, SHA1, etc...).
To do some static forensic, you have lots of open sources software : Autopsy, OS forensic, FTK, Encase, XRY, Kali, etc...

When you want to make a copy of an HDD, you cannot plug in the drive directly onto your computer because some meta-data will change on the disk. On different file system (NTFS, EX, etc...), there are some meta-data about last time it was mounted, is it was unmounted it normally, etc...To counter this, you have to get some write-blockers. You can, if you know correctly how to use Linux, do a write-blocker with software.
If you don't know what a device is doing exactly, don't touch it. You might damage the data.
To make the acquisition, there are many tools. Use some forensic tools (not DD) like FTK Imager. To be able to recover some documents (deleted files),

3. Order-Of-Volatility

you can also use some tools.
A proper image is a bit-level copy.
The problem is the size of everything you have to copy and analyze. You need as many storage as the suspect to copy it.
If a HDD has been overwritten, data is ungetable. For SSD, it is really different (due to wear leveling and garbage collection).

The problems when you do this are encryption, anti-forensic tools (kill switch), root-kits (intentionally or not), data hiding (stenography, etc...).

3.3 Live forensic

This is about investigating on a active and running system. You can gather some sensitive data like networking ones. Those data can't be acquired with static forensic.
Here, OOV are a bit worse than in static forensic. If you have some virtual machines. If you have some information on some servers, you might not be able to get the date from the company hosting it. But if you have some forensic tools, you can give it some VM disk images or dump RAM to be examined (using firewire or thunderbolt).
You can use some tools like Microsoft's COFEE (live USB), FTK, EnCase, LiveView, etc...
TRESIR is something to prevent encryption key being store in the RAM. Then it's store in the process.
Live forensic is much more about knowing you target, what you want to get.

The only tool you can't automate, it's your comprehension of the data.

4 Assignment

4.1 09/11/2015

4.1.1 Things to know

— ...

4.1.2 What's expected

— Investigate the evidence
— Maintain a proper decision log
— Write a report to the management

The report must have an management summary for non-technical persons. Then, there is the investigation in details (every steps we took, why, when, how, etc...), what were the results of each of those steps, etc...

4.1.3 Pro-tips

— Look at the reports examples and the decisions log.
— Distribute the work, improve efficiency
— Don't abuse of copy paste
— We'll have to talk to some people in the company

If you want to be right on your evidences, you have to respect the chain of custody. Here, if you want to check an evidence, you have to fill a evidence paper (ID of the evidence, description, location, released to, by, etc...). You also take pictures of the evidences before taking them. So, you know the state of it before packing it.

4.2 10/11/2015

4.2.1 Question to ask

— What is the thing Mrs. Maid has done and regret now ?
— Who took some photographs of her ?
— What's the exact date of the Christmas party ?
— Who are the « guys in the office » ?
— How many pictures does JL have ?
— What kind of « leverage » JL have ? Only pictures ? something else ? What's on the USB external drive ?
— What is the HR policy ? Are they any breach of it ?
— Why JL calls her « M&M » ?
— Pictures showed to whom ?
— What is the exciting stuff ? One which drive ?
— What are those two projects ? Threat for JL ?
— What's the motive of MM ? What does she want ?

The assignment is a disciplinary matter between MM and JL.
Company is okay with bringing their own device but those devices are subject to search and seizure, even if they are your own (in the policy).
We contact the legal Director to have the authorization to perform a search and seizure on JL and FT stuffs (because they are both involved in the case).

When we have it, we go to the IT to know what we are going to find (computer security, etc...).
We then get someone from HR to come with us. We go to the building staff to be able to get to their offices.
Then, we get someone from the security team if the suspects get violent.
To perform the search and seizure, we do it when the suspects are working (so we have all their devices, computers running, unlocked, etc...). Before entering in the open-space, you have to know the exact location of FT an JL. You have to make 2 groups :

— One to freeze JL
— One to freeze FT

We have to be sure they don't delete anything. Security is here to do this. Then, you start collecting all the evidences.
Regarding the interviews, all the 3 of them refuse to talk to us :

MM « I have already told you everything, just solve my problem »

JL « This is bullshit. I don't want to talk about this »

FT « This is bullshit. I don't want to talk about this »

After the search and seizure, we have a pack of pictures from JL and FT. We also have a system to make some searches in the mails (`145.92.7.241`).

4.2.2 Tips

— There is a difference between civil law and criminal law.
— We are in a bank. They are very strict rules the bank need to complains with.
— We are doing thing from the criminal standard.
— Remember the scope. If the investigation is going into some trouble, call your lawyer.
— If we find something out of the scope, we don't mess up with the cases. We make another case to check if this is important or not.

Références

[1] AUTHOR. *REF TITLE*. ORG. 2015. URL : http://www.url.com/.

[2] WIKIPEDIA. *European Convention on Human Rights*. Wikipedia. 2015. URL : https://en.wikipedia.org/wiki/European_Convention_on_Human_Rights#Article_8_-_privacy.