Technical and legal aspects of security

ESIEA ECOLE D'INGENIEURS DU MONDE NUMERIQUE

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

1.3 The process

2 Partie 2

2.1 Sous-titre 2

Références

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