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
2. Identification
3. Preservation
4. Collection
5. Processing
6. Review
7. Analysis
8. Production
9. Presentation

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.

1.2 The trigger

1.3 The process

1. Electronic discovery reference model

2 Partie 2

2.1 Sous-titre 2

Références

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