The M57 Patents Case

Investigating criminal activity within m57.biz
Part 1: Illegal digital materials

M57.biz is a new company that researches patent information for clients.

Facts of the case:

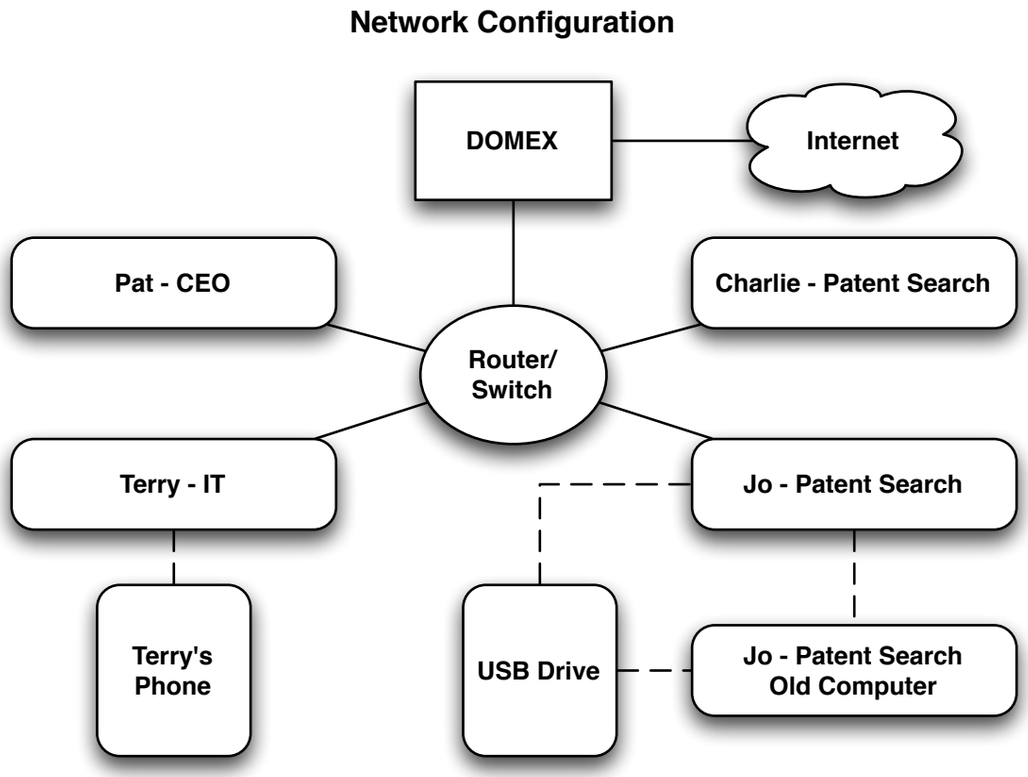
- 1 president / CEO
- 3 additional employees
- The firm is planning to hire more employees, so they have a lot of inventory on hand (computers, printers, etc).

Current employees:

- President: Pat McGoo
- Information Technology: Terry
- Patent Researchers: Jo, Charlie

M57.biz organization

Employees work onsite, and conduct most business exchanges over email. All of the employees work in Windows environments, although each employee prefers different software (e.g. Outlook vs. Thunderbird).



Note: In the above figure "DOMEX" is the local server managing external network access and email.

The case: illegal digital materials

A functioning workstation originally belonging to m57.biz was purchased on the secondary market. The buyer (Aaron Greene) realizes that the previous owner of the computer had not erased the drive, and finds illegal digital images and videos on it. Aaron reports this to the police, who take possession of the computer.

Police forensics investigators determine the following:

- The computer originally belonged to m57.biz
- The computer was used by Jo, an M57 employee, as a work machine.

Police contact Pat McGoo (the CEO). Pat authorizes imaging of all other computer equipment onsite at M57 to support additional investigation. Police further pursue a warrant to seize a personal thumb drive belonging to Jo.

The preliminary case: illegal digital materials

You are given disk images from all of the computers and USB devices found onsite at M57, along with a USB thumb drive belonging to Jo. You are also provided with four detective reports and a search warrant and affidavit associated with seizure of the USB drive.

- *For the purposes of the scenario, illegal images have been simulated with pictures and videos of cats produced exclusively for this corpus.*

Questions to answer:

- Is Jo the owner of these files? What evidence is there to confirm or reject this?
- How did the computer come to be sold on the secondary market?
- Who (if anyone) was involved in the sale (theft?) of the computer?
- Were any attempts made to hide these activities?

Electronic identities

Pat McGoo (President):

- pat@m57.biz (email password: mcgoo01)

Terry Johnson (IT Administrator):

- terry@m57.biz (email password: johnson01)

Jo Smith (Patent Researcher):

- jo@m57.biz (email password: smith01)

Charlie Brown (Patent Researcher):

- charlie@m57.biz (email password: brown01)

Your assignment

You have been given:

- A copy of all of the materials obtained by the police during their visit to M57.
- A copy of the detective reports, along with the search warrant and affadavit.
- EnCase

You are tasked with determining the following:

- Is Jo responsible for the files found on the purchased machine? What evidence is there to support this?
- How did this machine get onto the secondary market?
- Who (if anyone) from the company is responsible for the sale of the machine?
- Are there any other suspicious activities occurring within M57?

Corpus and Supporting Documents

The “Police Evidence” set of data includes the following:

- Hard drive images from all workstations in the office:
  - charlie-2009-12-11.E01, jo-2009-12-11-002.E01, pat-2009-12-11.E01, terry-2009-12-11-002.E01
- (Optional) RAM dumps from the machines taken during the police visit (mdd or windd images):
  - charlie-2009-12-11.mddramimage.zip, jo-2009-12-11.mddramimage.zip, pat-2009-12-11.mddramimage.zip, terry-2009-12-11.mddramimage.zip
- Three company USB drives found on-premises and one personal USB drive seized from Jo:
  - charlie-work-usb-2009-12-11.E01, jo-work-usb-2009-12-11.E01, terry-work-usb-2009-12-11.E01
  - jo-favorites-usb-2009-12-11.E01

Comments and Additional Activities

Use EnCase to examine the M57 Patents disk images.

- Most of EnCase features can be used on these images.
- They are big enough to be realistic, small enough so that the EnCase functionality will run in 5-30 minutes depending on the image being examined.

Try using FTK or SleuthKit to compare functionality.

A number of professional contacts and outside persons (friends of the employees) appear in this scenario. Who are they? Are they involved in any of the activities uncovered?

Note: Terry's phone is not available in the corpus. However, several files that originated from the phone exist somewhere in the corpus. Can you find them? Are they related to the case?