The M57 Patents Case

Investigating criminal activity within m57.biz
Part 2: Exfiltration of corporate intellectual property

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

Facts of the case:

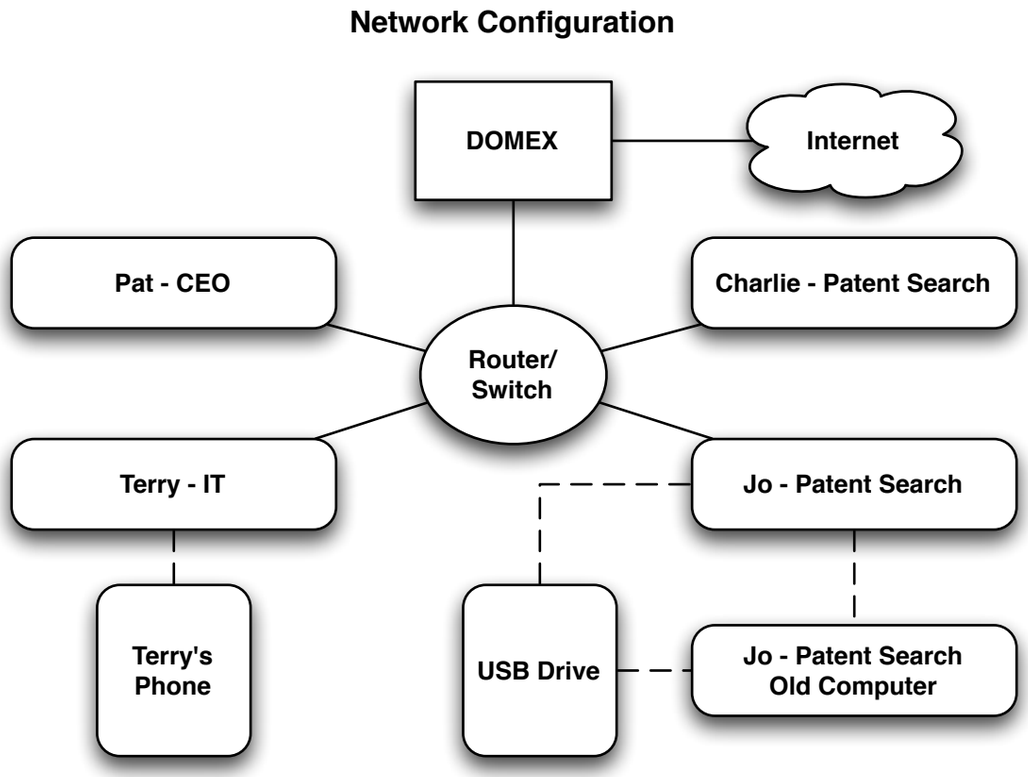
- 1 president / CEO
- 3 additional employees
- The firm is planning to hire more employees, so they have a lot of inventory on hand (computers, printers, etc).

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: exfiltration of corporate IP

One of the employees in M57 is stealing proprietary research from the company and passing it on to an outside entity. This employee has taken some measures to cover their tracks, but probably did not count on the company machines being imaged in the ongoing investigation of other criminal activity.

You are tasked with determining the following:

- Who is exfiltrating the data?
- How are they doing it? Can you identify the specific items they have stolen? What is required to access the data?
- Who is the outside contact?
- Is there anything in your analysis to suggest that this person might be charged with more than one criminal offense?

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)

Corpus and Supporting Documents

You have been given 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.

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?