# The M57 Patents Case

Investigating criminal activity within m57.biz
Part 3: Eavesdropping

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

Facts of the case:

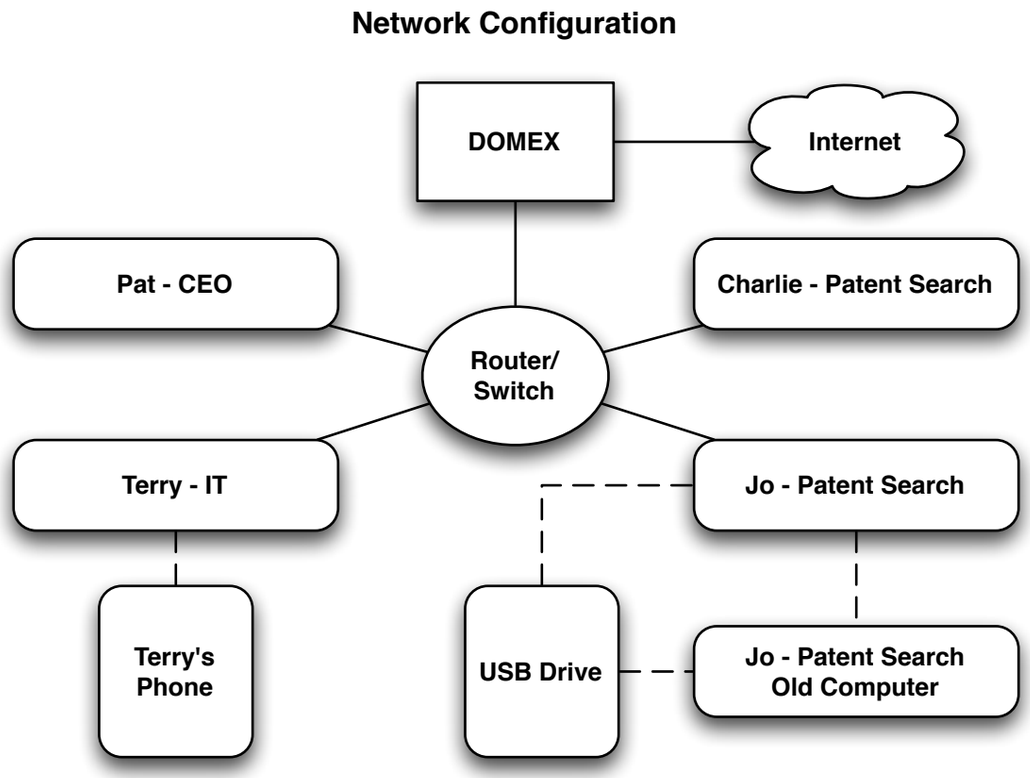
- 1 president / CEO
- 3 additional employees
- The firm is planning to hire more employees, so they have a lot of inventory on hand (computers, printers, etc).

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: electronic eavesdropping

One of the M57 employees is spying on the boss (Pat McGoo) electronically. This employee is concerned that Pat may find out about certain activities they have engaged in - activities that may be related (directly or indirectly) to another ongoing investigation.

You are tasked with determining the following:

- Who is spying on Pat?
- How are they doing it? Can you identify specific methods or software they have used to facilitate this?
- Why is the employee spying on Pat?
- Is anyone else involved? Would you characterize them as accomplices?

# 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?*