
# The case of M57.biz

Investigating the case of corporate exfiltration

# M57.biz is a hip web start-up developing a body art catalog.


---

Facts of the case:

- $3M in seed funding; now closing $10M round
- 2 founder/owners
- 10 employees hired first year

Current staff

- President: Alison Smith
- CFO: Jean
- Programmers: Bob, Carole, David, Emmy
- Marketing: Gina, Harris
- BizDev: Indy

# M57.biz is a virtual corporation

Programmers:

- Work out of their houses
- Daily online chat session; Weekly in-person meetings office park

Marketing & BizDev:

- Work out of hotel rooms or Starbucks (mostly on the road)
- In-person meetings once every two weeks.

Most documents are exchanged by email.

# The case: document exfiltration

A spreadsheet containing confidential information was posted as an attachment in the "technical support" forum of a competitor's website.

The spreadsheet came from CFO Jean's computer.

- You are given a copy of the spreadsheet, "m57plan.xlsx"

Questions to answer:

- How did the documents get on the competitor's website?

# Here is the spreadsheet:

forensics-in-a-nutshell.pdf

| M57.biz company | | | | |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| Name | | Position | Salary | SSN (for background check) |
| Alison | Smith | President | $140,000 | 103-44-3134 |
| Jean | Jones | CFO | $120,000 | 432-34-6432 |
| | | | | |
| Programmers: | | | | |
| Bob | Blackman | Apps 1 | 90,000 | 493-46-3329 |
| Carol | Canfred | Apps 2 | 110,000 | 894-33-4560 |
| Dave | Daubert | Q&A | 67,000 | 331-95-1020 |
| Emmy | Arlington | Entry Level | 57,000 | 404-98-4079 |
| | | | | |
| Marketing | | | | |
| Gina | Tangers | Creative 1 | 80,000 | 980-97-3311 |
| Harris | Jenkins | G & C | 105,000 | 887-33-5532 |
| | | | | |
| BizDev | | | | |
| Indy | Counterching | Outreach | 240,000 | 123-45-6789 |
| | | | | |
| | | | | |
| | | | | |
| Annual Salaries | | | $1,009,000 | |
| Benefits | | 30% | $302,700 | |
| | | | | |

# Summaries of interviews.

Alison (President):

- *I don't know what Jean is talking about.*
- *I never asked Jean for the spreadsheet.*
- *I never received the spreadsheet by email.*

Jean (CFO):

- *Alison asked me to prepare the spreadsheet as part of new funding round.*
- *Alison asked me to send the spreadsheet to her by email.*
- *That's all I know.*

# Electronic identities

Alison (President):

- alison@m57.biz ; password: "ab=8989

Jean (CFO):

- jean@m57.biz ; password: gick*1212

# Your assignment


You have been given:

- A copy of Jean's computer's hard drive
- A copy of the spreadsheet
- EnCase

The client, one of the first-round funders, wants to know:

- When did Jean create this spreadsheet?
- How did it get from her computer to competitor's website?
- Who else from the company is involved?

***Note: I have imaged Jean's computer for you:***

- jeanm57.E01 (EnCase format)
- jeanm57.aff (AFF format)

# Until lunch...

Use EnCase to examine the test image.

- Most of EnCase features can be used on this test image.
- It's big enough to be realistic, small enough so that the EnCase functionality will run in minutes.

If you solve the problem, try using FTK or SleuthKit and see how they compare.

You can also:

- Try to run the EnCase imager on one of our test media
- Try to carve the test image.