1. Planting Evidence

i. Excel spreadsheet of buyer’s information, meeting dates, agreed amount etc.

ii. Formal report of company announcing the date for press conference

- Both downloaded from company’s server

- Uploaded to personal Google Drive then downloaded again to send to buyers

iii. Screenshot of transaction history to be sent to the buyer to double confirm that suspect already received the money

iv. The actual design ideas stolen by suspect

2. Imaging and Registry

We decided to produce an image from suspect’s computer based on ‘Contents in a Folder’ because:

* **Time constraint**

The company Collin Star wants to have just enough evidences to start a law suit on suspect as soon as possible as their company’s reputation will be affected due to the case. The longer the time, the more money they lose.

By creating image based on folders save a lot of time and it requires lesser cost (less forensics resource team) to investigate the files.

* **Prior knowledge of potential evidences**

The company Collin Star has a list of suspects and have given the forensics team some evidences that are extracted from their company database. The forensics team can identify which type of files they are looking for to be extracted as evidences.

**CREATING IMAGE EVIDENCE**

**1. Adding Evidence Item: Documents and Settings File**

A screenshot of a cell phone

Description generated with high confidence

**A screenshot of a social media post

Description generated with very high confidence2. Adding potential evidences in Custom Content Sources, then click ‘Create Image’.**

**3. Add image destination with descriptions**

A screenshot of a social media post

Description generated with very high confidence

**4. Checking the hashes. Complete.**

**Note: The elapsed time is much more faster than creating image by using physical drive.**

**A screenshot of a social media post

Description generated with very high confidenceWhen we have larger physical drive, we should just focus on certain known files to save space, time and cost.**

**A screenshot of a social media post

Description generated with very high confidence\*Below image is for comparison purpose only:**

Also note that the file format will not be E01 when creating image by using folders.

However .ad1 can be converted into E01 if needed. In this case we need fast acquisition so it does not matter as long as the forensics team report what they did precisely to their leader throughout the evidence collection process.

**OBTAINING REGISTRY FILE**

**1. Locating the registry file.**

**A screenshot of a social media post

Description generated with very high confidence%systemroot% \system32\config**

**2. Exporting the common registry files**

A screenshot of a social media post

Description generated with very high confidence

**A screenshot of a social media post

Description generated with very high confidence3. Find and export registry files exclusive for each user by using similar steps.**

**4. Repeat Step 3 for Default User, Local Service and Network Service**

3. Answering Questions

a) What file system resides on the image?

Windows XP (NTFS 3.1)

A screenshot of a computer

Description generated with very high confidence

b) How many free clusters are there on the partition?

A screenshot of a computer

Description generated with very high confidence591,409

c) How many sectors are there on the image and how large is each sector?

10,458,252.

Size of cluster = 4096

A cluster has 4 sectors.

One sector = 4096/4 = 1024bytes

A screenshot of a social media post

Description generated with very high confidence

d) How much unallocated space is there on the image?

31,744+13,773,312 = 13805086

A screenshot of a social media post

Description generated with very high confidence

A screenshot of a social media post

Description generated with very high confidence

e) Look at the WINDOWS/Windows folder. What is its MFT number and what is the SID of its owner?

MFT number: 28 (28672)

Owner SID = S-1-5-32-544. Only owner will have administrator rights.

A screenshot of a social media post

Description generated with very high confidence

A screenshot of a social media post

Description generated with very high confidenceNote that owner is one of the users in among all users. Thus, same SID and name can be found in the users list

A screenshot of a cell phone

Description generated with very high confidencea) Report the RID and usernames of all users on the computer.

User 1: Administrator

RID: 500

A screenshot of a cell phone

Description generated with very high confidenceUser 2: Guest

RID: 501

A screenshot of a cell phone

Description generated with very high confidence

User 3: HelpAssistant

RID: 1000

A screenshot of a cell phone

Description generated with very high confidence

User 4: SUPPORT\_388945a0

RID: 1002

b) What time zone is the computer configured to use?

A screenshot of a cell phone

Description generated with very high confidencePacific Standard Time and Pacific Daylight Time with daylight bias of -60

A screenshot of a cell phone

Description generated with very high confidence

c) Who is the registered owner of the computer?

\SOFTWARE\Microsoft\WindowsNT\CurrentVersion

A screenshot of a social media post

Description generated with very high confidenceRegistered User: user

\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Products

Registered user ID: S-1-5-18

A screenshot of a cell phone

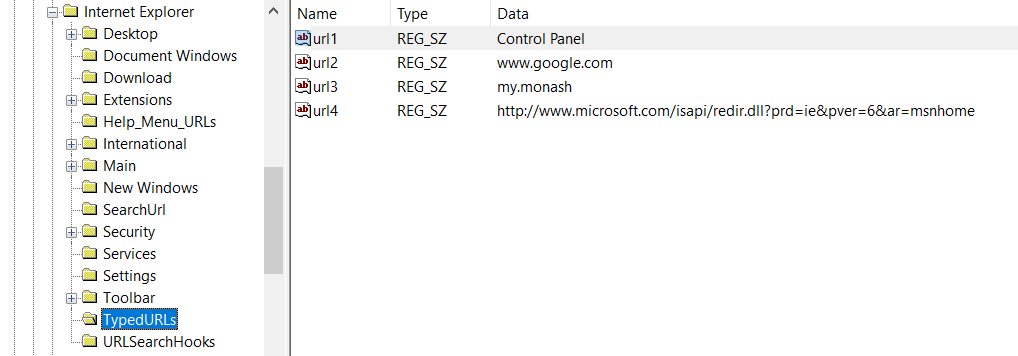
Description generated with very high confidence

d) What webpages did the user(s) visit?

A close up of a logo

Description generated with very high confidenceBy admin on Internet Explorer:

By admin on Google Chrome:



The other users did not log on at all. Thus, there is no browsing history for them.

e) When did the user(s) last log in?

Admin: 10/9/2018 5:00:38 UTC

A screenshot of a cell phone

Description generated with very high confidence

Guest: Never

A screenshot of a cell phone

Description generated with very high confidence

Help Assistant: Never

A screenshot of a cell phone

Description generated with very high confidence

Support: Never

A screenshot of a cell phone

Description generated with very high confidence