

## Project Scenario

The realtor, Betty Waterford, pulled up slowly to the 4-bedroom ranch-style house with the annoyingly lovely newlyweds still chattering away behind her. The wife seemed to find everything worth talking about, even paint drying. So, when she saw the simple orange coloring of the house, she scarcely took a breath from her discourse on trees, squirrels, and nuts to change to the new topic of houses and the pros and cons of each potential color they might paint their future home. Betty smiled and nodded while the husband threw in comments on which tools would apply each color best. "There's a difference???" Betty forced herself to keep nodding and smiling to hide her incredulous thoughts. This was her job, the couple was ready to sign, and she could use the inflow. She parked the car and jumped out, reveling in the moments of silence afforded her, the soft breeze easing the cacophony in her ears. Those moments weren't long enough though, because quickly the couple stepped out of the back of the Ford Taurus, the wife's voice getting a little shrill as she excitedly pointed out every "cute" and "adorable" feature of the house. Betty had to admit the two and a half acres were beautifully kept and relaxing after the Houston freeways. The old, brown oak to the left of the car was beautifully shaped, with one branch hanging so low, it felt as if it were calling to her to come and sit. Betty had loved crawling into the nestling branches of the trees around her neighborhood in her youth and could still feel the sense of comfort those havens provided her just by thinking of it. The breeze brought the sound of laughter to her and Betty snapped back to the present. She matched her face to her clients' and they began to walk towards to front of the house.

As they started on the curved concrete path to the front door, the garage door began to roll up and the rumble of a large vehicle growled from inside it. All three stopped, gaping at the garage. Betty's heart started to thud - no one was supposed to be here. The young wife's shocked silence was only momentary; she quickly recovered to express her dissatisfaction of the house being occupied when the paperwork had clearly indicated that it should be vacant and ready for immediate move in. The mother in Betty made her throw out her arms in front of the couple, placing herself between them and the dark vehicle slowly revealing itself. She tried to mutter reassuring phrases, her mind only half catching the complaints of the oblivious couple, as she began shepherding them away from the house. "Of course, I understand." "No, I'm not sure who it is." "Yes, I'm sure it will be fine." Betty caught sight of a stand of pine trees and led her newlyweds behind them. They were thin, soft wood trees, but it was better than being out in the open, right? All eyes watched as a navy SUV roared out of the garage, its tinted windows glinting in the morning sun. Betty's fingers, halfway wrapped around the cell in her purse, fumbled as a sickening crunch echoed across the lawn. The SUV swiped her poor, defenseless car - a humble but vital piece of her livelihood - as it tore down the driveway. Betty numbly watched her Taurus rock a time or two from the impact.

"Oh, dear Lord. How rude!" the wife exclaimed, her left hand flying to her chest and her right going to her husband's arm.

"I'm not so sure this is the kind of neighborhood we want to live in after all," the husband added. He gave a look to his wife.

Betty's eyes went from wide shock to narrow, seething anger as she glared in the direction of the SUV's escape. If that idiot just cost her her commission...

"Not to worry," Betty felt the husband's large hand pat her shoulder, "I caught three of the license plate's letters: XTS. It should help." Betty tossed a half-hearted smile his way as she reached back into her purse and withdrew her phone to call 911.

.....

Detective Timemaker sighed heavily as a new case was dropped on his desk. Reluctantly, he put his caffeine-rich coffee down and replaced it with the plain manila folder of the crime report. "Couldn't they splurge for some color, at least?" he muttered to himself. He sighed again as his eyes settled on the form in front of him and his mind shut out the world, slowly grinding to action in processing the new case.

An empty house up for sale had been discovered occupied by unknown person(s) by a realtor doing a showing to a newlywed couple.

At 09:23, a 911 call was made by the realtor, Betty Waterford, to report an intruder in a vacant house and a hit-and-run collision of an empty vehicle. First responders, Officer Garrison and Officer White, checked the house and took statements.

Inside the house, splatters of partially-dried blood were found on the tile floors of the oversized living room. Multiple hair samples and a few spots of dried bodily fluid were also collected from the area. From around the house, a littering of several crushed beer cans was recovered. In the bathroom, urine could be smelled, so samples from and around the toilet bowl were taken. Out the back door 15 yard to the northwest, several carcasses of kittens and rabbits were discovered. From the garage, tire marks were collected and a flash drive was found. Finally, paint samples were taken from the side of the realtor's car and a partial license plate was recorded.

Analysis showed the blood in the house to be from felines, Leporidae, and 3 types of canines. The hair that could be analyzed was from an American Pit Bull Terrier and a Birman cat, which matched two of the blood samples. The other two dog breeds were identified as American Bulldog Scott Type and Staffordshire Bull Terrier. The dried bodily fluid turned out to be spit, though no usable evidence, such as DNA, could be recovered from it. The paint sample revealed the escape vehicle to be a 2012 Graphite Blue Nissan Armada.

Detective Timemaker used the partial plate and information from the analysis of the paint samples to find the owner of the SUV, a Thomas "Brad" Bendgate. The scumbag's sheet showed past involvement in trafficking in controlled substances, petty theft, and a few months in county lockup. Detective Timemaker shook his head. Some idiots never learn.

Detective Timemaker hauled himself up out of his chair, tucked the back of his shirt into his pants, and began the measured steps of getting an audience with "Brad," whose scruffy mug looked nothing like the movie star's. He took the evidence to the courthouse and received a warrant from the judge to pick up Brad. While he was there, he used the rest of the evidence to ask the judge for a second warrant to allow the digital forensics department to search the recovered flash drive for evidence of further crimes, such as dog fighting and gambling - where the ring might be holding the next fight, what methods are used for taking and collecting on debts, who might be involved, and, most important in Detective Timemaker's mind, a location for where those poor animals were being abused. Next, after hauling Brad in from his girlfriend's apartment, Detective Timemaker interrogated him. It didn't take long for the guy to change his tune from ignorance to innocence; but either way, he was singing the same old song. He claimed to not know anything about what was going on. According to Brad he was taking some rabbits he had trapped to a guy named "Spindle," who apparently just had a love of the bunnies. Brad also claimed innocence of trespassing and breaking and entering, saying that the house had been open and he thought it belonged to a friend of Spindle.

"Come on, Bendgate. We already got you on the hit and run and trespassing. Do yourself a favor and give me a truthful answer. What were you doing at that house?"

"I told you, I was just taking a couple of rabbits to my guy Spindle. How was I to know it was supposed to be empty?"

"The lack of furniture, food, and toilet paper didn't clue you in, Brad? You been snorting something you want to confess to?"

"Oh, yeah. You're a real comedian, Detective. It's like I told you. He called and told me to meet him at his friend's house, so I went over there. How was I supposed to know? The door was open. And I just figured the dude was into fung shoe or something."

"Feng Shui" Detective Timemaker corrected him. "And that's on furniture placement, not lack of it."

"Whatever!"

"Fine. Who is Spindle; what's his real name?"

Brad blew out a heavy breath, his eyes getting huge in an attempt to project ignorance. "You know something, Detective? I really don't know. I... "

"You don't know?" Detective Timemaker interrupted, not bothering to hide the disbelief in his voice or on his face.

"No, I don't know." The huge eyes again as he shook his head. "I," Brad pointed a finger to the ceiling, "am a respecer of personages." He smiled and crossed his arms across his chest.

Unable to get anywhere with Brad, Detective Timemaker handed the flash drive over to you.

"If we are going to save these beautiful dogs and put a stop to this monstrosity, I need you to be diligent and thorough. Find any and every scrap of evidence about what may be going on here." With a clap on the shoulder, Detective Timemaker left, leaving you to your work.

.....

---



## Hidings Technique Summary

### 1. Bury Information

Budget.xlsx	Bury gambling data within sheet 3
Survival Game ... PaintballReservations_com.htm	Bury email address and password and two other passwords at bottom of code
Dogfighting Fact Sheet.docx	Bury that Josef's house is Site A in document
Office of ... Animal Rescues.htm	Bury the physical addresses of each site in middle of code at end of long comment section
HorseRiding.ppt	Bury S-Tools passphrase under picture of horse

### 2. Delete Evidence

Maps	Delete one of the maps
Emails	Delete some of the emails
701'.docx	Delete threatening letter to Josef

### 3. Hide Evidence

.emf files of maps	Hide all remaining maps using Windows file properties "hidden" checkbox
Budget.xlsx	Hide columns containing the gambling data
Work_Log.doc	Hide an email clue by setting font to white
Word_Jumble.docx	Hide clue using "hidden" font feature of MS Word

### 4. Cipher Square

Word_Jumble.docx	Two cipher squares, only one of which works
Jumbo.txt	The message in cipher code

### 5. Misdirection

Merger.docx	Password-protected to make it appear important
Resignation.docx	Password-protected to make it appear important
Web pages	Two or three copies of each for confusion
New Folder	Left the default name for the folder that contained all hidden maps - Folder looks empty
APT_Puppy	Two copies in different formats for confusion
American_Pitbull_Terrier.bmp	Used bmp extension to confuse since both image steganography tools only use bmp files

### 6. Password Protection

My_Home.bmp	Passphrase protect details for next fight with S-Tools
Work_Log.doc	Password-protected document that has clues to look for an email address

### 7. File Extension Change

KittyCat_Card.txt	Change bmp extension to txt
Brothers.txt	Changed jpg extension to txt to hide clue to "boss's" last name

## Hiding Tools Summary

### ProDiscover Basic

Flash drive

Used this Forensics Software tool to create a forensics image of the project files.

### AccessData PRTK 6

Work\_Log.docx

This password is not hidden anywhere, nor are there clues to what it could be. The PRTK software will need to be used to discover it.

### Hex Workshop

Love\_My\_Bulldogs.bmp

Used this application to change the file header.

My\_ToDo\_List.txt

My\_ToDo\_List2.txt

Used this application to bit-rotate these files so that they look corrupted.

Forensics\_Project.eve

Used this application to generate hash values for image.

### Invisible Ink

Dogs\_Battle\_Scrabble.bmp

KittyCat\_Card.bmp

Love\_My\_Bulldogs.bmp

Hid a message in each image using this software.

### IrfanView

Dogs\_Battle\_Scrabble.bmp

KittyCat\_Card.bmp

Love\_My\_Bulldogs.bmp

My\_Home.bmp

Used this software tool to change jpeg image to bmp format for compatibility with other software tools.

### Playfair Cipher

Word\_Jumble.docx

Two cipher squares, one of which has the current keyword.

Dogs\_Battle\_Scrabble.bmp

This image contains hidden text that gives a clue about which cipher square to use.

Jumbo.txt

The encoded message is written here.

### PlayMaker

Fight information

Used this software to encode information which would be hidden in the graphic My\_Home.bmp.

### S-Tools

My\_Home.bmp

This image contains hidden, encoded text using S-Tools software. This software requires each file to have a passphrase for decryption.

## Files on Flash Drive Summary

\*I = Innocent Information

\*C = Clue

\*H = Hidden

\*D = Deleted

*Animal Stories Folder*

Cats\_and\_Dogs.odt /I  
 Dog\_Cock\_Fighting.docx /I  
 Dogfighting Fact Sheet.docx /C  
 dogfighting\_statelaws.pdf /I  
 DogFightStory.docx /I  
 Jumbo.txt /I  
 KittyCat\_Card.txt /I  
 Suckers.doc /I  
 Dogfighting\_Poster.pdf /I

*My Stuff Folder**New Folder*

Adventure.emf /C, H  
 Car\_Show.emf /C, H  
 Fishing.emf /C, D  
 Flying.emf /C, H  
 Kite\_Flying.emf /C, D  
 Kite\_Flying.tiff /C, D  
 Riding.emf /C, H  
 Truck\_Rally.emf /C, H

*Puzzles Folder*

Cat\_Lovers\_Quest.doc /I  
 Discoid\_Fever.oxps /I  
 RainForest.docx /I  
 Sudoku.xlsx /I  
 Word\_Jumble.docx /C  
 WordSearchGreen.pdf /I

Budget.xlsx /C

FYI.docx /C

Houston.est /I

My\_ToDo\_List.txt /C

My\_ToDo\_List2.txt /C

901'.docx /C, D

*Pics Folder*

American\_Pitbull\_Terrier.bmp /I  
 American\_Pitbull\_Terrier\_Blue\_Bully\_Breed.jpg /I  
 APT\_Puppy.bmp /I  
 APT\_Puppy.jpg /I  
 Baby\_with\_Bulldog\_Puppies.jpg /I  
 Brothers.txt /C  
 Dogs\_Battle\_Scrabble.bmp /C  
 English\_Bulldog.jpg /I  
 Love\_My\_Bulldogs.bmp /C  
 Puppies.jpg /I

*Web Pages Folder**Houston, Texas\_files Folder*

image\_map.gif /I  
 image\_overview.gif /I  
 Houston, Texas.htm /I  
 Office of the Harris County Attorney - Vince Ryan -  
 Animal Rescue.mht /I  
 Office of the Harris County Attorney - Vince Ryan -  
 Animal Rescues.htm /C  
 Office of the Harris County Attorney - Vince Ryan -  
 Animal Rescues.mht /I  
 Survival Game Of Texas Paintball Field in Houston,  
 Texas - PaintballReservations\_com.htm /C  
 Survival Game Of Texas Paintball Field in Houston,  
 Texas - PaintballReservations\_com.mht /I

*Work Folder*

Merger.docx /I  
 Resignation.docx /I  
 Work\_Log.docx /C

## Question and Answer Summary

Q. What is Spindle's real name?

A. Spindle's real name is Mathias Jones.

Budget.xlsx file property tag "author" shows his real name.

Email "Volunteer needed this weekend" from volunteer supervisor is addressed to his real name, which can serve as secondary evidence.

Q. What was going on at the vacant house?

A. Spindle and Brad were training dogs to fight using kittens and rabbits. The kittens were secured illegally by Spindle through his volunteer position at the animal shelter.

Email "Meeting" from Spindle to Brad shows they were to meet.

Email "false alarm" from Spindle to volunteer supervisor says that kittens were sold to loving homes.

However, Spindle then emails his dog fighting "boss" that he had actually secured the kittens for themselves.

KittyCat\_Card.bmp was an attachment from Spindle's dog fighting "boss", which Spindle saved to his flash drive as proof in case he was ever pinched by the police. In it, the "boss" mentions what the kittens and rabbits were used for.

Q. Who is Spindle's dog fighting "boss"?

A. The boss's real name is Alan Smart.

Brothers.jpg is an image of a Houston Crime Stoppers poster with 3 men on it, wanted for various animal cruelty charges. Spindle saved it on his flash drive as a clue to his boss's real identity, because his boss has a brother who is wanted by the Houston Police for animal cruelty.

KittyCat\_Card.bmp has a secret message in it to Spindle. It is signed by "Alan".

My\_ToDo\_List2.txt is a bit-rotated message to Spindle telling him what to do about someone who won't pay on the gambling debt. It is signed by "Alan".

Email "loan" to Spindle talks about money due because of an event. It is signed by "A. Smart".

Q. Where are the dogs being kept?

A. The dogs are being kept at the home of one of the members, Josef Yergin. His home is labeled "Site A" and is represented by an airplane on the maps. The physical address is 12357 CR 280, Alvin, TX 77511. Josef's wife doesn't know about the horrible dog fighting ring and does her best to love on the dogs.

Word\_Jumble.docx has a cipher square that Spindle and Alan use to encode messages to each other sometimes. In the blank space is hidden a clue that the current keyword can be found in a picture.

Dogs\_Battle\_Scrabble.bmp has a clue about what the current keyword is to use. Spindle keeps this on his flash drive so he doesn't forget.

Email "Hilarious" to Alan has an attachment with the Dogs\_Battle\_Scrabble.bmp image with the latest keyword.

Jumbo.txt is the text file that has the coded message. It says that the dogs are kept at Josef's house.

Dogfighting Fact Sheet.docx has the information that Josef's house is Site A.

Love\_My\_Bulldogs.bmp has a hidden message expressing concern about the dogs being at Josef's because the wife is too soft with the dogs.

Office of the Harris County Attorney - Vince Ryan - Animal Rescues.htm has a list of the physical addresses for all the sites buried in the source code.

Budget.xlsx has Josef's last name in several of the fight attendees lists.

## Hiding Details

The flash drive recovered at the crime scene in the opening scenario belongs to a person who goes by the moniker "Spindle." Spindle considers himself a clever criminal and hides all his important information saved on the flash drive. He's seen too many bad guys get sent to the clink because things they've written or saved electronically were discovered by the police. Spindle feels those idiots deserved going to the slammer for just typing letters and debts up plainly.

But, it's not just the police Spindle has to be sneakily cautious for. There's always the competition who want to cut him out of the lucrative criminal business. Spindle hides his data so they can't learn the details of his business or snitch on him to the police.

Finally, Spindle knows that sometimes the police get lucky and might catch him on something - though he doubts it because he's just that good. However, should it happen, Spindle is not going down alone. He is keeping proof that he's not the one calling the shots or collecting all the illegally-gotten gains. He wants evidence against his criminal boss so he can trade for a lighter sentence should it come to that. Yes, the sly Spindle is ready should anyone, even the boss himself, come sniffing around....

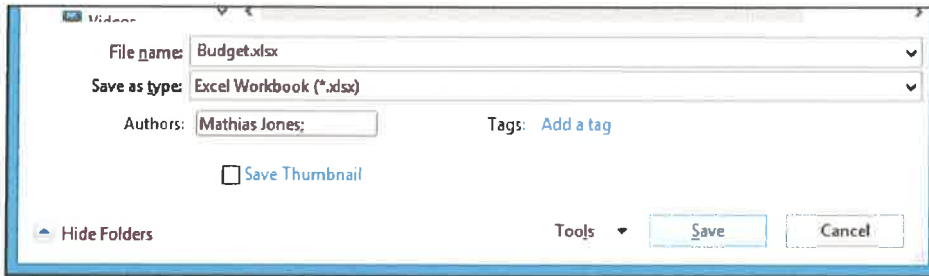
### 1. What is Spindle's real name?

#### 1.1 Saving a Microsoft Office file

File: Budget.xlsx

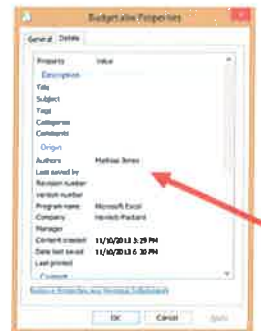
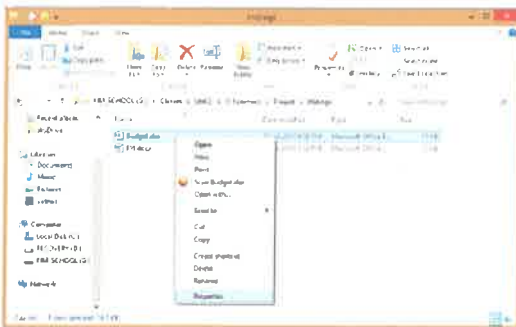
Tool: MS Office Features - General: File Properties

Office files have properties, which collect and store details such as author and save date. These tags are used to help organize and speed up searches for files when you filter with file properties. They are also a mountain of information that can reveal things you didn't intend to. For example, the file property "author" is automatically filled in with the listed user name when saving or resaving a document. Spindle does his best to ensure he removes those tags, but he's not perfect.

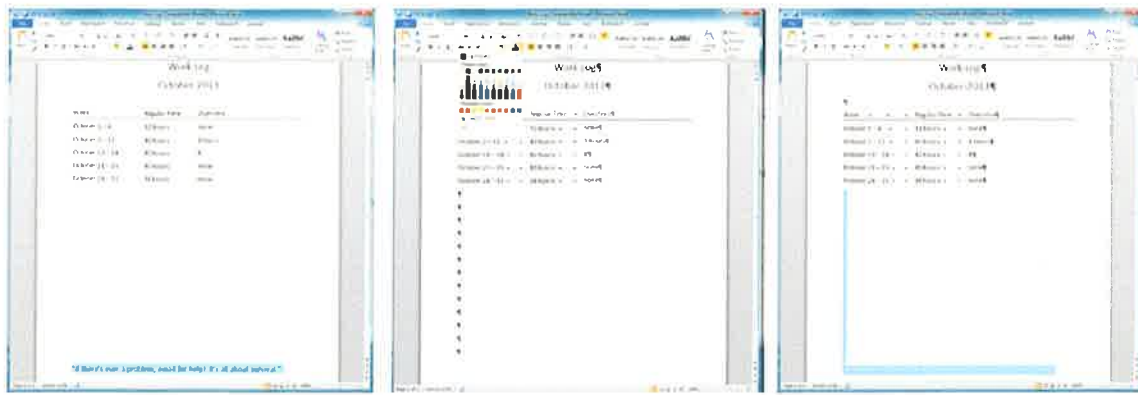


Notice my criminal forgot to delete his name when saving this.

An investigator can look at the workbook's properties to discover my criminal's real name!

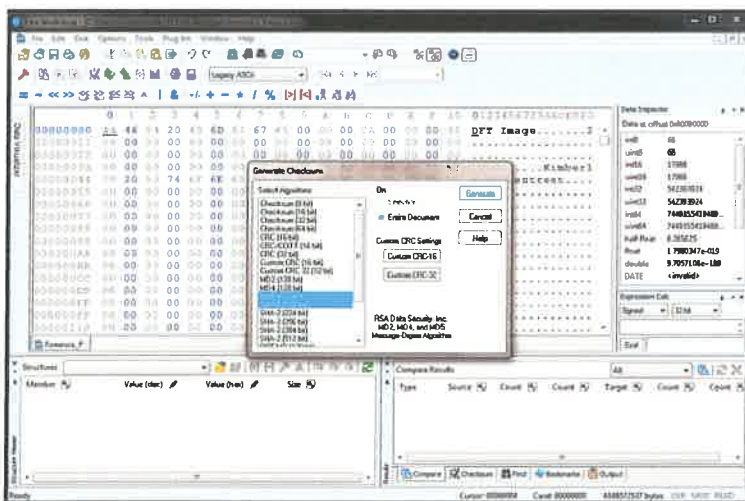






Of course, all this hiding was just fun and games for Spindle. He knew he was brilliant and slick. He'd never actually get caught and no one would ever see all the hard work he put into making his business the most secret around.

The flash drive (project) was imaged using ProDiscover Basic proprietary format: eve. It was then validated using Hex Workshop.



Hash Values for: Forensics\_Project.eve

By: Hex Workshop

MD5 (128 bit)

DBE3CA112890DCD971AEDCAD0B7BEE18

SHA-1 (160 bit)

7D4CE0A2DB40767A74CAC79C43F4D35E81E95D90