Assignment 7: Forensics

This project is due on **Friday, December 15, 2017** at **11:55 p.m.**. Late submissions will be penalized by 10% per day. If you have a conflict due to travel, interviews, etc., please plan accordingly andturn in your project early.

This is a group project; you will work in **teams of two or three** and submit one project per team. **Submissions by groups of size one or four+ will receive no credit**. Please find a partner as soon as possible. If you have trouble forming a team, post to Piazza's partner search forum. The final will cover project material, so you and your partner should collaborate on each part.

Strict no-leaks policy. In this project, you play the role of a computer forensic analyst working to solve a murder case. Since you don't want to be fired for jeopardizing an ongoing criminal investigation, you need to follow a strict policy on collaboration. The code and other answers your group submits must be entirely your own group's work. Undergraduate students are bound by the Honor System while graduate students are bound by the Graduate School's expectation of research integrity. You may consult published references, provided that you appropriately cite them (e.g., with program comments), as you would in an academic paper. **All Piazza posts relating to the solution of this assignment should be made private.** The number of pieces of evidence you find, the techniques you try, how successful said techniques are, the general process you follow, etc. are all considered part of your solution and must not be discussed with members of other groups, or potential future students of the class.

Start early. It may be impossible to complete this project before the deadline unless you begin several days beforehand. Please plan accordingly.

Solutions must be submitted electronically via Dropbox, following the submission checklist below. Please coordinate carefully with your partner to make sure at least one of you submits on time.

Introduction

In this project, you will play the role of a forensic analyst and investigate a murder mystery. On December 4, 2017, two terrible crimes were reported: the mascots of both Dartmouth and Cornell were shot. Both victims were last seen alive at home football games on December 3, 2017, and local reports show both victims dropped dead within 30 seconds of each other, despite the large distance between them. Times of death were 21:36:28 and 21:36:52, respectively. Officers recovered projectiles found in the costumes of the mascots. The projectile from one of the victims is shown below (Exhibit A), which appears, inexplicably, to have been the cause of death. Officers also recovered a Long Range Foam Ballistic Missile Launcher (LRFBML) left on Princeton Campus, and ballistics analysis reveals both projectiles to match the LRFBML.

The case went cold on December 6, when the leading suspect, Bobby McBobface, fled the country and disappeared. Officers seized their computer, but their lead computer forensics expert was nowhere to be seen after attending a Charter Friday, they didn't know where to turn.

Exhibit A — Projectile recovered at the crime scene. Ballistics experts have identified it as a "Nerf blaster dart."

After hearing about the case, Prof. Felten has recommend your team to lead the project.

Your job is to conduct a forensic examination of the disk image and document any evidence related to the murder. If you find sufficient evidence, Bobby McBobface will be extradited and face trial.

Objectives:

- Understand how computer use can leave persistent traces and why such evidence is often difficult to remove or conceal.
- Gain experience applying the security mindset to investigate computer misuse and intrusion.
- Learn how to retrieve information from a disk image without booting the operating system, and understand why this is necessary to preserve forensic integrity.

Getting Started

The tools and techniques you use for your investigation are up to you, but here are some suggestions to help you get started.

General Knowledge A general working knowledge of Linux is undoubtedly helpful for this project. For dead analysis, we recommend you continue to use Kali Linux, as you have for previous assignments. See http://en.wikipedia.org/wiki/Disk_partitioning for some additional background.

Live Analysis Live analysis is a forensic technique in which the investigator examines a running copy of the target system. We suggest using VirtualBox for this purpose.

1. Download the VMDK and OVF (8GB): ftp://ftp.cs.princeton.edu/pub/cos432/Forensics3.ovf, ftp://ftp.cs.princeton.edu/pub/cos432/Forensics3-disk1.vmdk. We recommend using `wget`, since you can use `wget -c` if your download fails.
2. Import the VM by opening Virtualbox and selecting "Import Appliance", then choosing the OVF file. Make sure the OVF file and the VMDK file are in the same directory, and that you haven't changed their names.
3. Start the VM and explore the system.

Dead Analysis In dead analysis, the forensic investigator examines data artifacts from a target system without the system running. We suggest trying dead analysis with the Autopsy open-source forensics tool. The procedure below assumes you are working on Kali Linux. You do not need Kali to complete this assignment, if you prefer another Linux distribution.

1. Decompress the disk image: `qemu-img convert -f vmdk Forensics3-disk1.vmdk -O raw Forensics3-disk1.raw`

2. Install the Autopsy digital forensics suite:
   `$ sudo apt-get install autopsy`

3. Launch Autopsy in the background and open the browser-based GUI:
   `$ sudo autopsy &`
   In a browser on the local machine, go to the URL http://localhost:9999/autopsy.

4. Create a new case and add the disk image:

   (a) Click New Case. Enter a case name and click New Case.

   (b) Go back to http://localhost:9999/autopsy and open the case you created.

   (c) Click Add Host. Enter a host name and click Add Host.

   (d) Click Add Image. Click Add Image File. Enter the path to the decompressed raw disk image. Make sure you select Type=Disk and Import Method=Symlink. Click Next.

   (e) Leave the Image File Details and File System Details as the defaults. (Note that the disk image contains 3 partitions, which Autopsy will allow you to examine separately.) Click Add. Click OK.

   (f) Select a partition to examine and click Analyze. The buttons at the top give you several analysis tools. Try File Analysis and Keyword Search to get started.

5. Consider a Linux live boot (Kali strongly recommended). This can be done in place of Autopsy

   (a) Create a VM by importing the OVF file

   (b) Add the ISO file to the IDE controller under VM storage settings, ensure Optical comes above Hard Disk in the boot order under system settings

   (c) Boot the VM. Kali should boot instead of the usual OS

6. In addition to hints dropped elsewhere, here is an incomplete list of things to try:

   - Search commonly used file areas.
   - Examine the system logs.
   - Check for deleted or encrypted files.
   - Search the drive image for strings that may indicate relevance to your investigation.

Password Cracking Password crackers may be helpful in trying to brute-force decrypt password-protected files. John the Ripper (http://www.openwall.com/john/) is the canonical Unix password cracker. Hydra (https://github.com/vanhauser-thc/thc-hydra) is a tool used to brute force remote login passwords, fcrackzip (http://home.schmorp.de/marc/fcrackzip.html) is a ZIP password cracker, and pdfcrack (http://sourceforge.net/projects/pdfcrack/) is a PDF password cracker. John, fcrackzip, and pdfcrack are conveniently available in the Debian package repositories and can be installed with `apt-get`. You may wish to use a dictionary attack first; if so consider this dictionary: https://gist.github.com/h3xx/1976236.

When using a password cracker, it is wise to make sure that the password is not susceptible to a dictionary attack and does not use a restricted character set (e.g., lowercase letters, letters only, letters and numbers only) before spending time on a full brute-force crack. It is also a good idea to crack a very vulnerable password first to make sure you are using the tool correctly.

Deleted File Recovery Many tools exist to find and recover deleted files. Some tools are `extundelete`, `debugfs`, and `foremost`. Be aware the live operating systems are constantly writing to the disk, so the longer the image is live, the less likely deleted file recover is to work.

Cryptocurrency You may want to perform analysis on cryptocurrency blockchains. Here are some sites for cryptocurrencies:

- Litecoin https://live.blockcypher.com/ltc/ https://liteaddress.org/
- Bitcoin https://blockchain.info/ https://www.bitaddress.org/
- Dogecoin https://dogechain.info/

Tasks and Deliverables

You will provide 4 answer files: `tokens.txt`, `procedure.txt`, `evidence.txt`, and `report.txt`, along with an `evidence/` directory of all relevant evidence. We provide templates for the files here https://www.cs.princeton.edu/courses/archive/fall17/cos432/assignments/a7/templates/ Your answers should be *complete* but *concise*. None of the questions should require more than 1–2 paragraphs to answer. Most should be as short as 1–2 sentences.

tokens.txt As you complete the investigation, findings and major steps will be marked with tokens formatted as `token-` followed by a 16 hex digits. You should list your collection of tokens in a file called `tokens.txt`, separated by newlines.

evidence.txt You will also find evidence of the crime along the way. Some of it won't have tokens, some of it will. You should document it in `evidence.txt`. For each piece of evidence you find, you should include the evidence in your `evidence/` folder, and explain in 1-2 sentences how this evidence contributes to the case. Organize your responses as follows: `filename:...response...`

procedure.txt Along the way, you'll overcome many roadblocks, traps, and misdirections. You should document each of these that you discover, how you noticed/found them, and how you overcame them. Be sure to include intermediate steps in your narrative. We're interested in your

process here, so you should write this up as your `procedure.txt` This file will be the bulk of your assignment grade, so make sure you touch on each step you took.
report.txt Finally, you should create a report called `report.txt`, that will answer the major questions of the case. You should answer the numbered questions below in 1-2 paragraphs

1. What are your team's NetIDs?
2. Try booting the suspect's machine and using it normally. What *specific* behaviors of this machine make this a bad idea?
3. What operating system does the suspect use? Be careful and specific; e.g., say "Windows 2000" instead of just "Windows."
4. What credentials did you find? What other login or impersonation mechanisms did you leverage?
5. Reconstruct the timeline of actions by the suspect that may be relevant to the investigation. (Make a list in this format: <date> <time>: <event description>.) Include any activities related to your other responses, if you can identify when they occurred. Include each time the suspect logged in to or booted the machine to do something interesting. When was the last activity before the suspect fled the country?
6. Are there any indications of co-conspirators or other new suspects?
7. What was the motivation behind the crime?
8. Did you find sufficient evidence to link Bobby McBobface to the crime?

Note: These numbered questions are meant to be a guide for you, and these questions are not comprehensive.
As you investigate, be on the lookout for evidence of any other machines or network services that the suspect may have used. These may contain important evidence and raise further questions you'll need to investigate (*hint, hint!*). Before attempting to access any such machines or accounts, be sure to contact your supervisor for permission by posting on Piazza. Failure to ask permission is guaranteed to be a waste of your time and may violate the course ethics policy. Again, start early; headquarters has been known to take up to 24 hours to approve such requests.

Policies and Hints

Collaboration: Strictly prohibited outside your group. As stated above, you are bound by the Honor Code not to communicate with anyone regarding any aspect of the case or your investigation (other than within your group or with course staff). The number of pieces of evidence you find, the techniques you try, how successful said techniques are, the general process you follow, etc. are all considered part of your solution and must not be discussed with members of other groups. If anyone brings up the project, start yelling "LALALALA" and refer them to your supervisor for an official spokesperson.

If you get stuck... Requesting Hints Given the nature of this assignment and its strict collaboration policy, HQ recognizes the need for some hints. We have standard hints for each question. If your group gets stuck, email `cos432.hints@gmail.com` with the names of your group members, the tokens you have found so far, the question for which you would like a hint, and the progress you have made thus far on that question. Please CC your group, and please designate a single spokesperson for your group.

Each group may receive a maximum of 3 hints, and we will enforce a one hour delay between hints for each group. Purely administrative questions, requests for access, or general questions about Linux do not count towards this limit.

Submission Checklist

Upload to Dropbox (https://dropbox.cs.princeton.edu/COS432_F2017/Forensics) a gzipped tar file named `assignment7.`*`netid1`*`.`*`netid2`*`.tar.gz` that contains only the files listed below. Please put netids in alphabetic order. These may be partially autograded, so make sure you have the proper filenames, formats, and behaviors. You can generate the tarball at the shell using this command:

```
tar -zcf assignment7.netid1.netid2.tar.gz report.txt
        evidence/ tokens.txt evidence.txt procedure.txt
```

The tarball should contain only the files below:

`tokens.txt`	A plain text file with your discovered tokens.
`evidence.txt`	A plain text file with your discussion of the evidence.
`report.txt`	A plain text file with your answers to the numbered prompts.
`procedure.txt`	A plain text file with your answers to the numbered prompts.
`evidence/`	A directory containing any recovered files referenced in your report.