OVERVIEW OF BASIC FORENSIC TOOLS

Justin Almanza, Digital Forensic Investigator, Georgia Bureau of Investigation
Mason Miller, Digital Forensic Investigator, Georgia Bureau of Investigation

This class will represent a "high-level" view of some of the tools used by a forensic investigator during a typical case. All the tools used are currently available as free downloads (links current and working as of 1/27/2020). If you are planning on using any of these tools for actual forensic work, always make sure you validate your tools and know the capabilities/limits of your tools.

RATool (Removable Access Tool v1.3) - Write-blocker
https://www.sordum.org/8104/ratool-v1-3-removable-access-tool/

"Removable Access Tool (a.k.a. Ratool) is a simple to use portable freeware application which aids in the control of external storage devices such as USB flash drives, CD/DVD drives, as well as floppy, tape and WPD devices. Ratool can disable USB storage access or enable write protection on all USB flash drives, thus preventing data from being modified or deleted, protecting your confidential data from being copied by others."

FTK Imager
https://accessdata.com/product-download/ftk-imager-version-4-2-1

"FTK® Imager is a data preview and imaging tool used to acquire data (evidence) in a forensically sound manner by creating copies of data without making changes to the original evidence."

Autopsy (Sleuthkit)
https://www.sleuthkit.org/autopsy/
https://www.autopsy.com/download/

"Autopsy® is a digital forensics platform and graphical interface to The Sleuth Kit® and other digital forensics tools. It is used by law enforcement, military, and corporate examiners to investigate what happened on a computer. You can even use it to recover photos from your camera's memory card."

IrfanView (Graphics File Viewer)
https://www.irfanview.com/

"IrfanView is a fast, compact and innovative FREEWARE (for non-commercial use) graphic viewer for Windows XP, Vista, 7, 8 and 10. It is designed to be simple for beginners and powerful for professionals."

HxD (Hex Editor and Disk Editor)
https://mh-nexus.de/en/hxd/

"HxD is a carefully designed and fast hex editor which, additionally to raw disk editing and modifying of main memory (RAM), handles files of any size."

7-zip (Archive/Compression Tool)
https://www.7-zip.org/

"7-Zip is a file archiver with a high compression ratio."

Scenario

Your organization has received a cybertip from the National Center for Missing and Exploited Ducklings (NCMED) which has been assigned to you.

The cybertip includes the following information:

From: Clickstagram ("Click"), social media platform
Subject ClickHandle: @BigBillXXX
Associated email: BigBillXXX@cybermail.com
User name associated with account: William "Bill" Waddleton
Incident: User @BigBillXXX was found to be sending illegal duckling photographs to multiple users via ClickMessenger.

The cybertip also includes an IP address that you are able to trace back a physical address:

101 Grace Hopper Lane, Augusta, Georgia (United States)

After some research, you discover that this is a residential address and the owner of the property is "William Waddleton." You also discover that 5 ducklings have gone missing in the area over the past 2 months, all reported within a .5 mile radius of the suspected address.

You get a search warrant that covers the house, vehicle(s), and anything on the person of Waddleton, including any devices capable of storing digital media.

As you approach the house, you hear what sounds like multiple "smashing" sounds coming from the basement. When you get to the door, the subject opens it and calmly tells you to come inside. You enter the house and begin talking to Waddleton, at which point he says, "I would never never view or share duckpics. Except maybe once when I accidentally clicked on a pop-up, but that was a mistake. But I didn't know what I was downloading. And I think I got a virus one time too. But that's it."

You search the premises and discover that all of the electronic devices have been destroyed except for one USB flash drive found in Waddleton's sock drawer next to a bottle of Mountain Dew. The drive has a note under it that says "FOR HOWARD."

Your task is to conduct a forensic examination of this drive and search for anything of potential evidentiary value.