November 12, 2021 [redacted]
[redacted]
[redacted]

- Prepared for trial testimony
- [redacted]
- Forensic examination – captures data (imaging – bit-for-bit copy), puts it through software to categorize information; huge amounts of data on computer; software helps organize to assist with review
- Information stored on a hard drive in a computer; hard drive stores non-volatile data (anything saved on the drive will be on drive if you unplug it); digital device to store data
- Typically knows nothing about a case when analyzes digital evidence
- [redacted] was shown GX 54 (has [redacted] initials, case number, unique identifier on it, date)
- Every piece of evidence that [redacted] examines gets unique bar code numbers and gets another sticker with case number, date initials, and reference to unique number on other sticker
- Received GX 54 in a box with photocopy of different drive on front; led [redacted] to believe was copy of drive on the front of it; had to determine how best to capture information on drive, had to see if image files or a clone
- [redacted] was shown GX 55: [redacted] first marked it; after marking it, connect hard drive to a writeblocker and connect that to computer to view data on drive without altering it; looked to figure out if image files or clone
- Clone: bit for bit copy of one piece of media to another (e.g., from one hard drive to another)
- As digital forensics progressed, moved away from clones and towards images; image is a bit for bit copy, but saved onto another hard drive as image files; advantage is that containerizes it, more difficult to change data on an image file than a clone
- After determined drive was a clone, [redacted] imaged it; [redacted] made a bit for bit copy of the clone; copies to storage area network for processing
- To make an image, have several tools available; FTK made by Access Data; also have FBI created product; also have physical devices that are duplicators (TX1 made by Tableau) to create image files
- Hard drive is electromechanical device, has platters spinning around, several motors and pieces of hardware; it will fail at some point, just a matter of when; so with all hard drives make original copy and work off of the copy
- Know that what is in the copy is an exact copy of the device because run a hash (mathematical algorithm), uniquely identifies data on drive; run against copy; comes out the same

- After made image, [redacted] placed data in Access Data Lab and processed for review
- From review of images of GX 54 and GX 55, [redacted] knows they are Dell computers
- [redacted] was shown GX 405 and 419 and confirmed recognized and accurate
    - Every windows computer has architecture inside it called registry, which stores settings, ton of stuff; comprised of five different files
    - Software hive: tells you what version of Windows was running, who registered owner and organization was, data installed (date computer clock set to when operating system was installed on it); product name
    - Registered org: when start up computer, asks who computer is; one identifier is organization and next asks who owner is; user inputtable data
- [redacted] reviewed the properties for GX 417, 418, 420, 421, 422 (GX 417B, 418B, 420B, 421B, 422B) and confirmed accuracy by running software (Access Data's Lab, AD Lab); confirmed GX 417 on GX 55 (NYC024349); GX 418, 420, 421, 422 on GX 54 (NYC024350); all word documents
- [redacted] confirmed GX 412 and GX 415 on GX 54; emails
- [redacted] remembers seeing GX 417 because it was at the root of the C drive, not normal spot for documents to be; would expect documents to be under user's profile in documents folder (that is Microsoft Word default)
- 2 reasons to be in C drive: either to hide it or to give another user easy access to it so don't have to go digging around; believes there were three documents in total at root of C drive
- 2 sets of metadata for Word documents: file system or embedded file within the word document; B exhibits are the latter (embedded file within word document)
- To access metadata in Word document, click on properties and will display information
- When Word doc is created, metadata is generated to reflect creation date of file; gets metadata from operating system; that is from system clock, which a user can change
- Author is pulled from the registry for the user signed in at the time the document is created
- If someone else created a Word document other than the user signed into the operating system, wouldn't be able to tell
- Last printed – when print document, it will update that field
- When document is last printed before creation date: means typed up document, printed it, and then "save as"; when hit "save as" it resets the created date; the "last printed" field wouldn't change
- If user had created document, printed it, and went to close document, and saved in response to prompting, document will have the creation date of when first started typing the document
- Total editing time: keeps running clock of when have document open to edit
- GX 418, 420, 421, and 422 were saved under Maxwell's user profile
- [redacted]

[redacted]