I. Border search exception: "Non-routine" searches

a. **"Non-routine"** border searches *at least* require *reasonable suspicion* that that thing to be searched contains evidence of an immigration or customs violation

b. ***U.S. v. Montoya de Hernandez***, 473 U.S. 531 (1985)

i. Detaining a traveler until she defecated to see if she was smuggling drugs in her digestive tract was a "non-routine" seizure and search that required "reasonable suspicion" that she was a drug mule

c. **"Highly intrusive"** and impact the **"dignity and privacy interests"** of individuals

i. Ex: body cavity searches

1. ***U.S. v. Flores-Montano***, 541 U.S. 149, 152 (2004)

d. Carried out in a **"particularly offensive manner"**

i. Ex: permanent destruction of property by drilling

1. ***U.S. v. Ramsey***, 431 U.S. 606, 618 n.13 (1977)

II. Border searches of digital data without a probable cause warrant violate the **Fourth Amendment**

a. ***Riley v. California***, 134 S.Ct. 2473 (2014)

i. Search-incident-to-arrest exception does not apply to cell phone seized during an arrest; probable cause warrant required

b. ***U.S. v. Cotterman***, 709 F.3d 952 (9th Cir. 2013) (en banc)

i. "Forensic" border search of digital device is "non-routine" and requires reasonable suspicion

c. But at least one court found that software is not "forensic" if it only conducts targeted searches of digital data

i. ***U.S. v. Feiten***, 2016 WL 894452 (E.D. Mich. 2016)

III. Border search cases: Circuit roundup after *Riley* & *Cotterman*

a. ***U.S. v. Molina-Gomez*, 781 F.3d 13 (1st Cir. 2015)**

i. Manual search of phone; but defendant challenged physical search that found hidden heroin; court ruled physical search "routine"

b. ***Alasaad v. Nielsen*, Slip Opinion, 2018 WL 2170323 (D. Mass. May 9, 2018)**

i. In a 52-page order, relying on *Riley* as a persuasive authority, District Court rejected the government's arguments that First and Fourth Amendment constitutional protections do not apply at the U.S. border.

ii. "Although defendants may be correct that the border is different, the Supreme Court and First Circuit have acknowledged that digital searches are different too since they 'implicate privacy concerns far beyond those implicated' in a typical container search." At *20.

c. ***U.S. v. Kolsuz*, --- F.3d ---, 2018 WL 2122085 (4th Cir. May 9, 2018)**
   i. Manual search of phone; forensic search after arrest for exporting guns; court followed *Cotterman*
   ii. Fourth Circuit held that in light of the immense privacy concerns, forensic searches of electronic devices seized at the border must be justified by individualized suspicion

d. **Fifth Circuit appeal pending: *U.S. v. Molina-Isidoro*, 2016 WL 8138926 (W.D. Tex. 2016)**
   i. Manual searches of WhatsApp and Uber phone apps after arrest for drugs; court felt constrained to apply no more than reasonable suspicion
   ii. "Were this Court free to decide this matter in the first instance, it might prefer that a warrant be required to search an individual's cell phone at the border."

e. ***U.S. v. Escarcega*, 2017 WL 1380555 (5th Cir. 2017)**
   i. Unpublished, one-page opinion upheld warrantless manual search of defendant's phone

f. ***U.S. v. Stewart*, 729 F.3d 517 (6th Cir. 2013)**
   i. Manual search of laptop 20 miles from the airport and 24-hours after seizure; court held search "routine"
   ii. Court declined to apply "extended border search doctrine" that requires reasonable suspicion; laptop had not yet been cleared for entry into the U.S.

g. Ninth Circuit appeals pending
   i. ***U.S. v. Caballero*, 178 F.Supp.3d 1008 (S.D. Cal. 2016)**
      1. Manual search of phone after arrest for drugs; court bound by *Cotterman*
      2. "If it could, this Court would apply *Riley*."
      3. "One can certainly say that *Riley* casts doubt on *Cotterman*'s approval of warrantless searches where an arrest is made."
   ii. ***U.S. v. Cano*, 222 F.Supp.3d 876 (S.D. Cal. 2016)**
      1. Manual and forensic searches of phone after arrest for drugs; court bound by *Cotterman*

h. ***U.S. v. Vergara***, 884 F.3d 1309 (11th Cir. 2018)
   i. Holding that *Riley* does not apply at the border, that border searches never require a warrant or probable cause, that at most, border searches require reasonable suspicion
   ii. Dissent disagrees in a well-reasoned and worthwhile read
i. Eleventh Circuit appeal pending
   i. ***U.S. v. Touset*, 2016 WL 1048047 (N.D. Ga. 2016)**
      1. Forensic search of laptop uncovered CP
      2. Court followed *Cotterman*, and failed to mention *Riley*

IV. Fifth Amendment

a. ***In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011***, 670 F.3d 1335 (11th Cir. 2012)
   i. Grand jury subpoena ordering production of decrypted hard drive content (by typing in passwords) violated Fifth Amendment
   ii. Government could not show that it knew that "certain files" of child porn existed on the devices such that production of decrypted content would not be "testimonial" (i.e., "foregone conclusion" doctrine)
b. **Regarding the "Foregone Conclusion" doctrine:**
c. ***Virginia v. Baust*, 89 Va. Cir. 267 (2014)** [state trial court, citing 11th Cir.]
   i. Compelling defendant to provide *password* to smartphone (that police suspected had video of defendant assaulting victim) violates Fifth Amendment; password is not "foregone conclusion," so compelled disclosure is "testimonial"
   ii. But compelling defendant to unlock smartphone with *fingerprint* does not violate Fifth Amendment; physical characteristics are non-testimonial
   iii. Compelling defendant to produce *unencrypted video* violates Fifth Amendment; existence and location of video is not "foregone conclusion," so compelled disclosure is "testimonial"
   iv. The recording is not a foregone conclusion b/c Defendant's production of the unencrypted recording **would be testimonial since Defendant would be admitting** the recording exists, it was in his possession and control, and that the recording is authentic
d. ***U.S. v. Djibo*, 151 F.Supp.3d 297 (E.D. N.Y. 2015)**

i. Defendant traveler in secondary screening was "in custody" so phone passcode = "statement;" defendant shared passcode prior to being *Mirandized* so it was suppressed
ii. Data from phone was further suppressed as "fruit" of non-*Mirandized* statement