INTRODUCTION TO MOBILE FORENSICS

Joe Walsh

DeSales University

BACKGROUND

- Cellular Industry
- Police Officer
- Internet Crimes Against Children Task Force Detective
- FBI Task Force Officer
- Private Sector
- Adjunct Professor
- Full-time Instructor at DeSales University

BACKGROUND

- B.S. in Information Systems
- M.A. in Criminal Justice/Digital Forensics
- Over 1000 hours of training
- Specialized training in JTAG and chip-off
- Several certifications
- Testified in court as an expert in computer crime and digital forensics

BACKGROUND - CERTIFICATIONS

- International Information Systems Security Certification Consortium – Certified Information Systems Security Professional (CISSP) and Certified Cyber Forensics Professional (CCFP)
- CompTIA – A+, Network+, Security+, CompTIA Advanced Security Practitioner (CASP)
- EC-Council Certified Ethical Hacker (CEH), Computer Hacking Forensic Investigator (CHFI)
- International Society of Forensic Computer Examiners (ISFCE) Certified Computer Examiner (CCE)
- International Assurance Certification Review Board (IACRB) Certified Computer Forensics Examiner (CCFE)
- Guidance Software EnCase Certified Examiner (EnCE)
- AccessData Certified Examiner (ACE)

WHAT IS A MOBILE DEVICE?

- Cellular phones
- Tablet computers
- MP3 players
- e-Readers
- Wearable devices

Why are we interested in mobile devices?

MOBILE DEVICES

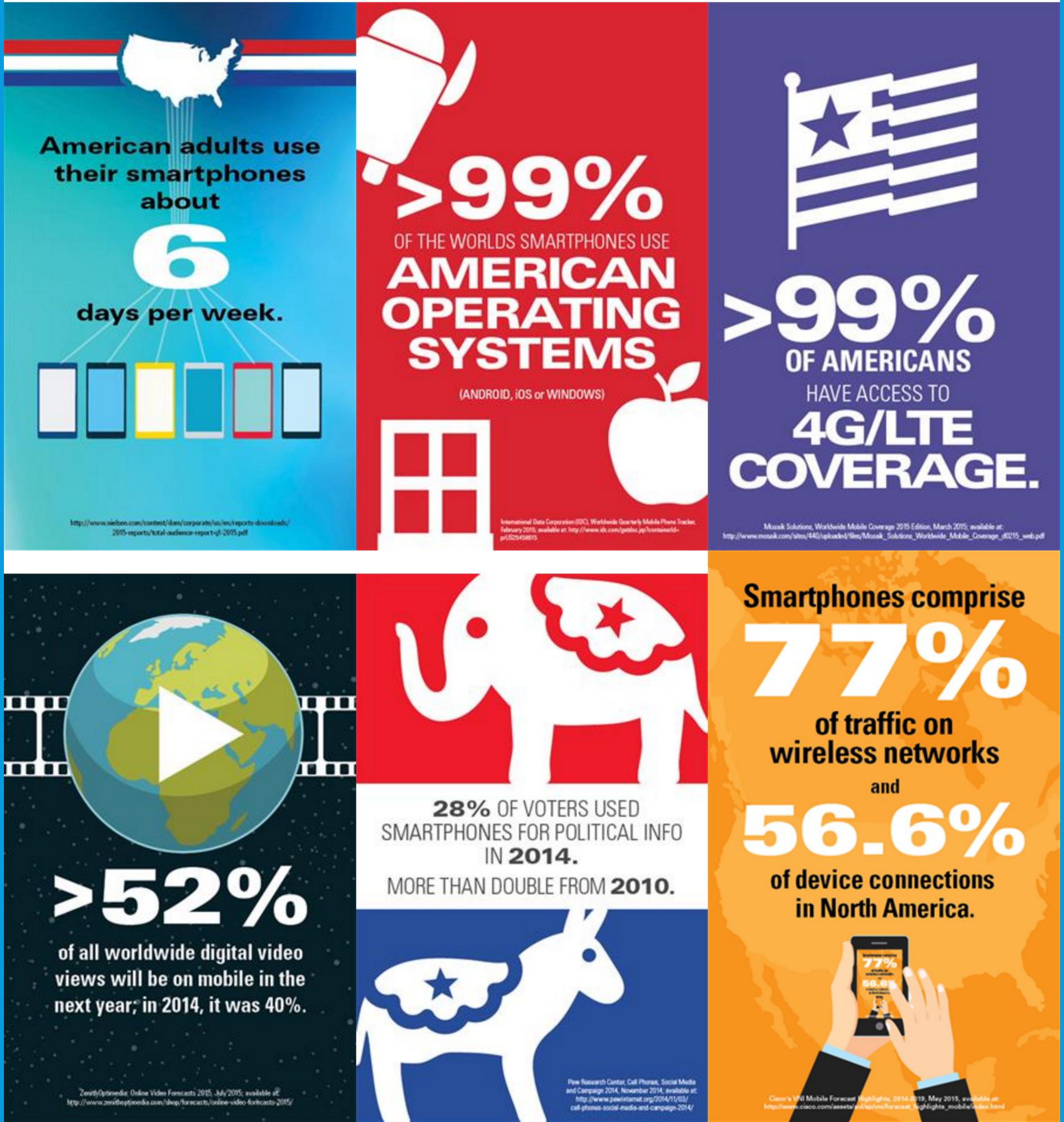
- More than 7 billion cellular subscriptions worldwide
- Portio Research Ltd. predicts there will be 8.5 billion by the end of 2016
- The majority of people have a cell phone (or phones)
- Most people always have their cell phone with them
- Cell phones are small computers which can store an immense amount of data
- Many households no longer have desktop or laptop computers

INTERESTING FACTS

- According to the CTIA:
  - 4 out of 10 Americans live in a wireless-only household
  - 1 in 10 Americans access the Internet exclusively from a smartphone
  - More than 90% of devices sold in the U.S. in 4Q2013 were smartphones
  - More than 335,650,000 active wireless lines as of Dec. 2013

INTERESTING FACTS

- More than 6 billion text messages and more than 330 million multimedia messages occur each day in the United States (as of December 2013, according to CTIA)
- Apple announced that users send over 40 billion iMessages per day (Februrary 2014)
- In 2016, Apple announced that users send an average of 200,000 messages per second.



American adults use their smartphones about 6 days per week.

http://www.nielsen.com/content/dam/corporate/us/en/reports-downloads/2015-reports/total-audience-report-q1-2015.pdf

>99% OF THE WORLDS SMARTPHONES USE AMERICAN OPERATING SYSTEMS

(ANDROID, iOS or WINDOWS)

International Data Corporation (IDC), Worldwide Quarterly Mobile Phone Tracker, February 2015; available at: http://www.idc.com/getdoc.jsp?containerId=prUS25450615

>99% OF AMERICANS HAVE ACCESS TO 4G/LTE COVERAGE.

Mosaik Solutions, Worldwide Mobile Coverage 2015 Edition, March 2015; available at: http://www.mosaik.com/sites/440/uploaded/files/Mosaik_Solutions_Worldwide_Mobile_Coverage_d0215_web.pdf

>52% of all worldwide digital video views will be on mobile in the next year; in 2014, it was 40%.

ZenithOptimedia; Online Video Forecasts 2015, July 2015; available at: http://www.zenithoptimedia.com/shop/forecasts/online-video-forecasts-2015/

28% OF VOTERS USED SMARTPHONES FOR POLITICAL INFO IN 2014.

MORE THAN DOUBLE FROM 2010.

Pew Research Center, Cell Phones, Social Media and Campaign 2014, November 2014; available at: http://www.pewinternet.org/2014/11/03/cell-phones-social-media-and-campaign-2014/

Smartphones comprise 77% of traffic on wireless networks and 56.6% of device connections in North America.

Cisco's VNI Mobile Forecast Highlights, 2014-2019, May 2015, available at: http://www.cisco.com/assets/sol/sp/vni/forecast_highlights_mobile/index.html

Photo from ctia.org

EVOLUTION OF CELL PHONES

- Over the years, cell phones
  - Have become smaller and lighter
  - Are less expensive (devices and service)
  - Are much faster
  - Use less power

CRIMES

- What crimes can be committed using a mobile device?
  - Crimes against children
  - Drugs
  - Harassment
  - Terroristic threats
  - Murder
- Civil wrongs can also be perpetrated using mobile devices

MOBILE FORENSICS

- Defined:
  - “a branch of digital forensics relating to recovery of digital evidence or data from a mobile device under forensically sound conditions” (Wikipedia)
- Digital forensics “is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime” (Wikipedia)

What does forensically sound mean?

FORENSICALLY SOUND

- Definition from a popular text book:

“term used extensively in the digital forensics community to qualify and justify the use of particular forensic technology or methodology”

COMPUTER FORENSICS VS. MOBILE FORENSICS

- Mobile forensics and computer forensics are different
- There are unique challenges involved in mobile forensics that are not usually involved in computer forensics

MOBILE FORENSICS CHALLENGES

- Many different types of hardware
- Large number of mobile operating systems
- Security features

MANUFACTURERS

- Apple
- BlackBerry
- HTC
- LG
- Motorola
- Samsung
- ZTE

MOBILE PHONE OPERATING SYSTEMS

- Android
- BlackBerry OS
- iOS
- Windows Phone
- Many different proprietary operating systems

What operating system does your phone use?

What are the phases of mobile forensics?

MOBILE FORENSICS PROCESS

- Seizure
- Acquisition
- Examination/analysis

SEIZURE

- Ensure that appropriate legal authority exists before seizing
- Determine the make, model, and IMEI/MEID/serial number
- Determine the goals of the examination
- Wear gloves when handling evidence

WHERE IS THE DATA STORED?

- Data can be stored in four different locations:
  - On the phone
  - On the SIM card inside the phone
  - On the memory card inside the phone
  - In the “cloud”
  - In the cellular provider’s records

What is a SIM card?

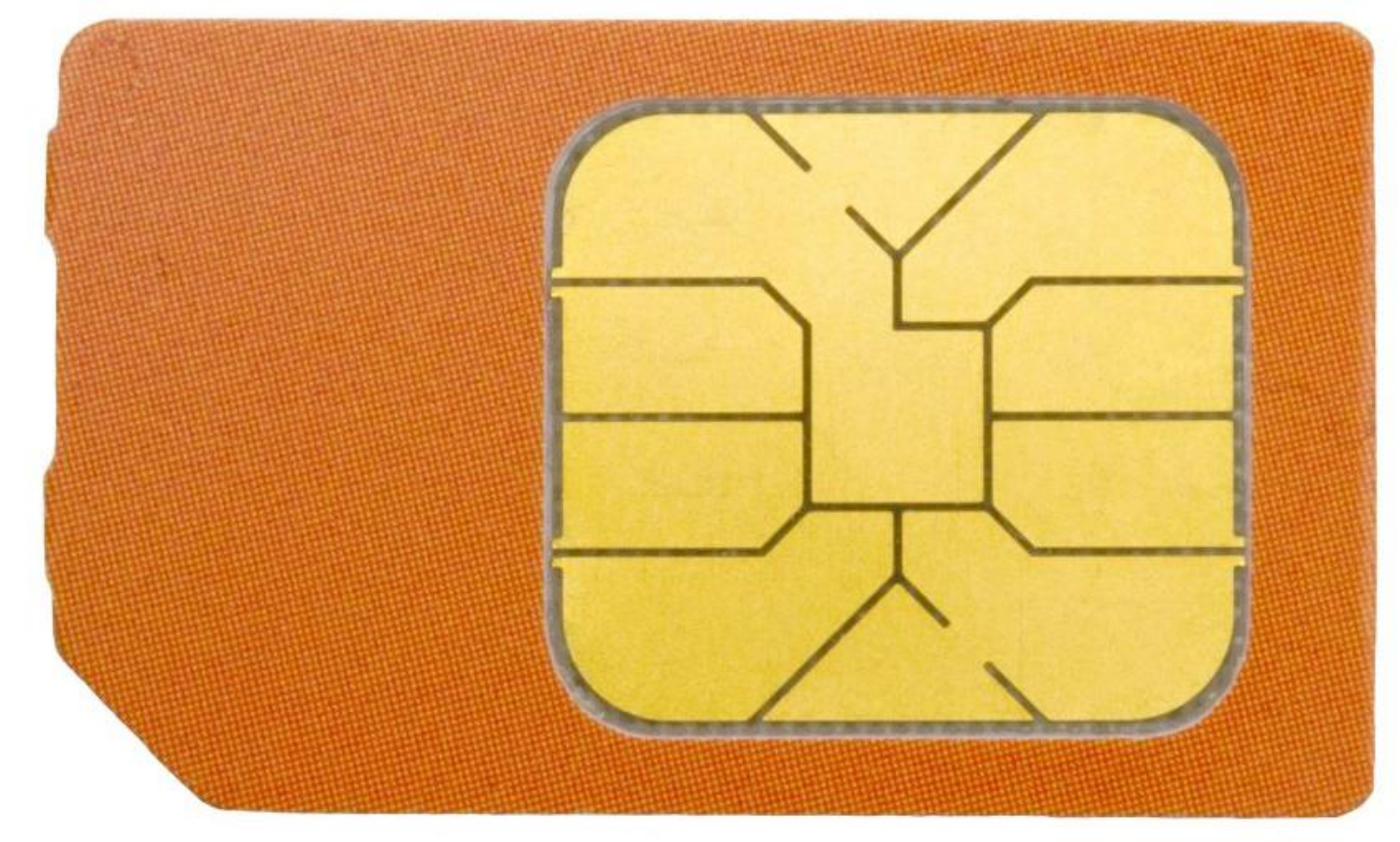


Photo from wisegeek.com

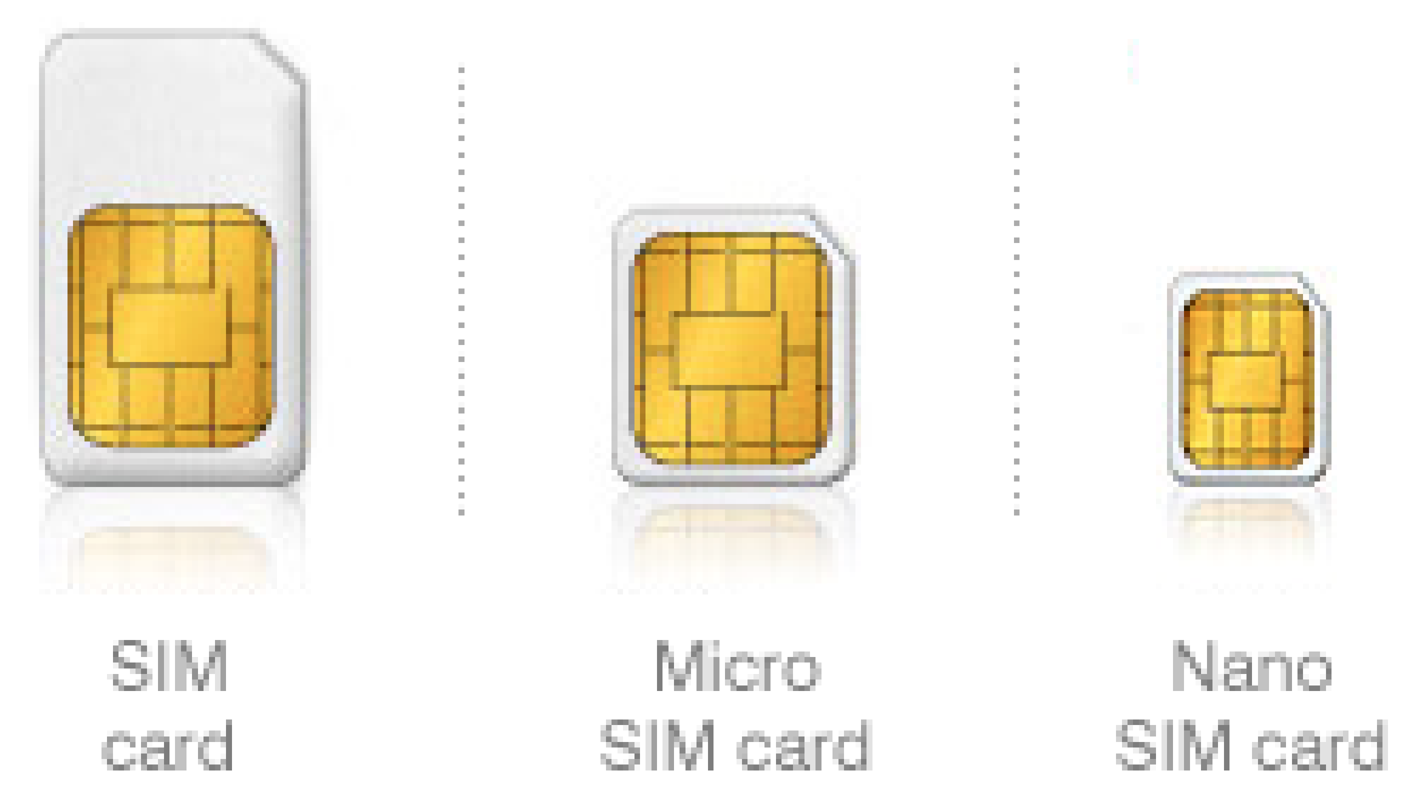


Photo from t-mobile.com

What is a memory card?

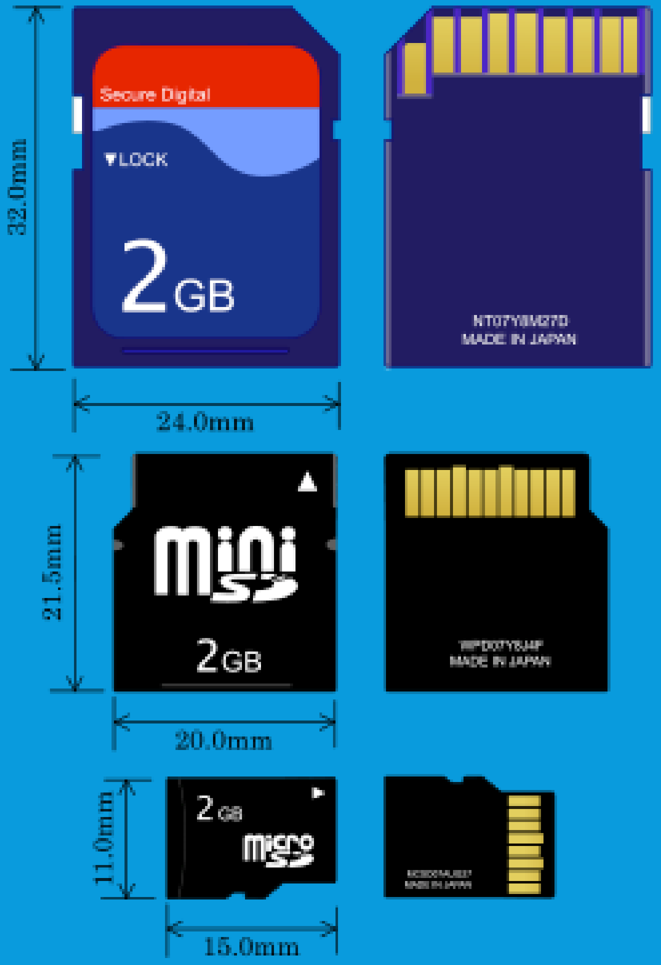


Photo from wikipedia.com

COMMUNICATION TYPES

- Phone calls
- SMS
- MMS
- Data

AVAILABLE RECORDS

- Depends on the carrier
- Call detail records (CDR)
- Detail records for SMS/MMS messages
- Detail records for data usage

Who are the major cellular carriers?

CELL PHONE PROVIDERS

- Verizon
- AT&T Mobility
- Sprint
- T-Mobile

How about regional carriers?

REGIONAL CELL PHONE PROVIDERS

- US Cellular

MVNO

- Mobile virtual network operator
  - TracFone
  - NET10 Wireless
  - 420 Wireless
  - H2O Wireless
  - Republic Wireless

420 WIRELESS™

★ GSM ★ CDMA ★ MOBILE INTERNET ★

The Nation's First Marijuana-Friendly Phone Service

Helping Legalize Marijuana in The U.S. By Donating 20% Proceeds to NORML

AVAILABLE NOW

ON THE TOP 3G/4G NETWORKS IN THE NATION

★ SAVE MONEY ★ CONTRACT-FREE ★

Order Now

IDENTIFYING THE CARRIER

- FoneFinder
- WhitePages

NUMBER PORTABILITY

- Allows consumers to bring their phone number to a new carrier
- Neustar administers the Number Portability Administration Center

NON-TRADITIONAL PHONE SERVICE

- Google Voice

PRESERVATION REQUEST

- Investigators should consider submitting a preservation request to preserve records before they are no longer available
- Generally offer the investigator 90 days to obtain and serve legal process

OBTAINING RECORDS

- Legal Process
- Contact the service provider to determine the records that are available and any specific language that should be used
- Request instructions for interpreting records
- Consider using the term “communication log”
- Talk to your prosecutor

Evidence can be tangible OR intangible

SEIZING TANGIBLE EVIDENCE

- Evidence could be stored on a variety of different types of devices
- Evidence could be stored on multiple devices
- Evidence could be stored in multiple locations
- Be aware of very small and disguised devices

PROTECTING EVIDENCE

- Photograph items before seizing
- You may want to bring a forensic examiner with you when executing the search warrant
- Consider RAM capture for desktop and laptop computers
- Place cellular devices in Airplane Mode if possible
- Don't forget about fingerprints and DNA evidence

CELL PHONES

- General rules for cell phones:
  - If they are powered on, then leave them on
  - If they are powered off, then leave them off
- If they are on, place the device in a Faraday bag to prevent wireless communications

FOLD TOP OF FARADAY BAG OVER TWICE FOR PROPER SIGNAL SHIELDING

Photo from faraday-bags.com

Where can suspects hide evidence?

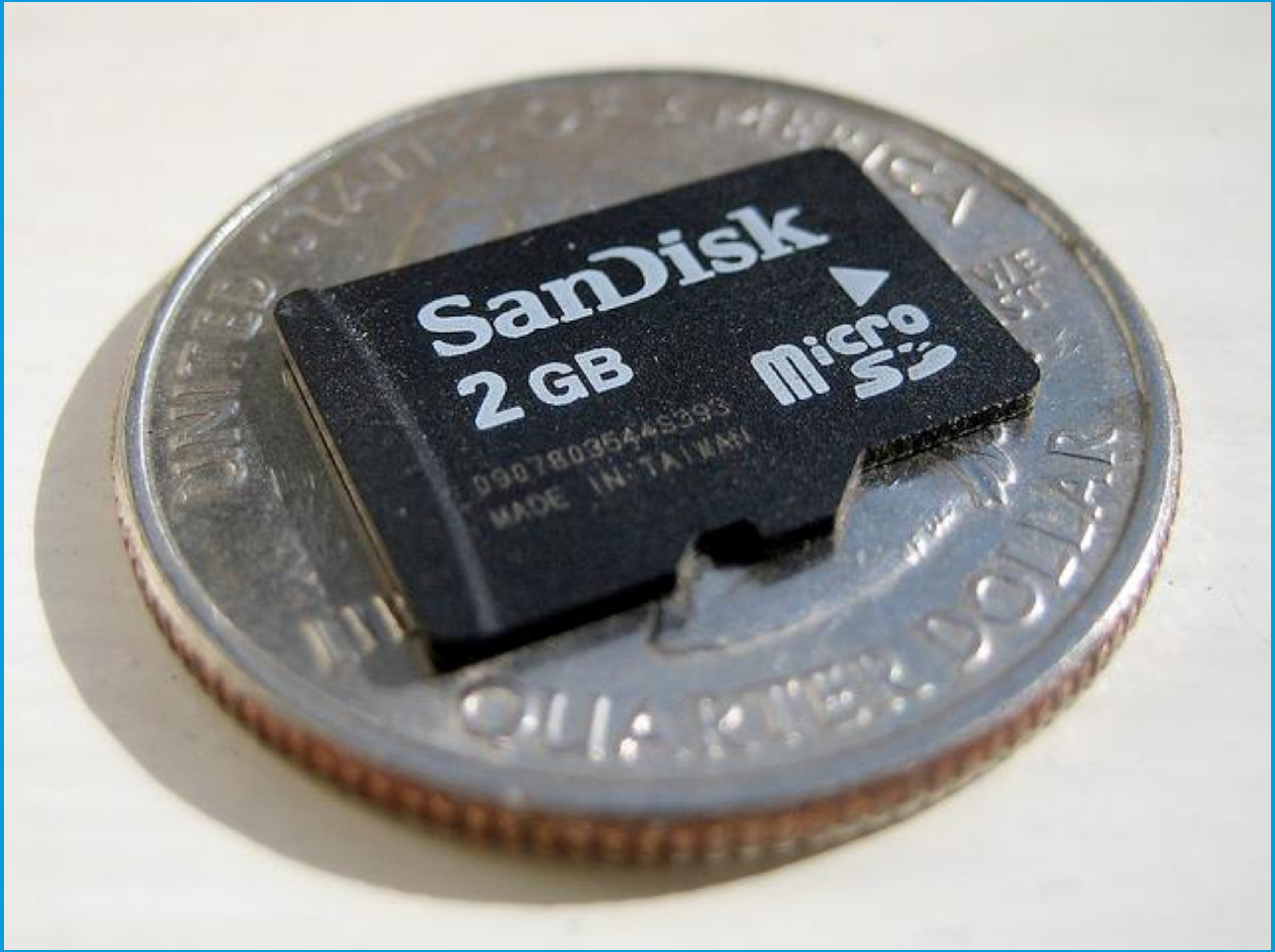


Photo from rascalmicro.com

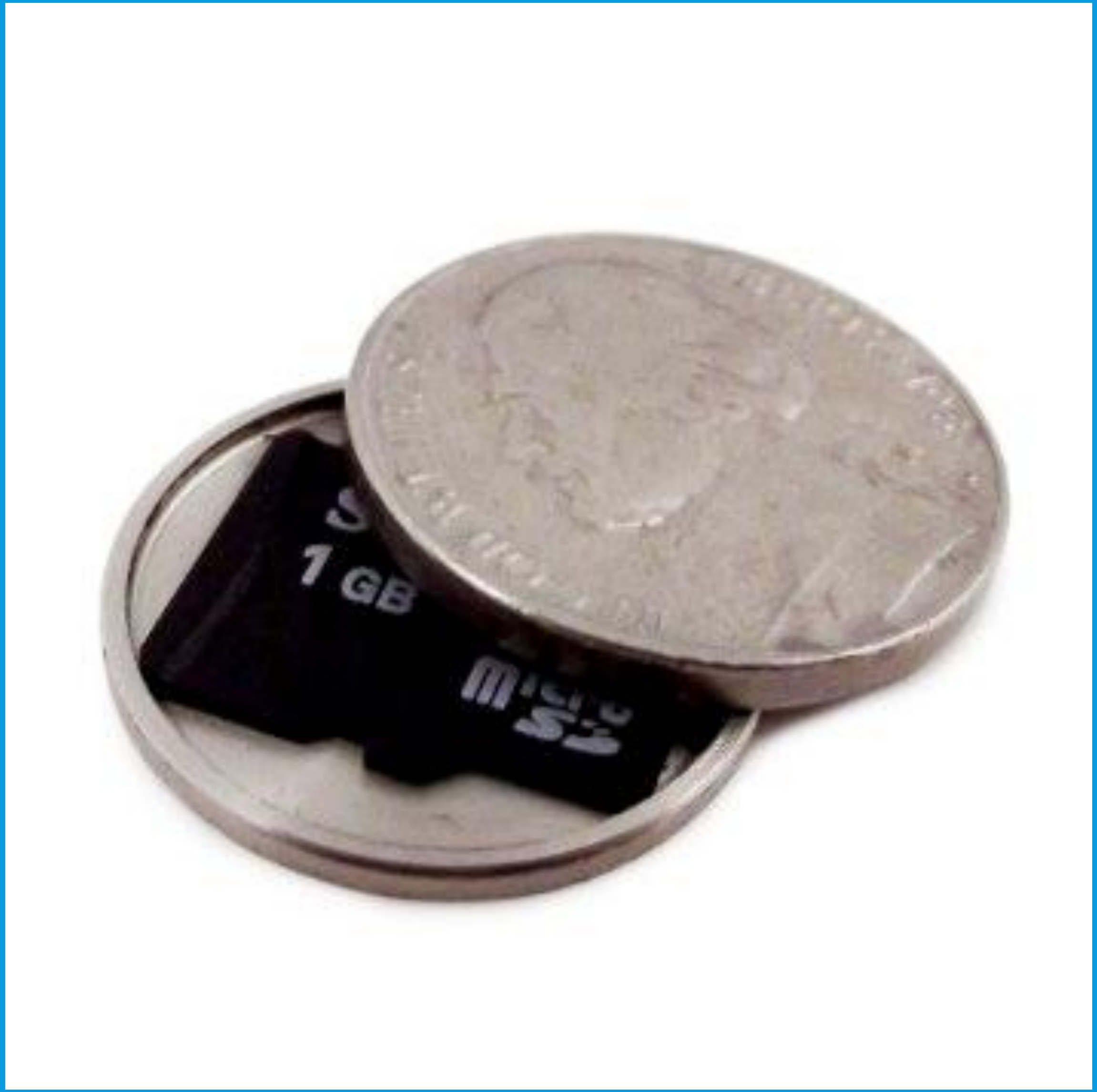


Photo from amazon.com

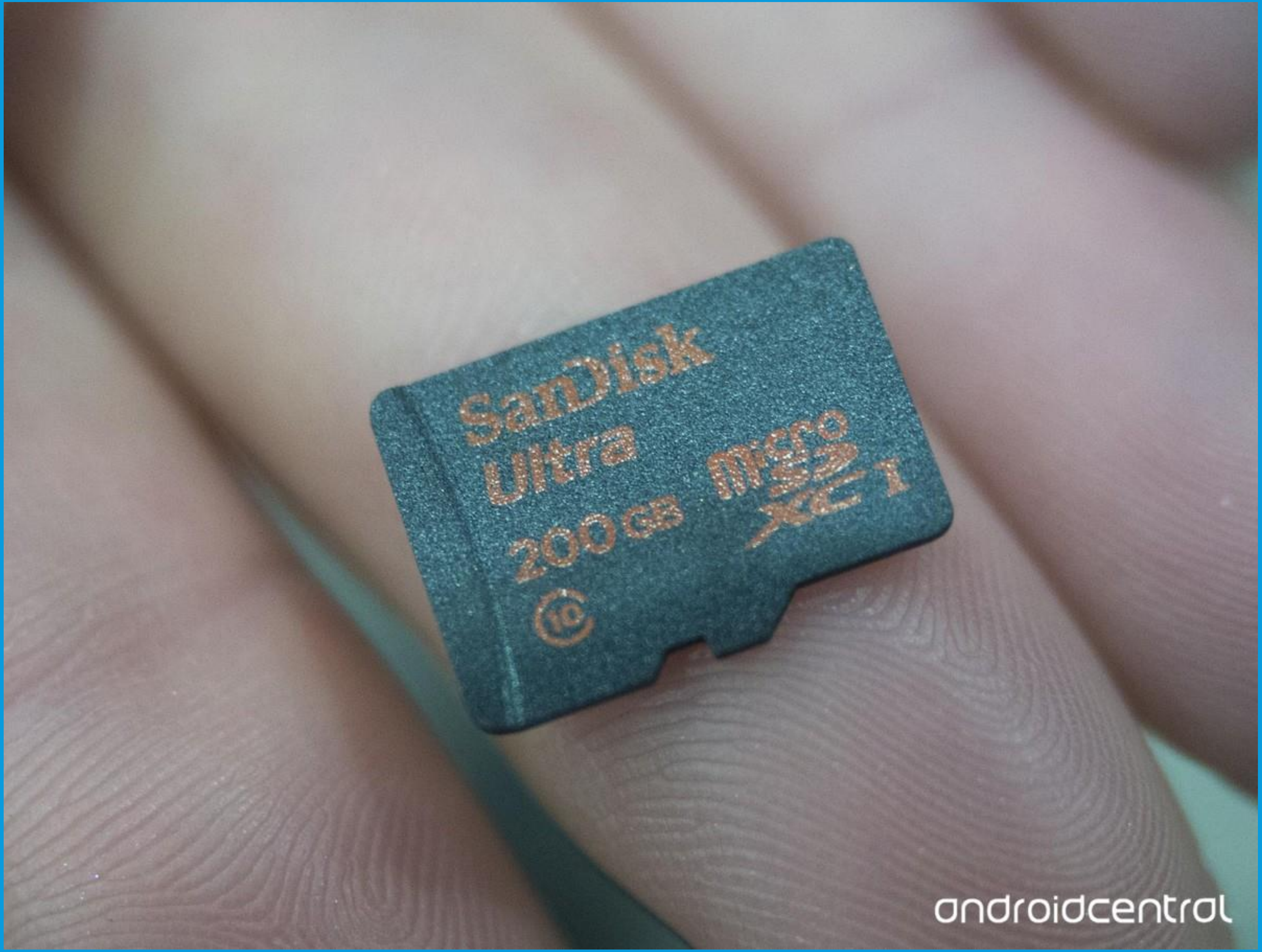


Photo from androidcentral.com

HOW MUCH DATA IS 200GB?

- 3,500,000 Word documents
- 55,000 PowerPoint presentations
- 120,000 high resolution photos
- 45,000 songs
- 100 full length movies

Photo from tricksdaddy.com

Photo from tricksdaddy.com

Photo from tricksdaddy.com

Photo from tricksdaddy.com

Photo from tricksdaddy.com

Photo from tricksdaddy.com

Photo from tricksdaddy.com

Photo from tricksdaddy.com

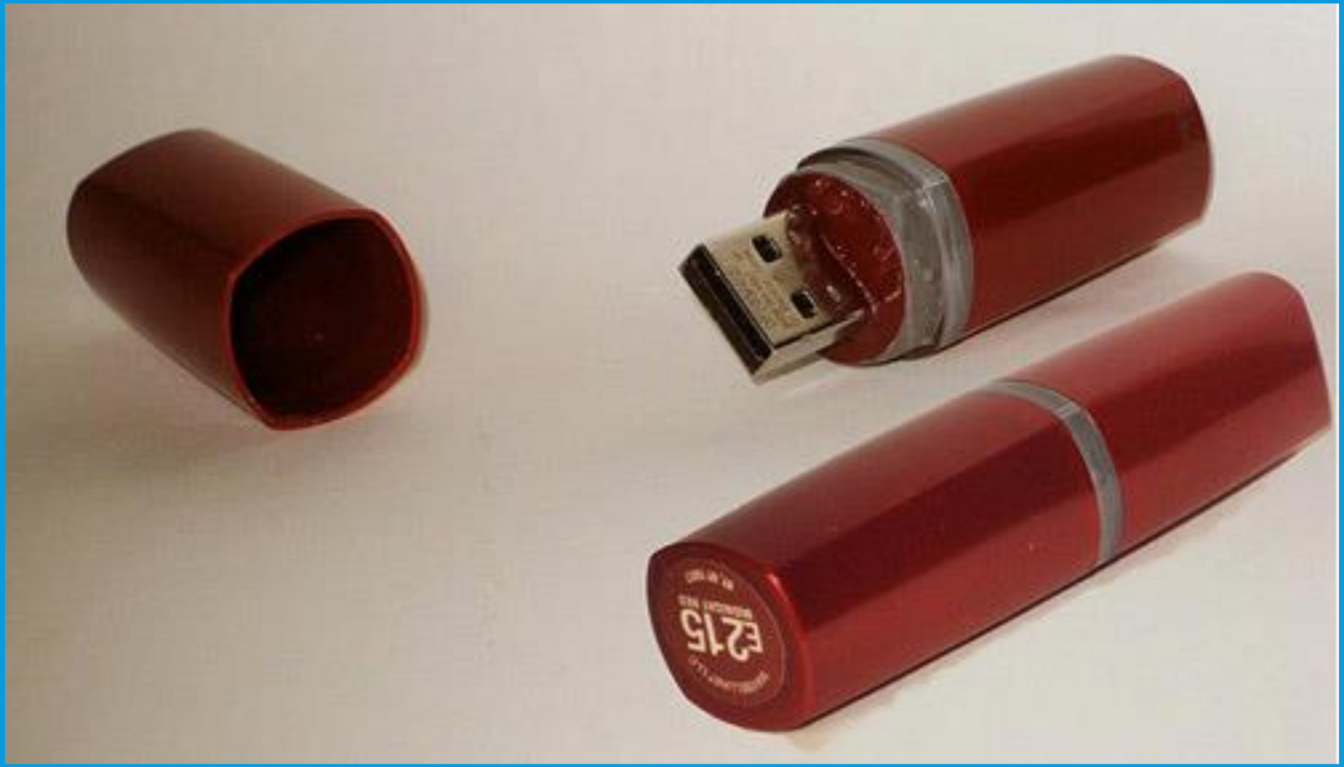


Photo from tricksdaddy.com

Photo from tricksdaddy.com

Photo from tricksdaddy.com

Photo from funcage.com

Photo from hasee-xing.com

Photo from pinterest.com

Photo from ruamhua.com

Photo from promokeychain.com

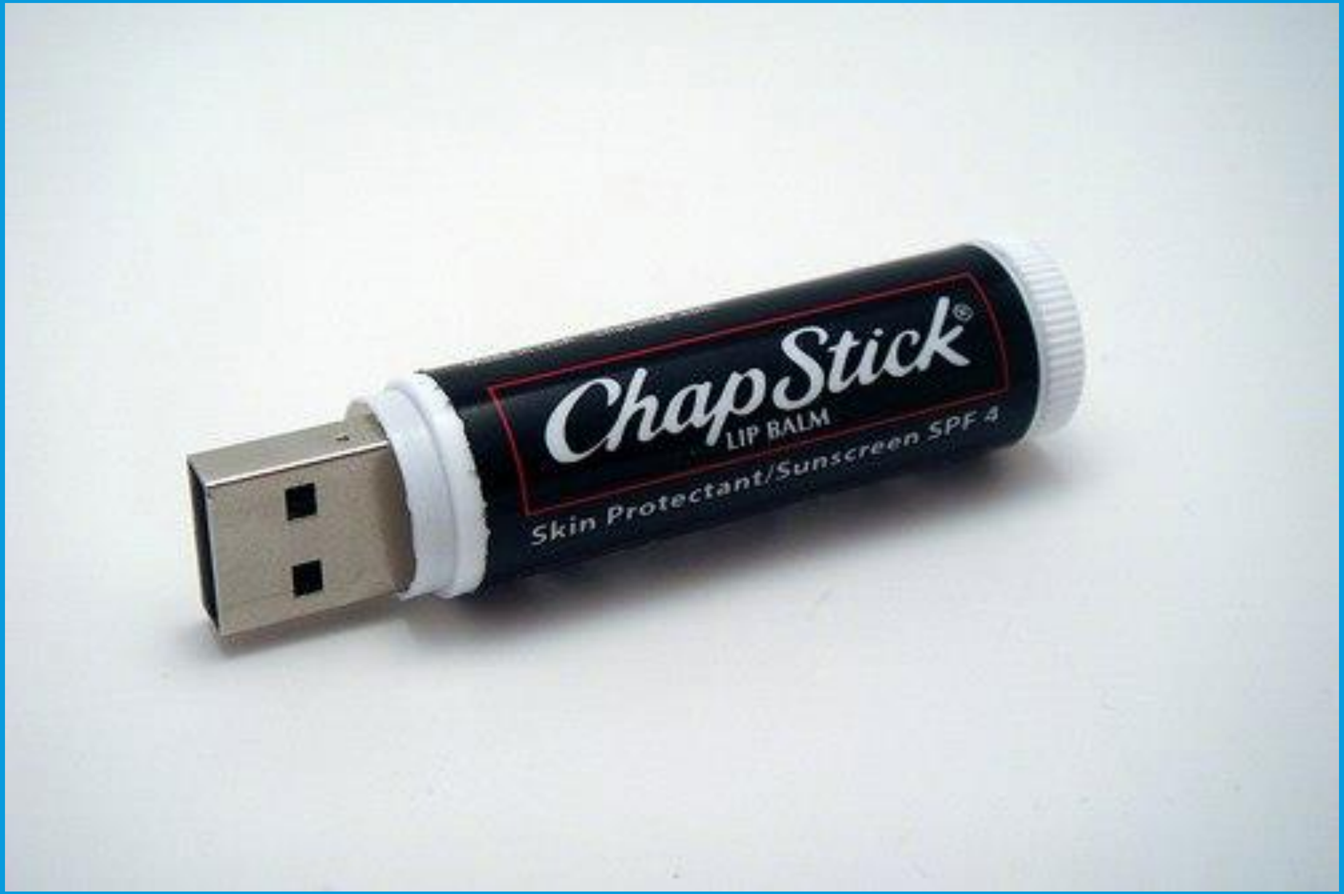


Photo from wonderhowto.com

Photo from bestbuy.com

EXAMINATION/ANALYSIS

- The examination/analysis will depend on the type of data you are looking for

ANALYZING TANGIBLE EVIDENCE

- Prevent officers from “taking a peek” at the evidence
- Submit the evidence to a qualified examiner
- You may need the examiner’s assistance when reviewing the results

What types of data will be found?

TYPES OF DATA

- Address book
- Call history
- SMS
- MMS
- E-mail
- Web browser history
- Photos
- Videos
- Music
- Documents
- Calendar
- Notes
- Maps
- Social networking data
- Application data
- Deleted data

RULES OF EVIDENCE

- For evidence to be admissible, it must be:
  - Authentic
  - Complete
  - Reliable
  - Believable

PROPER FORENSIC PRACTICES

- Secure the evidence
- Preserve the evidence
- Document the evidence
- Document all changes

What about locked phones?

EASIEST METHOD FOR LOCKED PHONES

- What is the easiest way of dealing with a locked phone?
- Ask the suspect for the password!

SMUDGE ATTACK

- It may be possible to view the suspect’s pattern

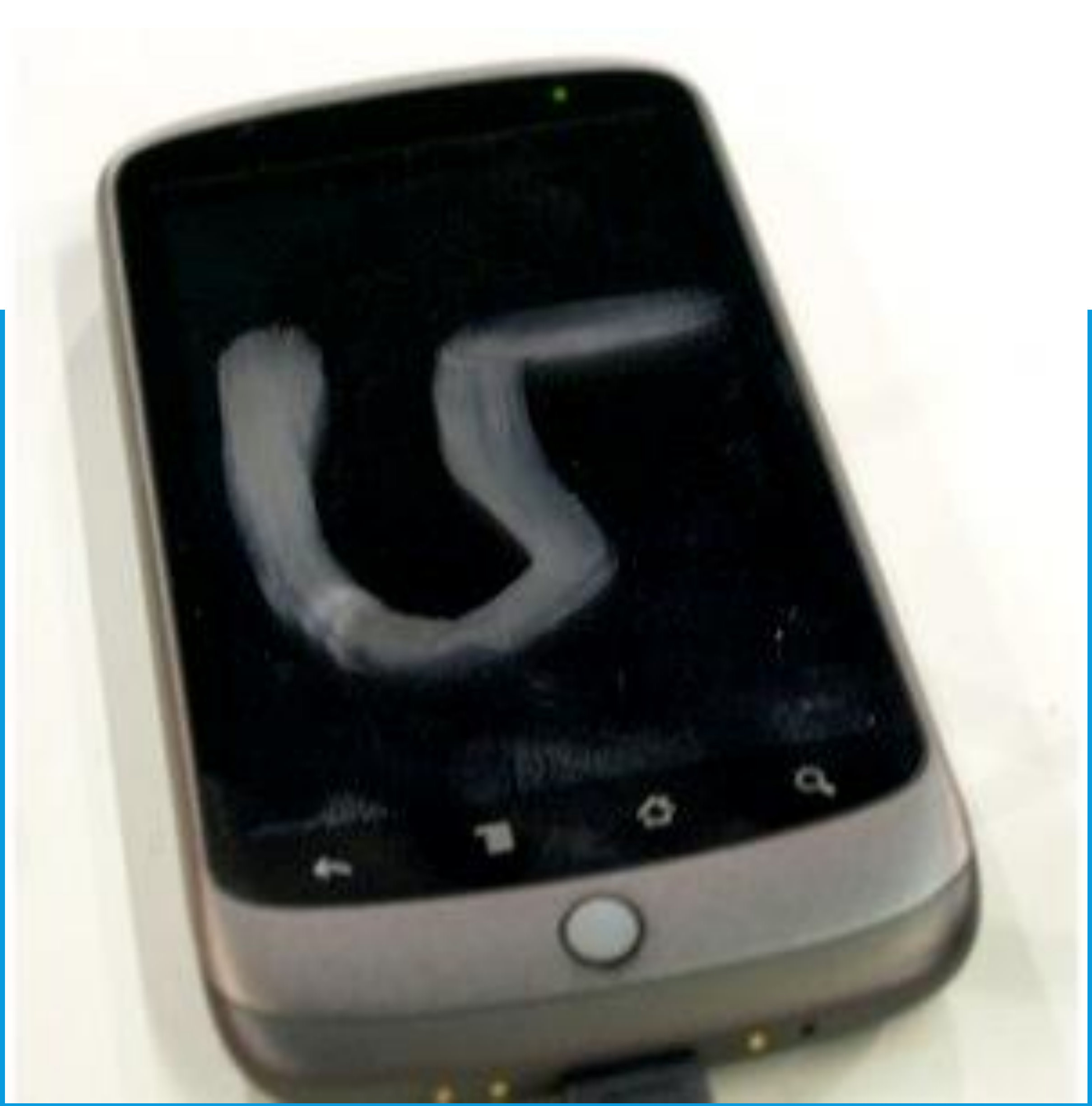


Photo from guardianproject.info

MICROSD CARD

- Even if the phone is locked, the examiner may be able to locate valuable evidence on the microSD card

JTAG

- Joint Test Action Group
- The examiner connects to TAPs (Test Action Ports) to obtain an extraction of a locked or damaged phone

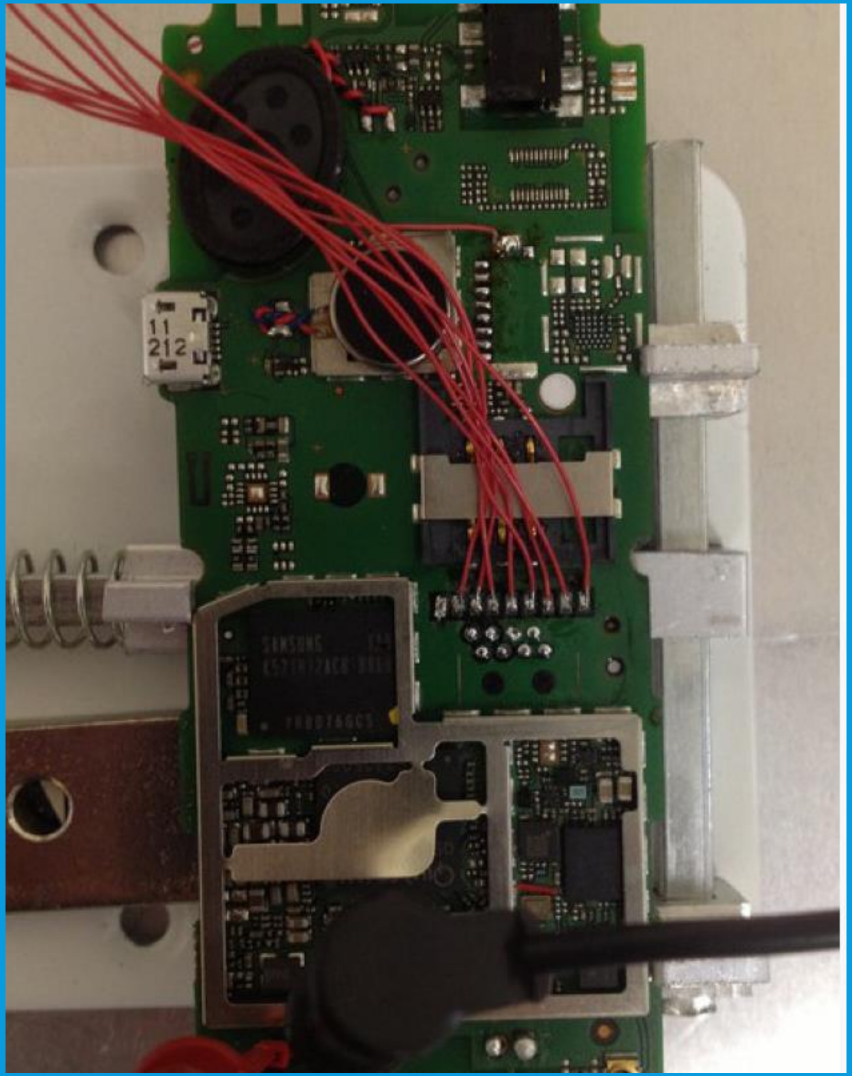


Photo from binaryintel.com

CHIP OFF

- The memory “chip” is removed from the device and placed in a special reader

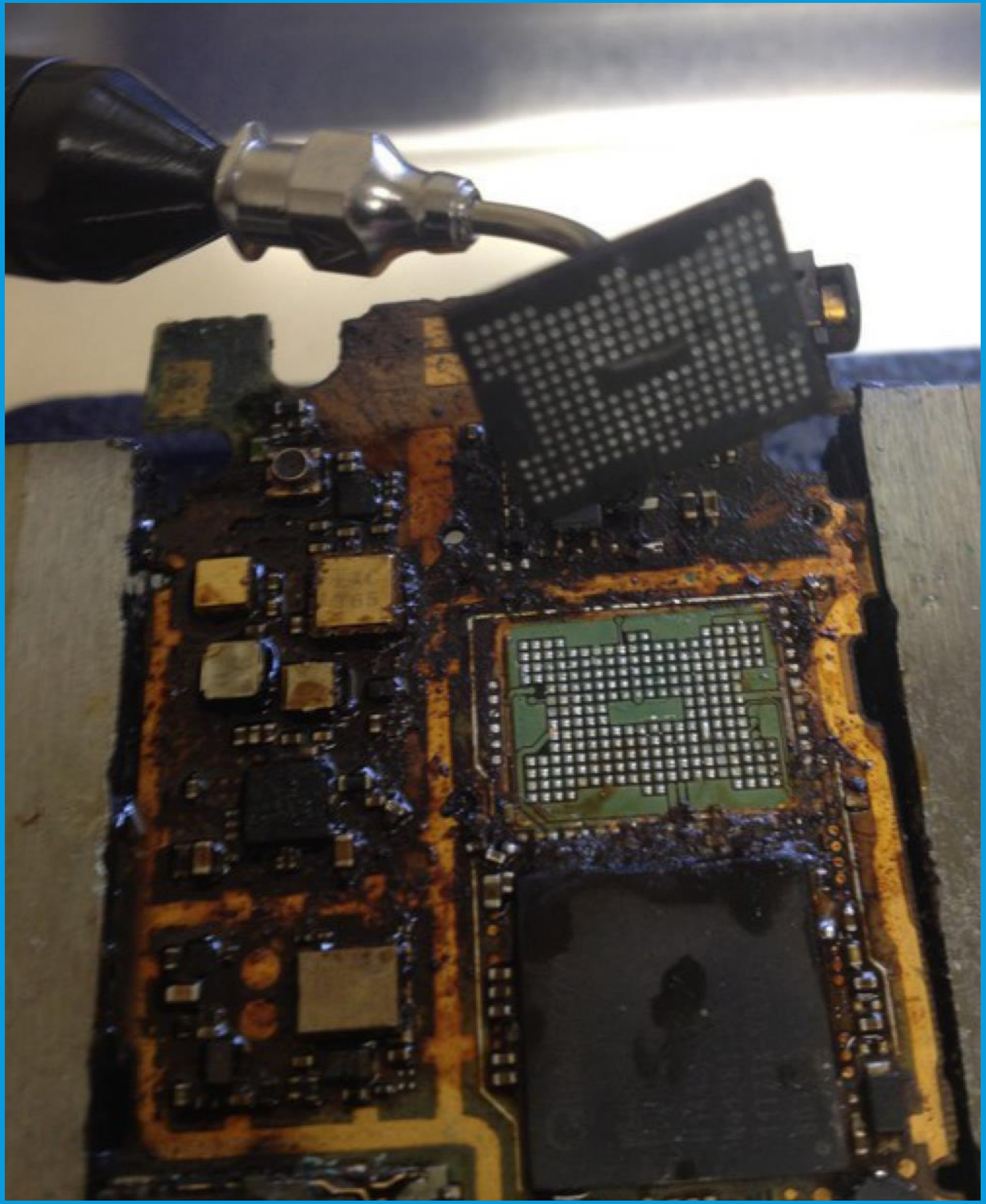


Photo from binaryintel.com

Photo from up48.com

ASSISTANCE FROM THE MANUFACTURER

- You may be able to obtain assistance from the manufacturer
- FBI vs. Apple

INTANGIBLE EVIDENCE

- Intangible evidence can be just as valuable as tangible evidence (sometimes more valuable)
- Examples include
  - Email messages
  - Cloud storage
  - Social networking profiles

INTANGIBLE EVIDENCE

- Investigators should look for and seize intangible evidence
- Examples include
  - Email messages
  - Cloud storage
  - Social networking profiles

EMAIL

- GMail
- Hotmail/Outlook.com
- iCloud Mail
- Yahoo Mail
- Mail.com
- Inbox.com

CLOUD STORAGE

- Dropbox
- Google Drive
- Box
- Microsoft OneDrive

SOCIAL NETWORKING

- Facebook
- Twitter
- LinkedIn
- Pinterest
- Google Plus
- Tumblr
- Instagram

ADDITIONAL TRAINING

- Forensic Product Vendors – Cellebrite, XRY, Lantern
- DeSales University
- Internet Crimes Against Children Task Force
- Federal Law Enforcement Training Center
- United Stated Secret Service
- National White Collar Crime Center (NW3C)

DESALES UNIVERSITY

- Bachelor of Arts in Criminal Justice – Digital Forensics Track
- Master of Arts in Criminal Justice – Digital Forensics concentration
- Graduate Certificate in Digital Forensics

Questions?

Joseph.Walsh@desales.edu

(610) 282-1100 X 1463