PACE UNIVERSITY

Seidenberg School of Computer Science & Information Systems

IT 670

Mobile Forensics Investigation

Jagdeep Kainth

#U01840609

Lesson 1 : Weekly Journal

The Lecture start with computer forensics definition, in which we concluded that computer forensics is not just limited to computers only, but can be anything that contains a digital evidence for example SD cards, gps system , mp3 player.

There is 3 main things to prove someone guilty in digital forensics, those are control, intent, ownership. When we talk about control, that means that the suspect have control of the computer which can be proved by examining the login information that is saved on the computer, and intent can be proved by checking the number of times the suspect opened or visited a specific website or thing and ownership can be proved by confirming that a person shares a specific file with somebody else or created or modified it.

There is a lot of importance of digital forensics due to growth in digital crime and due to the fact that every crime nowadays involved digital evidence. Good careers opportunities in digital

forensics with high paying salaries. Not only common government sectors(FBI, narcotics, revenue agency) but also private sector(software companies) hires digital forensics expert. A digital forensics expert should be a bilingual with great skills in writing, mathematics, computing and law. Knowing multiple languages is important due to the fact that criminal activities are internationally spreading every day, great communication and writing skills help in explain to others about the evidence that is collected. Mathematics and computer science knowledge is a must when dealing with digital technology. Knowledge of law is important because if forensics examiner needs to examine someone's computer then , it should be proved to the judge in court that there is criminal activity happened and there are chances of evidence in a specific location, then judge grants a warrant. Without knowledge of rights and laws, a digital investigator can get in legal issues.

Real case studies in the past include scott Peterson murder case, in which recent web search of boats and knots and timing of local tides was used as an evidence to make suspect guilty. Case of enron involves examination of hundreds of computers and thousands of emails.

Types of investigations includes public and private. Public investigations includes law enforcement of local, county, state, federal bodies, whereas private includes non government agencies.

Types of evidence includes system files, which shows when a file was created or modified or deleted emails , websites visited in past, programs installed. Devices that stored digital data can be used as an evidence for example hard disk, floppy ,cd PlayStation, USB. Forensics are also used in corporate investigations which involves misuse of assets , internet abuse, falsification of data.

Digital forensics experts work on fighting cyber terrorism, identity theft and child pornography. Experts needs to follow a proper protocol to handle and store data/evidence with case number, description, location of seizure. To prevent any kind of date tampering.

Difference between Mobile and computer forensics. Mobile forensics refers to finding digital evidence that is created by mobile device. Sometimes investigator get warrant for the telecommunication companies like Verizon and social media companies like Instagram to collect digital evidence against the suspect. Digital forensics evidence includes smart phones, tablets, gps, xbox, e readers. Mobile devices are very common in crimes nowadays and are more useful because its always on tells about person personal thing like health, includes voice data of user, location tracking due to different food apps like starbucks.

Mobile device don't use hdd but are built on embedded chip. Has different file system, call logs, locational data, .

In mobile phones location information is very easily assesible due to so many reasons for example a person using apple iphones can be located by the mac address of the phones tracked by the apple id logged in by the user.

History of mobile devices tells a lot about blackberry and motorlla in 1970s,80s,90s.

Later on UME got used by law enforcement to investigate cellphones because it can merge sim card data and phones data and can can transfer altogether at once to another cellphone.

CAST teams can prove using the cellphone companies call recored details and can proof the suspect guily by examining the call logs, for example a person make a phones call to someone,

then the closest cell tower will be used for that call and the location of users can be identied. This cell site concept is also used in google maps to find out the quantity of a traffic on a particular road.

Higinio got arrested by the picture she posted on the internet. FBI used that image to find the the exact coordinate of where in Australia she was located

Michael Jackson murder case involves a iphone which was used as an evidence later in the case. Evidence include conrad murray iphones which had a 4 minute long voice msg. the time square shooting incident involves cellphones seizures of number of people. The suspect was shot dead by the police and the cellphone evidence was used to proof that there was not misconduct happened.

Lesson 2 : Weekly Journal

Class starts with an introduction of everyone in the class. Professor Darren R. Hayes Starts with Differentiating between digital security and digital forensics and taught the class that Digital Forensics is the subset of Digital Security or Cyber Security. Cyber Security is something that is related to prevent any kind of attack on digital database. Digital Forensics is something that is needed after an attack occurred, for example how incidence response teams work in a company, they may use the practise of digital forensics investigation. In the class we were discussing a real life incident which was a murder case happened at Gilgo beach, Long Island, New York. We learned that how that incident was related to digital forensics. There was evidence that includes phone records, Online activity, communication via phone that clearly gives a lot of evidence related to the victim and the suspect. The investigators could have found something inside the PC or mobile phone of the suspect to discover evidence for example search history, location data, and activity on other social media applications.

Cellular network components Includes a lot of stages that has users device/mobile stations such as iPad, iPhone. The Second stage is base transceiver station(BTS)/or antenna cell That is further controlled by base station controller(BSC). The third stage is Mobile Switching Centre have Home Location Registerer(HLR) and authentication centre. When we make a call we connect with cell tower. Cell shape includes cell tower and antenna mobile station. A cell tower has three panels which includes antenna in the middle known as transmitter and the outer two are receivers. A tower 200 feet high contains multiple antennas. These antennas are placed in the side of buildings. 4G antennas don’t support 5G connections because 5G do not travel very far and do not travel across tress and buildings, that is why we need more 5G towers as compared to 4G. In 5G, our digital device connects to many towers unlike 4G. Beam forming concept in 5G enables our phones to continuously look for better signals every second. 5G high frequency range between 3 kilo hertz to 300 giga hertz. 5G uses the high frequency and short wavelength concept. Lower frequency means stronger signal. 5G have short unstable waves that is the reason it need more cell towers. For example Verizon uses 5G ultra-wide band on millimetre waves on 28 giga hertz and 39 giga hertz. Mobile Switching Centre(MSC) keeps track of all calls that made by the users. The Forensics investigators gets

in touch with the MSC to get all the information of the suspect or victim carrier. They have customer carrier report also. They even have the location records of the towers the user might have connected to. Mobile station container two things, first is handset and second is subscriber identity module(SIM). International Mobile Station Equipment(IMEI) is another factor that can be used by the mobile forensics experts. The IMEI numbers tells everything about the device weather it is IOS or Android, The model number, network, country of origin, warranty information, Date of purchase. Base Station Controller(BTS) towers are constructed, owned and managed by other companies other than Verizon and T mobile. BTS is the equipment that manages communication. Soft handoff works with one base station to another and not relies on one station only, whereas Hard handoff based on one BTS only.

Teams of forensics investigators practise cell site analysis to find digital evidence. Cell site analysis(CSA) has to be requested before used in an investigation which is mostly in csv format. It tells the Information about the location of the user during the calls that subscriber made. Call detail records(CDR) tells dates, time and cell sites quadrant. In an investigation, if Investigator get mobile phone at the crime scene with SIM and it is pin protected, then law enforcement can request pin unlocking key from the phone or telecommunication company. According to US code 2703{required disclosure of customer communication or records} there is a law that telecommunications companies needs to follow, that is to preserve all call records as evidence for 90 days. A mobile equipment identifier (MEID) International identifier used to identify physical mobile station equipment. Then comes ESN which stands for electronic serial number which is written by the manufacturer on the microchip of the wireless phone. In mobile networks , there is a Subsidy lock which make users to get stick to one network only. For example if a person buys a phone with a phone plan from a telecommunication company that sells sim cards, sometimes the user is not allowed to change the network carrier on that phone. Mobile switching centre is responsible for specific network activity such as if user calling another user that have different carrier, then call will be routed by the mobile switching centre to public switched telephone network. public switch telephone network(PSTN) is another type of circuit switched telephone network. Forensics examiners can also use Equipment identity register(EIR) and authentication centre(AUC) to track stolen device and to get the encryption keys of a device Global system mobile(GSM) network is a type of SIM card that can be used in different nations. International Mobile Subscriber Identity(IMSI) is a unique number automatically generated and stored in the SIM. Law enforcement uses IMSI catcher to catch the criminals and suspects. Mobile Subscriber Identity Number(MSIN) is also a unique identification number which identifies mobile network subscription. Mobile Station International Subscriber Directory Number(MSISDN) tells everything about the subscriber by using this concept, first three digits tells country code. Then number plan area(NPA) also known as area code or mobile network code contains 2-3 digits, then Comes the MSIN contains 3-4 digits. A SIM card contains a 19-20 digits id printed on the SIM in which first 2 digits are major industry identifier. Code Division Multiple Access (CDMA) used by Verizon was developed during world war 2. It allows frequency hopping and direct sequencing. Universal Mobile Telecommunication system(UMTS) is a 3G cellular network which can store more data files than a normal SIM. Mobile Phone Network Operator also provides Mobile phone service

but do not own SIM cards. In an Investigation, Law enforcement need two warrants to investigate, one for the mobile phone network operator and one for MVNO mobile virtual network operator.

5G is famous for its 3 mains keys that is High band width, in 4G there is only 200 megabits of bandwidth only. 5G has 1 gigabit or more. 4G Response time 100 milliseconds or more, whereas 5G response time 1 millisecond. 5G has Dense connection as compared to 4G. 5G uses radio technology. Radio frequencies of 5G has SUB 6 concept which means 600 megahertz to 6 gigahertz. This is also used by current 4G LTE. 5G also use higher bandwidth of 24 gigahertz to 86 gigahertz. 5G use small cells known as cellular towers. 5G uses the concept of beam forming that improves the signal strength by eliminating undesirable interference sources and focus on transmitted signals to specific locations. 5G has the feature to avoid blunting due to low latency benefit. 5G can power cars and Bridges can tell when they need repair. As the technology is evolving continuously One day there will be no need of router. We will get connected with Internet service provider ISP directly by our devices. Let's talk about the inner workings of cellular Networks that was discovered in 1949, 1G was discovered 1979, 5G was discovered in 2019. Cellular networks divided into Cells each cell in the shape of hexagon. Two towers get connected via land lines with the mobiles switching centres cell towers. When a Subscriber make a call, it connected and goes through MSC. Cellular network Signals has frequency ranging between 100 to billions of hertz. higher the frequency the greater the band width.

Lesson 3 : Weekly Journal

As the week 3 class lecture starts, Professor Darren Hayes begin with talking about different cellular network companies like Verizon, AT and T, T mobile, and we talked about that who owns the Cellular towers of these companies. Mostly in united states, a huge percentage of cell towers and telecommunication infrastructure are owned by American Tower, Crown Castle and SBA Communications. Then Professor asked the class that how authentication happens in a cellular network. When the user tries to authenticate, The IMSI of the user SIM has been sent to cell tower which further transferred to authentication centre, authentication centre Send RAND(random number) to the user, user Mobile phones use RAND to create SRES, then send it to authentication centre, auth compares the SRES of the user and the database of the company, if matches then gives session key to user to establish communication with the cellular network. We talked about 4G(4^{th} generation) LTE(long-term evolution) and 5G(5^{th} generation), GSM(global system for mobile communication) ,3G(3^{rd} generation) , CDMA(code division multiple access).

GSM is a standard created by Europe ETSI(European telecommunication standard institute) and 3G, 4G LTE are all based on GSM. What happens when we make a call from our mobile phone.? When we dial a specific number to reach someone over the phone, it connect to the cell tower(base station) then it further transfer is to MSC(mobile switching centre). MSC identifies the receiver, if the receiver is on same or different network. If it is same then the

receiver phones establish connection with the sender otherwise if different network , then MSC routes the call via PSTN(public switched telephone network).Law enforcement agencies can get information from carrier of both caller and recipient phone, date and time of the call, duration of the call, call type weather incoming or outgoing, IMSI numbers, cell tower information, SMS records, location data, subscriber information. Law enforcement can also request the cell ID for example in a specific timeframe, they can request when a specific users connected to a tower in a given time frame. Cell ID is a unique id of cell tower. Cell id required by law enforcement o find the information of the location of users when it is connected to the tower. Sprint PCT (personal communication technology) provides phones services including CDMA networks. The concept of timing advance introduced to help the mobile devices in such a way that when signals from the devices going towards the cell tower reach there at the right time. This avoid the overlapping of signals. Distance matter a lot in the signal of the cell tower, the strength of the signal of mobile device decrease as the distance of the cell tower increase. There are some mobile devices now days which support multiple eSIMs. eSIM cards can be embedded directly into the device, which can be programmed remotely and does not require a need of physical SIM card. There are a lot of phones that support dual sim for example iPhone 13, Samsung galaxy s20 ,etc. Although phone numbers are still required to connect calls, companies are placing less importance on individual phone numbers due to the changing telecommunications environment brought about by internet-based communication, regulatory changes, and customer behaviour. Rather, they are now more focused on offering reliable network services and data-driven solutions. Law enforcement can also use EMSI catcher for investigation. EMSI catcher emits signals that cell phones can identity as a legitimate signal coming from a real cell tower. Then the cell phone automatically connects with the IMSI catcher and law enforcement can found evidence related to the suspect such as call content, location data , subscriber information. The cell towers also knows our approximate location with the method of time used by the signals to travel a specific distance. When we talk about IOS, it works differently then windows, its OS has a case sensitive file system that makes a big challenge in the world of digital forensics. Investigator needs to sure that the data they are collecting is legitimate or not. Investigator can face a hard time in court due to document file names in IOS. checkm8 is a exploit in IOS help investigator extract IOS data easily, before this extraction of data in IOS was impossible using conventional methods. iPhone use AES (advanced encryption Standard) 256 bit keys. Wi-Fi access points plays a important role in mobile communications and can significantly help in locating device, view network logs like MAC address and timestamps, data recovery. SSID(service set identifier) is the name of the Wi-Fi network .PSK (pre shared key) is a password or passphrase used to secure the Wi-Fi network.

In the class, there was a discussion about a murder case of a couple and the suspect was an ex-boyfriend of the female victim. Professor asked us how digital investigators know that the suspect is the ex-boyfriend. Professor told us that the investigator inspect DHCP logs of the Wi-Fi and find out that the suspect phone was connected to the Wi-Fi in that timeframe, due to logs investigator also find out that what was the exact location of the suspect how long he was standing outside the house window.

A sim card is very important for identifying subscriber on cellular networks, particularly in GSM and IDA networks, it also stores user data including IMSI and make connectivity for devices like smartphones, tablets, smartwatches and satellite phones. SIM cards have evolved in size from the credit card to Mini Sim to micro sim, then nano sim and now it is embedded sim or eSIM. The ETSI(European telecommunication standards institute) make several standards for these technologies. UMTS (universal mobile telecommunication system) is a 3G standard based on GSM developed by 3GPP(3rd generation partnership project). It makes use of U-SIM, or Universal Subscriber Identity Module, which has a larger file storage capacity than a conventional SIM. Through the use of embedded subscriber IDs, eSIMs enable connectivity in Internet of Things (IoT) devices in the absence of a conventional SIM card. A combination of RAM (Random Access Memory), EEPROM (Electrically Erasable Programmable Read-Only Memory), and ROM (Read-Only Memory) may be found in SIM cards. Different file types, including the Master File (MF), Dedicated Files, and Elementary Files, which can include SMS messages and other telecom data, are included in the SIM file system. Phones are not mass media storage devices, hence instruments like Cellebrite UFED are needed for SIM card investigation. SD and SIM cards need to be taken out for independent inspection. A PUK (Personal Unblocking Key) or PIN (Personal Identification Number), which may be acquired via the carrier, may be needed in order to access SIM data. The SIM may lock permanently after many erroneous tries. The security features of SIM cards can make forensic access to data challenging. The difficulty is in getting data while preserving the accuracy of the information contained therein. With estimates indicating that there will be 20 billion IoT devices worldwide by 2023 many of which will function without conventional SIM cards.integrated SIMs have become increasingly prevalent in IoT devices. Based on smart card technology, SIM cards are usually issued by mobile providers and are detachable. They have the profiles required to establish a network connection, enabling customers to exchange SIM cards to alter their operator or phone number. There may occasionally be an empty entry for the Mobile Station International Subscriber Directory Number (MSISDN), as it is frequently assigned dynamically by the operator and may not be recorded on the SIM card itself. Changing the SIM card in millions of IoT devices has special obstacles, unlike switching smartphones. The embedded SIM (eSIM) is a solution that is becoming more and more important to address these problems. There are several form factors of eSIMs (Embedded Subscriber Identity Modules) to choose from, such as 2FF, 3FF, and 4FF in addition to the more recent MFF2.Harmonious Worldwide. The binary values given in the DF_TELECOM file can be very useful for forensic analysis because it tell everything about the read , unread , sent , unsent , deleted messages.EF_ADN tells about the dialled number, EF_LND tell us about the last dialed number, EF_LOCI tell us about the location where the phone was last powered off.

Lesson 4 : Weekly Journal

Professor assistant gave a brief on PowerPoint about the week 4 content which include IOS study. Class learned about different tools

Checkm8 and checkra1n. the tools are mainly used for the jailbreaking of the device by using exploits.

Magnet axiom is a digital forensic tool developed by magnet forensics to pull out data of the computers and mobile devices. It allow investigators to develop forensic images, run scans on collected data and analyse evidence. We discussed about Cellebrite, a digital forensics tool for extracting digital data from the mobile devices. We can use that tool in our digital forensics lab and students use and study magnet axiom at home also

Learned about IOS forensics 2019, latest tech team of apple announced in 2019 , IOS 13 comes with latest features , user has more option to allow users location and defend its privacy. Which means that we can choose to provide access of location in different categories for example we can tell apps to never track us , or ask next time , or allow while using app or always allow ,so this means that in IOS 13 there is limited user location data. Apps need permissions for this . we can silence unknown callers. Phone ask permission to access contacts. User can strip location data from a photo before sharing it. User may also receive notifications about allowing an app access to Bluetooth. User may also receive notifications that an app is tracking users location. USB restricted mode is security feature, on iso 11.4.1 which prevents a trusted computer from unlocking the iOS mobile device for example if we synchronise our iPhone with our computer then our computer becomes a trusted device, USB restricted mode made the user enter the iPhone password again if the device was disconnected for over an hour. Law enforcement personnel/forensic investigators do this thing they connect a lighting cable after the phone has been seized in the first hour to prevent the USB restricted mode.

In iPhone 11 support face id over touch id, iOS 13 come with 18 watt Lighting USB-C fast charger that benefit investigators , storage range from 64 Gigabyte to 256 Gigabyte to 512 Gigabyte not it is compatible with 5G but compatible with Wi-Fi 6. Apple watch monitor users heart rate, continuously ,user can enable notification of heart rate going too up or too low. How is heart rate monitored by the watch , due to optical heart sensor ,this technology is photoplethysmography, watch uses light sensitive photodiodes. Increase blood flow simultaneously increasees absorption of green light, optical heart sensor flashes its led lights. flashes its led light 100 times per seconds , that's why higher absorption of green light calculates increase in blood flow . The ECG app uses electrodes used by watches that monitors electrical signals coming from the heart.

Series 5 watch is good for investigators in so many ways, health data linked to iCloud account , backed up , and there is a solution or way to pull this data from a person iCloud account like heart rate , sleeping habits, location points., workouts , steps , walking routines. Low energy sensors are used to truly monitor the users activity , apple has been looking to place a health monitoring capabilities in their apple air pods .

We talked about Jamak khasiggi murder case. He was murdered in Saudi Arabian embassy in turkey. The Saudi crown prince gave the killings order. His murder was recorded by his apple watch. Watches detected heart rate activity and location and also exact time of death.

Apple watch can be used in so many trails worldwide. Hussein khavari was accused of raping and murdering a 19 year old girl, later on refused to unlock his iPhone. Law enforcement successfully unlocks it and found few things in health app. The uses the recorded data of footsteps and correlated it with the foot steps towards the river and found him guilty
Myrna Nilsson murder case was also very known due to apple watch. Caroline nilsson, the daughter in law claimed that there were attackers in the place of incident and victim argued with them for continuously 20 mins. Apple watch data was not matching with Caroline story and later she charged with murder
The Boston Red Sox were discovered stealing signs from the New York Yankees in 2017 by means of Apple Watches. This dispute began when the Yankees' general manager, Brian Cashman, submitted a complaint with the MLB commissioner, alleging that the Red Sox were electronically relaying signals from the Yankees' catcher to their players.

The Red Sox training staff members in the dugout were reportedly using an Apple Watch to receive signals, which were then sent to the players. The hand signals of the other team were then sent to the players on the field. Red Sox training staff members acknowledged the misbehaviour throughout the inquiry, and the commissioner received video footage from the YES Network. Many conversations concerning the morality of sign-stealing and the usage of technology in baseball were sparked by this episode. After that, MLB punished the Red Sox for their behaviour and tightened the regulations on using electronics during games.
We learned about checkra1n and checkm8 how they help forensics in investigator in investigation. Both of these are jailbreaking tools that are very valuable when dealing with ios devices especially the ones that were older before iPhone X . Checkm8 is a hardware based exploit can cant be patched always exploited. Checkra1n jailbreaking tool built on the checkm8 exploit. It bypasses iphone security features which includes passcodes and restrictions

Lesson 5 : Weekly Journal

The lecture started with the very foundational knowledge of IOS system and professor explained to the class about the importance of IOS forensics in digital investigation. Professor talked about checkra1n, which is jail breaking tool for IOS devices. And also talked about a feature in IOS devices which almost all class was unaware of, if our phone is restarted or switched off before and turned on, the exact same moment before entering our IOS passcode , we got a call from someone in our contact list but instead of the contact name we will get the contact number only but if we enter our passcode before receiving the call , the we will able to see the saved contact name. this feature in IOS is based on authentication protocols designed for IOS devices security and is responsible for preventing unauthorized access to user sensitive data such as contact database. The IOS devices utilizes the AES(Advanced Encryption Standard) with a 256-bit key for data encryption. As we know 256 bit key is very

secure, but is indeed not practical for everyday use of the users because it is very hard to remember such a long key. Therefore apple allows users to create a shorter passcode for mobile decryption. In apple devices, there are unique identifiers for each file created by APFS(Apple File System) for managing the overall file system on the device. There is a difference between SSID(service set Identifier) and PSK(pre-shared key). SSID is the name of the wireless network whereas PSK is a password that is used in a Wi-Fi network for authentication purposes. Why we need mac address? Physical address or MAC(Media Access Control) address is unique number that is related to a specific device. MAC address is found only in devices that have the ability to connect to the internet. When a device wants to connect to a device in the same network, MAC address helps in differentiating it. Whenever there is a need to send data to another device on same network, ARP(address resolution protocol) binds the IP address to the MAC address and found out the MAC address of the particular device to the destination IP address. Particularly when it comes to cybersecurity and digital forensics, investigators need to know both MAC addresses and IP addresses. IP addresses are essential for more extensive internet-based research, although MAC addresses are more pertinent for local network communications. When combined, they offer a thorough picture of network activity, which is crucial for efficient forensic investigation and incident handling. For a number of reasons, the randomization of Bluetooth MAC addresses in iOS and other operating systems can make investigations more difficult. Investigators find it more difficult to follow a particular device over time and across multiple places when its MAC address is randomised. The shifting MAC addresses might be confusing for an investigator attempting to compile a chronology or track behaviour. The IOS sensors can be a life saver for forensic investigator because it provides movement analysis and investigator can find that weather the device was in motion or rest during a car chase. Health sensors can provide data related to physical activities like heart rate, and that tells the investigator that weather the suspect was excited or resting during a criminal activity. Journaling is a file system feature that keeps track of user files and makes them available to the user in the event of a system crash by restoring the most recent stored copy of the file. Journaling in HFS+ is case-sensitive. Journaling is possible with Window NTFS, however NTFS does not care about case in file names. To put it another way, files xyz.docx and XYZ.docx can coexist in the same directory under NTFS, but not under HFS+ or APFS(apple file system.

Apple file system was developed in 1984 along with the first apple Macintosh. MAC is based on UNIX Operating system and before it was only developed to store files and data on floppy disk drives. Then hierarchical file (HFS) system was introduced in 1985. Then in 1998 apple launches MAC operating system Extended or (HFS)+ that can easily support larger file system. APFS(Apple file system) is the latest file system to be released by apple. APFS is compatible to both Macintosh and IOS and was released in 2017 alongside with Mac OS Sierra. If we upgrade to IOS version 10.3, then APFS is the default system and it will automatically replace the hierarchal file system. MAC OS Sierra installer offer non-destructive upgrades from HFS + to APFS. APFS or apple file system can be found on Watch OS, IOS MAC OS, TV OS. This file system is for flash and solid state drive(SSD) memory which is more capable in increasing read and write speeds. In the most recent years, there has been a sudden increase in utilization of

SSD(solid state drive) or flash drive and all of the sudden there has been a shift from the HDD(Hard drives). Initialization is the term used to formatting a drive in a Mac OS X and can be done using Disk Utility tool which has further 6 more options in the tools section which are as follows: Mac OS extended(Journaled), Mac OS Extended (Journaled, Encrypted), Mac OS Extended(Case-sensitive, Journaled), Mac OS Extended(Case-sensitive, Journaled, Encrypted), ExFAT, MS-DOS (FAT). Intel based Mac devices can run different kind of file system which are NTFS, FAT32, FAT64,(exFAT), EXT3. Intel based Macintosh can run multiple file system at once using Boot camp tool. Mac OS has data fork which stores meta data and application information, resource fork files when place in a different file system for example windows will be unidentified. HFS volume is 65,536. HFS+ was introduced with MAC OS 8.1 in 1998. HFS + has more allocation of disk space. The max is 232 for about 4.3 billion , more block means less wasted space on a volume. file names can contain 255 characters of Unicode. Max file size is 263 bites. HFS+ is a case sensitive file system. For example Jagdeep.file and jagdeep.file are two different files in the APFS file system. NTFS is not a case sensitive device that's why it is advised to use it while examining a MAC or a IOS device. Allocation block is a unit of space which it 512 bytes for a hard drive and a allocation block is a 32 bit number that identifies as a allocation block. Volumes header tells the time and date of creation of a file and the number of files stored in that volumes. Catalog file contains the details of the file for example sequence number, it is structured as a b tree. Catalog ID is a unique number that tells when a new file is created. There is a feature in apple devices , that if a file is deleted , that the catalog ID is deleted, but the number will never be repeated. In short, the NTFS devices don't allow the MFT record identifier to be reused once the file is deleted on a windows PC. There is some feature of the HFS+ file system. The dates and times are the creation of files, even the modified date is stored in the system. If the user tries to duplicate the files, then it is saved that from which original file, the duplicate file is inherited while creation or modification. So, due to this, a digital forensic expert can identity while looking at the files , that which system the files belong to. Alternate data stream is very important topic in forensics. The NTFS allows files to have multiple data streams that can only be visible only by master file table. Hacker can use alternate data stream to hide data. HFS+ maintains a link between the object and its original source. This link can be found in KMD ITEM WHERE ARE FROMs. Core storage displays partition on multiple drives as one drive. Currently fusion drives are not compatible with APFS, but can be in future if apple gives a solution. APFS have 9 quintillion addressable objects compared to 4 billion in HFS +.if we compare HFS+ and APFS, 1 nanosecond is equal to 1 second in HFS+. Before, HFS+ has journaling which has been replaced by copy on writes in APFS. Copy on write is more efficient than journaling in terms of data integrity because it create a clone of files, and only changes to the files, that are made the clone file, checksums are used for the integrity of files metadata. Space sharing feature in APFS can be referred to as APFS container, allowing multiple files systems to share same free space on a physical volume. Snapshot is the backup of APFS backup the deleted data. APFS has strong multi key encryption, which however has a separate key for sensitive metadata. File vault2 uses XTS-AES 128 BIT encryption on the startup disk on the MAC. DMG is a file system in mac OS 10

and can contain many encrypted files in it. A mac is needed to recognize a file vault, core storage, fusion drives, HFS+, APFS file system.
Mobile forensics of IOS contains a logical image and physical image of a mobile device, which is bit per bit copy of the user data. Physical image will tell the investigator the system related files along with the user created files. System files tell when application started , sensor information tells heart rate and footsteps and time timeline of events which is very useful. JTAG helps connect wires with the system and power on circuit board and download data from the device. ISP(in system programming) helps in obtaining a logical image of the IOS device and we can download the user data from the device without takin the chip of printed circuit board. There is many amendments for user to protect their confidential data, which includes fingerprint, faced , Touch ID , password. There so many other government rules that protect the user personal data but we can still access other user data for example call details , cell site location information, iCloud activity, photographs of device, etc, but due to 4rth amendment a warrant is required. Nowadays cars also help investigator in solving a case. For example apple CarPlay and android play can tell the law enforcement about user call logs and location logs. Talking about the iPhone 11 all models, it has a face ID feature, 18 w lighting to USB -c fast charger with a maximum storage capacity of 512 GB. Whereas iPhone 13 has up to 1 tb of space. It come with A 15 bionic chip. Location can be accessed with Wi-Fi network in the iPhone 13 . I beacons feature in iPhone 13 helps the examiner to know about the users location more accurately, in short it's a micro location technology. In IOS 13 user has more option to give location to a specific application, for example there are 4 options namely, never, ask next time, while using app, always. USB restricted mode forced user to re - enter password for iPhone after an iPhone has been disconnected for 1 hour. So investigator use apple lighting cable to prevent this. IOS 15 has share play feature , which allows movies and series on facetime sessions, Ultra-wide band support for car keys helps user to lock and unlock cars. Auto reply feature helps if someone is driving, automated reply will be sent from user iPhone. Health data can be shared. iCloud private relay feature prevent MITM attack due to encrypted medium while browsing in safari. Hide my email feature in latest IOS helps user to hide their real email address. Apple watch inspect users heart rate with the help of optical sensors and light sensitive photodiodes. As we know blood absorbs green light so watch uses green light to detect heart rate of the user.

Lesson 8 : Weekly Journal

The class kicked off with the introduction to android operating system. Professor gave a brief introduction on various android features, and from a forensics point of view, why we need to learn about android. Nowadays, android are in so many things that we use on a regular basis for example smartphones, Tablets, Smartwatches, Televisions, Set-top Boxes, gaming consoles, car infotainment systems, cameras, projectors, POS(point-of-sale) systems. We

revised some important topics from previous lessons, such as timing advance which is used when a base station is receiving signal from 2 different mobile devices, and the one device is a little bit far and other one is close to the tower. Based on the distance between tower and mobile device, timing advance make sure signal reaches to the tower at the right time without any delay in the network service. For the law enforcement during an investigation, physical image of a phone is more important than the logical image due to number of reasons, like for example physical image provide complete copy of the device data and deleted and hidden files, moreover physical image has everything the logical image contains. Physical image capture system files, logs which can provide evidence. Logical image fails to clearly detect malware while doing comprehensive analysis, on the other hand physical image easily detect. There are 1.6 billion android users worldwide. If talk about the statistics of 2021, 72.84 percent of the total mobile operating systems globally were android. There are 51.9 percent of tablets are android. 6.4 billion smartphones subscription are of android. 87 percent of smartphones have android operating system. There are 2.79 million android applications. The most downloaded application of android is Instagram. All this information is very important to know, because, even if in the United States, every third person uses IOS, but the global smartphone users prefer android more over IOS. Samsung galaxy is the top selling smartphone in the world. After 1 month of the release of Samsung galaxy S4, the sales surpassed 10 million units which is equal to 4 units every second. The dual shot feature in the S4 enables user to use both the front and rear camera at the same time simultaneously. Galaxy S5 comes in 2014 with 16 megapixel camera with HD video recording. Comes with fingerprint scanner, and heart rate monitor and KitKat android version 4.2.2. In the year 2019, Samsung galaxy note 10/+ and galaxy fold released. In 2020, galaxy S20 and galaxy Chromebook released. By the year 2021, 19.6 percent of tablets were Samsung globally. Taking about CarPlay's, they are all based on android operating system. The Shanghai Automotive Industry Corporation (SAIC) integrated android 2.1 in the automobile vehicles which includes GPS, Media Player, DVD, etc. Several other automobile companies like ford and Audi start doing this technology in their cars. Nevada Department of vehicles (United States) has approved android for theirs elf driving cars. For the law enforcement, these car entertainment systems that synced with mobile phones, Contacts, calls can be very useful evidence in an investigation. Android auto is a system that is integrated into a vehicle dashboard and run from an android smartphone and supports google voice activation, Google (artificial intelligence). User can put navigations using just the voice and can apply that on google maps and Waze. Driver can also use other applications such as telegram, Webex, and listen to music using supported apps. Driver/user can use cellular features in the car for example making calls and use apps such as skype, webchat , listen to music on Spotify. There are 500 car models that supports android auto. Ovens(kitchen appliance) have android and even other home appliances such as refrigerators like they scans every item inside the refrigerator and set the temperature according to the requirement. There are even Air conditioners , Washing machines and dryers based on android operating system. IOT devices have android in them for example thermostats, artificial intelligence speakers. Android operating system can be found in smart phones and tablets and consumer electronics. Android supported

smartphones can be found on CDMA iDEN, GSM networks. T mobile and AT&T operates on GSM, on the other hand Verizon operates on CDMA. There are some android tablets also that supports cellular capabilities, for example amazon E reader(kindle) and Samsung Galaxy Tablet. Android is an open source operating system which is based on Linux 2.6 Kernel. Google acquired android in the year 2005 and it is managed by OHA(open Handset Alliance). OHA is a joint alliance of telecommunication, semiconductor and software companies. There are some of the early android operating systems, which comes mostly in the 2010,11,12,13. These are Froyo(2.2), Gingerbread(2.3.x), Honeycomb(3.x.x), Ice cream Sandwich(4.0.x), Jellybean(4.1.x), KitKat(4.4). some later versions of android from the year 2014- 2021 are Lollipop(5.0-5.1.1), Marshmallow(6.0-6.0.1), Nougat(7.0-7.1.2), Oreo(8.0-8.1), Pie(9.0), Quince Tart(10.0), Red Velvet Cake(11.0), Snow Cone(12.0). all these android versions support full disk encryption, make digital investigation really tough for the investigators. Even though there are exploits and vulnerabilities to extract user data from the android devices. Android support different kinds of file system which are YAFFS, YAFFS2(Yet another flash file system), EXT3, EXT4, RFS, FAT32, VFAT. YAFFS2 is an open source file system developed to use with NAND flash memory. A forensic analyst can download the YAFFS2 source code and review the files in hex decimals for an investigation. EXT4 is a Linux file system, which is very similar to android. FAT32 file system found on micro SD cards. VFAT is the Linux file system driver for FAT32. YAFFS2. NAND flash memory is a non-volatile and durable storage technology and it can store data without the need of power. It can be found in USB Flash Drives. YAFFS2 supports Ware-Levelling which make sure that all the memory blocks are used evenly over time. Bad Block handling prevents the repetition of bad blocks. Later on, the file system shifted from YAFFS2 to EXT due to number of following reasons, NAND flash replaced by eMMC chips, and EXT is more stable and delivers high performance. YAFFS2 was a single threaded and have issues supporting Dual-Core systems. Talking about the Robust File System(RFS), which is a Samsung FAT File System. It has no object header and no file names. Therefore, Samsung shifted to EXT4 later on. In terms of TEMP File system, tmpfs is the most important in an investigation. This is the copy of RAM and its data is stored in a different chip. Rootfs is responsible for mounting the Root file system at startup. Sysfs is virtual file system. Proc delivers information about Kernal, Processes and configuration. Devpts is responsible for simulated terminal sessions. Cramfs contains compressed ROM file system. We should not just rely on android device itself for mass storage data in an investigation. There so many things that are indirectly related to android which can be used as evidence. For example Micro SD card(FAT file system), eMMC chip, Sim card, are different devices that can be used to obtain evidence. If an android has been connected to a computer than that computer can also be used to obtain evidence. Law enforcement can also send warrants to third parties in an investigation such as google and Facebook. There is no cloud storage in android, unlike in apple device, there is iCloud that can be useful for obtaining backups of contacts, WhatsApp messages, photos and Videos. SD(Secure Digital) Card can be found on some android devices which has FAT32 file system, there can be importance evidence found in this card which can be a photo, video or other Large document files. A write blocker can be used to download data from the SD card. To do this we need to remove SD card from the device and connect it

to investigator computer though a USB slot. The main purpose of using the write blocker is to ensure that the traffic is one way, means we are just downloading data for viewing and reading , and not alter or deleting anything that is already on the card. There is a drawback of using this forensic technique is that some android devices requires a complete switch off for the removal of the SD card. NAND(memory) is type of non-volatile flash memory with High Density means can be used to store large amount of data in a small physical space. Its come with some bad blocks which make some its space unusable from the beginning due to manufacturing. It is susceptible to ware levelling which makes even distribution of write cycles across the memory cells. There are limited overwrites(10,000-100,000). eMMC(Embedded Multimedia Card) is non removable card and has FAT32 file system. There are some digital forensics tools to read the sim card data of an android device for example ,paraben SIM card Seizure, Ultra-Block Forensic Card Reader, Access Data MPE+. In the digital investigation of a crime, Investigator can send subpoenas to third party companies(Facebook, Instagram) to find out when the suspect was logged in at a certain date and time. Warrants can be used also to obtain evidence related to messages, calls, contacts, Pictures and Videos. Investigator needs to prove in court the cause of warrant due to fourth amendment which is search and seizure. Telecommunications companies can also provide a lot of evidence related to the phones calls, text messages, locations, call logs, which towers used when making a call. Logical and Physical ways of user data extraction require hardware and software. There are some mobile forensics software's which helps us to extract just the user data through logical acquisition but cannot extract the system files. To acquire system files, investigator needs the physical image of the device. JTAG using RIFF Box is yet another way of extracting user data bypassing android security and encryption. It is used to acquire the data from the circuit board on the cell phone. NAND memory can be fully Extracted from the eMMC chip by soldering the connector carefully onto the JTAG points on the circuit board. There is a method called Chip off which does not give 100 percent success rate when it comes to successfully obtaining the data because in this method the chip has to be manually removed from the circuit board which demands a lot of skills and tools. This method is also very costly, and still very dangerous because chip can be damaged due to infrared and hot air while removing the chip from the circuit board. after the removal it can be attached to the adaptor to extract data. The last method is ISP (in system programming) which is practice of connecting an eMMC flash memory chip to access files stored on the chip. In this method, instead of removing the chip, we attached that chip with the protruding connections using wires. Some people root their android device to upgrade the operating system, create Wi-Fi hotspot, Eliminate Bloatware(pre-installed applications), Obtain User Files for investigation. ADB (Android Debug Bridge) is a command Line tool which is used to communicate and send requests to the android device from a computer. To do this, phone should be rooted to access image of the device or the user files. To root the device we need to use exploit which can be achieved with a known vulnerability. There is drawback for rooting a device, its changes the file system of the device and an investigator have to explain to the court, that why there are sudden changes occur in the evidence. USB debugging mode must be turned on when we connect an android with a computer. Android emulator is an application that runs android in a virtual machine

likewise oracle virtual box in the PC. It is used to understand the behaviour of the malware by executing it inside the emulator and understand its working. Investigator can also understand the app behaviour related to permissions and DNS connections using the android emulator. The android applications has been developed using java programming language. They have .apk extension and runs in Dalvik virtual machine(DVM) and the applications has a unique User ID and process. This is useful for applications security and helpful in data sharing with other apps. In an investigation, it is very useful because the date and time of app execution is stored on a device. The developer of the application has settled everything already that what data will be available to view and what data will not, which means some data can be encrypted and some can be in plain text. There are 4 kinds of data storage which preference, files, SQLite database, cloud. Data partition involves various types which are Dalvik Cache which are running, applications which are .apk android application package files, data which is subdirectory for each application with SQLite Database, Misc Includes DHCP, Wi-Fi, etc, System involves packages.xml. Android partitions has different categories first one is a boot which includes kernel and round disk associated with boot img. Second is the system partition which contain android framework. Third is recovery which has recovery data. Fourth is cache which stores temporary data. Fifth is Misc is used by the recovery partition. User data contains user installed application and data this one is most important as a forensic prospective. Metadata is used when the device is encrypted. SQLite databases can be great source of evidence for the investigator. SQLite database involves tables(RDMS-relational database management system) which is linked by a unique(primary) key and a foreign key. There are some tools which can be used to view SQLite databases for example SQLite database browser, SQLite Viewer, SQLite Analyzer. The cache. WIFI file contains Wi-Fi evidence. If a user walk past a Wi-Fi access point, regardless of the fact that the user tries to connect to that wifi or not, the information of that access point will be stored in cahche.wifi file and can be used as evidence in digital forensics. Fb.db file contains user Facebook messages, contact, searches and photos. RCS(rich communication services) is a cross-platform messaging standard in the android that is used for sms and mms services in an android. It is also known as chat is an android. Its is similar to whatsapp and imessages in ios. Its is not an app but a protocol and does not support end-to end encryption like the imessage in apple. Wpa_supplicant.conf tells about the SSID network security protocol such as the WPA and WPA2 and the signal strength. Herravad database in com.google.android.gms/databases/herravad can be used to access the SSID and BSSID or access point for MAC address that the user can connected to. Oxygen forensic tool can be helpful study herravad file of an android device and tells us about the SSID and BSSID of each connection and also the Wi-Fi security protocol like the WPA and WPA2, and a timestamp. Wigle.net website can help the law enforcement to locate a certain connection by using its specific SSID and BSSID. Imaging an android device can be done by connected the android device with our computer by turning on the USD Debugging. This can be achieved by using a live exploit to get a root access of the device while it is booted or it can be a dead exploit where phone is Booted into a different mode. To imaging an android device, it is important to have the root access of the device. With the root access to the device data, investigator can run commands to extract user data through the USB connection. There is a

difference between a live and a dead exploit. With a live exploit, Android should be running in real time and evidence does not affected, whereas the dead exploit boot into another mode for example clockwordmod and this can be achieved using tools such cellebrite, which uses bootloader runtime exploit and no code is written to the device. An exploit is actually piece of code that uses a known vulnerability of android to gain root access of the device. Root privilege is important for a full access of the device with zero restrictions. Different android versions have different kinds of exploits. There are 8 main different kind of rooting tools for the android device which are Z4, superoneclick, rageagainstthecage, motofail tool, killingmesoftly, gingerbreak, Psnueter. There are some demerits of rooting an android device, phone cant be normally used after that, there will be a partition added to the device to gain access to the device. Rooting a device will change the system files, means it will not be the same as it was when the suspect stopped using it. The android security can be obtained by Pin protection, password, pattern lock, biometric. The data related to pattern lock can be found in a file called gesture.key. password data can be found in file data/system/pc/key. Password can be cracked using bruteforce. A pin has a maximum of 8 digits. If a user entered wrong pin multiple times, than the android request the user to enter the gmail credential, which is another way of gaining access to a mobile device.

Lesson 9 : Weekly Journal

Cell sites in normal language means base transceiver station(BTS). It contains 2 structures called antenna and tower. Cell sites are mostly fixed to the buildings. Sometimes cell sites are attached to multiple antennas. This also known as distributed antenna system. There is real life example of this term. Sometimes we see a one cell ID with different coordinates(latitude and longitude) associated with that cell site. One cell site can have multiple antennas. Cells on wheels (cows) helps in providing extra bandwidth in a particular location when needed for example at the time of a concert. This is important to know because sometimes we see a specific cell ID is a network and a week later when checked again, it disappears because been moved to someplace else where needed. The is a real life example of distributed antenna system, at an event of a big stadium, there is one cell ID, but there are multiple antennas distributed throughout the arena, so that multiple attendees are not relying on one single antenna.

Graphical representation of a 4G cellular network consist of cells(graphical area) which contains antenna(eNodeB) which represents a base station of a 4G network. Cell contains 3 sectors, each covers 120 degree coverage, in total covers 360 degree coverage. UE stands for user equipment(user cell phone). Cell phone authenticated with cell site and network with the help of two methods IMEI(associated with equipment), IMSI(associated with Sim). Antenna has 3 sectors, sector 1 is called alpha, sector 2 is beta, and sector 3 is Gamma. Azimuth is the direction in which the sector of the antenna is pointing. There are 2 types of cell sites, cell site with sectors and Omnidirectional cell site. Omnidirectional cell site has one

antenna with 360 degree coverage. When we talk about the history of telecommunications technologies. We can start by 1G which was a Analog Communication with voice only system. 2G Global System for Mobile communications(GSM) refer to as GPRS and GSM evolution(EDGE). In 2G we have moved from analog to Digital communication, and it can support SMS and MMS.

Talking about 3G(universal Mobile Telecommunication System(UMTS), 3gpp is also associated with 3G and it set standards for 3G communications. The 3gpp2 set standards for CDMA. CDMA is a telecommunications protocol that is used by Verizon and sprint, whereas AT&T and T mobile uses GSM protocol. IMT-2000 is also associate with 3G, by which users can access internet on there phone and do video calling over the phone. 4G long term evolution(LTE) enables users to do gaming and watch HD videos while moving in a train or moving in a car and it was a lot faster. 5G new radio(NR) is even faster than 4G and 6G is under development. Now 5G is a lot faster as it gives more download speed and lower latency(delay in communication) and it also consumes less energy.

5G will enable the development of smart cities, which is meant these cities will be able to hold greater capacity of users. It is critical of IOT devices, which means any smart refrigerator or a AI speaker. Self- driving vehicles development can also be enhanced with the help of 5G. In United States, the telecommunications companies infrastructure is paid by the telecommunications companies itself and not from the government. So during the time of requesting information from the companies by the law enforcement, the law enforcement pays for that evidence that is not kept in the regular course of business. An example of this is a title 3 wiretap that needs a technician to install. In 5G, we also have Multi-access Edge Computing (MEC) which is move away from centralized networks to edge computing, which means device to device communications. This means that no central hub device communication(telecom) is needed.

Impact of 5G is a lot on automobile companies such as tesla which is vehicle to vehicle communication, which means is when a tesla owner passes another, both cars will exchange data with each other. This is also known as mesh network. We can have self-driving police vehicles also in the future. CTIA also discussed about encrypting the IMSI, which uniquely identifies a user in a network and it's a unique identifier associated with a sim Card. Future of stingrays is also impacted by 5G. stingrays is a device that is used to identify wanted criminals by giving information about the IMSI of the user. We have the Mobile connect which is based on subscriber single sign-on(SSO). In this user don't have to log into multiple websites and applications one by one and can do it altogether by one Sign On feature. General Packet Radio Service(GPRS) was widely used in the year 2000 with 2G Mobile networks. It is a packet switching protocol for wireless and cellular communication. Its on a best effort basis. Its connectionless and packet could be sent out of sequence but it is faster that way. It was standardized by the 3rd generation partnership project (3ggp). So there is one important thing from forensics perspective, which is while a Mobile station(user handset) is connected to a Base Transceiver station(BTS){tower}. It is not the closest tower by physical distance that the phone is connected to, instead it is that which tower gives the highest performance in terms of internet speed. Due to this while we change a protocol while using our phone, the tower

also changes. For example I am texting somebody and my phone is using a tower is providing a speed required to text someone. I immediately changed my mind and start watching a Video on YouTube, this will affect the internet usage and the tower my handset was using may not be good enough to provide me a better connection for a different protocol. So it's my phone who decides which tower to use. So my phone will use a different tower when I am watching a video and use different when I am texting someone. The cellular communications are FDX which means full duplex communication which also means simultaneous communication in both directions. For example, if I am using Netflix and watching a movie on that, my phone is getting a downlink which is coming through the antenna to my phone. An example of uplink is when I want to send something to the icloud server. It will go through the users handset up to the antenna of the tower and all the way to the icloud network. There is MCC(Mobile country code) in every country, for united states its 310. Each BTS has a global cell ID which also refer to as a call detail records from a provider as GCI or eCGI. Cell ID is a globally unique for a particular cell site. Cellular providers in United states are AT&T, T-Mobile, Sprint, Verizon and US cellular, and they actually own the telecommunication infrastructure. MVNOs (Mobile virtual network operators) buy minutes of use from those mobile networks operators. Cricket, Mint Mobile and H2O wireless will use the networks that are owned by one the big companies and mobile network operators.

When a suspect mobile seized, there is a lot of information that we get. But if the law enforcement don't have the mobile, still can get a lot of information by filling a subpoena and warrant to the telecommunication companies. What are the types of evidence can law enforcement get. They can get subscriber records which is information about the particular user related to its phone number, name, address, social security number, credit card information. Credit report of the user can also be available on request. Call detail records like regular phone calls, SMS, MMS , or internet communications, toll records includes records that are accessed by different providers like a Verizon customer calling a T-Mobile. Propagation maps includes GPS information of the device. Cell companies maintains all these records related to GPS data. Tower dumps includes records related to calls and internet activity. It is called cell dump in UK. Ping data gives real time relative location of the individual device for example a abducted child and law enforcement wants to locate the child.so the pings are basically sending a signal to get an approximate location of a certain device. Pen register trap and trace refer to monitoring incoming outgoing calls to particular device. It does not include content , just number called by the device and incoming calls. Title 3 (wire trap) is very difficult for law enforcements to get. It is basically helps law enforcement to listen to ongoing calls communication in real time. PIN unblocking key PUK which helps in unlocking the SIM. PUK can be requested in a situation where suspect is not sharing the key, so a default key can be asked from the company. Law enforcement can request voicemail reset and cell site identifiers(history of cell site location information). cell site identifiers are important because call detail records are for a particular day and that particular day can be clashed with a special event that demands cells on wheels. So historical data of the cell sites is very important in an investigation.

Law enforcement by using ping request can get an email every 15mins about the approximate location of the device. Per call measurement data (PCMD) also known as true call and NELOS. Basically telecommunication companies stores location information about the device at a particular time when a phone call was made. Tower dumps can be requested, which is a download data related to a certain antenna. An law enforcement can request all companies to give tower dumps for a specific antenna because suspect can be a customer of anyone , it can AT&T and it can be Verizon. It information can be requested for a specific sector. When we talk about data related to Tower coverage, it is different for different companies, cell site location and azimuth data is provided by all companies, Sprint, T-Mobile, AT&T and Verizon. Antenna height and antenna beamwidth is only provided by T-Mobile and AT&T. Verizon provides Antenna Beamwidth.

Available resources for cell site analysis are Numbering plans, FreeCarrierLookUP.com, OpenCellIDm, AntennaSearch, BatchGeo, fonefinder, GSM arena, spydialer and Point 2 point. Batchgeo ask latitude and longitude and tell the location. Numbering plans tells the telecommunications company related to a specific phone number and device. Freecarrierlookupservice ask the phone number and tell the service provider name. antenna searches tell the cell sites location in a particular area. IMEI can be access by enter *#06#. Field test mode can be done by pressing 3001#12345#* and tell what cell tower the user is connected to. Then there is option called serving cell info, after clicking that, we get PLMN(public land mobile network), band info, bandwidth, cell ID. Cell ID identifies the antenna the user is connected to. Let's learn with example, MCC(Mobile country code) and MNC(mobile network code) is 310 480. 310 is united states and 480 is wave runner LLC. A cell ID 21775372 when typed in a website which tells network type which is LTE 4G, we get hex of the cell ID, eNB ID which tells it's a 4G tower. Sector ID talks about the sector related to a particular antenna. PCI (physical cell identity) is assigned to each cell in a network, TAC (tracking area code) is a geographic location, EARFCN DL (E-ULTRA Absolute Radio Frequency Channel Number) DL (Down) used to specify the frequency channel for the downlink(DL) communication between the tower and the mobile.

Lesson 10 : Weekly Journal

In the lecture 10 of Mobile security, Professor discussed about preventive measures to protect our mobile phone from a cyber-attack. For example not picking unknown calls, make strong pass key, don't install apps from unknown sources, don't always enable Bluetooth connectivity, don't connect to public networks and Wi-Fi . We were discussing if attacker has physical access of a mobile device of the victim and it is locked how can the data be accessed information from the phone even if the phone is locked.

Bluesnarfing is known as the unauthorized access over the Bluetooth data, this data includes, calendar, contracts, etc. to perform this attack, the threat actor need to be physically close to the victim device. The users phone also needs to be in discoverable mode, which means it

should Bluetooth enabled already. Bluebugging is yet another attack similar to Bluesnarfing, in this also hacker needs physically close to the device. This attack enables the attacker to access all the features of the users phone. Blue jacking is another Bluetooth attack, which allows the hacker to send unsolicited messages to victims device.

According to Kaspersky, in the second half of 2021, there were 900000 installation packages of malware. Out of these malware packages, 24604 were mobile banking trojans. 3623 packages were mobile ransomware trojans. Google play protect application is a mobile application that is developed to detect malware on google play. Most targeted countries for mobile malware attacks are Iran, Saudi Arabia and China.

Scareware can be on the mobile device or the computer which show up as a banner. It's like an advertisement that alert the user, saying there is a malware on the users device, but there really isn't. Jesta Digital is the company that creates scareware where a user playing angry birds and a virus scan advertisement shows up over the phone. A 9.99 monthly bill was sent to consumers for ringtones and mobile content. This whole process was carried out by wireless access protocol(WAP) billing. Later on, the FTC(federal trade commissioner) filed charges against the company in 2013 and the company agrees to refund the 1.2 million fines for scamming the consumers.

There are premium SMS services that make people scammed easily. Some of these involved SMS messages sent to the mobile with fake claims of giving free gift cards of Walmart, Target, and Best buy. When the folks clicks on the link, it automatically subscribe them to some kind of premium service. Later on these companies got legal charges for exporting unsolicited scammed SMS messages send to there devices. There is one more case which involved superior affiliate management, which claims to the users/victims to give free 1000 dollars Walmart gift card. Its start with a link that user clicks, which redirected towards several websites. Websites asks users personal information. After users gives their information, they automatically get charged 9.99 monthly fees. Consumer asked to pay for different weight loss products. The goal of these premium SMS services is to charge for services reward for click through and commission on sales. So what was happening is every time a user clicks on the link, they made a commission and earned millions with that.

Symbian is a outdated discontinued mobile operating system that used to be found on variety of different mobile devices including Nokia company mobile devices. So there is a Symbian based malware known as metal gear solid which disables the antivirus from users device. Cabir virus is another malware which is actually a computer worm, developed in 2004 and spreads through Bluetooth. It can also spread to a different device from one another through a Bluetooth channel. Mobile games can also help hackers to spread malware. there is angry bird Rio unlocker, which is the widely downloaded malware with a clickjacking of 60000 every day, which makes 20 million revenue every day. This malware tells users that it will unlock a certain level of angry bird, which was actually a malware. The deadliest type of malwares are mobile banking malwares for example ZitMo (Zeus-in-the-mobile) is a HTML injection that manipulates bank websites. It asks the user to install a security app which helps it to intercept any legitimate SMS from the bank and gains account access of the users by doing so.

Malware is also sometimes politically motivated. There was a malware that targets Saudi Arabian women defying driving ban. Its basically an android app resembles as a support app for women. Once installed and user plugged in the headphones and plays a YouTube video, a bob Marley song get played which is no women, no drive. While this song continues to play, its impossible to listen to audio or make a phone call. It basically steals users phone contacts. There are a lot of Android antivirus protection program, such as Bitdefender, Norton, McAfee, TrendMicro, AVG, Avira, Avast, ESET and F-Secure. all these are specially for android because android is most susceptible to malware and the reason for this it is always depending on the manufacturer to push out new updates to the users, and sometimes the manufacturer didn't quite push every android update to the user. Sometimes the android device itself get out of date and can't get updated, meaning the hardware don't support the software anymore. This is reason, some android devices still gets vulnerable to such kind of attacks. Many android mobile application developers uses libraries from other developers. If anyone of these libraries have malware, then that malware will affect multiple applications. Google uses google play protect to detect malware on google play. Handset Manufacturers control patches and upgrades and oftentimes they make delays in pushing these upgrades to the users. Android does have an inbuild malware scanner in the system.

Smishing is yet another type of mobile malware attack in which malware enter the users device through text message or through SMS. Smishing attack sometimes can also involve installing Photoviewer.apk. This app once installed sends SMS to everyone is the contact list of the users device, by this they make money by the clicking on advertisements. This whole process is carried out by sending parameter from a remote server, which means they can change the malware over time. There is way to get rid of this malware, this can be done by installing F-Secure Mobile Security application. A DHL notification is being sent to android device of the user through text message. Once malware spreads in the device, it steals users Phone number, Model, IMEI(information related to handset), IMSI(information related to SIM). An SMS sent from the remote server make the attack successful. This whole attack is based on stealing users contact information.

Eurecom is the group of French Researchers who experiments on Man in the attack which occur in the SSL(Secure Socket Layer) traffic. The researcher were actually examining 2000 different android applications. While they were experimenting, they found out that 1710 of these apps were connected to 250000 URLs. In fact, many of these URLs are associated with malware domains. There are applications called Geotagged Apps which located users geolocations. Some of examples are Creepy, local scope.

There is an application called Brightest Flashlight which is an application that make up rethink and compare different kinds of permissions we gave to the mobile applications. Its makes users phone into a flashlight. It also makes the user to assign different permissions over the device. It gives the brightest flashlight the ability to write to the external storage. For example, if we connect our android device with the computer, the application in android can actually write files over the computer. Its has access to the Wi-Fi networks, that user connected to or walked past. It has access to users locations information through cell sites and Wi-Fi. It can

open, close or disable status bar and its icons, read phone state, access users camera, open network sockets, access location based on GPS and access the flashlight.

Pegasus was a high profile malware developed for the iPhone, it is basically a spyware that was developed by the NSO group for spying over Palestinians. It was also used to spy on Dubai Princess's lawyers during child custody battle. A recent ruling state that Facebook can now pursue a case against NSO because the software also monitors WhatsApp messages. It is also a fact that NSO licence is being purchased by many governments and they use it to spy on investigative journalists and Imperilled the lives of some journalists. Apple launches a new IOS version 14.8 to protect apple iPhones and iPads from Pegasus Spyware.

There is an application called Vaulty Stocks which is seemed to be an application delivering information related to stocks but can actually used to send text messages. There are also some calculator app that is being used for messaging. Who touched my phone app works as a security app which take picture of the person every time someone picks up the iPhone. Key me is an app that allows user to scan a key and enable us to send request to a locksmith in close proximity to the user. For example it can take picture of your key send it to locksmith to create a duplicate key which can be further used to breach you personal security. Flexispy is yet another harmful application that can work in stealth mode(means no icon available after being installed by someone) and keep spying on the users device by listening to the users phone calls and read emails and chats. It is a felony to install this application on anyone's device.

Many companies uses MDM (Mobile Device Management) and here is the list of its products, Apple configurator used to control all apple devices. Jamf pro is used to remotely lock and sends messages to the thief in case of stolen phone emergency. Rippling, Microsoft endpoint manager, Ivanti unified endpoint manager and IBM MaaS360 are other products of MDM. MDM is not like antivirus or security related products but are more like controlling devices products. (dating app)Tinder application is not a secure app in terms of users privacy. It can connect to users Spotify profile, Instagram and has a deep linking ability to connect to multiple applications and access data. What is more horrifying is when a user swipe left in tinder app to different user, all the information related to Spotify playlist and Instagram(private account too) has been sent to the user. This person does not exit .com is website that creates fake pictures of persons that does not exist.

TikTok is a threat to national security, its Headquarters are in Beijing. It monitors User Location through GPS, Wi-Fi and cell sites. Its can read contacts. It has system level privilege to the device and can install malware over the device. It can view US government applications running on users device. It has poor encryption standards, mostly in plaintext. Launcher permissions are scary because it allows the developer to access the device photos, reads SMS, text messages, ability to make calls, send/receive messages and can install files all of these without the users permission and can also activate device camera. The main concern about the TikTok is the facial recognition. Chinese police use facial recognition glasses, that was also used in Hong Kong protest. It is also used in recognizing ID and passports in Hong Kong. The Safran Identity and Security company(French company) is the same company that works with the US government state department. This company works on making projects where facial

recognition is widely used. There are over 200 million CCTV cameras in China. Facial is used to access public transport in China, for example if someone in China want to use public transportation, then has to scan the face before using it. In Uyghurs in Xinjiang, China are identified using facial recognition and then being sent to re-education centres. The smart glasses that used by Chinese police to identity criminals using Facial recognition are Banned in Europe for the general public because of the GDP(general data protection regulation) law. The biggest breach of the century related to TikTok is OPM(office of personnel management) breach where 20 million government Employees personal data Compromised. FaceApp of Russia has some similar features of TikTok.

We can conclude that older cell phones are more secure as compared to modern ones. It is good to disable location services for most of the apps in the device. It is a fact that a hacker can alter or change Caller ID and Email Sender Name. A user should not click the links in the email or the text message. iPhone is more secure than android because of the fact that iPhone is maintained by one single company called apple whereas android have multiple manufacturers, and sometimes they make delays in pushing important updates to the users.

Lesson 11 : Weekly Journal

In the lesson 11 lecture, we learned about mobile apps files, mobile apps for terrorism, Static vs Dynamic analysis, Tinder and Uber. The apps in IOS has IPA extension built with Xcode and only a developer can test these apps. These are an app called test flight where user can find the beta version of an individual application. We have /private/var/mobile/applications directory in mobile which have application folder, which includes further different folders such as documents, library, application code, TMP. The library folder contains all important user data such as cache, cookies. All the data in these folders can be in plaintext or encrypted and depends on the manufacturer of the device decide that the data should be plaintext or cyphertext.

APK is the android application package file and can be developed by using Kotlin, Java, C++, C# and Python. To get different android Emulators, there is SDK(android software development kit). Android manifest.xml is very important file which tells names, functionality, permissions and hardware/software requirements of the application. As an investigator it is very important to know about this, because by viewing this xml file, we can know weather the application can alter information on different device or no, and it can be done by default by the developer. For example if we connect our mobile phone with computer, the files on the computer can be altered by the phone using that app. SQLite database is relational database in android and IOS comprised of number of tables and have small footprint, means a lot of storage. Name of tinder SQLite database is tinder2sqlite, we can download number of SQLite databases for free. The android manifest .xml can tell location information about the user, its includes access_coarse_location, access_fine_location, access_network_state, access_wifi_state. It use Wi-Fi access points, cell site data and GPS to detect users location.

Telegram is an application that is widely used by right extremist groups and terrorist organisations for spreading photos and videos related to lone wolf attacks and how to make bombs and other disturbing things. It is majorly used by ISIS group and some organisations even use this to teach hacking. There are some Islamic states channels that promote violence and There are some telegram channels in which people ask horrible advice on unnecessary things for example, a person asking advice from other people by telling his sister do party in night clubs and don't live Islamic traditional lifestyle. There are lot of photos and videos on telegram that resembles Islamic states propaganda.

LinkedIn SQLite file is LinkedIn. SQLite and file associated with the IOS version of LinkedIn is com.linkedin.LinkedIn.plist. if you have LinkedIn app, as an investigator, we can view a lot of information such as connections, profile, invitations, messages and notifications in the SQLite database of the LinkedIn app.

Performing a static and dynamic analysis of Tinder, Bumble and Grindr is really important to understand the real working of the app. Grindr app is under investigation in Europe because there were a lot of cases where a someone swipe to go on data an later on get raped or murdered. Static analysis is actually reverse engineering the code in the APK file and examining the SQLite database to see the information related to the app permissions in the manifest. Dynamic analysis of the mobile app is running the mobile app and looking for the DNS connections. This can be done by using tools like Wireshark. Dynamic analysis also tells us about the type of data that is being sent to third parties. There is thing called deep linking with social media accounts where someone use a credential of there social media accounts for logging into different kind of service. For example, the tinder account can be linked to Spotify or Instagram.

While performing the static analysis is necessary to reverse engineer the APK and IOS app File. This can be done by using dex2jar, File Viewer Plus. This whole process will allow us to view permission manifest file. We can image the mobile device and look at the SQLite database using different number of different tools such as Cellebrite.

Dynamic analysis is actually the process of looking at the wireless communications between the mobile app and other servers around the world, such as DNS connection and http requests. Debookee is tool on mac which allows user to do MITM attack successfully, where user can decrypt the data in motion and found out, what information is being shared with the third party. Once we get information related to a app company privacy policies and EULA using this tool, we can see if the company is violating any rules or not.

Tinder has been used for human Trafficking and has deep linking with Instagram, Facebook and Spotify. Matches suggestions based on location of the users. In tinder there is a concept of swipes, if a person swipe left to a profile than it is a dislike. Swipe right means liking a profile. If someone do a swipe up, then that means it is a super like and a notification is being sent to other user and if other user do the same then a connection is being made. User can also block other users. It is available is android and IOS and people can use this to chat and text messages only and not for calling. It has 57 Million users and is available in 190 Countries with 40 different language options. 50 percent of the tinder users active after 9 pm and login 4 times a day, with core base of 18-14 age group. The company that owns tinder is match

group revenue with a net worth of 1.3 billion in 2017. The individual revenue created by tinder in 2018 was 800 million. 95 percent of tinder users meet their matches within 1 week. Average male message is 12 characters long, whereas 122 characters for women. It someone has a connection on tinder, then the user can view other connected person Spotify playlist and Instagram account. In the Tinder2.sqlite, there is location data stored locally in plaintext. There is information related to link with the Instagram account. Tinder have connection with Taplytics which is a third party company works with tinder to collect users birthday, city, country, data provider, gender, language, location, radius, device model, IOS version, UID and age. Crashlytics monitor app crashes. in tinder we can view incoming conversations in plaintext. As an investigator we can see pictures, conversations very easily, nothing is encrypted.

Grindr is yet another app which has unsecured communications, has different services such as Smaato which records users location, gender, device type. Octopus-X which records IP Address for the user.

Advertising ID is the common ID used for all social media applications such as Facebook, Instagram, and WhatsApp. We can change this ID manually and also ask apps not to track us to improve our security. This advertising ID can tell law enforcement about the location information of a particular suspect.

Talking about uber, we know some apps tell a person location information but it can even tell which kind of building the user in residing, whether it's a private building or government building.

Lesson 12 : Weekly Journal

This lesson is the basic introduction of united states legal system, congressional Legislation(related to digital forensics), Landmark Decisions of supreme court, Legal Requests, Available Evidence.

US Telecommunications Industry Funds Its own infrastructure, for example, In the US, the development of 5G technology and telecommunications are handled by the companies itself which is not the case in other countries such as Unites Kingdom, where government provide funds to the telecommunications companies. In the US, telecommunications companies needs to remove Chinese telecommunications equipment's, which is enforced by the trump administration and continued by the Biden administration. In 2019 Chinese telecommunications infrastructure were banned for the use of federal agencies. In 2020, the federal communications commissioner(FCC) formally designated Huawei and ZTE a threat to national security. This whole thing bars US firms from tapping an 8.3 billion dollar government funds to purchase equipment from these companies. The FCC says, they will be Eligible for reimbursements of 1.6 billion dollars to replace Chinese telecommunications equipment's. the US government was funding the telecommunication companies, In case if they purchased a equipment of China recently and wants to get a new equipment from a trusted source. It is a known fact that telecommunication companies only charge Law enforcement for certain

requests. They have a pricing list specially for the Law Enforcement for certain types of information. Encryption means that Wiretaps are less Effective for law enforcement in getting information about a particular case.

US legal system is found in common law and English Law and is based on case and precedent and with laws derived from court decision decisions with precedent court decisions are binding on future decisions in a particular jurisdiction. Similarly, these laws are not derived from the legislation, but are based on court decisions. There is only one exception for this, which is Louisiana where legal system was based on Napoleonic Code. There are total of three bodies of law exist in the United States, which is Constitutional, Statutory and regulatory law. Statutory law is written law set forth by a legislature at the national, state or local level and are also codified and uncodified laws in statutory law. Codified laws are statutes that are organized by subject matter for example Regulatory law governs the activities of government administrative agencies. This body of law involves tribunals, commissions and boards that are responsible for decision making. The taxation, environment and international trade gets highly affected. both civil and criminal trials can take place in either federal or in state court Jurisdiction does play a role in determining where a case is tried. For example, a criminal case that straddles multiple jurisdictions may end up in federal court, generally more serious crimes, including terrorism, cases will be tried in federal court. Cases that relate to the US constitution will be tried in federal court. An example of this would be a case that relates to freedom of speech, which is protected under the First Amendment to the US Constitution. the federal Wiretap Act of 1968 which is commonly referred to as Title Three. Detailing how law enforcement is prohibited from using a wiretap without permission from a judge. In fact, law enforcement can be penalized for any unauthorized use of a wiretap. A wiretap is authorized by the Department of Justice, signed off by the US District Court or court appeals judge and is valid for up to 30 days.

Under title 18 of the US constitution, section 2511, service carriers may, on occasion, monitor and intercept communications to combat fraud or theft of service. The Federal Wiretap Act has been amended several times to account for changes in technology.

The Electronic Communications Privacy Act of 1986 or ECPA, was developed to extend the restrictions placed on law enforcement by the Federal Wiretap Act. This act extend the wiretap act to include electronic data transmitted by a computer from merely including telephone intercepts. as part of the ECPA Congress included the Stored Communications Act or SCA when An individual uses an Internet service provider or ISP or an electronic mail service provider, there are no protections under the Fourth Amendment.

The Communications Assistance for Law Enforcement Act was introduced in 1994 during the Clinton Administration. This Act was introduced to facilitate electronic surveillance requests by government agencies, electronic surveillance refers to call identifying information, including origin, direction, destination or termination of a communication generated or received by the surveyed subject and the interception of the communications content. While this act was enacted, congress nearly spend 500 million to the telecommunication carrier compliance to ensure the successful implementation of CALEA. As part of this agreement, the attorney general would reimburse telecommunications companies for costs associated with

equipment modification and services installed prior to the first of January 1995. from February 1995 onwards, the management was delegated to the Federal Bureau of Investigation, or FBI. Cisco has published a lawful intercept Configuration Guide, which outlines the schematics for communications interceptions by law enforcement under CALEA. CALEA is very problematic For law enforcement who are looking to find information from communications apps such as WhatsApp, Telegram, signal and other communications apps, which include strong encryption. CALEA mandates that telecommunications companies support law enforcement intercepts, they do not specify the architecture or the technical solution for that, for facilitating that intercept from law enforcement.

The USA Patriot act in section 201 says provides the government with the authority to intercept wire, oral and electronic communications that relate to terrorism investigations, law enforcement must, however, apply for a court order and establish probable cause. Section 202 states that law enforcement have the authority to intercept voice communications in computer hacking investigations which was before not possible due to the Computer Fraud and Abuse Act. Section 210 broadens the amount of personal information that a government agent has access to with The use of a subpoena. Subsection 2703 c2 includes records of session times and durations, as well as any temporarily assigned network address. 210 also makes agents to obtain credit card and bank information for internet users which was previously unavailable without a subpoena. This is helpful in a condition where a user who used a false identity but a real credit card can now be identified without the use of a warrant. The USA Freedom Act was written into law in 2015 which imposed restrictions on telecommunications metadata on US citizens, metadata that was made available to intelligence agencies, including the National Security Agency or NSA. additionally, call detail records provision was added to FISA. FISA is the Foreign Intelligence Surveillance Act, and this was done via the USA Freedom Act. The USA Freedom Act includes a provision for roving wiretaps and tracking lone wolf terrorists. The roving wiretap access to business records and lone wolf provisions have been part of FISA for more than a decade, according to the Michael J Orlando, Deputy Assistant Director of the FBI between 2015 and 2018, on average, the government sought and obtained records under this provision less than 76 times per year. So in terms of telecommunications data or information related to an investigation, the investigator has to make three types of determinations. First, determine the type of investigation. Second, determine the type of records that are required for that investigation. And third, then determine the legal requirements to obtain the records that are required for a particular investigation.

The first piece of data that we're going to talk about are call detail records or CDRs. They relate to a mobile phone, and they include telephone numbers both outgoing and incoming, the duration of a call, the date and time of that call, and often a cell site code, which refers to a particular identifier for a cell site, meaning, like a cell tower, or if it's an urban area, a cell antenna. The legal requirement for obtaining this information is a subpoena, and the person who approves this is a judge. This is geodata that relates to the location of a mobile phone when a call was made, and this will include a code for that cell site, as well as the longitude and latitude for the location of that cell site, meaning cell tower. The legal requirement for

this is a warrant, which has only changed recently because of a landmark Supreme Court decision, and a judge is required and obviously probable cause, because a warrant is required, and this is subject to fourth amendment, and then we have subscriber data or subscriber information. . It includes the name, the address, credit card number of the subscriber. social security number for running a background check and a credit report and invoices or billing information for that subscriber. there's probably been a credit report that has been run on you by the telecommunications company. So to obtain the subscriber data, law enforcement does need to have a subpoena, which is approved by a judge.

Let’s talk about the carpenter versus the United States in 2018. a five to four Supreme Court decision authored by Chief Justice Roberts stated that when government obtains historical cell phone records that contain cell site location information without a warrant, then They are violating the Fourth Amendment. Call detail records only require a Subpoena(not requiring of giving probable cause). Let’s talk about a case. This case cantered on armed robberies at a Radio Shack shop and a T Mobile store in Michigan, the four thieves were caught and arrested. The FBI obtained call logs from one of the robbers, which ultimately included call logs from Timothy Carpenter, who was the petitioner in this case, and who was not initially viewed as a suspect. Historical cell site information, location information, or CLSI, data tracked carpenter for 127 days, on average, 101 data points per day. whereby concerns were raised about continuous GPS tracking without a warrant. Cell site location information (CSLI) can track a person's movements over time, raising significant privacy concerns greater than GPS monitoring due to its near-perfect surveillance capabilities and long retention policies. Despite a Supreme Court ruling requiring warrants for CSLI data, the Sixth Circuit upheld Carpenter's 116-year sentence, ruling that the FBI's collection of this data was lawful and exempt from the exclusionary rule, which typically bars evidence obtained without a warrant.

Riley versus California case tells that Riley was stopped for a traffic violation which led to an arrest based on weapon charges. Police officer searched riley mobile phone and found a term related to a street band. After this incident, supreme court made it clear, that a warrantless search of a cell phone leads to a arrest is illegal.

The law enforcement get some new rules for the warrantless search, with the first thing is consent and the second is exigent circumstances, which means that if the law enforcement finds out that the search is very important and can prevent a terrorist attack or saves somebodies life. Third is plain view which means if a car is pulled over and there is something that can be viewed from plain sight, such as a drugs or alcohol. In this scenario a search can be conducted. Fourth is border search, for example if someone about the enter the united states and is officially not entered. Then a search can be conducted. Court order issued by court and is a lot easier to obtained than a warrant because there is no need to show the probable cause. Subpoena is a type of court order that demands a person to testify or bring evidence to court. A search warrant is court order which tells law enforcement to search a person or a place. Wiretap is most difficult to obtain. It is generally reviewed by a lot of judges.

In the Telecom Data, Subscriber information includes can be obtained by the law enforcement which includes, credit card information, social security number, we have call detail record both outgoing and incoming calls, cell tower locations, range of tower(distance of the user from a

tower while making a call), SMS content. All these things can be obtained. Law enforcement can get the call type, call start time, duration, calling number, called number, first cell ID, last cell ID. Cell Hawk tool can tell where subscriber was in term of location when they made a call.

Targeted equipment interference states that a telecommunication company will actually install a device to obtain certain types of requests asked by the law enforcement and they do get charged for it. Pen register is a device that records telephone numbers called from a specific telephone line. Trap and trace device tells the numbers dialled into specific telephone number(incoming calls). Electronic communication privacy act(ECPA) exist a 2703(d) order which compels the provider to disclose more detailed records of the subscriber use of their services. IMSI catcher/StingRay is also used by law enforcement and also by FBI.

We can conclude apple is less supportive to Law enforcement because they says the password related encryption keys(256 bit key) are locally located in the users device and they their database have no information about that. A subpoena can give access the law enforcement information related to users iCloud which is privacy concern.