WEATHERED SECURITY LLC

2023 Course Catalog

COURSE INFORMATION

All courses are updated every 90 days. Payment terms and conditions are presented in contract or purchase order agreements. Credit Card payments may require an additional transaction fee!

Basic Signature Awareness (BSA) Course

- No prerequisite required
- 5 days

The Basic Signature Course has two purposes; make clients aware of how they can be electronically hunted and targeted by Nation States, terrorist and criminal elements and how to mitigate and counter these efforts. Cadre will give classes and live practical demonstrations on techniques to familiarize students with electronic signature relating to the conduct of surveillance, counter-surveillance, and intelligence operations in conjunction with electronic device/digital-hygiene relating to the daily use of personal/operational electronic devices, wireless networks, vehicles and the Internet. Students will be shown the latest commercial-off-the-shelf (COTS) hardware and software available to the adversary that would expose the electronic signature of surveillance/counter-surveillance teams and LE/military/intelligence operators. In addition, students will be shown the latest commercial-off-the-shelf (COTS) hardware and software available to allow them to encrypt, mask and secure communications and operational activities while using COTS electronic devices during the conduct of operations at home and abroad. Students will be exposed to open source software capable of conducting link-analyses of social media that allows hostile elements the ability to identify, surveil, and conduct hostile actions against the students and/or their families. Students will be shown countermeasures and given guidelines for the safe usage of social media and will be given proper protocols for use of both personal and government electronic devices while travelling overseas. Demonstrations of vehicle forensic equipment and software will be used to expose gaps in digital security when in vehicles. Students will be exposed to live demonstrations of software define radio's and Infrared exploits that are being used by hostile forces. At the conclusion of this UNCLASSIFIED 3-day course, participants will be able to:

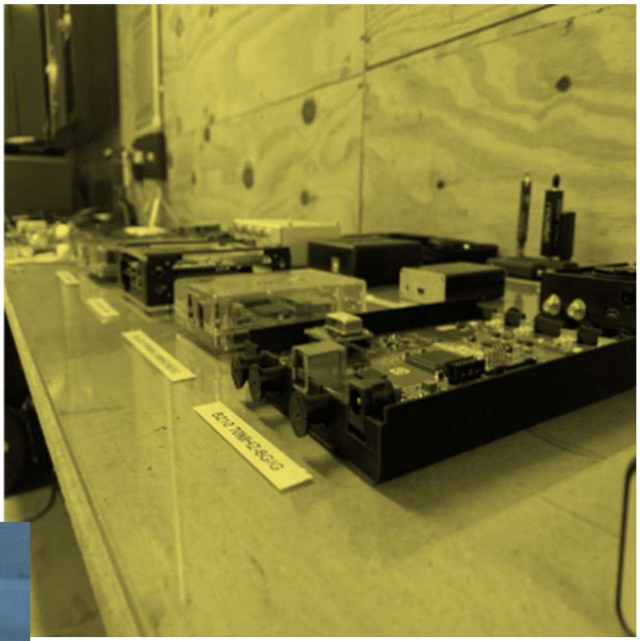
Weathered Security Course Book - Data-Blockers for safely charging their equipment in public.

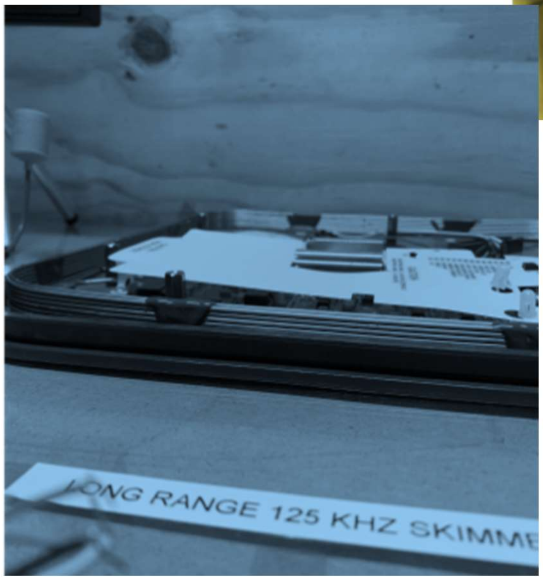
*********Option to have Weathered Security set-up VPN accounts for students. (If this is requested it will require a price adjustment to the course. *********

Digital Operators Course (DOC)

- No prerequisite required
- 5 days

The Digital Operator Course is designed to enhance the capability of participants to protect themselves against digital and electric threats from Nation States, Partner Forces and rouge actors. Participants receive practical demonstrations of techniques being used to target personnel exploiting their electronic, digital and light signatures while conducting operations. This includes cyber-hygiene and vulnerability relating to the daily use of personal /government electronic devices, wireless networks, passports, building access cards, infrared devices, navigation and communication equipment. Students will be shown the latest commercial-off-the-shelf (COTS) hardware and software globally available to an adversary that would exploit the signatures of personnel and adversely affect the mission. Participants will be shown open source techniques capable of conducting link-analysis exposing military members, families and host nation personnel, which facilitates an adversary's ability to identify, surveil, and conduct nefarious actions. Personnel will be shown recommended tactics, techniques and procedures for use of both personal and government electronic devices while travelling overseas. Students will conduct practical exercises in social media evaluations demonstrating vulnerabilities of personal and unit information available on the internet. Will be exposed to techniques that allow recognition of threat profiles in common mobile devices and government equipment.

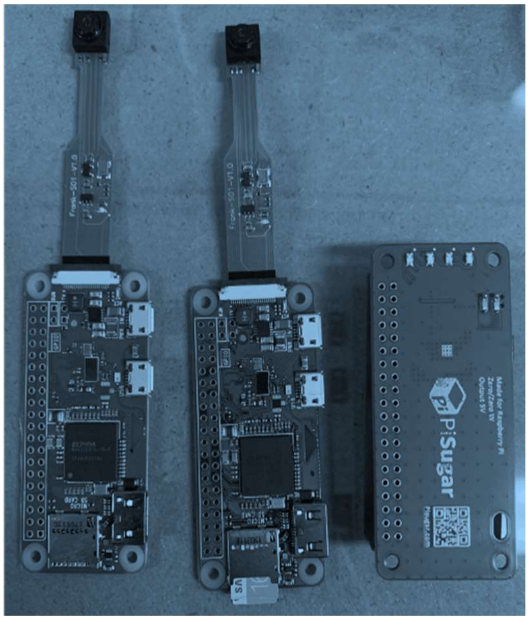




Electronic Signature: Risks of exploitable signature of personal electronic devices
Software defined Radio: RTL-SDR's, Hackrf, Industrial SDR's
RFID Skimmers: Description and live demos of protecting against known exploits
IT Security: Defense against day-to-day electronic threats -
Vehicle electronic systems: Description of vehicle computer systems with demonstration of information left behind by users

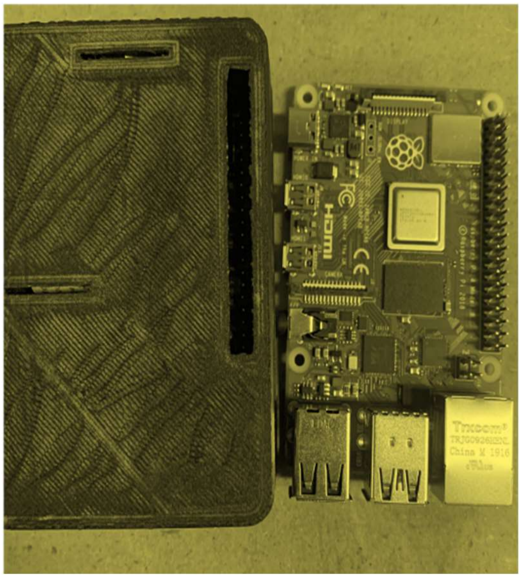
Advanced PI Exploitation (APEX) Course

- No prerequisite required
- 5 days



The APEX course is designed to give students the ability to create their own sensors and electronic detection equipment. Students will learn advanced techniques for using Linux and Raspberry Pi's to monitor organic and adversary electronic communications.

Students will create Microprocessor systems that will monitor Wi-Fi, Bluetooth, Nordic technology. Students will also create force protection systems to monitor movements around operational locations. These systems will also have the ability to feed camera data to an operator. Students will have practical exercises to triggers systems with both wireless signatures and environmental changes. Use common items found in homes and hotels to communicate in unique ways. This course will give students the ability to create open source operating systems assessable on any laptop or microprocessor for experimentation and creation of Software Defined Radios (SDR) protocols.

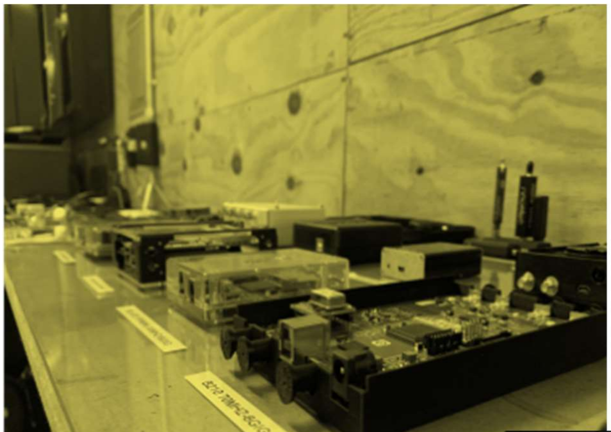


The use of SDRs are ubiquitous in commercial industry and the current availability makes them a perfect Commercial Off the Shelf (COTS) tools for global use. Students will build SDR operating systems from scratch. They will learn how to problem solve SDR software and load drivers. Student will then learn how to manipulate hardware sold globally for watching wireless television to monitor and discover signals ranging from 27 MHz to 1.7 GHz. They will use commercially available SDRs to monitor and evaluate signals ranging from 1 MHz to 6 GHz.

This introductory course provides the fundamentals needed to understand and be comfortable trouble shooting multiple types of SDRs. Students will have multiple practical exercises identifying signals and locating their origin using the FCC database to identify equipment from the signals collected.

Dangerous Device Signature Identification and Trigger (D2SIT)™ Course

- No prerequisite required
- 5 days



The D2SIT course is designed to give students an advanced knowledge of the current threats that can be exploited. Students will learn how to identify RF, light and thermal signatures. Student will learn how to use systems that will Identify multiple variables of signatures including but not limited to Wi-Fi, Bluetooth, Nordic technology, and vehicle networks plus alarm system. Students will have practical exercises to triggers systems with both wireless signatures and environmental changes.

- Understand IRE and URE (Intended and Unintended Radiated Emissions) and how they are generated.
- Detecting suspicious packages for RF emissions / signature
- Build and utilized COT items to perform passive diagnostics to detect, identify, and locate radiated emissions.
- Learn how to identify emerging technology & threats to trigger devices
- Understand RF technology used by cellular phones:
- How to demodulate basic amplitude, frequency and phase modulation:
- Identify Vehicle networks and interaction with devices:
- Media Orientated System Transport (MOST) Network:
- The electromagnetic spectrum
- Self-signature testing techniques
- Operate Mini MIRA III, Bat detector and NF-5035
- Build and utilized COT items to perform passive diagnostics to detect, identify, and locate radiated emissions
- Threat assessment process for RS operations

Equipment provided:
4 X EOD Devices

SNIPER MISSION PLANNING COURSE (SMPC)

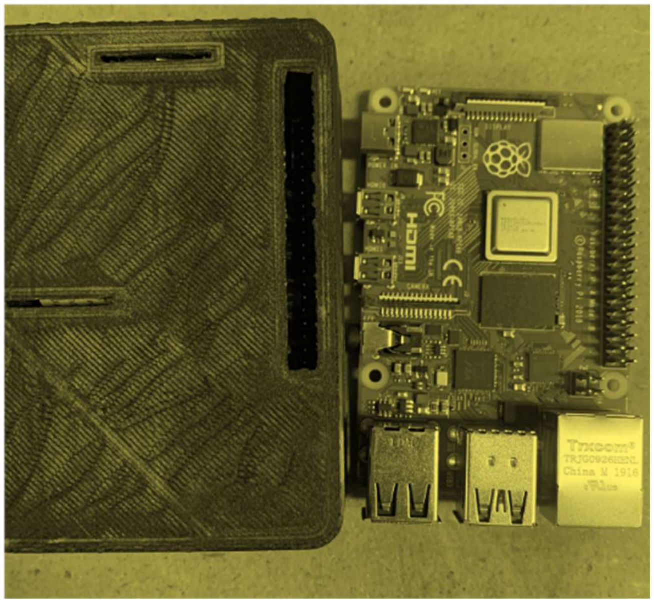
- No prerequisite required
- 5 days

The SNIPER MISSION PLANNING COURSE (SMPC) is designed to enhance the capability of qualified military/government snipers to protect themselves against digital and electronic threats from peer and near-peer adversaries within urban, suburban, and rural operational areas. This course will demonstrate how to use issued equipment in a safe manner for mission planning. Showing secure ways to set up equipment that will be used INCONUS and how to change your mission planning when working overseas. This course of instruction combines doctrine in Social Media, Radio Frequency replay attacks, vehicle security, GPS forensics and controlling digital signatures that can be targeted against users.

The SIN Protocol represents a proprietary process by Weathered Security that assists in detecting threat vectors against clients and their existing technology and selection of the most useful and secure new technology to assist them in accomplishment of their mission objectives. Participants receive practical demonstrations of techniques being used to target Sniper Teams exploiting their electronic, digital and light signatures of their operational gear that could lead to compromise or targeting by the adversary.
This course includes instruction on cyber-hygiene and vulnerability relating to the operational use of personal /government electronic devices, wireless networks, building access cards, infrared devices, navigation and communication equipment. Students will be shown the latest commercial-off-the-shelf (COTS) hardware and software globally available to an adversary that would exploit the signatures of Snipers and their operational gear. Participants will be shown open source techniques capable of conducting link-analysis exposing military members, families and host nation personnel, which facilitates an adversary's ability to identify, surveil, and conduct nefarious actions. Personnel will be shown recommended tactics, techniques and procedures for use of both personal and government electronic devices while traveling overseas conducting pre-mission activities. Will be exposed to techniques that allow recognition of threat profiles in common mobile devices and government equipment.
Electronic Signature: Risks of exploitable signature of personal/government electronic devices.
Software Defined Radio: RTL-SDR's, Hackrf, Industrial SDR's and multiple other Software defined radios and their deployment by adversaries including use with Gnu-Radio Companion Software.
RFID Skimmers: Description and live demos of protecting against known exploits.
IT Security: Defense against day-to-day electronic threats
Vehicle Electronic Systems: Description of vehicle computer systems with demonstration of information left behind by users.

Skills and Techniques Course

- Any Weathered Security Course
- 5 days



This is a custom course designed to allow students to develop unit or organization tactics, techniques and procedures based on other Weathered Security course skills in an operational environment.

Weathered Security will offer students the most secure and expeditious methods for maintaining safe and secure communications and practical application for the physical and digital world.

The course format involves students receiving mission folders that outline the mission requirements. Students then develop a mission plan, create/build technology, then conduct the mission. Full mission debriefed are conducted post mission with lessons learned allowing students to take knowledge base back to unit or organization for use.

Course length can be three to five days depending on client requirements.

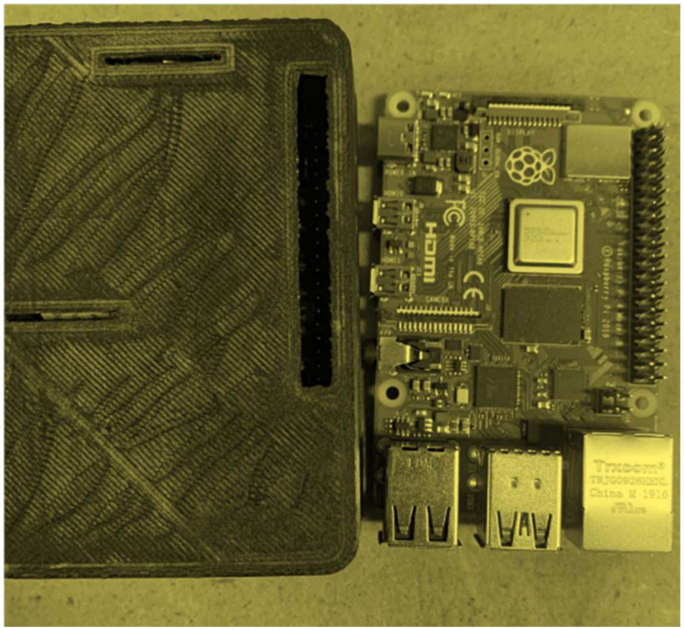
Price varies according to course length and type of equipment required for the course.

Basic Commercial off the Shelf Software Defined Radio (CORE) Course

- Recommended prerequisite- DOC
- 5 days

CORE Basic will give students the ability to create open source operating systems assessable on any laptop to experiment with and develop Software Defined Radios (SDR) protocols. SDRs are a growing industry and the current availability makes them a perfect Commercial Off the Shelf (COTS) tools for global use. Students will build SDR operating systems from scratch. They will learn how to problem solve SDR software and load drivers. Student will then learn how to manipulate hardware sold globally for watching wireless television to monitor and discover signals ranging from 27 MHz to 1.7 GHz. They will use commercially available SDRs to monitor and evaluate signals ranging from 1 MHz to 6 GHz. This introductory course provides the fundamentals needed to understand and be comfortable trouble shooting multiple types of SDRs. Students will have multiple practical exercises identifying signals and locating their origin using FCC data base to identify equipment from the signals collected. Students will leave the course with the ability to:

- Create SDR environments with open source software.
- Vehicle attacks
- Security system defeat techniques
- Understand jargon and nomenclatures of SDRs.
- Have hands on experience with 5 of the most common SDRs in the COTS realm.
- Test government grade signal analysis equipment to identify how it looks to adversaries using cots equipment.
- Create spectrum analyzers to detect RF signals in their area.
- Record and replay RF signals.
- Replay attacks against transponders and receivers used by the internet of things.

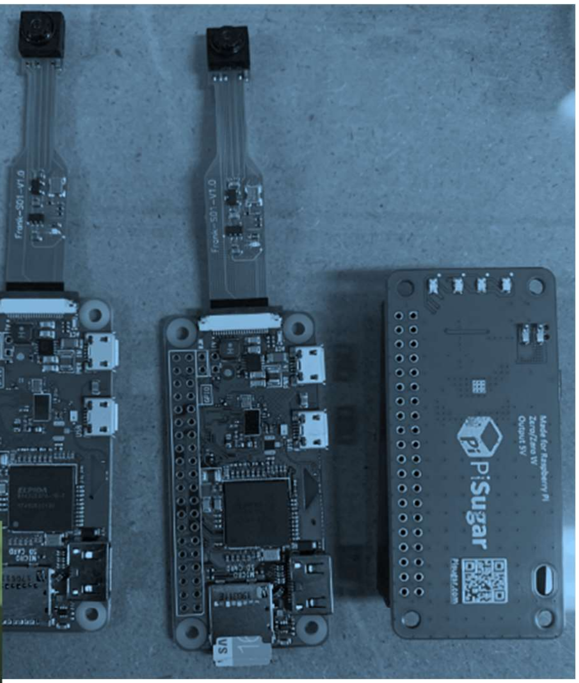


Equipment issued to students:
HackRF
Porta-Pak
RTL-SDR
Antennas
Reference Materials

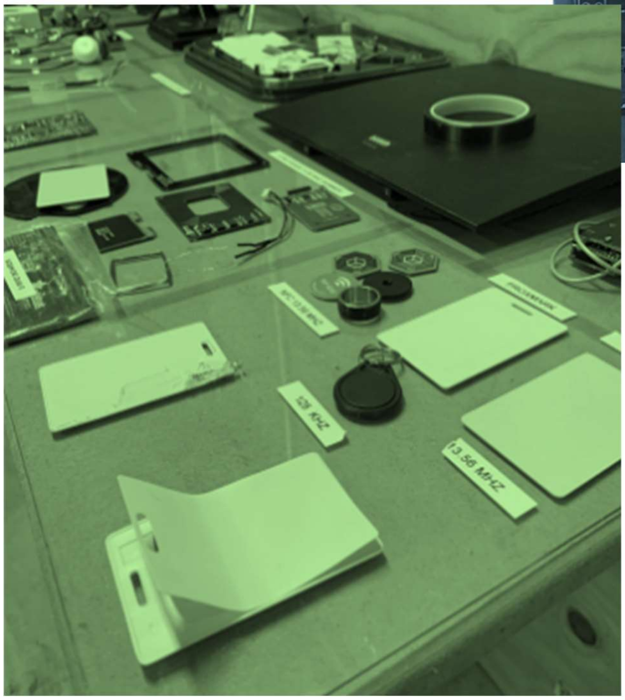
Commercial off the Shelf Software Defined Radio (CORE) Refresher Course

These modules are designed as 3-day refresher and enhancement courses for graduates of the CORE Advance Course. Each class will be:

- 3 days
- ROM $20,000



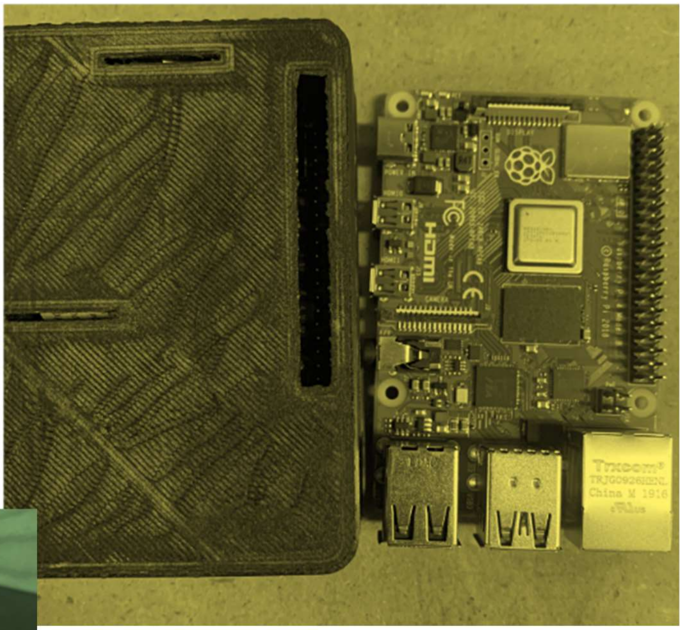
*Fox and Hound"
This course reviews SDR concepts to identify and find RF signals. This 3-day block will evaluate student's ability to hunt signals. Students will be guided through the steps of identifying new signals used to communicate. Signals such as Vehicle key fobs, Gotenna's, Xbee and alternative video offload frequencies will then be hunted and identified using only COTS SDR equipment. This exercise will be a continuing education course with feedback on both techniques, skill and actions in the physical world evaluated by trained surveillance members.



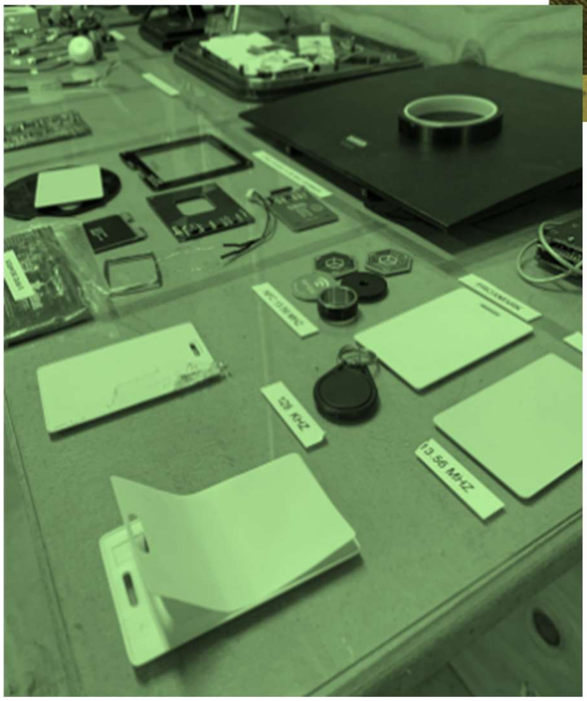
*Analyze and Replay
This module will teach users how to analyze signals and create replay attacks. Students will be required to evaluate and break it down to the raw 1's and 0's look for which bits change with different commands and then create a replay attack to replicate or modify the locks and monitoring equipment receiving the signal. Students will develop the skills to determine vulnerabilities in transmitters and sensors used for communication. Students will learn techniques to exploit vehicles for entry and denial of service. This class will show how to use SDR's to attack IOT devices used by adversaries and security

Android Collection Devices Course

- Recommended prerequisite- DOC
- 5 days



This course teaches graduates of Core Advanced how to create collection platforms and force protection tools on Android devices. Students will modify a tablet and a 4G cell phone to become capable of collecting Wi-Fi, Bluetooth, and running SDRs. These devices will still function as normally intended but will give a handheld COTS platform to drive SDRs and other collection platforms using open source software and hardware. These devices can be used to evaluate cell towers and for alternative communication. Students will leave the course with the ability to:
Use command line android programming tool.
Flash firmware and operating systems on android devices.



Use android programing commands to load apps to android devices without connecting to networks.
Load Linux operating systems on android devices.
Collect Wi-Fi, Bluetooth, Cellular data on devices made in course.
Run SDRs with android devices and alternative operating systems.
Equipment issued to students:
Android tablet with screen protector and case
Android phone with screen protector and case
2 OTG cables
RTL-SDR
Wi-Fi Dongle
Ubertooth