- **Network Protocols 101**
  - TCP/IP & OSI Models
  - Internet Protocol (IP)
  - Transportation Protocols (TCP/UDP)
  - Dynamic Host Configuration Protocol (DHCP)
  - ARP Protocol
  - Routing & Switching
  - Domain Name Protocol (DNS)
  - Web Application Protocol (HTTP)
  - File Transfer Protocol (FTP)
  - Email Transfer Protocols (SMTP/POP/IMAP)
  - Evasion theories

- **Tcpdump**
  - Tools history
  - Tool installation & usage
  - Basic filtering
  - Advanced filtering
  - Packet capturing
  - Stealing passwords

- **Tshark**
  - Tool history
  - Installing tshark
  - Capturing packets
  - Read pcap files
  - HTTP Analysis
  - Parsing user-agents
  - Advanced HTTP filtering
  - DNS analysis
  - Extracting files from packets

- **Wireshark**
  - User interface.
  - Display filters vs capture filters
  - Packets statistics
  - Reassembling packet streams
  - Extracting files from packets
  - Recompiling phone calls from VoIP
  - Selecting the right decoding
  - Analyzing SSL Certificate exchanges
  - Analyzing malicious packets

- **Snort & Bro**
  - Introduction to Snort
  - Running it as an IDS
  - Creating Snort rules
  - Introduction to Bro
  - Running Bro
  - Analyzing Bro output logs

- **Python Scapy**
  - Packet crafting with Scapy
  - Crafting packets to network or files
  - Reading packets from the network or files
  - Automatically sniffing passwords with Scapy

- **Detecting Network Attacks**
  - Detecting man in the middle attacks
  - Detecting port scanning
  - Detecting OS-fingerprinting
  - Detecting vulnerability scanning

- **Network Forensic Investigation**
  - Theory of network forensics
  - Using Opensource tools for Network forensics
  - Analyzing malware trafficPractice with network forensic scenarios