MID-TERM Examination

Subject: AT 83.04 IoT Security

|  |  |
| --- | --- |
| **Student Name** | **Tanawin Siriwan** |
| **Student ID** | **St123975** |

# Examination Instruction

**Examinations Part 1&2: The students will be in-person, online and open everything, duration 3 hours.**

* **Part B: Lab-based exam (50% with 50 score)**
* Only one version of answer per one question. If more than one version of answer is found, the score will be given to the answer that got the **lowest score**.
* How to do the lab exam:
  + Access to the exam file on the google drive (QR code will provide before you test)
  + Only English language in the document file. The other languages will not be considered.
  + The document file and code must be submitted to the email **[kalika@ait.asia]** before the time up.
* Please be ready with your own stationery.
* If Plagiarism and Academic Misconduct are found, the exam score is set to zero.
* For one who got “F” on the mid-term exam, you will have one special lab and plus more 30 mins.

**Prerequisite**

* Computer (Windows OS or Mac OS) and Kali Linux VM
* Wireshark
* Jupyter notebook or Google colab (account)
* Python
* ChatGPT

# Part 1: You will use Figure 1 to answer Q1 to Q 4.

## Assume you are a cyber cop. There is a pcap file (WiFi\_pcap) on a desktop of a raspberry pi. You must investigate the file. Fig. 1 show the network architecture of the WiFi system that you need to investigate.

|  |  |
| --- | --- |
| Wi-Fi Access Point | |
| SSID | IoTSec |
| Password | IoTSec2023 |

A diagram of a computer network

Description automatically generated

### Q1. Find the number of hosts in this network and their IP addresses? Hint: use “nmap” command to scan the network. To answer, you need to capture your screen and show which command you use and the result of the command. [5 marks]

1. How many hosts is up?
2. IP address of pi#1 & pi#2
3. Host ip, 1 host IoTSec

A screenshot of a computer

Description automatically generated

PI 1 : 192.168.0.52 and PI 2 : 192.168.0.56

### Q2. Find pcap files in “WPA\_pcap” directory and copy them to your computer. [5 marks]

Hint:

|  |  |
| --- | --- |
|  | Command |
| Connect host with file transfer protocol | sftp kali@IP\_address |
| List files in the remote directory | ls |
| Copy a file to a local computer | get **filename** new\_local \_location |

Via CLI

A screenshot of a computer

Description automatically generated

Download Result

A screenshot of a computer

Description automatically generated

### Q3. Investigate pcap files in the WPA\_pcap directory on your local computer. Find “EAPOL” packets on the pcap file. [5 marks]

1. Which pcap file contain “EAPOL” packets?

A screenshot of a computer

Description automatically generated

### Q4. Decrypt the pcap file with SSID and Password which corresponding to the EAPOL. [5 marks]

Step1: Open pcap file with Wireshark

Step2: Go to “preference”

Step3: Go to “Protocols” and select “IEEE 802.11” and “Decryption keys” 🡪 Edit

A screenshot of a computer

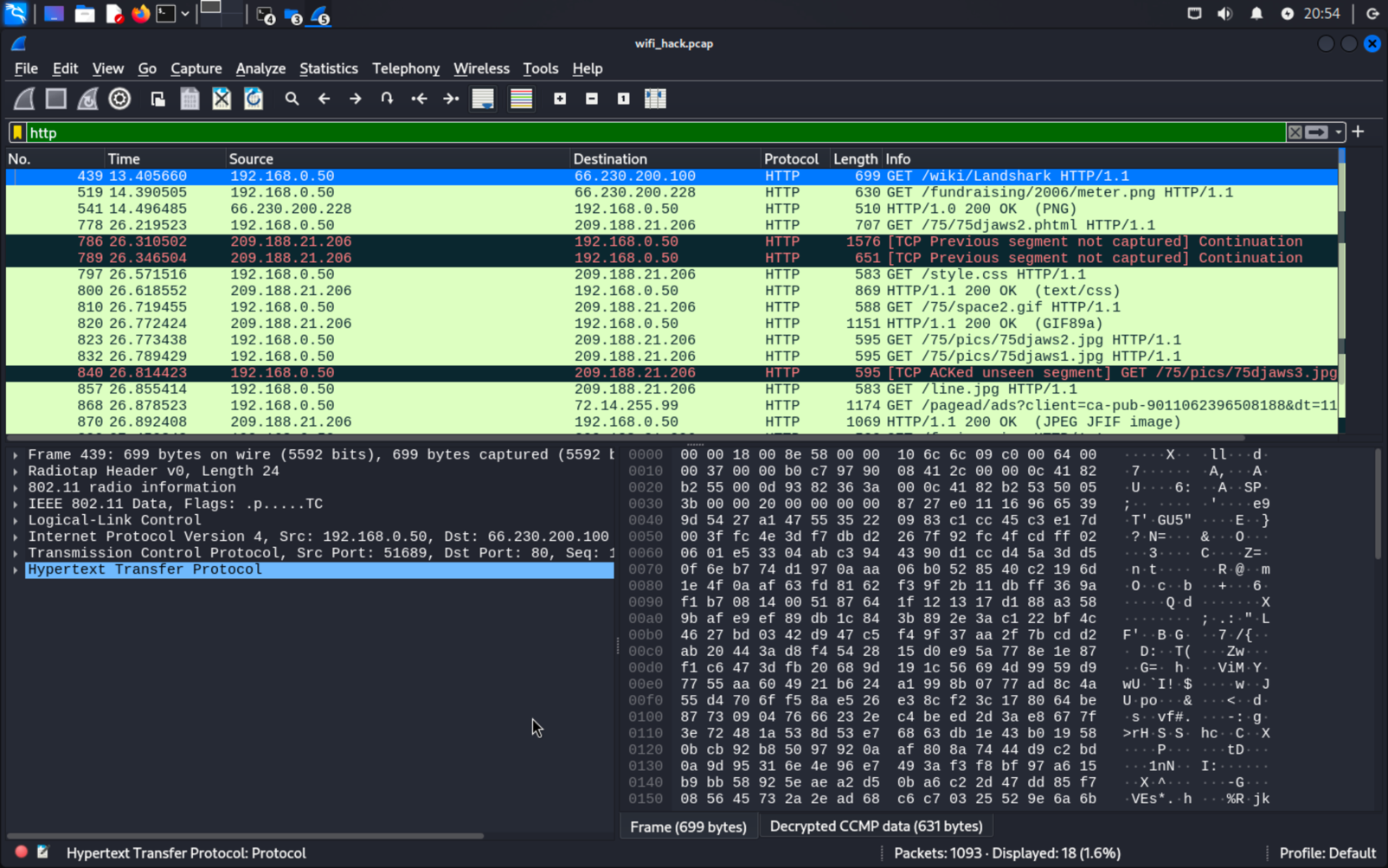
Description automatically generated

Step4: Select key type “wpa-pwd” and Key “SSID:Password”.

A screenshot of a computer

Description automatically generated

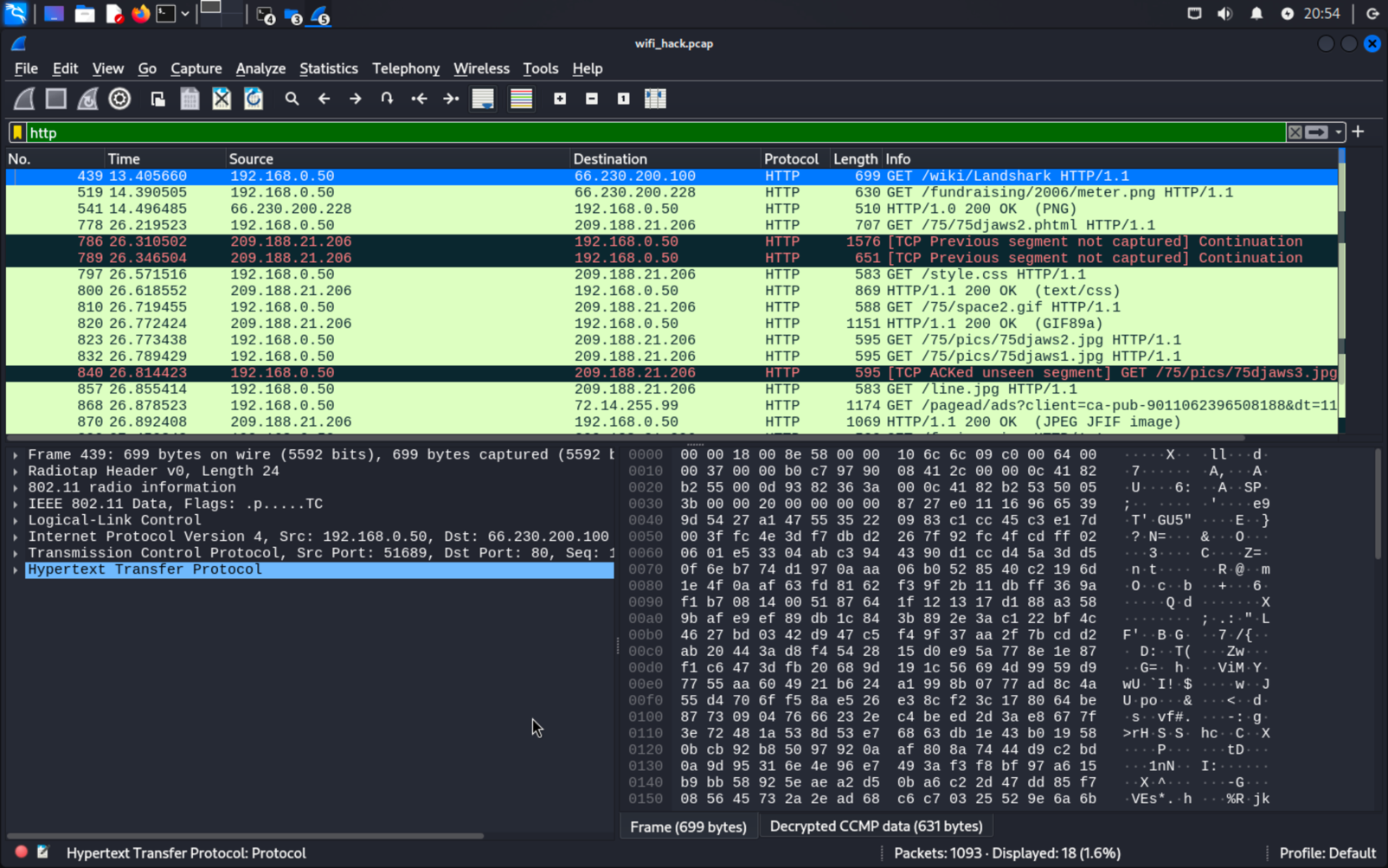
Step:5 list all “http” packets



### Q5. Which pcap file can decrypt with the SSID and Password. Tell me why that file can be decrypted? [10 marks]

wifi\_hack.pcap via “SSID-Password” ->Induction

These file can decrypted via Induction.



Decrypting a pcap file requires the SSID and password of the Wi-Fi network to derive encryption keys and decrypt the encrypted network traffic.

### Q6. Show ARP cache of Pi#1 and Pi#2 [10 marks]

Screens screenshot of a computer

Description automatically generated

### Q7. Use WireShark to capture the packets on your Wireless interface during perform “nmap” scan Pi#1 and Pi#2 in the network. Then, save your pcap file and hash this pcap file with sha256. [10 marks]