Mubariz Saeed
CSF 432 - Lab#11
Fall 2021

Lab 11: 4-way Handshake Over EAPoL and WiFi Cracking With aircrack-ng

Part 1: Understanding the 4-way Handshake

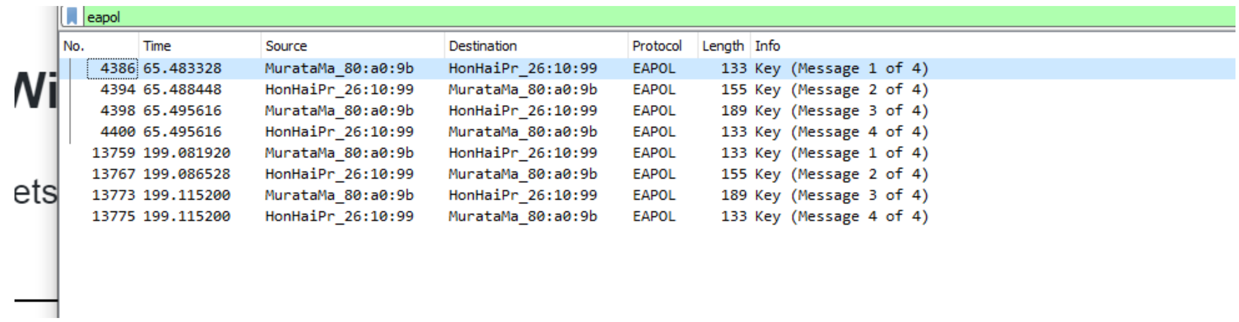
Nothing to submit.

Part 2: Analyzing a Wireless Capture File

⁉️ Question 1 - How many sets of 4-way handshake exchanges are there (4 messages in one set)

2

⁉️ Question 2 - Submit a screenshot of your filtered results.



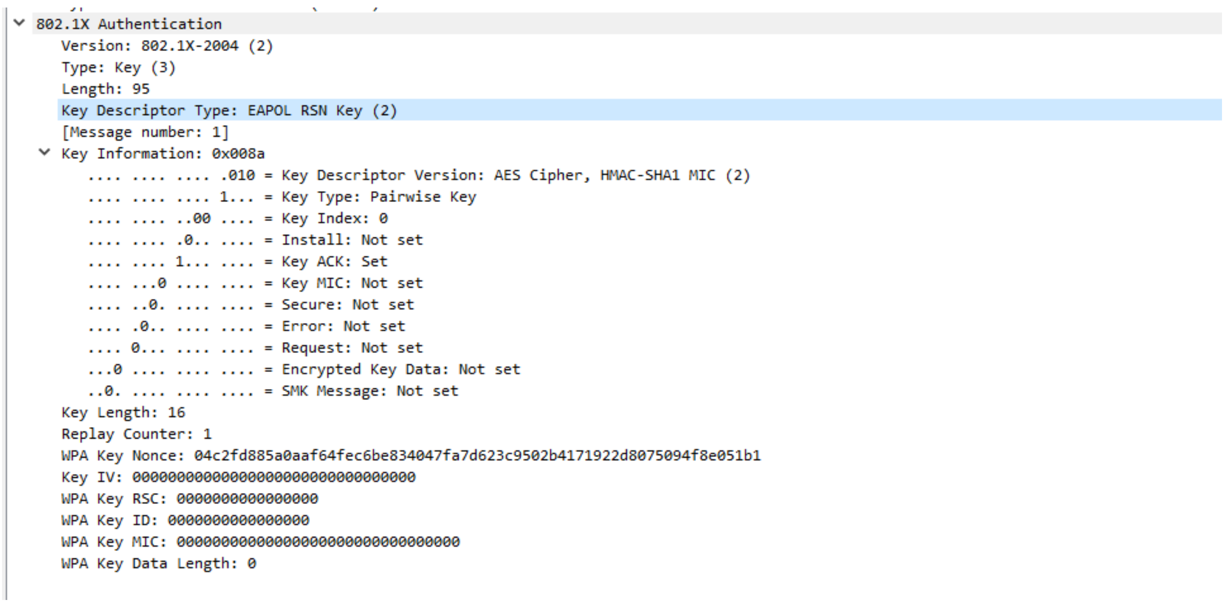
eapol

No.	Time	Source	Destination	Protocol	Length	Info
4386	65.483328	MurataMa_80:a0:9b	HonHaiPr_26:10:99	EAPOL	133	Key (Message 1 of 4)
4394	65.488448	HonHaiPr_26:10:99	MurataMa_80:a0:9b	EAPOL	155	Key (Message 2 of 4)
4398	65.495616	MurataMa_80:a0:9b	HonHaiPr_26:10:99	EAPOL	189	Key (Message 3 of 4)
4400	65.495616	HonHaiPr_26:10:99	MurataMa_80:a0:9b	EAPOL	133	Key (Message 4 of 4)
13759	199.081920	MurataMa_80:a0:9b	HonHaiPr_26:10:99	EAPOL	133	Key (Message 1 of 4)
13767	199.086528	HonHaiPr_26:10:99	MurataMa_80:a0:9b	EAPOL	155	Key (Message 2 of 4)
13773	199.115200	MurataMa_80:a0:9b	HonHaiPr_26:10:99	EAPOL	189	Key (Message 3 of 4)
13775	199.115200	HonHaiPr_26:10:99	MurataMa_80:a0:9b	EAPOL	133	Key (Message 4 of 4)

⁉️ Question 3 - What protocol is listed under the protocol column?

EAPOL

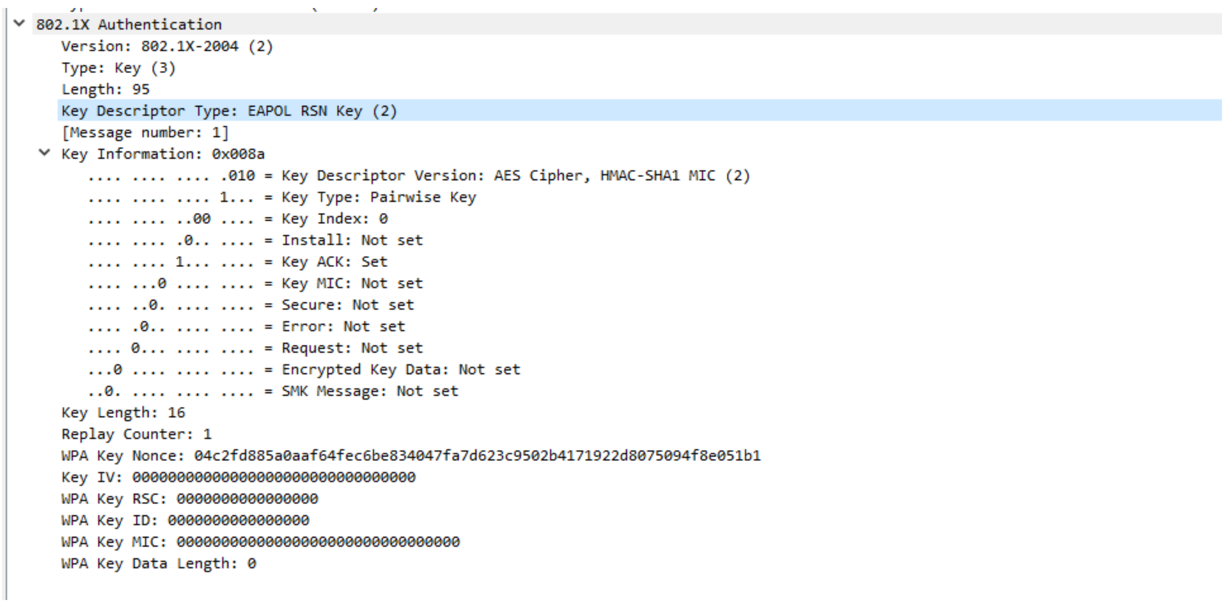
⁉️ Question 4 - What encryption key type is being used for this key exchange?



```
802.1X Authentication
    Version: 802.1X-2004 (2)
    Type: Key (3)
    Length: 95
    Key Descriptor Type: EAPOL RSN Key (2)
    [Message number: 1]
    Key Information: 0x008a
        .... .... .... .010 = Key Descriptor Version: AES Cipher, HMAC-SHA1 MIC (2)
        .... .... .... 1... = Key Type: Pairwise Key
        .... .... ..00 .... = Key Index: 0
        .... .... .0.. .... = Install: Not set
        .... .... 1... .... = Key ACK: Set
        .... ...0 .... .... = Key MIC: Not set
        .... ..0. .... .... = Secure: Not set
        .... .0.. .... .... = Error: Not set
        .... 0... .... .... = Request: Not set
        ...0 .... .... .... = Encrypted Key Data: Not set
        ..0. .... .... .... = SMK Message: Not set
    Key Length: 16
    Replay Counter: 1
    WPA Key Nonce: 04c2fd885a0aaf64fec6be834047fa7d623c9502b4171922d8075094f8e051b1
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 00000000000000000000000000000000
    WPA Key Data Length: 0
```

Anonce

⁉️ Question 5 - Based on that encryption key type, what possible encryption standards are being used for this communication?



```
802.1X Authentication
    Version: 802.1X-2004 (2)
    Type: Key (3)
    Length: 95
    Key Descriptor Type: EAPOL RSN Key (2)
    [Message number: 1]
    Key Information: 0x008a
        .... .... .... .010 = Key Descriptor Version: AES Cipher, HMAC-SHA1 MIC (2)
        .... .... .... 1... = Key Type: Pairwise Key
        .... .... ..00 .... = Key Index: 0
        .... .... .0.. .... = Install: Not set
        .... .... 1... .... = Key ACK: Set
        .... ...0 .... .... = Key MIC: Not set
        .... ..0. .... .... = Secure: Not set
        .... .0.. .... .... = Error: Not set
        .... 0... .... .... = Request: Not set
        ...0 .... .... .... = Encrypted Key Data: Not set
        ..0. .... .... .... = SMK Message: Not set
    Key Length: 16
    Replay Counter: 1
    WPA Key Nonce: 04c2fd885a0aaf64fec6be834047fa7d623c9502b4171922d8075094f8e051b1
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 00000000000000000000000000000000
    WPA Key Data Length: 0
```

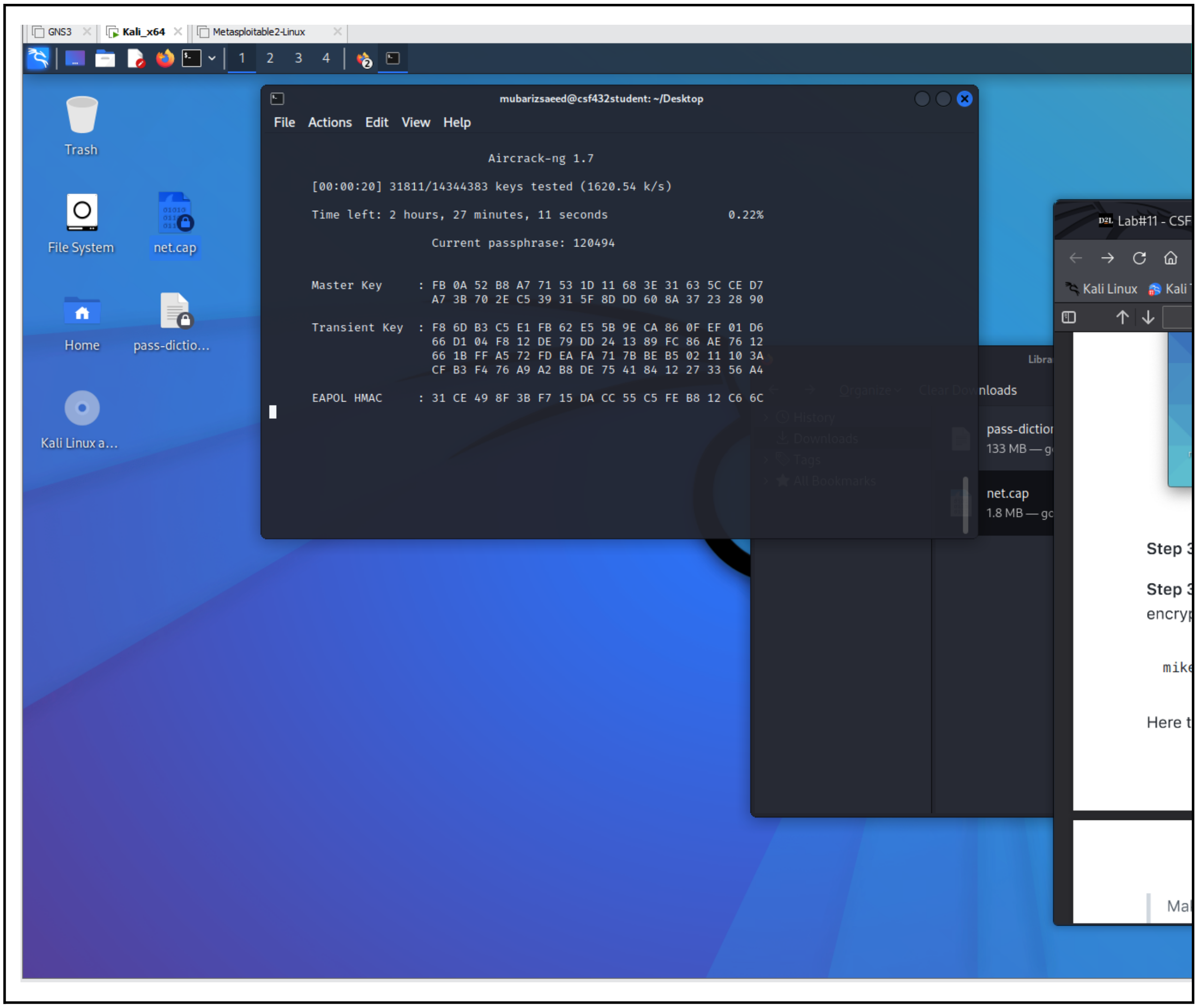
WPA, AES

⁉️ Question 6 - Look through the first set of key exchanges under the `802.1x Authentication > Key Information` field. What changes do you notice during the handshake.

Replay counter, Key nonce and the length

Part 3: Key Cracking with aircrack-ng

⁉️ Question 7 - Submit a screenshot of your terminal running the aircrack-ng program.



```
                            Aircrack-ng 1.7

      [00:00:20] 31811/14344383 keys tested (1620.54 k/s)

      Time left: 2 hours, 27 minutes, 11 seconds                 0.22%

                           Current passphrase: 120494


      Master Key     : FB 0A 52 B8 A7 71 53 1D 11 68 3E 31 63 5C CE D7
                       A7 3B 70 2E C5 39 31 5F 8D DD 60 8A 37 23 28 90

      Transient Key  : F8 6D B3 C5 E1 FB 62 E5 5B 9E CA 86 0F EF 01 D6
                       66 D1 04 F8 12 DE 79 DD 24 13 89 FC 86 AE 76 12
                       66 1B FF A5 72 FD EA FA 71 7B BE B5 02 11 10 3A
                       CF B3 F4 76 A9 A2 B8 DE 75 41 84 12 27 33 56 A4

      EAPOL HMAC     : 31 CE 49 8F 3B F7 15 DA CC 55 C5 FE B8 12 C6 6C
```

⁉️ Question 8 - What are the three fields on the left hand side of the aircrack-ng display. Match each one of these fields with the key abbreviations described in Part 1 of this lab.

Master key → mpk and the transient key is PTK and Eapol Mac HMac is Snonce

⁉️ Question 9 - In your own words, what is aircrack-ng doing and what is it solving for?

Aircrack ng is decrypting all of the information in the plain text that is encrypted in the file via the PSK

Part 4: Submission

Convert your network document into a .PDF and upload a single `lastname_lab11.pdf` file to Brightspace through the attachment uploads option.