Experiment–04

4.1 Aim:

Packet Capture and Analysis with Wireshark: Understand how to capture network traffic and analyze packets to identify protocols, communication patterns, and potentially sensitive information.

4.2 Course Outcome:

Apply network monitoring techniques and packet analysis skills to interpret communication protocols, detect anomalies, and secure network systems.

4.3 Lab Objective:

To capture live network traffic using Wireshark and analyze packets to identify protocols, endpoints, and extract potentially sensitive information.

4.4 Requirements:

- **Operating System:** Windows / Linux / macOS
- **Tool:** Wireshark (latest stable version)
- **Network Access:** Internet connection or local network traffic
- **Optional:** Browser or ping utility to generate traffic

4.5 Theory:

Wireshark is a free and open-source packet analyzer widely used for network troubleshooting, analysis, and protocol development. It allows users to capture live traffic and analyze individual packets to understand communication patterns and identify issues or sensitive data exposure.

Key Features:

- Real-time packet capture
- Protocol decoding (e.g., HTTP, DNS, TCP, TLS, etc.)
- Filters for specific hosts, ports, or protocols
- Visualization of conversation flows
- Export of session or packet data

Applications:

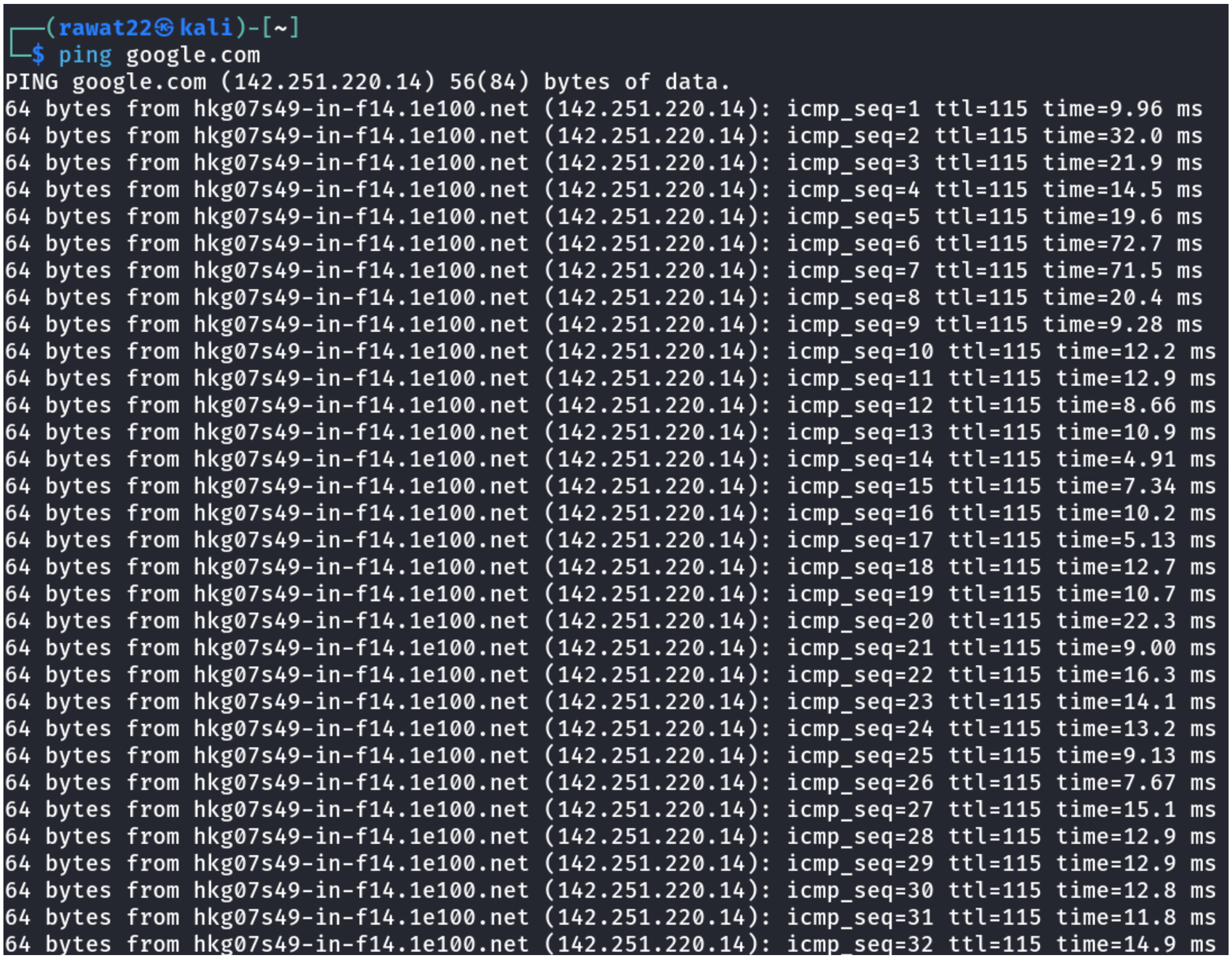
- Troubleshooting network issues
- Analyzing suspicious activity or attacks
- Verifying proper network configurations
- Training and research in cybersecurity

4.6 Tasks:

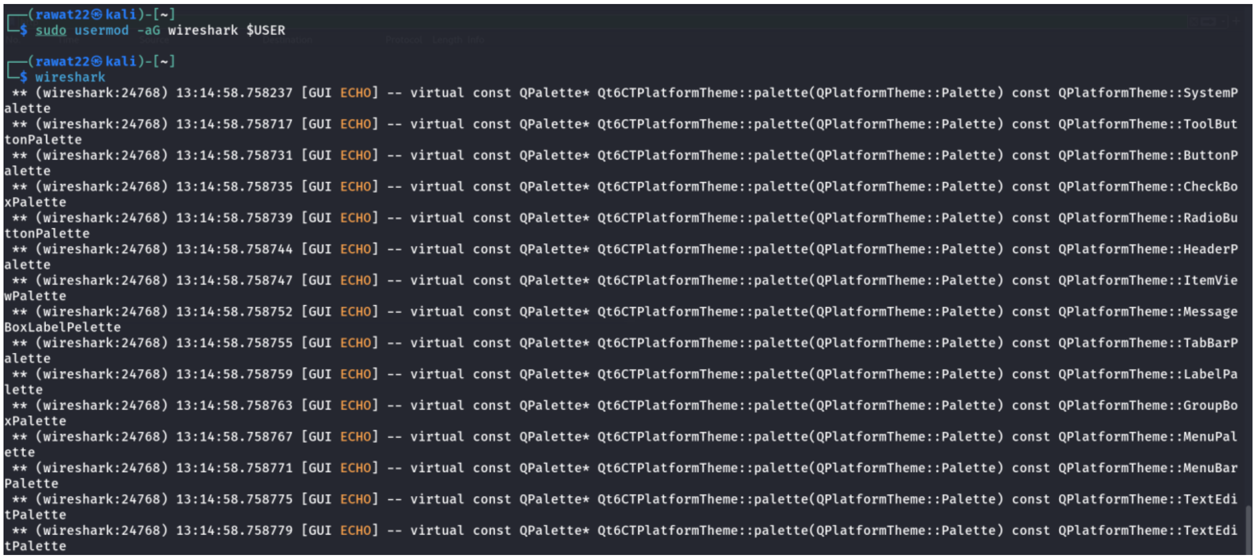
1. Launch Wireshark and start a live capture on the active network interface.
2. Visit a few websites or use the `ping` command to generate network traffic.
3. Stop the capture and filter for HTTP traffic using the display filter `http`.
4. Identify the source and destination IP addresses involved in HTTP communication.
5. Analyze TCP packets to view the 3-way handshake (SYN, SYN-ACK, ACK).
6. Apply the filter `dns` and identify domain name queries and corresponding IPs.
7. Capture a login form submission (on a test or demo site) to demonstrate sensitive information in plaintext (if unencrypted).
8. Save the capture file for documentation and future analysis.

4.7 Output Screenshots:

First Google Wireshark packet capture



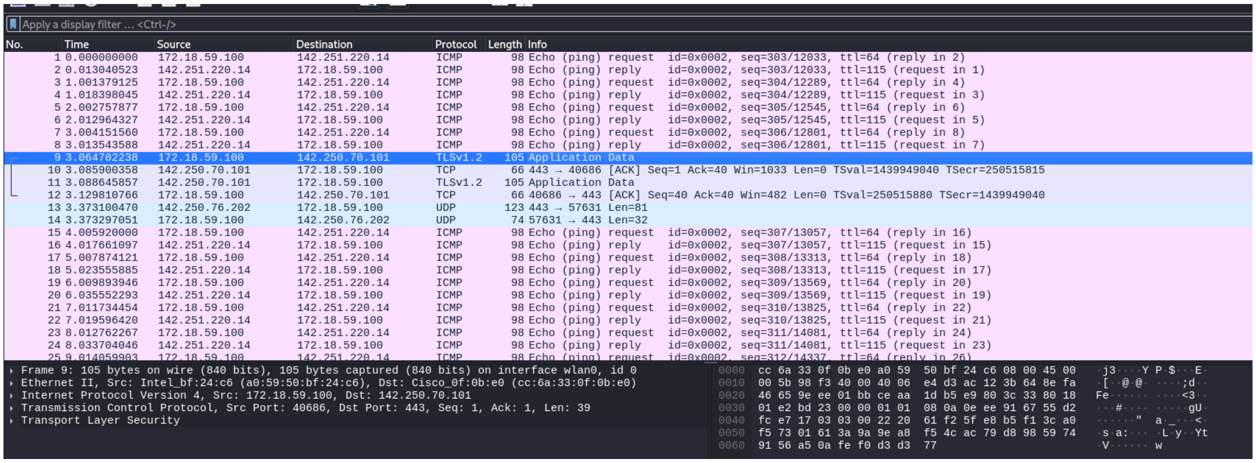
```
┌──(rawat22㉿kali)-[~]
└─$ ping google.com
PING google.com (142.251.220.14) 56(84) bytes of data.
64 bytes from hkg07s49-in-f14.1e100.net (142.251.220.14): icmp_seq=1 ttl=115 time=9.96 ms
64 bytes from hkg07s49-in-f14.1e100.net (142.251.220.14): icmp_seq=2 ttl=115 time=32.0 ms
64 bytes from hkg07s49-in-f14.1e100.net (142.251.220.14): icmp_seq=3 ttl=115 time=21.9 ms
64 bytes from hkg07s49-in-f14.1e100.net (142.251.220.14): icmp_seq=4 ttl=115 time=14.5 ms
64 bytes from hkg07s49-in-f14.1e100.net (142.251.220.14): icmp_seq=5 ttl=115 time=19.6 ms
64 bytes from hkg07s49-in-f14.1e100.net (142.251.220.14): icmp_seq=6 ttl=115 time=72.7 ms
64 bytes from hkg07s49-in-f14.1e100.net (142.251.220.14): icmp_seq=7 ttl=115 time=71.5 ms
64 bytes from hkg07s49-in-f14.1e100.net (142.251.220.14): icmp_seq=8 ttl=115 time=20.4 ms
64 bytes from hkg07s49-in-f14.1e100.net (142.251.220.14): icmp_seq=9 ttl=115 time=9.28 ms
64 bytes from hkg07s49-in-f14.1e100.net (142.251.220.14): icmp_seq=10 ttl=115 time=12.2 ms
64 bytes from hkg07s49-in-f14.1e100.net (142.251.220.14): icmp_seq=11 ttl=115 time=12.9 ms
64 bytes from hkg07s49-in-f14.1e100.net (142.251.220.14): icmp_seq=12 ttl=115 time=8.66 ms
64 bytes from hkg07s49-in-f14.1e100.net (142.251.220.14): icmp_seq=13 ttl=115 time=10.9 ms
64 bytes from hkg07s49-in-f14.1e100.net (142.251.220.14): icmp_seq=14 ttl=115 time=4.91 ms
64 bytes from hkg07s49-in-f14.1e100.net (142.251.220.14): icmp_seq=15 ttl=115 time=7.34 ms
64 bytes from hkg07s49-in-f14.1e100.net (142.251.220.14): icmp_seq=16 ttl=115 time=10.2 ms
64 bytes from hkg07s49-in-f14.1e100.net (142.251.220.14): icmp_seq=17 ttl=115 time=5.13 ms
64 bytes from hkg07s49-in-f14.1e100.net (142.251.220.14): icmp_seq=18 ttl=115 time=12.7 ms
64 bytes from hkg07s49-in-f14.1e100.net (142.251.220.14): icmp_seq=19 ttl=115 time=10.7 ms
64 bytes from hkg07s49-in-f14.1e100.net (142.251.220.14): icmp_seq=20 ttl=115 time=22.3 ms
64 bytes from hkg07s49-in-f14.1e100.net (142.251.220.14): icmp_seq=21 ttl=115 time=9.00 ms
64 bytes from hkg07s49-in-f14.1e100.net (142.251.220.14): icmp_seq=22 ttl=115 time=16.3 ms
64 bytes from hkg07s49-in-f14.1e100.net (142.251.220.14): icmp_seq=23 ttl=115 time=14.1 ms
64 bytes from hkg07s49-in-f14.1e100.net (142.251.220.14): icmp_seq=24 ttl=115 time=13.2 ms
64 bytes from hkg07s49-in-f14.1e100.net (142.251.220.14): icmp_seq=25 ttl=115 time=9.13 ms
64 bytes from hkg07s49-in-f14.1e100.net (142.251.220.14): icmp_seq=26 ttl=115 time=7.67 ms
64 bytes from hkg07s49-in-f14.1e100.net (142.251.220.14): icmp_seq=27 ttl=115 time=15.1 ms
64 bytes from hkg07s49-in-f14.1e100.net (142.251.220.14): icmp_seq=28 ttl=115 time=12.9 ms
64 bytes from hkg07s49-in-f14.1e100.net (142.251.220.14): icmp_seq=29 ttl=115 time=12.9 ms
64 bytes from hkg07s49-in-f14.1e100.net (142.251.220.14): icmp_seq=30 ttl=115 time=12.8 ms
64 bytes from hkg07s49-in-f14.1e100.net (142.251.220.14): icmp_seq=31 ttl=115 time=11.8 ms
64 bytes from hkg07s49-in-f14.1e100.net (142.251.220.14): icmp_seq=32 ttl=115 time=14.9 ms
```



```
┌──(rawat22㉿kali)-[~]
└─$ sudo usermod -aG wireshark $USER

┌──(rawat22㉿kali)-[~]
└─$ wireshark
 ** (wireshark:24768) 13:14:58.758237 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::SystemP
alette
 ** (wireshark:24768) 13:14:58.758717 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::ToolBut
tonPalette
 ** (wireshark:24768) 13:14:58.758731 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::ButtonP
alette
 ** (wireshark:24768) 13:14:58.758735 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::CheckBo
xPalette
 ** (wireshark:24768) 13:14:58.758739 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::RadioBu
ttonPalette
 ** (wireshark:24768) 13:14:58.758744 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::HeaderP
alette
 ** (wireshark:24768) 13:14:58.758747 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::ItemVie
wPalette
 ** (wireshark:24768) 13:14:58.758752 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::Message
BoxLabelPelette
 ** (wireshark:24768) 13:14:58.758755 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::TabBarP
alette
 ** (wireshark:24768) 13:14:58.758759 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::LabelPa
lette
 ** (wireshark:24768) 13:14:58.758763 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::GroupBo
xPalette
 ** (wireshark:24768) 13:14:58.758767 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::MenuPal
ette
 ** (wireshark:24768) 13:14:58.758771 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::MenuBar
Palette
 ** (wireshark:24768) 13:14:58.758775 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::TextEdi
tPalette
 ** (wireshark:24768) 13:14:58.758779 [GUI ECHO] -- virtual const QPalette* Qt6CTPlatformTheme::palette(QPlatformTheme::Palette) const QPlatformTheme::TextEdi
tPalette
```

Executing the WireShark Tool

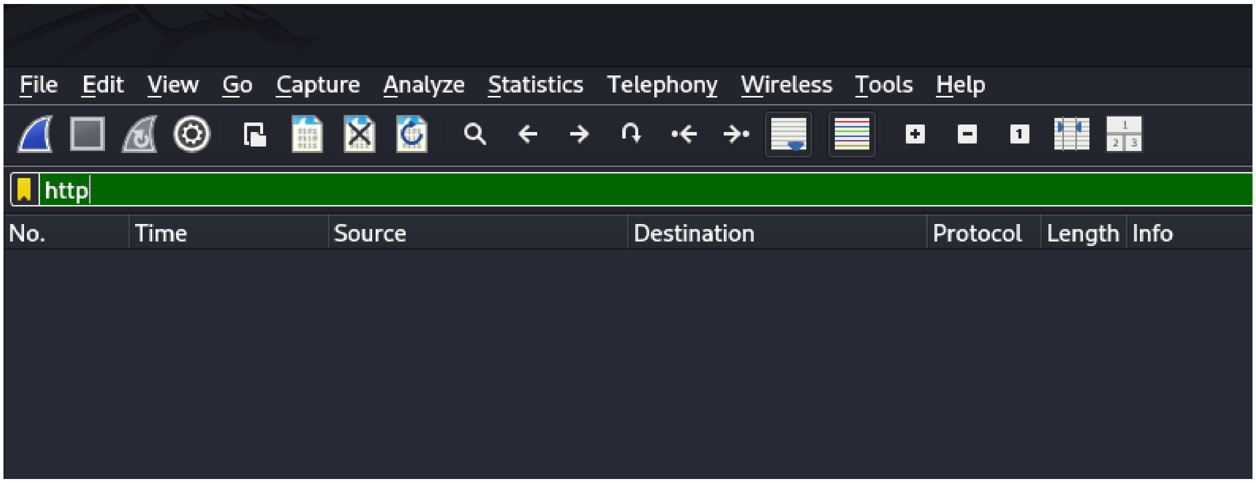


```
No.    Time         Source           Destination      Protocol  Length Info
     1 0.000000000  172.18.59.100    142.251.220.14   ICMP        98 Echo (ping) request  id=0x0002, seq=303/12033, ttl=64 (reply in 2)
     2 0.013040523  142.251.220.14   172.18.59.100    ICMP        98 Echo (ping) reply    id=0x0002, seq=303/12033, ttl=115 (request in 1)
     3 1.001379125  172.18.59.100    142.251.220.14   ICMP        98 Echo (ping) request  id=0x0002, seq=304/12289, ttl=64 (reply in 4)
     4 1.018398045  142.251.220.14   172.18.59.100    ICMP        98 Echo (ping) reply    id=0x0002, seq=304/12289, ttl=115 (request in 3)
     5 2.002757877  172.18.59.100    142.251.220.14   ICMP        98 Echo (ping) request  id=0x0002, seq=305/12545, ttl=64 (reply in 6)
     6 2.012964327  142.251.220.14   172.18.59.100    ICMP        98 Echo (ping) reply    id=0x0002, seq=305/12545, ttl=115 (request in 5)
     7 3.004151560  172.18.59.100    142.251.220.14   ICMP        98 Echo (ping) request  id=0x0002, seq=306/12801, ttl=64 (reply in 8)
     8 3.013543588  142.251.220.14   172.18.59.100    ICMP        98 Echo (ping) reply    id=0x0002, seq=306/12801, ttl=115 (request in 7)
     9 3.064702238  172.18.59.100    142.250.70.101   TLSv1.2    105 Application Data
    10 3.085900358  142.250.70.101   172.18.59.100    TCP         66 443 → 40686 [ACK] Seq=1 Ack=40 Win=1033 Len=0 TSval=1439949040 TSecr=250515815
    11 3.088645857  142.250.70.101   172.18.59.100    TLSv1.2    105 Application Data
    12 3.129810766  172.18.59.100    142.250.70.101   TCP         66 40686 → 443 [ACK] Seq=40 Ack=40 Win=482 Len=0 TSval=250515880 TSecr=1439949040
    13 3.373100470  142.250.76.202   172.18.59.100    UDP        123 443 → 57631 Len=81
    14 3.373297051  172.18.59.100    142.250.76.202   UDP         74 57631 → 443 Len=32
    15 4.005920000  172.18.59.100    142.251.220.14   ICMP        98 Echo (ping) request  id=0x0002, seq=307/13057, ttl=64 (reply in 16)
    16 4.017661097  142.251.220.14   172.18.59.100    ICMP        98 Echo (ping) reply    id=0x0002, seq=307/13057, ttl=115 (request in 15)
    17 5.007874121  172.18.59.100    142.251.220.14   ICMP        98 Echo (ping) request  id=0x0002, seq=308/13313, ttl=64 (reply in 18)
    18 5.023555885  142.251.220.14   172.18.59.100    ICMP        98 Echo (ping) reply    id=0x0002, seq=308/13313, ttl=115 (request in 17)
    19 6.009893946  172.18.59.100    142.251.220.14   ICMP        98 Echo (ping) request  id=0x0002, seq=309/13569, ttl=64 (reply in 20)
    20 6.035552293  142.251.220.14   172.18.59.100    ICMP        98 Echo (ping) reply    id=0x0002, seq=309/13569, ttl=115 (request in 19)
    21 7.011734454  172.18.59.100    142.251.220.14   ICMP        98 Echo (ping) request  id=0x0002, seq=310/13825, ttl=64 (reply in 22)
    22 7.019596420  142.251.220.14   172.18.59.100    ICMP        98 Echo (ping) reply    id=0x0002, seq=310/13825, ttl=115 (request in 21)
    23 8.012762267  172.18.59.100    142.251.220.14   ICMP        98 Echo (ping) request  id=0x0002, seq=311/14081, ttl=64 (reply in 24)
    24 8.033704046  142.251.220.14   172.18.59.100    ICMP        98 Echo (ping) reply    id=0x0002, seq=311/14081, ttl=115 (request in 23)
    25 9.014059903  172.18.59.100    142.251.220.14   ICMP        98 Echo (ping) request  id=0x0002, seq=312/14337, ttl=64 (reply in 26)
```

```
› Frame 9: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on interface wlan0, id 0
› Ethernet II, Src: Intel_bf:24:c6 (a0:59:50:bf:24:c6), Dst: Cisco_0f:0b:e0 (cc:6a:33:0f:0b:e0)
› Internet Protocol Version 4, Src: 172.18.59.100, Dst: 142.250.70.101
› Transmission Control Protocol, Src Port: 40686, Dst Port: 443, Seq: 1, Ack: 1, Len: 39
› Transport Layer Security
```

```
0000  cc 6a 33 0f 0b e0 a0 59  50 bf 24 c6 08 00 45 00   ·j3···Y P·$···E·
0010  00 5b 98 f3 40 00 40 06  e4 d3 ac 12 3b 64 8e fa   ·[··@·@· ····;d··
0020  46 65 9e ee 01 bb ce aa  1d b5 e9 80 3c 33 80 18   Fe······ ····<3··
0030  01 e2 bd 23 00 00 01 01  08 0a 0e ee 91 67 55 d2   ···#···· ·····gU·
0040  fc e7 17 03 03 00 22 20  61 f2 5f e8 b5 f1 3c a0   ······"  a·_···<·
0050  f5 73 01 61 3a 9a 9e a8  f5 4c ac 79 d8 98 59 74   ·s·a:··· ·L·y··Yt
0060  91 56 a5 0a fe f0 d3 d3  77                        ·V······ w
```

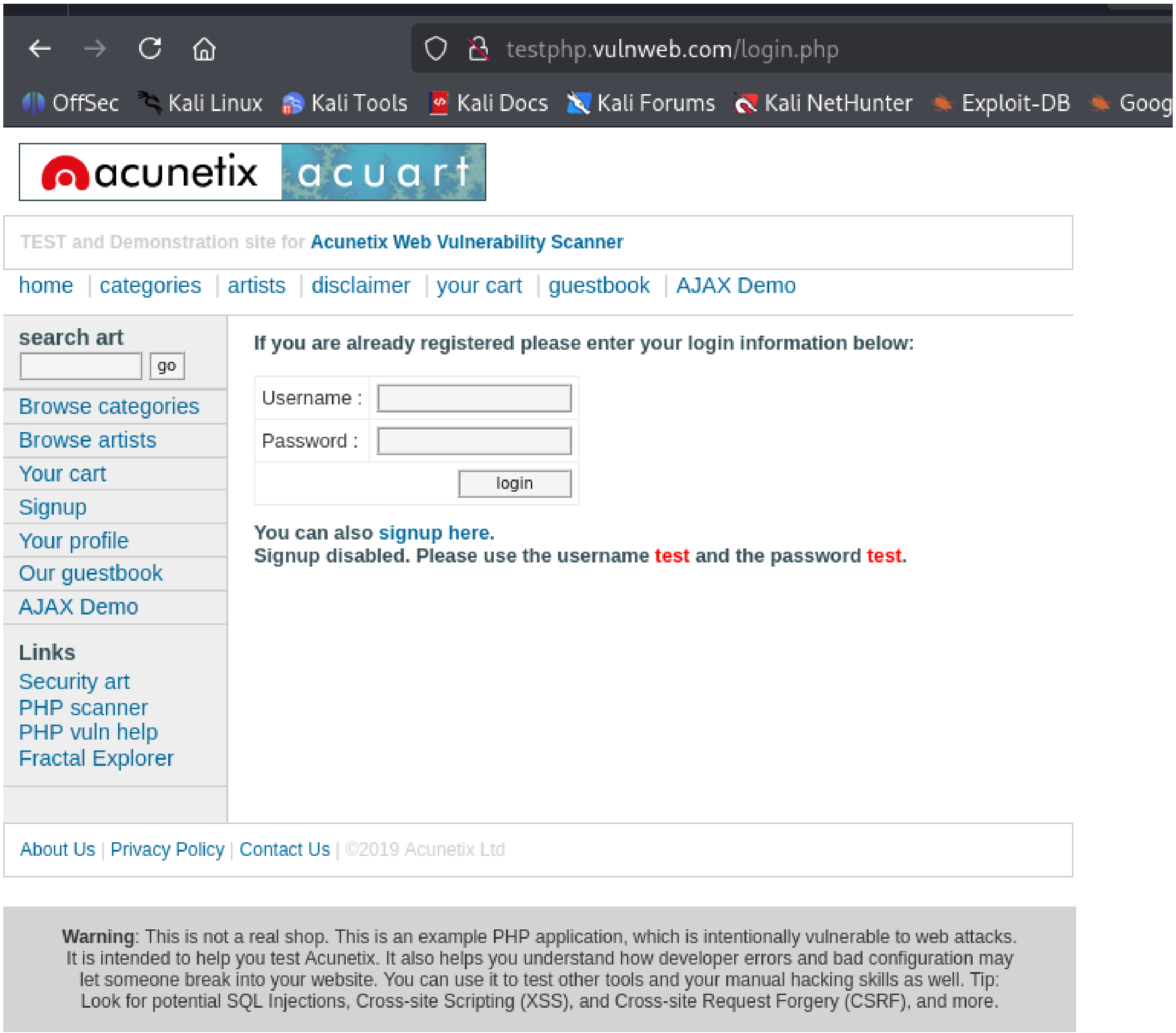
Analyzing the Captured traffic



http

No. | Time | Source | Destination | Protocol | Length | Info

Now capturing the Username and Password from using the
http://testphp.vulnweb.com/login.php



TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

If you are already registered please enter your login information below:

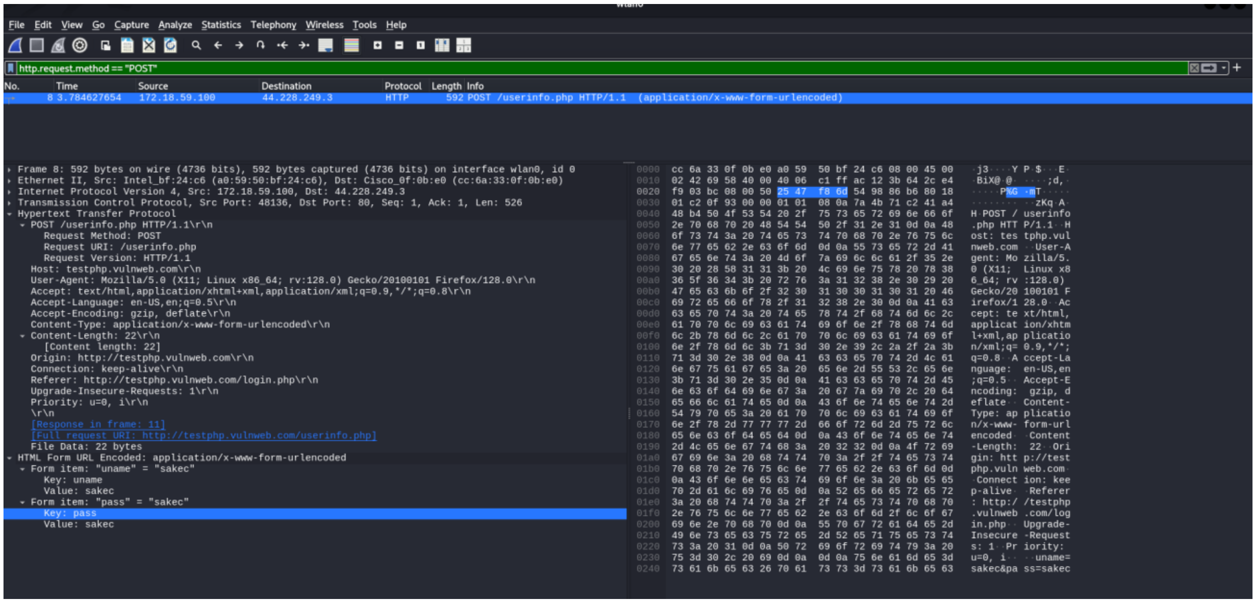
Username :	
Password :	

You can also signup here.
Signup disabled. Please use the username test and the password test.

©2019 Acunetix Ltd

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

Captured the credentials



```
http.request.method == "POST"

No.     Time          Source          Destination     Protocol  Length Info
      8 3.784627654   172.18.59.100   44.228.249.3    HTTP        592 POST /userinfo.php HTTP/1.1  (application/x-www-form-urlencoded)
```

```
› Frame 8: 592 bytes on wire (4736 bits), 592 bytes captured (4736 bits) on interface wlan0, id 0
› Ethernet II, Src: Intel_bf:24:c6 (a0:59:50:bf:24:c6), Dst: Cisco_0f:0b:e0 (cc:6a:33:0f:0b:e0)
› Internet Protocol Version 4, Src: 172.18.59.100, Dst: 44.228.249.3
› Transmission Control Protocol, Src Port: 48136, Dst Port: 80, Seq: 1, Ack: 1, Len: 526
⌄ Hypertext Transfer Protocol
  ⌄ POST /userinfo.php HTTP/1.1\r\n
      Request Method: POST
      Request URI: /userinfo.php
      Request Version: HTTP/1.1
    Host: testphp.vulnweb.com\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Content-Type: application/x-www-form-urlencoded\r\n
  ⌄ Content-Length: 22\r\n
      [Content length: 22]
    Origin: http://testphp.vulnweb.com\r\n
    Connection: keep-alive\r\n
    Referer: http://testphp.vulnweb.com/login.php\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Priority: u=0, i\r\n
    \r\n
    [Response in frame: 11]
    [Full request URI: http://testphp.vulnweb.com/userinfo.php]
    File Data: 22 bytes
⌄ HTML Form URL Encoded: application/x-www-form-urlencoded
  ⌄ Form item: "uname" = "sakec"
      Key: uname
      Value: sakec
  ⌄ Form item: "pass" = "sakec"
      Key: pass
      Value: sakec
```

```
0000  cc 6a 33 0f 0b e0 a0 59  50 bf 24 c6 08 00 45 00   ·j3···Y P·$···E·
0010  02 42 69 58 40 00 40 06  c1 ff ac 12 3b 64 2c e4   ·BiX@·@· ····;d,·
0020  f9 03 bc 08 00 50 25 47  f8 6d 54 98 86 b6 80 18   ·····P%G ·mT·····
0030  01 c2 0f 93 00 00 01 01  08 0a 7a 4b 71 c2 41 a4   ········ ··zKq·A·
0040  48 b4 50 4f 53 54 20 2f  75 73 65 72 69 6e 66 6f   H·POST / userinfo
0050  2e 70 68 70 20 48 54 54  50 2f 31 2e 31 0d 0a 48   .php HTT P/1.1··H
0060  6f 73 74 3a 20 74 65 73  74 70 68 70 2e 76 75 6c   ost: tes tphp.vul
0070  6e 77 65 62 2e 63 6f 6d  0d 0a 55 73 65 72 2d 41   nweb.com ··User-A
0080  67 65 6e 74 3a 20 4d 6f  7a 69 6c 6c 61 2f 35 2e   gent: Mo zilla/5.
0090  30 20 28 58 31 31 3b 20  4c 69 6e 75 78 20 78 38   0 (X11;  Linux x8
00a0  36 5f 36 34 3b 20 72 76  3a 31 32 38 2e 30 29 20   6_64; rv :128.0)
00b0  47 65 63 6b 6f 2f 32 30  31 30 30 31 30 31 20 46   Gecko/20 100101 F
00c0  69 72 65 66 6f 78 2f 31  32 38 2e 30 0d 0a 41 63   irefox/1 28.0··Ac
00d0  63 65 70 74 3a 20 74 65  78 74 2f 68 74 6d 6c 2c   cept: te xt/html,
00e0  61 70 70 6c 69 63 61 74  69 6f 6e 2f 78 68 74 6d   applicat ion/xhtm
00f0  6c 2b 78 6d 6c 2c 61 70  70 6c 69 63 61 74 69 6f   l+xml,ap plicatio
0100  6e 2f 78 6d 6c 3b 71 3d  30 2e 39 2c 2a 2f 2a 3b   n/xml;q= 0.9,*/*;
0110  71 3d 30 2e 38 0d 0a 41  63 63 65 70 74 2d 4c 61   q=0.8··A ccept-La
0120  6e 67 75 61 67 65 3a 20  65 6e 2d 55 53 2c 65 6e   nguage:  en-US,en
0130  3b 71 3d 30 2e 35 0d 0a  41 63 63 65 70 74 2d 45   ;q=0.5·· Accept-E
0140  6e 63 6f 64 69 6e 67 3a  20 67 7a 69 70 2c 20 64   ncoding:  gzip, d
0150  65 66 6c 61 74 65 0d 0a  43 6f 6e 74 65 6e 74 2d   eflate·· Content-
0160  54 79 70 65 3a 20 61 70  70 6c 69 63 61 74 69 6f   Type: ap plicatio
0170  6e 2f 78 2d 77 77 77 2d  66 6f 72 6d 2d 75 72 6c   n/x-www- form-url
0180  65 6e 63 6f 64 65 64 0d  0a 43 6f 6e 74 65 6e 74   encoded· ·Content
0190  2d 4c 65 6e 67 74 68 3a  20 32 32 0d 0a 4f 72 69   -Length:  22··Ori
01a0  67 69 6e 3a 20 68 74 74  70 3a 2f 2f 74 65 73 74   gin: htt p://test
01b0  70 68 70 2e 76 75 6c 6e  77 65 62 2e 63 6f 6d 0d   php.vuln web.com·
01c0  0a 43 6f 6e 6e 65 63 74  69 6f 6e 3a 20 6b 65 65   ·Connect ion: kee
01d0  70 2d 61 6c 69 76 65 0d  0a 52 65 66 65 72 65 72   p-alive· ·Referer
01e0  3a 20 68 74 74 70 3a 2f  2f 74 65 73 74 70 68 70   : http:/ /testphp
01f0  2e 76 75 6c 6e 77 65 62  2e 63 6f 6d 2f 6c 6f 67   .vulnweb .com/log
0200  69 6e 2e 70 68 70 0d 0a  55 70 67 72 61 64 65 2d   in.php·· Upgrade-
0210  49 6e 73 65 63 75 72 65  2d 52 65 71 75 65 73 74   Insecure -Request
0220  73 3a 20 31 0d 0a 50 72  69 6f 72 69 74 79 3a 20   s: 1··Pr iority:
0230  75 3d 30 2c 20 69 0d 0a  0d 0a 75 6e 61 6d 65 3d   u=0, i·· ··uname=
0240  73 61 6b 65 63 26 70 61  73 73 3d 73 61 6b 65 63   sakec&pa ss=sakec
```

4.8 Conclusion:

In this experiment, we explored the capabilities of Wireshark to capture and analyze real-time network traffic. We successfully identified and filtered various network protocols such as HTTP, TCP, and DNS, and examined packet structures to extract meaningful insights like IP addresses, HTTP responses, and TCP handshakes. The exercise demonstrated how unencrypted protocols can expose sensitive data such as login credentials. Through hands-on tasks like filtering for HTTP and DNS traffic, identifying endpoints, and analyzing session flows, we gained practical experience in interpreting packet-level data for security analysis, troubleshooting, and protocol understanding. This experiment deepened our skills in network monitoring and reinforced the importance of encryption and proper network configurations in safeguarding sensitive information.