Faculty of Engineering and Technology

Electrical and Computer Engineering

Department ENCS4130 || Computer Networks

Laboratory

TODO 6

EXP. No. 10

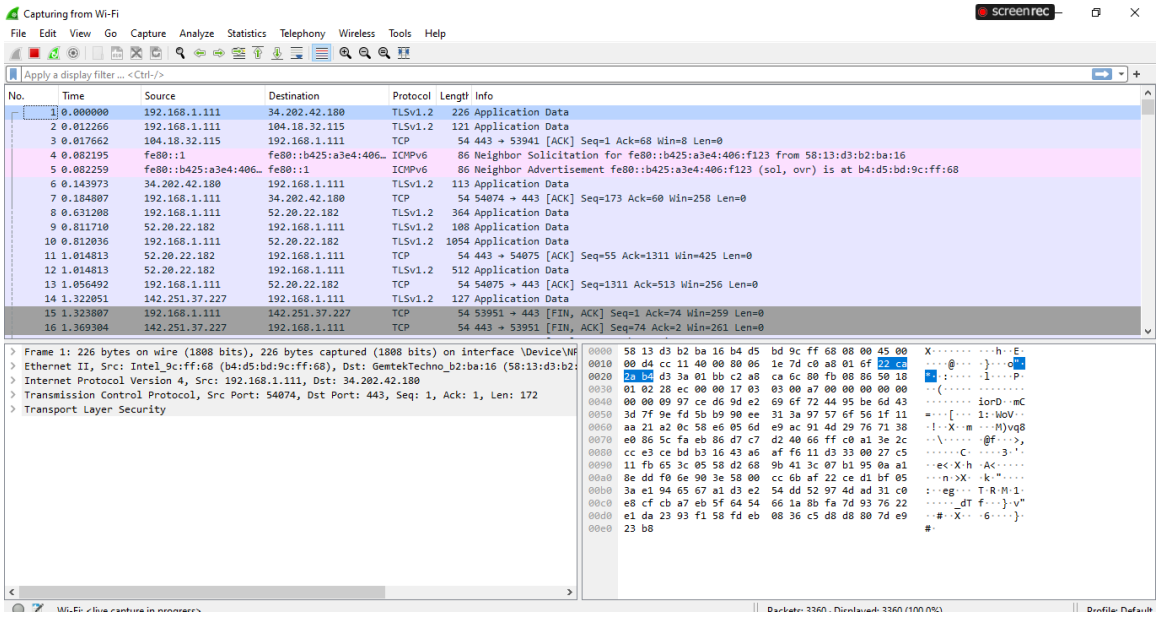
Prepared By: Eman Asfour 1200206

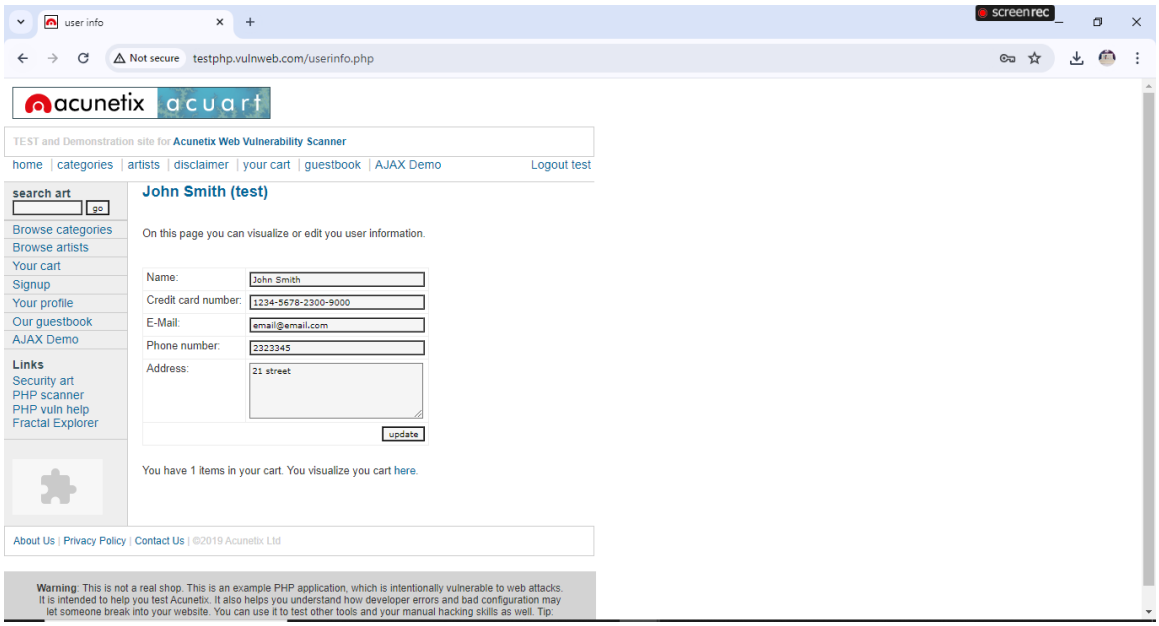
Instructor: Dr. Ismail Khater

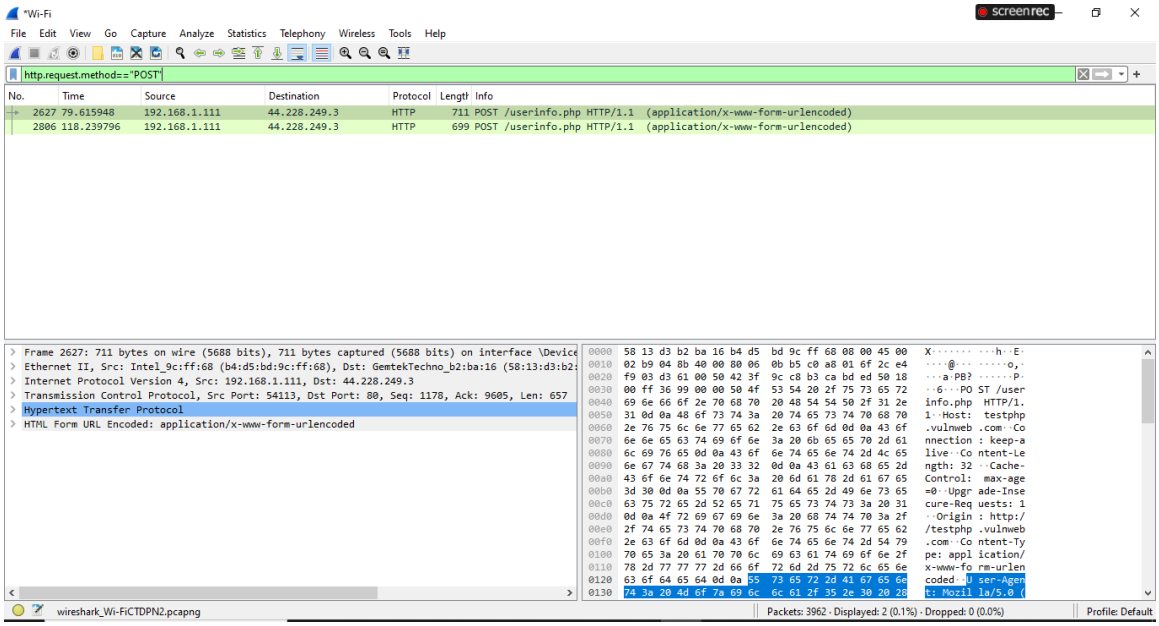
T.A: Eng. Burhan Dar Assi

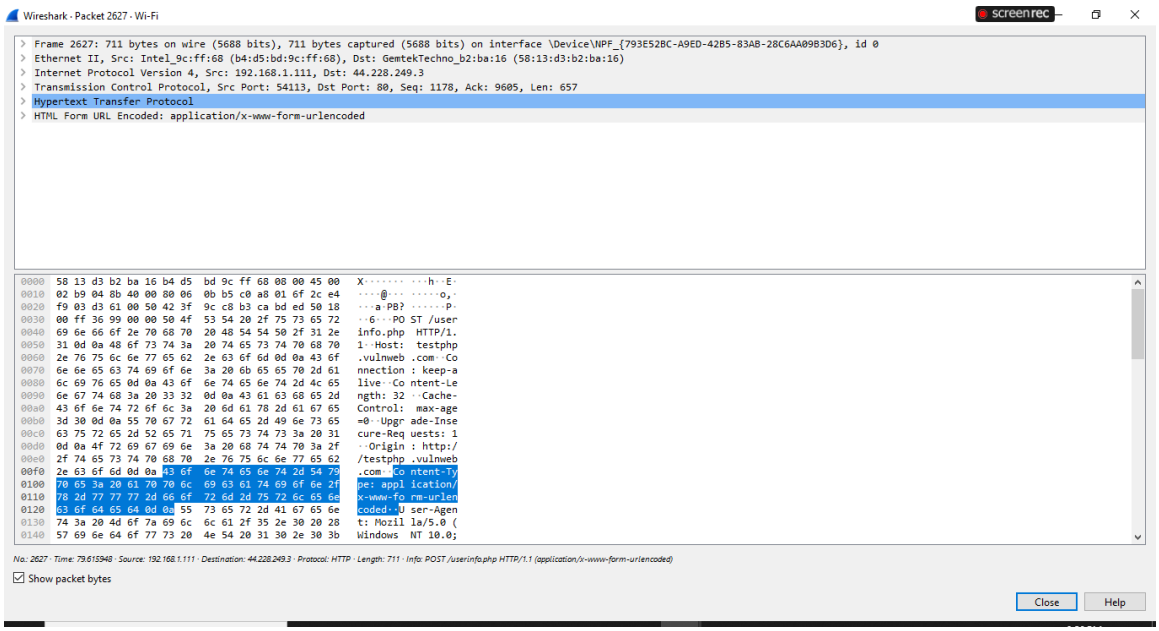
Section: 2

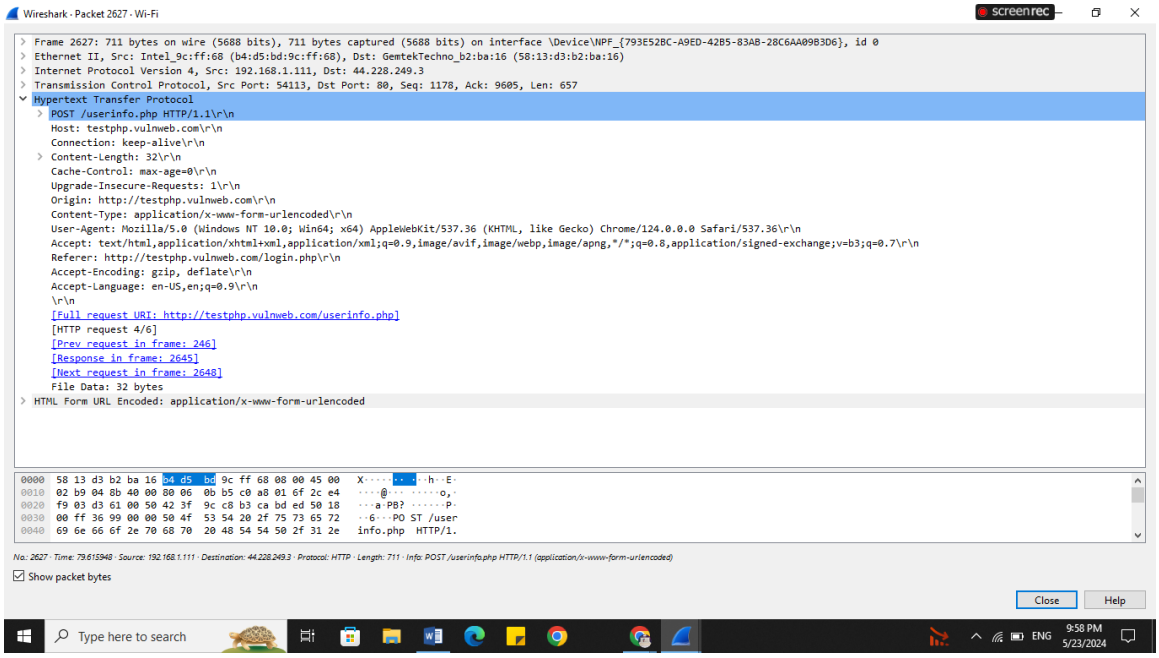
Part one

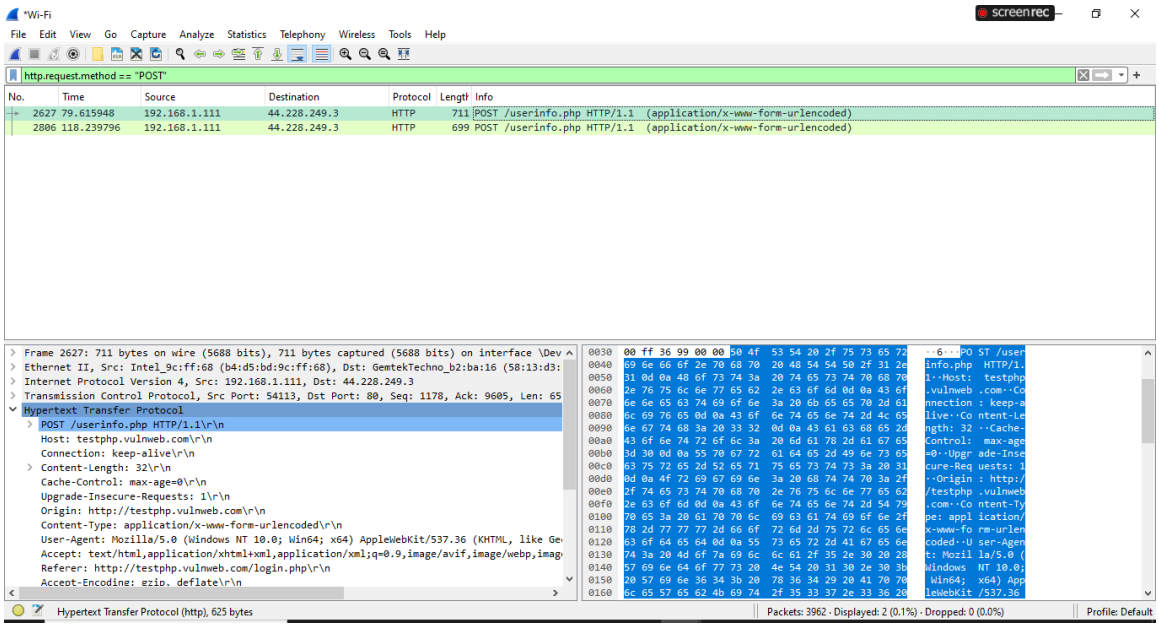

Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.1.111 34.202.42.180 TLSv1.2 226 Application Data
2 0.012266 192.168.1.111 104.18.32.115 TLSv1.2 121 Application Data
3 0.017662 104.18.32.115 192.168.1.111 TCP 54 443 → 53941 [ACK] Seq=1 Ack=68 Win=8 Len=0
4 0.082195 fe80::1 fe80::b425:a3e4:406… ICMPv6 86 Neighbor Solicitation for fe80::b425:a3e4:406:f123 from 58:13:d3:b2:ba:16
5 0.082259 fe80::b425:a3e4:406… fe80::1 ICMPv6 86 Neighbor Advertisement fe80::b425:a3e4:406:f123 (sol, ovr) is at b4:d5:bd:9c:ff:68
6 0.143973 34.202.42.180 192.168.1.111 TLSv1.2 113 Application Data
7 0.184807 192.168.1.111 34.202.42.180 TCP 54 54074 → 443 [ACK] Seq=173 Ack=60 Win=258 Len=0
8 0.631208 192.168.1.111 52.20.22.182 TLSv1.2 364 Application Data
9 0.811710 52.20.22.182 192.168.1.111 TLSv1.2 108 Application Data
10 0.812036 192.168.1.111 52.20.22.182 TLSv1.2 1054 Application Data
11 1.014813 52.20.22.182 192.168.1.111 TCP 54 443 → 54075 [ACK] Seq=55 Ack=1311 Win=425 Len=0
12 1.014813 52.20.22.182 192.168.1.111 TLSv1.2 512 Application Data
13 1.056492 192.168.1.111 52.20.22.182 TCP 54 54075 → 443 [ACK] Seq=1311 Ack=513 Win=256 Len=0
14 1.322051 142.251.37.227 192.168.1.111 TLSv1.2 127 Application Data
15 1.323807 192.168.1.111 142.251.37.227 TCP 54 53951 → 443 [FIN, ACK] Seq=1 Ack=74 Win=259 Len=0
16 1.369304 142.251.37.227 192.168.1.111 TCP 54 443 → 53951 [FIN, ACK] Seq=74 Ack=2 Win=261 Len=0
Frame 1: 226 bytes on wire (1808 bits), 226 bytes captured (1808 bits) on interface \Device\NF
Ethernet II, Src: Intel_9c:ff:68 (b4:d5:bd:9c:ff:68), Dst: GemtekTechno_b2:ba:16 (58:13:d3:b2:
Internet Protocol Version 4, Src: 192.168.1.111, Dst: 34.202.42.180
Transmission Control Protocol, Src Port: 54074, Dst Port: 443, Seq: 1, Ack: 1, Len: 172
Transport Layer Security
0000 58 13 d3 b2 ba 16 b4 d5 bd 9c ff 68 08 00 45 00
0010 00 d4 cc 11 40 00 80 06 1e 7d c0 a8 01 6f 22 ca
0020 2a b4 d3 3a 01 bb c2 a8 ca 6c 80 fb 08 86 50 18
0030 01 02 28 ec 00 00 17 03 03 00 a7 00 00 00 00 00
0040 00 00 09 97 ce d6 9d e2 69 6f 72 44 95 be 6d 43
0050 3d 7f 9e fd 5b b9 90 ee 31 3a 97 57 6f 56 1f 11
0060 aa 21 a2 0c 58 e6 05 6d e9 ac 91 4d 29 76 71 38
0070 e0 86 5c fa eb 86 d7 c7 d2 40 66 ff c0 a1 3e 2c
0080 cc e3 ce bd b3 16 43 a6 af f6 11 d3 33 00 27 c5
0090 11 fb 65 3c 05 58 d2 68 9b 41 3c 07 b1 95 0a a1
00a0 8e dd f0 6e 90 3e 58 00 cc 6b af 22 ce d1 bf 05
00b0 3a e1 94 65 67 a1 d3 e2 54 dd 52 97 4d ad 31 c0
00c0 e8 cf cb a7 eb 5f 64 54 66 1a 8b fa 7d 93 76 22
00d0 e1 da 23 93 f1 58 fd eb 08 36 c5 d8 d8 80 7d e9
00e0 23 b8
Packets: 3360 · Displayed: 3360 (100.0%)
Profile: Default

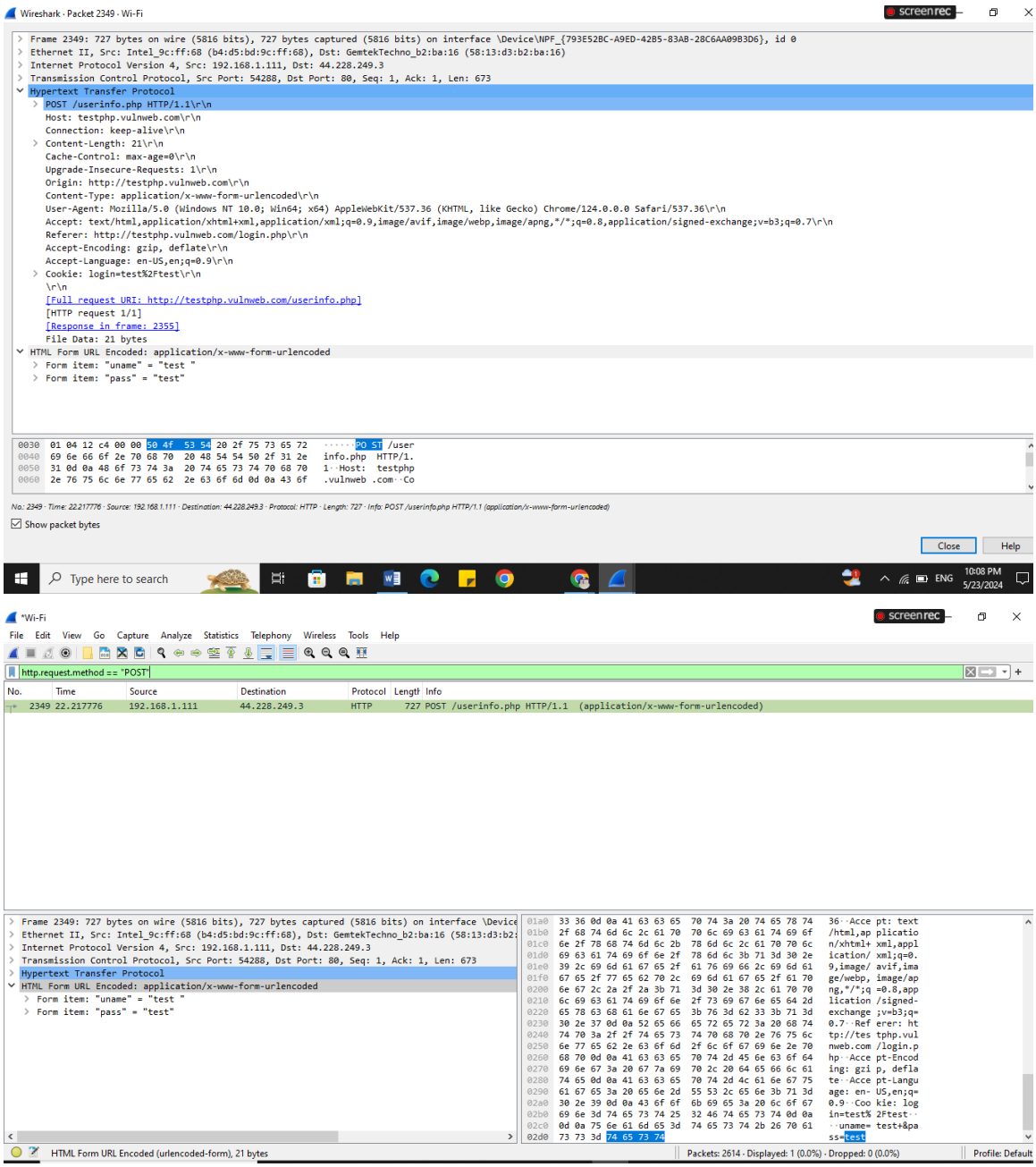

user info
Not secure testphp.vulnweb.com/userinfo.php
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
Logout test
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
John Smith (test)
On this page you can visualize or edit you user information.
Name: John Smith
Credit card number: 1234-5678-2300-9000
E-Mail: email@email.com
Phone number: 2323345
Address: 21 street
update
You have 1 items in your cart. You visualize you cart here.
About Us | Privacy Policy | Contact Us | ©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:


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.request.method=="POST"
No. Time Source Destination Protocol Length Info
2627 79.615948 192.168.1.111 44.228.249.3 HTTP 711 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
2806 118.239796 192.168.1.111 44.228.249.3 HTTP 699 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
Frame 2627: 711 bytes on wire (5688 bits), 711 bytes captured (5688 bits) on interface \Device
Ethernet II, Src: Intel_9c:ff:68 (b4:d5:bd:9c:ff:68), Dst: GemtekTechno_b2:ba:16 (58:13:d3:b2:
Internet Protocol Version 4, Src: 192.168.1.111, Dst: 44.228.249.3
Transmission Control Protocol, Src Port: 54113, Dst Port: 80, Seq: 1178, Ack: 9605, Len: 657
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
0000 58 13 d3 b2 ba 16 b4 d5 bd 9c ff 68 08 00 45 00 X·····h··E·
0010 02 b9 04 8b 40 00 80 06 0b b5 c0 a8 01 6f 2c e4 ····@····o,·
0020 f9 03 d3 61 00 50 42 3f 9c c8 b3 ca bd ed 50 18 ···a·PB? ·····P·
0030 00 ff 36 99 00 00 50 4f 53 54 20 2f 75 73 65 72 ··6···PO ST /user
0040 69 6e 66 6f 2e 70 68 70 20 48 54 54 50 2f 31 2e info.php HTTP/1.
0050 31 0d 0a 48 6f 73 74 3a 20 74 65 73 74 70 68 70 1··Host: testphp
0060 2e 76 75 6c 6e 77 65 62 2e 63 6f 6d 0d 0a 43 6f .vulnweb .com··Co
0070 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 nnection : keep-a
0080 6c 69 76 65 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 live··Co ntent-Le
0090 6e 67 74 68 3a 20 33 32 0d 0a 43 61 63 68 65 2d ngth: 32 ··Cache-
00a0 43 6f 6e 74 72 6f 6c 3a 20 6d 61 78 2d 61 67 65 Control: max-age
00b0 3d 30 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 =0··Upgr ade-Inse
00c0 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a 20 31 cure-Req uests: 1
00d0 0d 0a 4f 72 69 67 69 6e 3a 20 68 74 74 70 3a 2f ··Origin : http:/
00e0 2f 74 65 73 74 70 68 70 2e 76 75 6c 6e 77 65 62 /testphp .vulnweb
00f0 2e 63 6f 6d 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 .com··Co ntent-Ty
0100 70 65 3a 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f pe: appl ication/
0110 78 2d 77 77 77 2d 66 6f 72 6d 2d 75 72 6c 65 6e x-www-fo rm-urlen
0120 63 6f 64 65 64 0d 0a 55 73 65 72 2d 41 67 65 6e coded··U ser-Agen
0130 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 t: Mozil la/5.0 (
wireshark_Wi-FiCTDPN2.pcapng
Packets: 3962 · Displayed: 2 (0.1%) · Dropped: 0 (0.0%)
Profile: Default

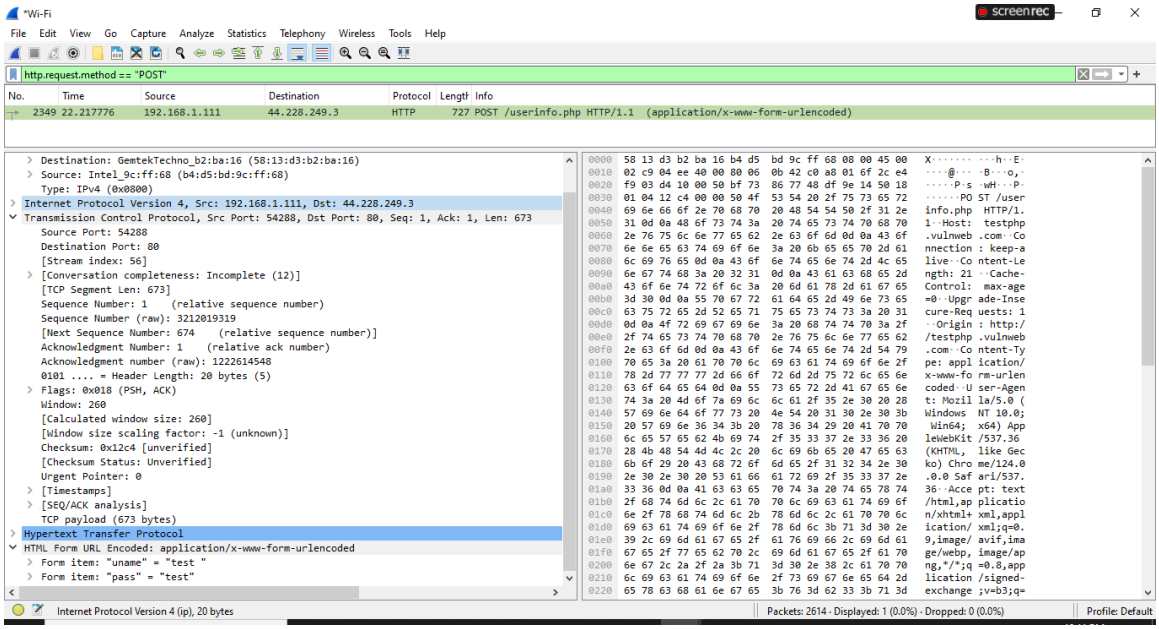

Wireshark · Packet 2627 · Wi-Fi
screenrec
Frame 2627: 711 bytes on wire (5688 bits), 711 bytes captured (5688 bits) on interface \Device\NPF_{793E52BC-A9ED-42B5-83AB-28C6AA09B3D6}, id 0
Ethernet II, Src: Intel_9c:ff:68 (b4:d5:bd:9c:ff:68), Dst: GemtekTechno_b2:ba:16 (58:13:d3:b2:ba:16)
Internet Protocol Version 4, Src: 192.168.1.111, Dst: 44.228.249.3
Transmission Control Protocol, Src Port: 54113, Dst Port: 80, Seq: 1178, Ack: 9605, Len: 657
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
0000 58 13 d3 b2 ba 16 b4 d5 bd 9c ff 68 08 00 45 00 X·····h··E·
0010 02 b9 04 8b 40 00 80 06 0b b5 c0 a8 01 6f 2c e4 ····@····o,·
0020 f9 03 d3 61 00 50 42 3f 9c c8 b3 ca bd ed 50 18 ···a·PB?·····P·
0030 00 ff 36 99 00 00 50 4f 53 54 20 2f 75 73 65 72 ··6···PO ST /user
0040 69 6e 66 6f 2e 70 68 70 20 48 54 54 50 2f 31 2e info.php HTTP/1.
0050 31 0d 0a 48 6f 73 74 3a 20 74 65 73 74 70 68 70 1··Host: testphp
0060 2e 76 75 6c 6e 77 65 62 2e 63 6f 6d 0d 0a 43 6f .vulnweb .com··Co
0070 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 nnection : keep-a
0080 6c 69 76 65 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 live··Co ntent-Le
0090 6e 67 74 68 3a 20 33 32 0d 0a 43 61 63 68 65 2d ngth: 32 ··Cache-
00a0 43 6f 6e 74 72 6f 6c 3a 20 6d 61 78 2d 61 67 65 Control: max-age
00b0 3d 30 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 =0··Upgr ade-Inse
00c0 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a 20 31 cure-Req uests: 1
00d0 0d 0a 4f 72 69 67 69 6e 3a 20 68 74 74 70 3a 2f ··Origin : http:/
00e0 2f 74 65 73 74 70 68 70 2e 76 75 6c 6e 77 65 62 /testphp .vulnweb
00f0 2e 63 6f 6d 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 .com··Co ntent-Ty
0100 70 65 3a 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f pe: appl ication/
0110 78 2d 77 77 77 2d 66 6f 72 6d 2d 75 72 6c 65 6e x-www-fo rm-urlen
0120 63 6f 64 65 64 0d 0a 55 73 65 72 2d 41 67 65 6e coded··U ser-Agen
0130 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 t: Mozil la/5.0 (
0140 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 3b Windows NT 10.0;
No.: 2627 · Time: 79.615948 · Source: 192.168.1.111 · Destination: 44.228.249.3 · Protocol: HTTP · Length: 711 · Info: POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
Show packet bytes
Close
Help

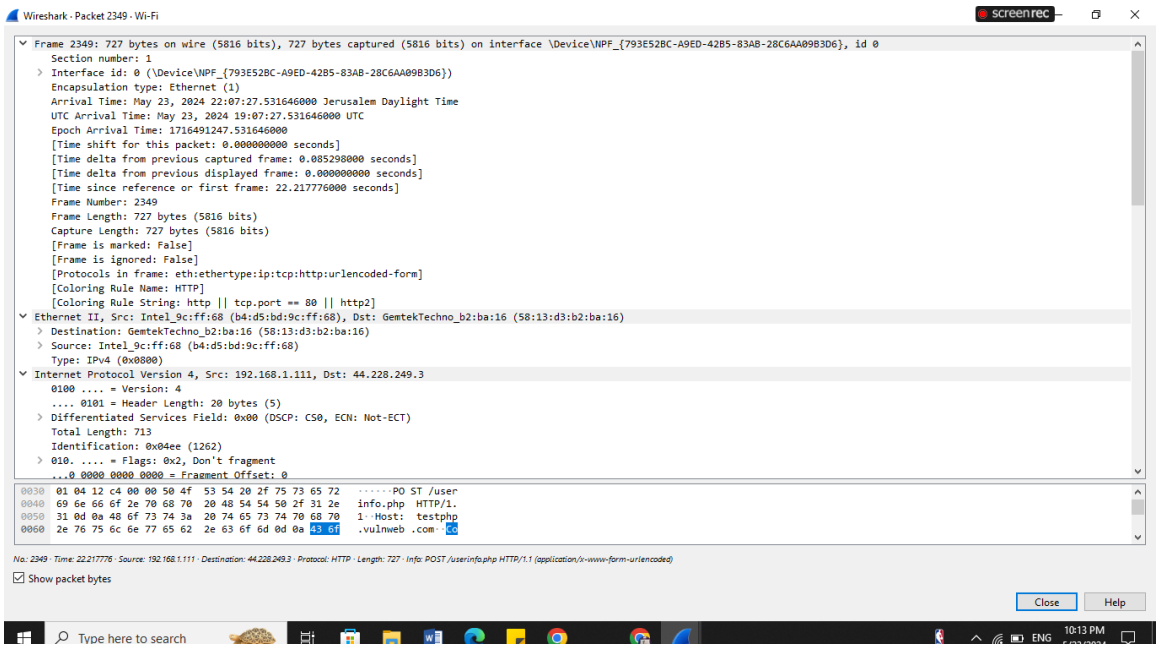

Wireshark · Packet 2627 · Wi-Fi
screenrec
Frame 2627: 711 bytes on wire (5688 bits), 711 bytes captured (5688 bits) on interface \Device\NPF_{793E52BC-A9ED-42B5-83AB-28C6AA09B3D6}, id 0
Ethernet II, Src: Intel_9c:ff:68 (b4:d5:bd:9c:ff:68), Dst: GemtekTechno_b2:ba:16 (58:13:d3:b2:ba:16)
Internet Protocol Version 4, Src: 192.168.1.111, Dst: 44.228.249.3
Transmission Control Protocol, Src Port: 54113, Dst Port: 80, Seq: 1178, Ack: 9605, Len: 657
Hypertext Transfer Protocol
POST /userinfo.php HTTP/1.1\r\n
Host: testphp.vulnweb.com\r\n
Connection: keep-alive\r\n
Content-Length: 32\r\n
Cache-Control: max-age=0\r\n
Upgrade-Insecure-Requests: 1\r\n
Origin: http://testphp.vulnweb.com\r\n
Content-Type: application/x-www-form-urlencoded\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
Referer: http://testphp.vulnweb.com/login.php\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
\r\n
[Full request URI: http://testphp.vulnweb.com/userinfo.php]
[HTTP request 4/6]
[Prev request in frame: 246]
[Response in frame: 2645]
[Next request in frame: 2648]
File Data: 32 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
0000 58 13 d3 b2 ba 16 b4 d5 bd 9c ff 68 08 00 45 00 X·····h··E·
0010 02 b9 04 8b 40 00 80 06 0b b5 c0 a8 01 6f 2c e4 ····@····o,·
0020 f9 03 d3 61 00 50 42 3f 9c c8 b3 ca bd ed 50 18 ···a·PB?·····P·
0030 00 ff 36 99 00 00 50 4f 53 54 20 2f 75 73 65 72 ··6···PO ST /user
0040 69 6e 66 6f 2e 70 68 70 20 48 54 54 50 2f 31 2e info.php HTTP/1.
No.: 2627 · Time: 79.615948 · Source: 192.168.1.111 · Destination: 44.228.249.3 · Protocol: HTTP · Length: 711 · Info: POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
Show packet bytes
Close
Help
Type here to search
ENG
9:58 PM
5/23/2024

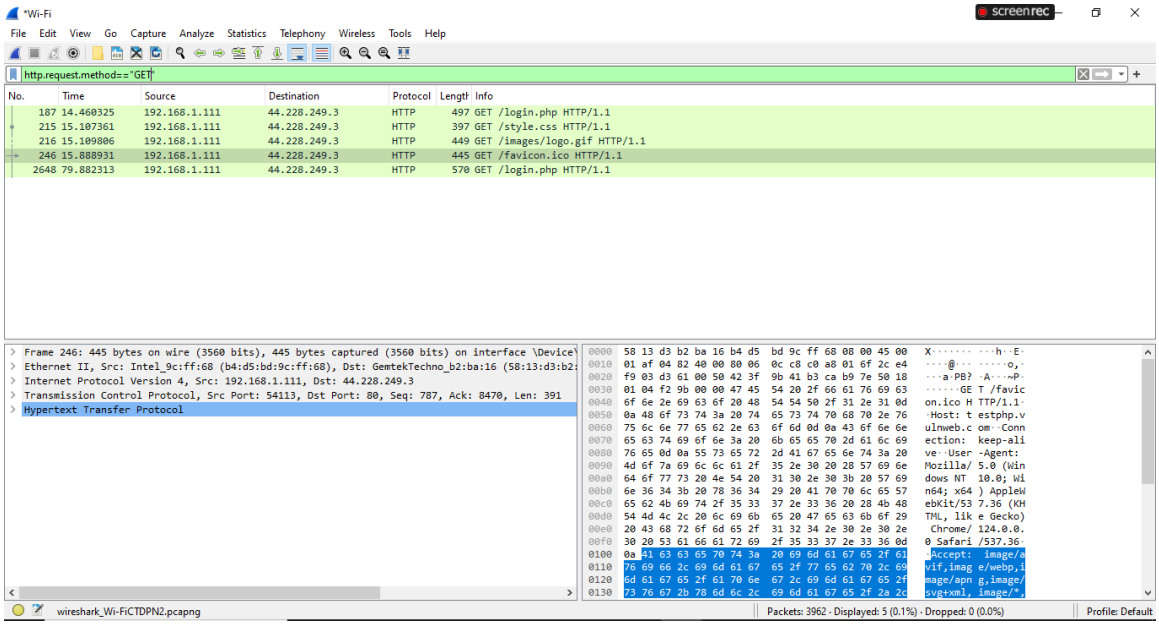

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.request.method == "POST"
No. Time Source Destination Protocol Length Info
2627 79.615948 192.168.1.111 44.228.249.3 HTTP 711 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
2806 118.239796 192.168.1.111 44.228.249.3 HTTP 699 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
Frame 2627: 711 bytes on wire (5688 bits), 711 bytes captured (5688 bits) on interface \Dev
Ethernet II, Src: Intel_9c:ff:68 (b4:d5:bd:9c:ff:68), Dst: GemtekTechno_b2:ba:16 (58:13:d3:
Internet Protocol Version 4, Src: 192.168.1.111, Dst: 44.228.249.3
Transmission Control Protocol, Src Port: 54113, Dst Port: 80, Seq: 1178, Ack: 9605, Len: 65
Hypertext Transfer Protocol
POST /userinfo.php HTTP/1.1\r\n
Host: testphp.vulnweb.com\r\n
Connection: keep-alive\r\n
Content-Length: 32\r\n
Cache-Control: max-age=0\r\n
Upgrade-Insecure-Requests: 1\r\n
Origin: http://testphp.vulnweb.com\r\n
Content-Type: application/x-www-form-urlencoded\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Ge
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag
Referer: http://testphp.vulnweb.com/login.php\r\n
Accept-Encoding: gzip, deflate\r\n
0030 00 ff 36 99 00 00 50 4f 53 54 20 2f 75 73 65 72
0040 69 6e 66 6f 2e 70 68 70 20 48 54 54 50 2f 31 2e
0050 31 0d 0a 48 6f 73 74 3a 20 74 65 73 74 70 68 70
0060 2e 76 75 6c 6e 77 65 62 2e 63 6f 6d 0d 0a 43 6f
0070 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61
0080 6c 69 76 65 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65
0090 6e 67 74 68 3a 20 33 32 0d 0a 43 61 63 68 65 2d
00a0 43 6f 6e 74 72 6f 6c 3a 20 6d 61 78 2d 61 67 65
00b0 3d 30 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65
00c0 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a 20 31
00d0 0d 0a 4f 72 69 67 69 6e 3a 20 68 74 74 70 3a 2f
00e0 2f 74 65 73 74 70 68 70 2e 76 75 6c 6e 77 65 62
00f0 2e 63 6f 6d 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79
0100 70 65 3a 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f
0110 78 2d 77 77 77 2d 66 6f 72 6d 2d 75 72 6c 65 6e
0120 63 6f 64 65 64 0d 0a 55 73 65 72 2d 41 67 65 6e
0130 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28
0140 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 3b
0150 20 57 69 6e 36 34 3b 20 78 36 34 29 20 41 70 70
0160 6c 65 57 65 62 4b 69 74 2f 35 33 37 2e 33 36 20
Hypertext Transfer Protocol (http), 625 bytes
Packets: 3962 · Displayed: 2 (0.1%) · Dropped: 0 (0.0%)
Profile: Default

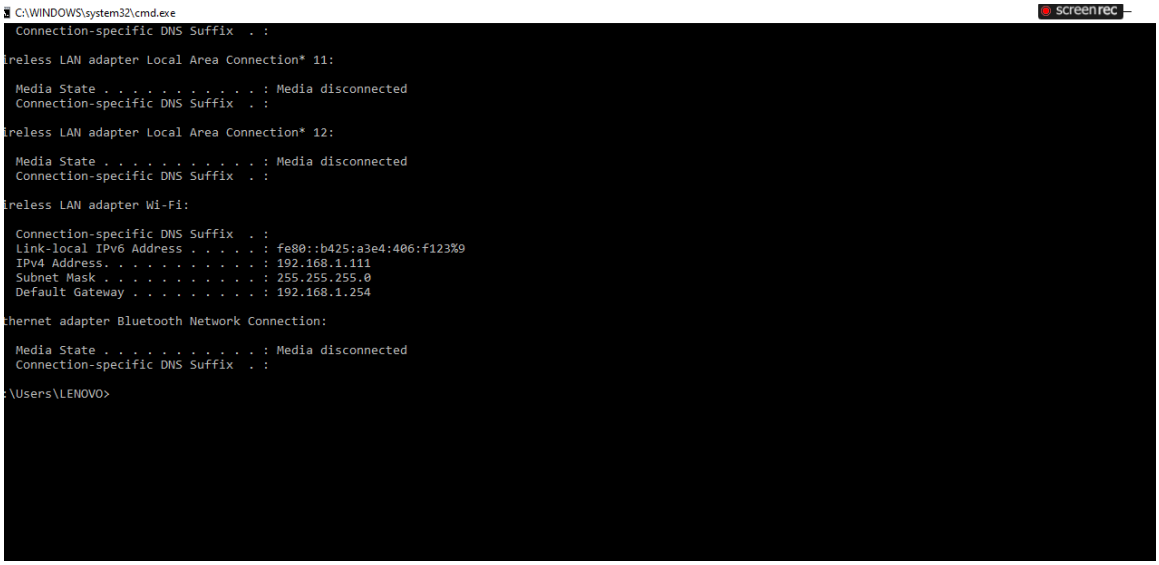

Wireshark · Packet 2349 · Wi-Fi
screenrec
Frame 2349: 727 bytes on wire (5816 bits), 727 bytes captured (5816 bits) on interface \Device\NPF_{793E52BC-A9ED-42B5-83AB-28C6AA09B3D6}, id 0
Ethernet II, Src: Intel_9c:ff:68 (b4:d5:bd:9c:ff:68), Dst: GemtekTechno_b2:ba:16 (58:13:d3:b2:ba:16)
Internet Protocol Version 4, Src: 192.168.1.111, Dst: 44.228.249.3
Transmission Control Protocol, Src Port: 54288, Dst Port: 80, Seq: 1, Ack: 1, Len: 673
Hypertext Transfer Protocol
POST /userinfo.php HTTP/1.1\r\n
Host: testphp.vulnweb.com\r\n
Connection: keep-alive\r\n
Content-Length: 21\r\n
Cache-Control: max-age=0\r\n
Upgrade-Insecure-Requests: 1\r\n
Origin: http://testphp.vulnweb.com\r\n
Content-Type: application/x-www-form-urlencoded\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
Referer: http://testphp.vulnweb.com/login.php\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
Cookie: login=test%2Ftest\r\n
\r\n
[Full request URI: http://testphp.vulnweb.com/userinfo.php]
[HTTP request 1/1]
[Response in frame: 2355]
File Data: 21 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "uname" = "test "
Form item: "pass" = "test"
0030 01 04 12 c4 00 00 50 4f 53 54 20 2f 75 73 65 72 ····· PO ST /user
0040 69 6e 66 6f 2e 70 68 70 20 48 54 54 50 2f 31 2e info.php HTTP/1.
0050 31 0d 0a 48 6f 73 74 3a 20 74 65 73 74 70 68 70 1··Host: testphp
0060 2e 76 75 6c 6e 77 65 62 2e 63 6f 6d 0d 0a 43 6f .vulnweb .com··Co
No.: 2349 · Time: 22.217776 · Source: 192.168.1.111 · Destination: 44.228.249.3 · Protocol: HTTP · Length: 727 · Info: POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
Show packet bytes
Close
Help
Type here to search
ENG
10:08 PM
5/23/2024

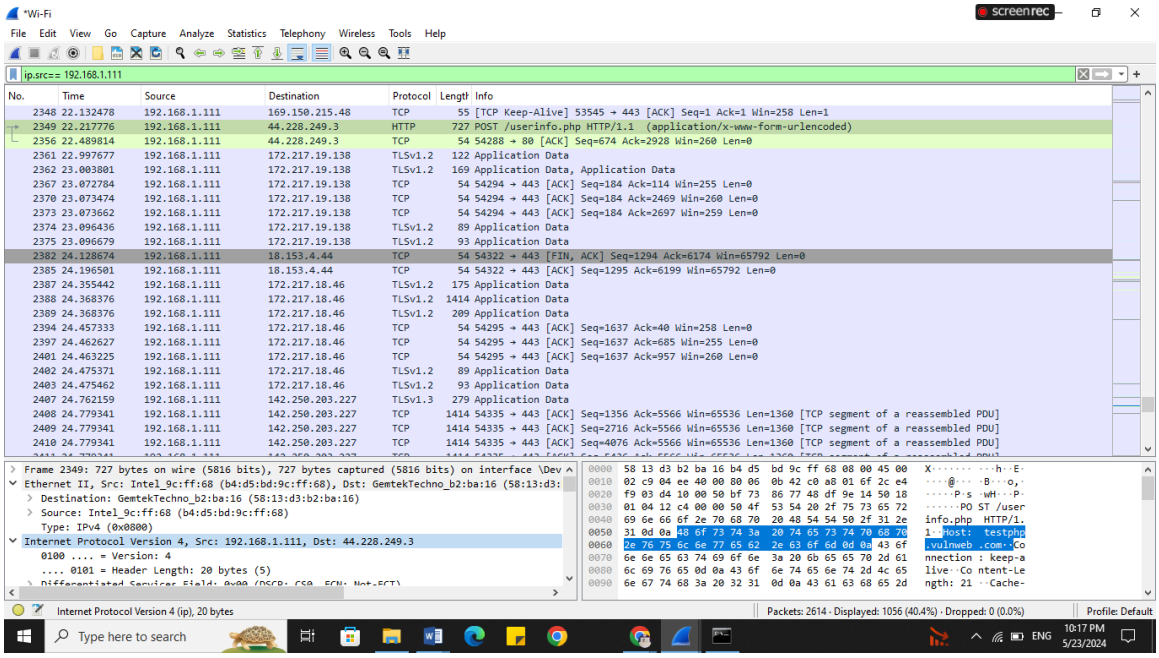
*Wi-Fi
screenrec
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.request.method == "POST"
No. Time Source Destination Protocol Length Info
2349 22.217776 192.168.1.111 44.228.249.3 HTTP 727 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
Frame 2349: 727 bytes on wire (5816 bits), 727 bytes captured (5816 bits) on interface \Device
Ethernet II, Src: Intel_9c:ff:68 (b4:d5:bd:9c:ff:68), Dst: GemtekTechno_b2:ba:16 (58:13:d3:b2:
Internet Protocol Version 4, Src: 192.168.1.111, Dst: 44.228.249.3
Transmission Control Protocol, Src Port: 54288, Dst Port: 80, Seq: 1, Ack: 1, Len: 673
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "uname" = "test "
Form item: "pass" = "test"
01a0 33 36 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 36··Acce pt: text
01b0 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f /html,ap plicatio
01c0 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c n/xhtml+ xml,appl
01d0 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e ication/ xml;q=0.
01e0 39 2c 69 6d 61 67 65 2f 61 76 69 66 2c 69 6d 61 9,image/ avif,ima
01f0 67 65 2f 77 65 62 70 2c 69 6d 61 67 65 2f 61 70 ge/webp, image/ap
0200 6e 67 2c 2a 2f 2a 3b 71 3d 30 2e 38 2c 61 70 70 ng,*/*;q =0.8,app
0210 6c 69 63 61 74 69 6f 6e 2f 73 69 67 6e 65 64 2d lication /signed-
0220 65 78 63 68 61 6e 67 65 3b 76 3d 62 33 3b 71 3d exchange ;v=b3;q=
0230 30 2e 37 0d 0a 52 65 66 65 72 65 72 3a 20 68 74 0.7··Ref erer: ht
0240 74 70 3a 2f 2f 74 65 73 74 70 68 70 2e 76 75 6c tp://tes tphp.vul
0250 6e 77 65 62 2e 63 6f 6d 2f 6c 6f 67 69 6e 2e 70 nweb.com /login.p
0260 68 70 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 hp··Acce pt-Encod
0270 69 6e 67 3a 20 67 7a 69 70 2c 20 64 65 66 6c 61 ing: gzi p, defla
0280 74 65 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 te··Acce pt-Langu
0290 61 67 65 3a 20 65 6e 2d 55 53 2c 65 6e 3b 71 3d age: en- US,en;q=
02a0 30 2e 39 0d 0a 43 6f 6f 6b 69 65 3a 20 6c 6f 67 0.9··Coo kie: log
02b0 69 6e 3d 74 65 73 74 25 32 46 74 65 73 74 0d 0a in=test% 2Ftest··
02c0 0d 0a 75 6e 61 6d 65 3d 74 65 73 74 2b 26 70 61 ··uname= test+&pa
02d0 73 73 3d 74 65 73 74 ss=test
HTML Form URL Encoded (urlencoded-form), 21 bytes
Packets: 2614 · Displayed: 1 (0.0%) · Dropped: 0 (0.0%)
Profile: Default

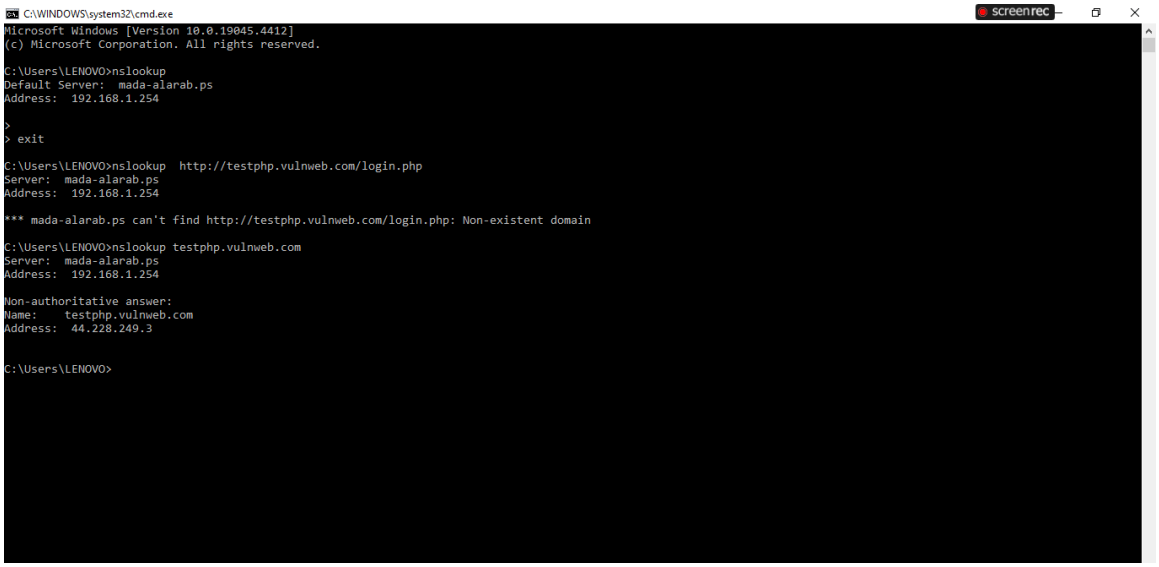

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.request.method == "POST"
No. Time Source Destination Protocol Length Info
2349 22.217776 192.168.1.111 44.228.249.3 HTTP 727 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
Destination: GemtekTechno_b2:ba:16 (58:13:d3:b2:ba:16)
Source: Intel_9c:ff:68 (b4:d5:bd:9c:ff:68)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.1.111, Dst: 44.228.249.3
Transmission Control Protocol, Src Port: 54288, Dst Port: 80, Seq: 1, Ack: 1, Len: 673
Source Port: 54288
Destination Port: 80
[Stream index: 56]
[Conversation completeness: Incomplete (12)]
[TCP Segment Len: 673]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 3212019319
[Next Sequence Number: 674 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 1222614548
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window: 260
[Calculated window size: 260]
[Window size scaling factor: -1 (unknown)]
Checksum: 0x12c4 [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
[Timestamps]
[SEQ/ACK analysis]
TCP payload (673 bytes)
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "uname" = "test "
Form item: "pass" = "test"
0000 58 13 d3 b2 ba 16 b4 d5 bd 9c ff 68 08 00 45 00 X·····h··E·
0010 02 c9 04 ee 40 00 80 06 0b 42 c0 a8 01 6f 2c e4 ····@···B···o,·
0020 f9 03 d4 10 00 50 bf 73 86 77 48 df 9e 14 50 18 ·····P·s ·wH···P·
0030 01 04 12 c4 00 00 50 4f 53 54 20 2f 75 73 65 72 ·····PO ST /user
0040 69 6e 66 6f 2e 70 68 70 20 48 54 54 50 2f 31 2e info.php HTTP/1.
0050 31 0d 0a 48 6f 73 74 3a 20 74 65 73 74 70 68 70 1··Host: testphp
0060 2e 76 75 6c 6e 77 65 62 2e 63 6f 6d 0d 0a 43 6f .vulnweb .com··Co
0070 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 nnection : keep-a
0080 6c 69 76 65 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 live··Co ntent-Le
0090 6e 67 74 68 3a 20 32 31 0d 0a 43 61 63 68 65 2d ngth: 21 ··Cache-
00a0 43 6f 6e 74 72 6f 6c 3a 20 6d 61 78 2d 61 67 65 Control: max-age
00b0 3d 30 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 =0··Upgr ade-Inse
00c0 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a 20 31 cure-Req uests: 1
00d0 0d 0a 4f 72 69 67 69 6e 3a 20 68 74 74 70 3a 2f ··Origin : http:/
00e0 2f 74 65 73 74 70 68 70 2e 76 75 6c 6e 77 65 62 /testphp .vulnweb
00f0 2e 63 6f 6d 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 .com··Co ntent-Ty
0100 70 65 3a 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f pe: appl ication/
0110 78 2d 77 77 77 2d 66 6f 72 6d 2d 75 72 6c 65 6e x-www-fo rm-urlen
0120 63 6f 64 65 64 0d 0a 55 73 65 72 2d 41 67 65 6e coded··U ser-Agen
0130 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 t: Mozil la/5.0 (
0140 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 3b Windows NT 10.0;
0150 20 57 69 6e 36 34 3b 20 78 36 34 29 20 41 70 70 Win64; x64) App
0160 6c 65 57 65 62 4b 69 74 2f 35 33 37 2e 33 36 20 leWebKit /537.36
0170 28 4b 48 54 4d 4c 2c 20 6c 69 6b 65 20 47 65 63 (KHTML, like Gec
0180 6b 6f 29 20 43 68 72 6f 6d 65 2f 31 32 34 2e 30 ko) Chro me/124.0
0190 2e 30 2e 30 20 53 61 66 61 72 69 2f 35 33 37 2e .0.0 Saf ari/537.
01a0 33 36 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 36··Acce pt: text
01b0 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f /html,ap plicatio
01c0 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c n/xhtml+ xml,appl
01d0 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e ication/ xml;q=0.
01e0 39 2c 69 6d 61 67 65 2f 61 76 69 66 2c 69 6d 61 9,image/ avif,ima
01f0 67 65 2f 77 65 62 70 2c 69 6d 61 67 65 2f 61 70 ge/webp, image/ap
0200 6e 67 2c 2a 2f 2a 3b 71 3d 30 2e 38 2c 61 70 70 ng,*/*;q =0.8,app
0210 6c 69 63 61 74 69 6f 6e 2f 73 69 67 6e 65 64 2d lication /signed-
0220 65 78 63 68 61 6e 67 65 3b 76 3d 62 33 3b 71 3d exchange ;v=b3;q=
Internet Protocol Version 4 (ip), 20 bytes
Packets: 2614 · Displayed: 1 (0.0%) · Dropped: 0 (0.0%)
Profile: Default

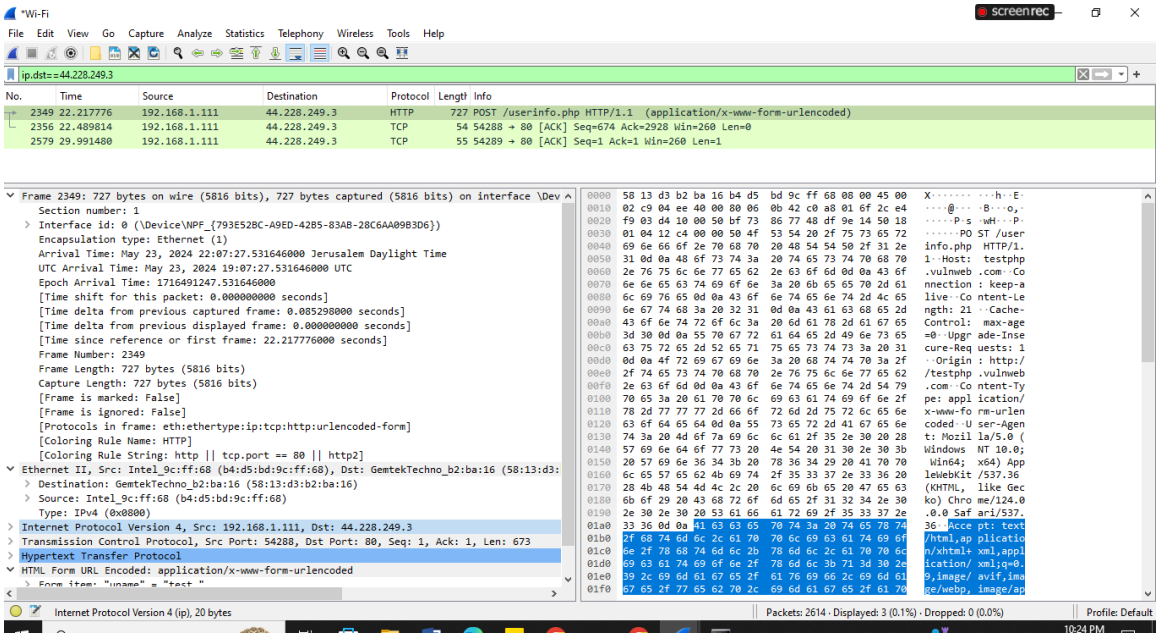

Wireshark · Packet 2349 · Wi-Fi
Frame 2349: 727 bytes on wire (5816 bits), 727 bytes captured (5816 bits) on interface \Device\NPF_{793E52BC-A9ED-42B5-83AB-28C6AA09B3D6}, id 0
Section number: 1
Interface id: 0 (\Device\NPF_{793E52BC-A9ED-42B5-83AB-28C6AA09B3D6})
Encapsulation type: Ethernet (1)
Arrival Time: May 23, 2024 22:07:27.531646000 Jerusalem Daylight Time
UTC Arrival Time: May 23, 2024 19:07:27.531646000 UTC
Epoch Arrival Time: 1716491247.531646000
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.085298000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 22.217776000 seconds]
Frame Number: 2349
Frame Length: 727 bytes (5816 bits)
Capture Length: 727 bytes (5816 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:http:urlencoded-form]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: Intel_9c:ff:68 (b4:d5:bd:9c:ff:68), Dst: GemtekTechno_b2:ba:16 (58:13:d3:b2:ba:16)
Destination: GemtekTechno_b2:ba:16 (58:13:d3:b2:ba:16)
Source: Intel_9c:ff:68 (b4:d5:bd:9c:ff:68)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.1.111, Dst: 44.228.249.3
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 713
Identification: 0x04ee (1262)
010. .... = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
0030 01 04 12 c4 00 00 50 4f 53 54 20 2f 75 73 65 72 ·····PO ST /user
0040 69 6e 66 6f 2e 70 68 70 20 48 54 54 50 2f 31 2e info.php HTTP/1.
0050 31 0d 0a 48 6f 73 74 3a 20 74 65 73 74 70 68 70 1··Host: testphp
0060 2e 76 75 6c 6e 77 65 62 2e 63 6f 6d 0d 0a 43 6f .vulnweb .com··Co
No.: 2349 · Time: 22.217776 · Source: 192.168.1.111 · Destination: 44.228.249.3 · Protocol: HTTP · Length: 727 · Info: POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
Show packet bytes
Close
Help
Type here to search
ENG
10:13 PM

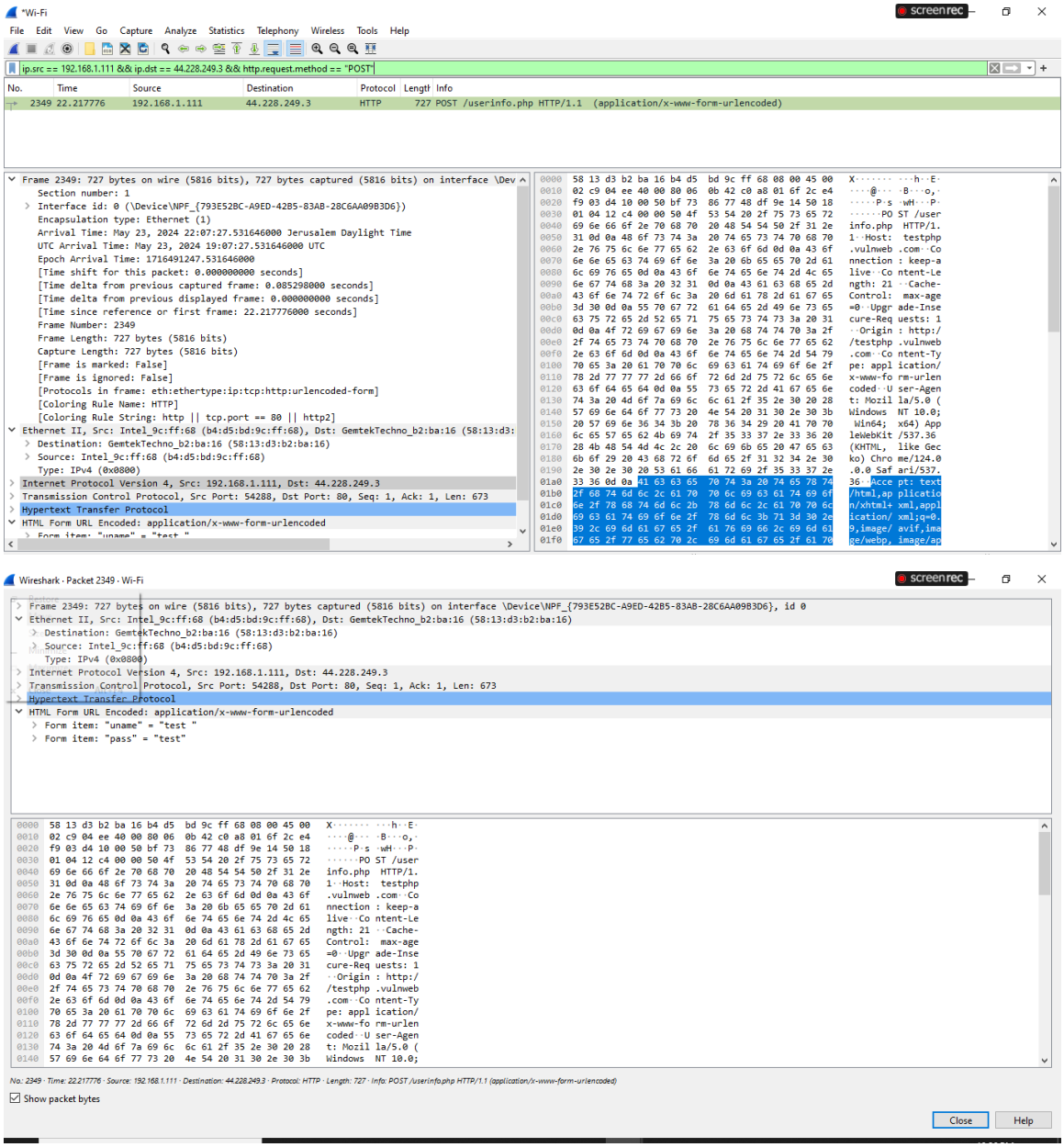

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.request.method=="GET"
No. Time Source Destination Protocol Length Info
187 14.460325 192.168.1.111 44.228.249.3 HTTP 497 GET /login.php HTTP/1.1
215 15.107361 192.168.1.111 44.228.249.3 HTTP 397 GET /style.css HTTP/1.1
216 15.109806 192.168.1.111 44.228.249.3 HTTP 449 GET /images/logo.gif HTTP/1.1
246 15.888931 192.168.1.111 44.228.249.3 HTTP 445 GET /favicon.ico HTTP/1.1
2648 79.882313 192.168.1.111 44.228.249.3 HTTP 570 GET /login.php HTTP/1.1
Frame 246: 445 bytes on wire (3560 bits), 445 bytes captured (3560 bits) on interface \Device\
Ethernet II, Src: Intel_9c:ff:68 (b4:d5:bd:9c:ff:68), Dst: GemtekTechno_b2:ba:16 (58:13:d3:b2:
Internet Protocol Version 4, Src: 192.168.1.111, Dst: 44.228.249.3
Transmission Control Protocol, Src Port: 54113, Dst Port: 80, Seq: 787, Ack: 8470, Len: 391
Hypertext Transfer Protocol
0000 58 13 d3 b2 ba 16 b4 d5 bd 9c ff 68 08 00 45 00
0010 01 af 04 82 40 00 80 06 0c c8 c0 a8 01 6f 2c e4
0020 f9 03 d3 61 00 50 42 3f 9b 41 b3 ca b9 7e 50 18
0030 01 04 f2 9b 00 00 47 45 54 20 2f 66 61 76 69 63
0040 6f 6e 2e 69 63 6f 20 48 54 54 50 2f 31 2e 31 0d
0050 0a 48 6f 73 74 3a 20 74 65 73 74 70 68 70 2e 76
0060 75 6c 6e 77 65 62 2e 63 6f 6d 0d 0a 43 6f 6e 6e
0070 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69
0080 76 65 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20
0090 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e
00a0 64 6f 77 73 20 4e 54 20 31 30 2e 30 3b 20 57 69
00b0 6e 36 34 3b 20 78 36 34 29 20 41 70 70 6c 65 57
00c0 65 62 4b 69 74 2f 35 33 37 2e 33 36 20 28 4b 48
00d0 54 4d 4c 2c 20 6c 69 6b 65 20 47 65 63 6b 6f 29
00e0 20 43 68 72 6f 6d 65 2f 31 32 34 2e 30 2e 30 2e
00f0 30 20 53 61 66 61 72 69 2f 35 33 37 2e 33 36 0d
0100 0a 41 63 63 65 70 74 3a 20 69 6d 61 67 65 2f 61
0110 76 69 66 2c 69 6d 61 67 65 2f 77 65 62 70 2c 69
0120 6d 61 67 65 2f 61 70 6e 67 2c 69 6d 61 67 65 2f
0130 73 76 67 2b 78 6d 6c 2c 69 6d 61 67 65 2f 2a 2c
wireshark_Wi-FiCTDPN2.pcapng
Packets: 3962 · Displayed: 5 (0.1%) · Dropped: 0 (0.0%)
Profile: Default


C:\WINDOWS\system32\cmd.exe
Connection-specific DNS Suffix . :
ireless LAN adapter Local Area Connection* 11:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
ireless LAN adapter Local Area Connection* 12:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
ireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::b425:a3e4:406:f123%9
IPv4 Address. . . . . : 192.168.1.111
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.254
thernet adapter Bluetooth Network Connection:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
:\Users\LENOVO>


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.src== 192.168.1.111
No. Time Source Destination Protocol Length Info
2348 22.132478 192.168.1.111 169.150.215.48 TCP 55 [TCP Keep-Alive] 53545 → 443 [ACK] Seq=1 Ack=1 Win=258 Len=1
2349 22.217776 192.168.1.111 44.228.249.3 HTTP 727 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
2356 22.489814 192.168.1.111 44.228.249.3 TCP 54 54288 → 80 [ACK] Seq=674 Ack=2928 Win=260 Len=0
2361 22.997677 192.168.1.111 172.217.19.138 TLSv1.2 122 Application Data
2362 23.003801 192.168.1.111 172.217.19.138 TLSv1.2 169 Application Data, Application Data
2367 23.072784 192.168.1.111 172.217.19.138 TCP 54 54294 → 443 [ACK] Seq=184 Ack=114 Win=255 Len=0
2370 23.073474 192.168.1.111 172.217.19.138 TCP 54 54294 → 443 [ACK] Seq=184 Ack=2469 Win=260 Len=0
2373 23.073662 192.168.1.111 172.217.19.138 TCP 54 54294 → 443 [ACK] Seq=184 Ack=2697 Win=259 Len=0
2374 23.096436 192.168.1.111 172.217.19.138 TLSv1.2 89 Application Data
2375 23.096679 192.168.1.111 172.217.19.138 TLSv1.2 93 Application Data
2382 24.128674 192.168.1.111 18.153.4.44 TCP 54 54322 → 443 [FIN, ACK] Seq=1294 Ack=6174 Win=65792 Len=0
2385 24.196501 192.168.1.111 18.153.4.44 TCP 54 54322 → 443 [ACK] Seq=1295 Ack=6199 Win=65792 Len=0
2387 24.355442 192.168.1.111 172.217.18.46 TLSv1.2 175 Application Data
2388 24.368376 192.168.1.111 172.217.18.46 TLSv1.2 1414 Application Data
2389 24.368376 192.168.1.111 172.217.18.46 TLSv1.2 209 Application Data
2394 24.457333 192.168.1.111 172.217.18.46 TCP 54 54295 → 443 [ACK] Seq=1637 Ack=40 Win=258 Len=0
2397 24.462627 192.168.1.111 172.217.18.46 TCP 54 54295 → 443 [ACK] Seq=1637 Ack=685 Win=255 Len=0
2401 24.463225 192.168.1.111 172.217.18.46 TCP 54 54295 → 443 [ACK] Seq=1637 Ack=957 Win=260 Len=0
2402 24.475371 192.168.1.111 172.217.18.46 TLSv1.2 89 Application Data
2403 24.475462 192.168.1.111 172.217.18.46 TLSv1.2 93 Application Data
2407 24.762159 192.168.1.111 142.250.203.227 TLSv1.3 279 Application Data
2408 24.779341 192.168.1.111 142.250.203.227 TCP 1414 54335 → 443 [ACK] Seq=1356 Ack=5566 Win=65536 Len=1360 [TCP segment of a reassembled PDU]
2409 24.779341 192.168.1.111 142.250.203.227 TCP 1414 54335 → 443 [ACK] Seq=2716 Ack=5566 Win=65536 Len=1360 [TCP segment of a reassembled PDU]
2410 24.779341 192.168.1.111 142.250.203.227 TCP 1414 54335 → 443 [ACK] Seq=4076 Ack=5566 Win=65536 Len=1360 [TCP segment of a reassembled PDU]
Frame 2349: 727 bytes on wire (5816 bits), 727 bytes captured (5816 bits) on interface \Dev
Ethernet II, Src: Intel_9c:ff:68 (b4:d5:bd:9c:ff:68), Dst: GemtekTechno_b2:ba:16 (58:13:d3:
Destination: GemtekTechno_b2:ba:16 (58:13:d3:b2:ba:16)
Source: Intel_9c:ff:68 (b4:d5:bd:9c:ff:68)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.1.111, Dst: 44.228.249.3
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
0000 58 13 d3 b2 ba 16 b4 d5 bd 9c ff 68 08 00 45 00 X·····h··E·
0010 02 c9 04 ee 40 00 80 06 0b 42 c0 a8 01 6f 2c e4 ····@···· ·B···o,·
0020 f9 03 d4 10 00 50 bf 73 86 77 48 df 9e 14 50 18 ·····P·s ·wH···P·
0030 01 04 12 c4 00 00 50 4f 53 54 20 2f 75 73 65 72 ·····PO ST /user
0040 69 6e 66 6f 2e 70 68 70 20 48 54 54 50 2f 31 2e info.php HTTP/1.
0050 31 0d 0a 48 6f 73 74 3a 20 74 65 73 74 70 68 70 1··Host: testphp
0060 2e 76 75 6c 6e 77 65 62 2e 63 6f 6d 0d 0a 43 6f .vulnweb .com··Co
0070 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 nnection : keep-a
0080 6c 69 76 65 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 live··Co ntent-Le
0090 6e 67 74 68 3a 20 32 31 0d 0a 43 61 63 68 65 2d ngth: 21 ··Cache-
Internet Protocol Version 4 (ip), 20 bytes
Packets: 2614 · Displayed: 1056 (40.4%) · Dropped: 0 (0.0%)
Profile: Default
Type here to search
ENG
10:17 PM
5/23/2024


C:\WINDOWS\system32\cmd.exe
screenrec
Microsoft Windows [Version 10.0.19045.4412]
(c) Microsoft Corporation. All rights reserved.
C:\Users\LENOVO>nslookup
Default Server: mada-alarab.ps
Address: 192.168.1.254
> exit
C:\Users\LENOVO>nslookup http://testphp.vulnweb.com/login.php
Server: mada-alarab.ps
Address: 192.168.1.254
*** mada-alarab.ps can't find http://testphp.vulnweb.com/login.php: Non-existent domain
C:\Users\LENOVO>nslookup testphp.vulnweb.com
Server: mada-alarab.ps
Address: 192.168.1.254
Non-authoritative answer:
Name: testphp.vulnweb.com
Address: 44.228.249.3
C:\Users\LENOVO>


*Wi-Fi
screenrec
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.dst==44.228.249.3
No. Time Source Destination Protocol Length Info
2349 22.217776 192.168.1.111 44.228.249.3 HTTP 727 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
2356 22.489814 192.168.1.111 44.228.249.3 TCP 54 54288 → 80 [ACK] Seq=674 Ack=2928 Win=260 Len=0
2579 29.991480 192.168.1.111 44.228.249.3 TCP 55 54289 → 80 [ACK] Seq=1 Ack=1 Win=260 Len=1
Frame 2349: 727 bytes on wire (5816 bits), 727 bytes captured (5816 bits) on interface \Dev
Section number: 1
Interface id: 0 (\Device\NPF_{793E52BC-A9ED-42B5-83AB-28C6AA09B3D6})
Encapsulation type: Ethernet (1)
Arrival Time: May 23, 2024 22:07:27.531646000 Jerusalem Daylight Time
UTC Arrival Time: May 23, 2024 19:07:27.531646000 UTC
Epoch Arrival Time: 1716491247.531646000
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.085298000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 22.217776000 seconds]
Frame Number: 2349
Frame Length: 727 bytes (5816 bits)
Capture Length: 727 bytes (5816 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:http:urlencoded-form]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: Intel_9c:ff:68 (b4:d5:bd:9c:ff:68), Dst: GemtekTechno_b2:ba:16 (58:13:d3:
Destination: GemtekTechno_b2:ba:16 (58:13:d3:b2:ba:16)
Source: Intel_9c:ff:68 (b4:d5:bd:9c:ff:68)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.1.111, Dst: 44.228.249.3
Transmission Control Protocol, Src Port: 54288, Dst Port: 80, Seq: 1, Ack: 1, Len: 673
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "uname" = "test "
0000 58 13 d3 b2 ba 16 b4 d5 bd 9c ff 68 08 00 45 00 X·····h··E·
0010 02 c9 04 ee 40 00 80 06 0b 42 c0 a8 01 6f 2c e4 ····@···· ·B···o,·
0020 f9 03 d4 10 00 50 bf 73 86 77 48 df 9e 14 50 18 ·····P·s ·wH···P·
0030 01 04 12 c4 00 00 50 4f 53 54 20 2f 75 73 65 72 ·····PO ST /user
0040 69 6e 66 6f 2e 70 68 70 20 48 54 54 50 2f 31 2e info.php HTTP/1.
0050 31 0d 0a 48 6f 73 74 3a 20 74 65 73 74 70 68 70 1··Host: testphp
0060 2e 76 75 6c 6e 77 65 62 2e 63 6f 6d 0d 0a 43 6f .vulnweb .com··Co
0070 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 nnection : keep-a
0080 6c 69 76 65 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 live··Co ntent-Le
0090 6e 67 74 68 3a 20 32 31 0d 0a 43 61 63 68 65 2d ngth: 21 ··Cache-
00a0 43 6f 6e 74 72 6f 6c 3a 20 6d 61 78 2d 61 67 65 Control: max-age
00b0 3d 30 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 =0··Upgr ade-Inse
00c0 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a 20 31 cure-Req uests: 1
00d0 0d 0a 4f 72 69 67 69 6e 3a 20 68 74 74 70 3a 2f ··Origin : http:/
00e0 2f 74 65 73 74 70 68 70 2e 76 75 6c 6e 77 65 62 /testphp .vulnweb
00f0 2e 63 6f 6d 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 .com··Co ntent-Ty
0100 70 65 3a 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f pe: appl ication/
0110 78 2d 77 77 77 2d 66 6f 72 6d 2d 75 72 6c 65 6e x-www-fo rm-urlen
0120 63 6f 64 65 64 0d 0a 55 73 65 72 2d 41 67 65 6e coded··U ser-Agen
0130 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 t: Mozil la/5.0 (
0140 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 3b Windows NT 10.0;
0150 20 57 69 6e 36 34 3b 20 78 36 34 29 20 41 70 70 Win64; x64) App
0160 6c 65 57 65 62 4b 69 74 2f 35 33 37 2e 33 36 20 leWebKit /537.36
0170 28 4b 48 54 4d 4c 2c 20 6c 69 6b 65 20 47 65 63 (KHTML, like Gec
0180 6b 6f 29 20 43 68 72 6f 6d 65 2f 31 32 34 2e 30 ko) Chro me/124.0
0190 2e 30 2e 30 20 53 61 66 61 72 69 2f 35 33 37 2e .0.0 Saf ari/537.
01a0 33 36 0d 0a 41 63 63 65 70 74 3a 20 74 65 78 74 36 ··Acce pt: text
01b0 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74 69 6f /html,ap plicatio
01c0 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 70 6c n/xhtml+ xml,appl
01d0 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d 30 2e ication/ xml;q=0.
01e0 39 2c 69 6d 61 67 65 2f 61 76 69 66 2c 69 6d 61 9,image/ avif,ima
01f0 67 65 2f 77 65 62 70 2c 69 6d 61 67 65 2f 61 70 ge/webp, image/ap
Internet Protocol Version 4 (ip), 20 bytes
Packets: 2614 · Displayed: 3 (0.1%) · Dropped: 0 (0.0%)
Profile: Default
10:24 PM



Part two:

1. *What is DNS?*

DNS (Domain Name System) is like the Internet's phonebook. It translates human-friendly domain names (like www.google.com) into numerical IP addresses (like 172.217.5.110), which computers use to communicate with each other. For example, when you type "www.google.com" into your web browser, DNS finds the corresponding IP address and directs your request to the right server, so you can see Google' homepage.

This process happens quickly and behind the scenes, making it easy for users to browse the web without needing to remember IP addresses.

2. *Does DNS work on UDP or TCP or both? Explain*

DNS primarily uses the User Datagram Protocol (UDP) on port 53 for most queries due to its speed and efficiency. However, it can also use the Transmission Control Protocol (TCP) in specific situations:

1. When the response size exceeds 512 bytes, requiring a more reliable connection.

2. For zone transfers between DNS servers, which involve larger data amounts.

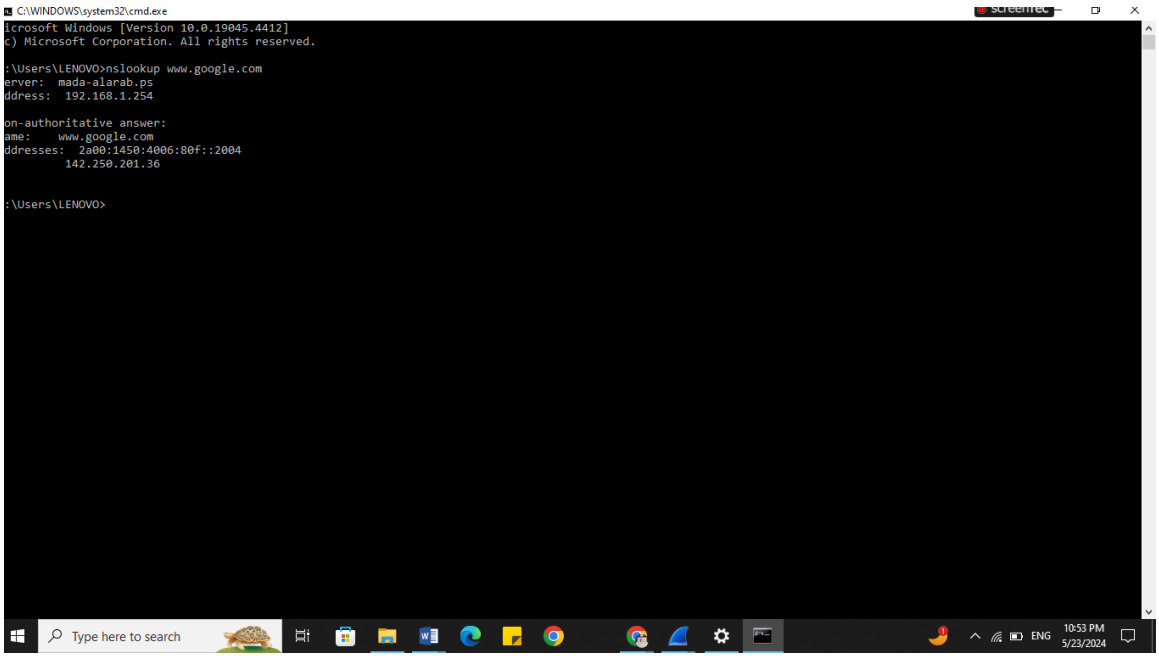
3. When a query response is truncated over UDP, prompting a retry using TCP.

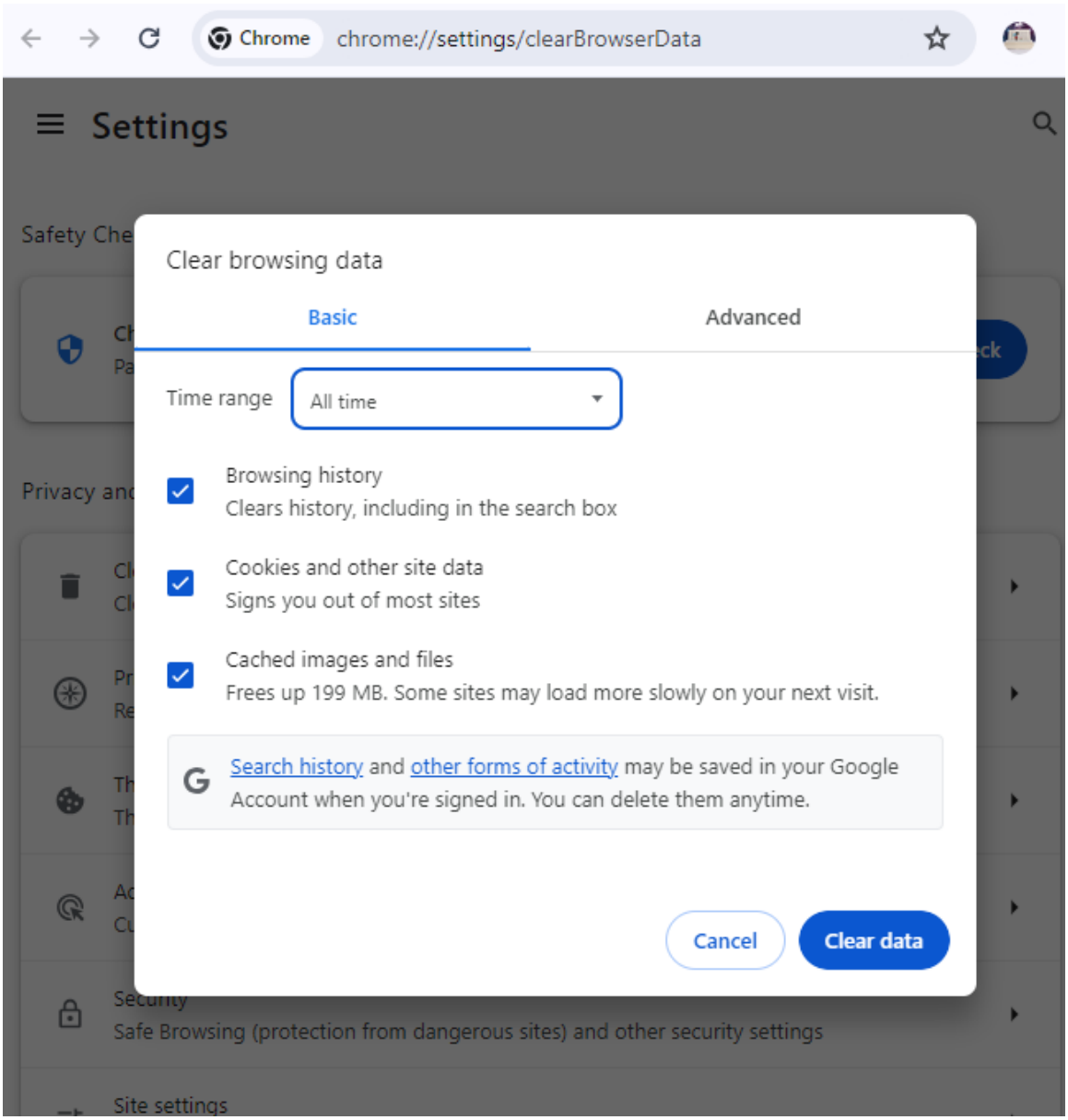
1. In these cases, TCP ensures reliable data transfer, making it suitable for handling larger or more complex DNS tasks. DNS Protocols: Uses both UDP (primarily) and TCP (in specific cases) on port 53.

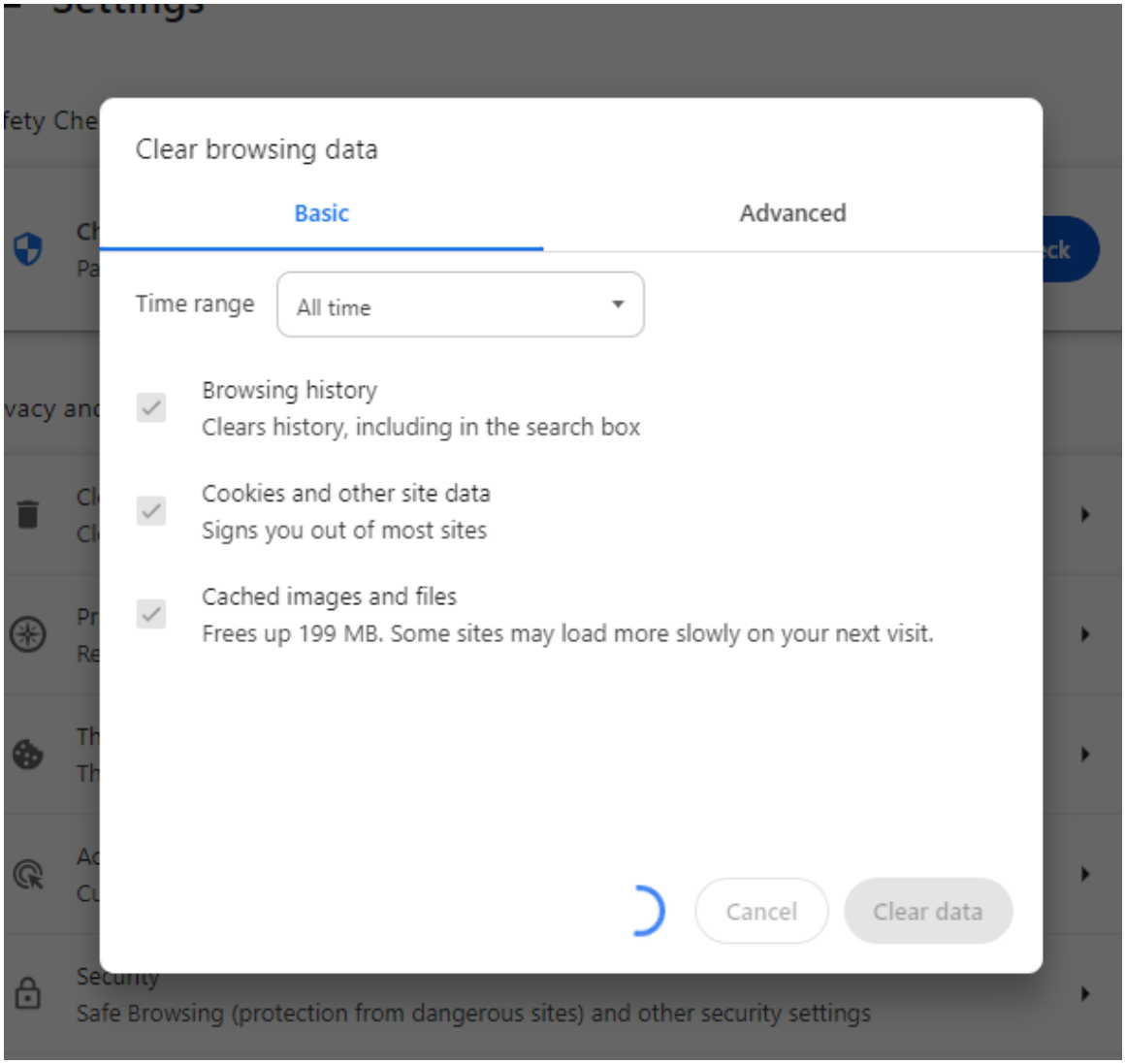
3. *What is the domain name of the following IP address: 8.8.8.8?*

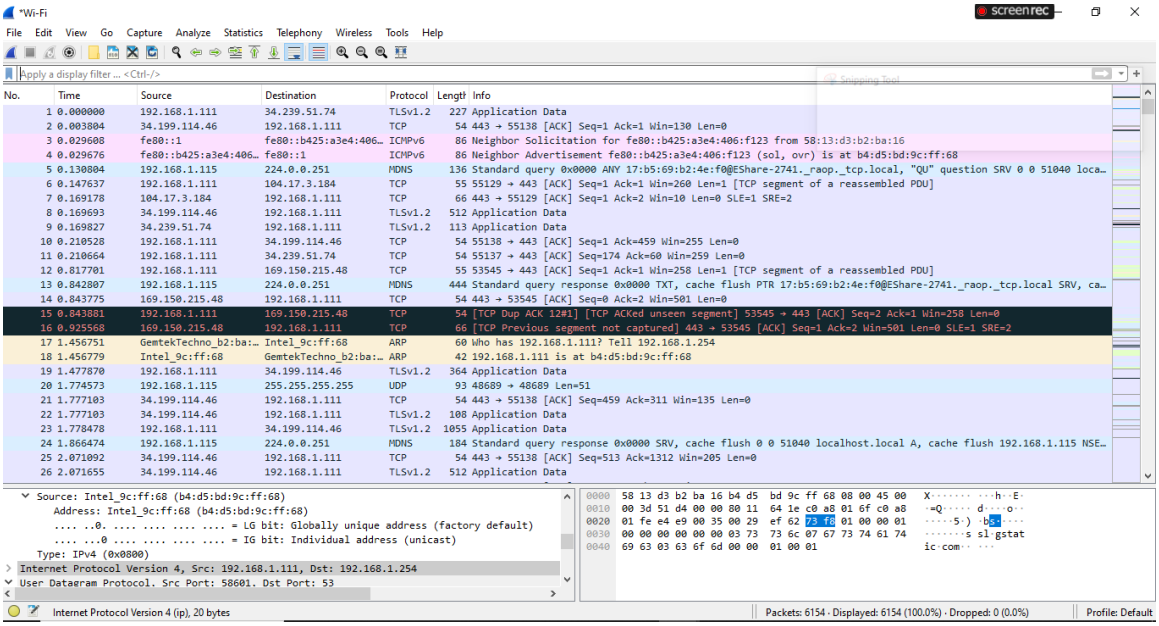
One of Google's publicly accessible DNS server addresses is 8.8.8.8. It is known as "Google Public DNS," but unlike other websites, it does not have a single domain name connected with it. Domain Name for 8.8.8.8: Commonly referred to as "Google Public DNS

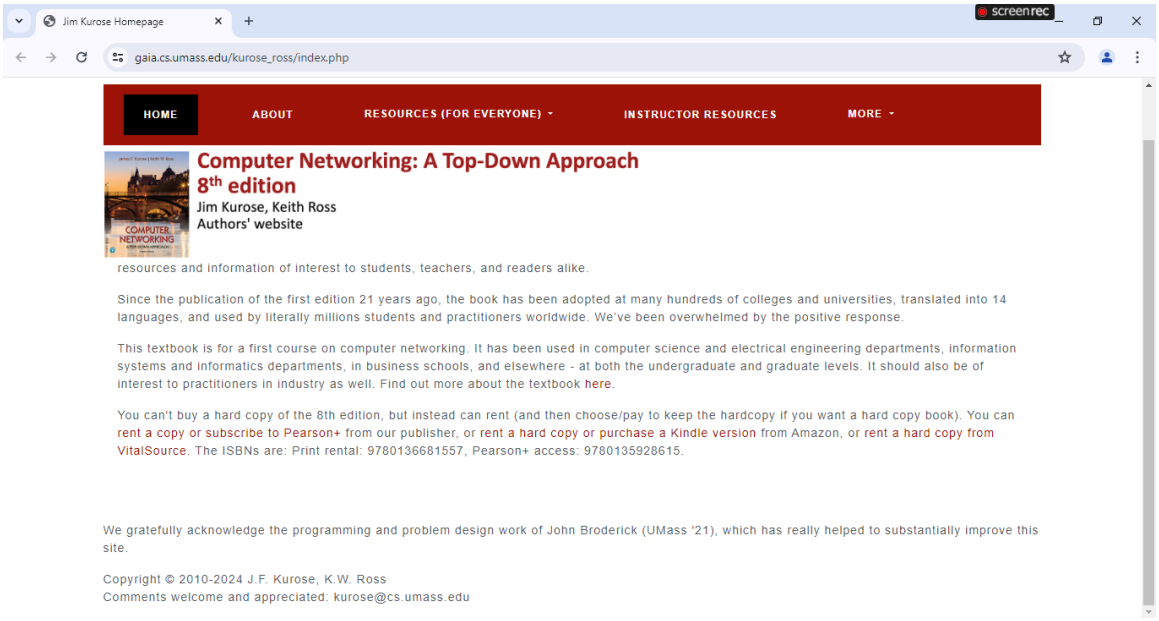
4. *What is the IP address for the Google website?*

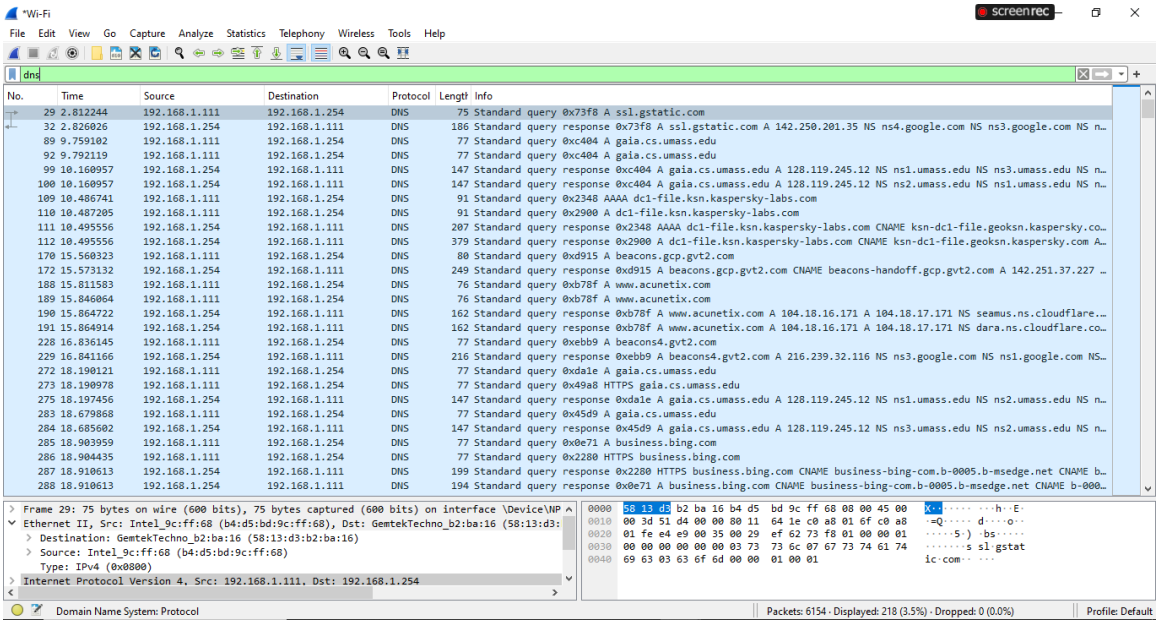

C:\WINDOWS\system32\cmd.exe
Screenrec
lcrosoft Windows [Version 10.0.19045.4412]
c) Microsoft Corporation. All rights reserved.
:\Users\LENOVO>nslookup www.google.com
erver: mada-alarab.ps
ddress: 192.168.1.254
on-authoritative answer:
ame: www.google.com
ddresses: 2a00:1450:4006:80f::2004
          142.250.201.36
:\Users\LENOVO>
Type here to search
ENG
10:53 PM
5/23/2024

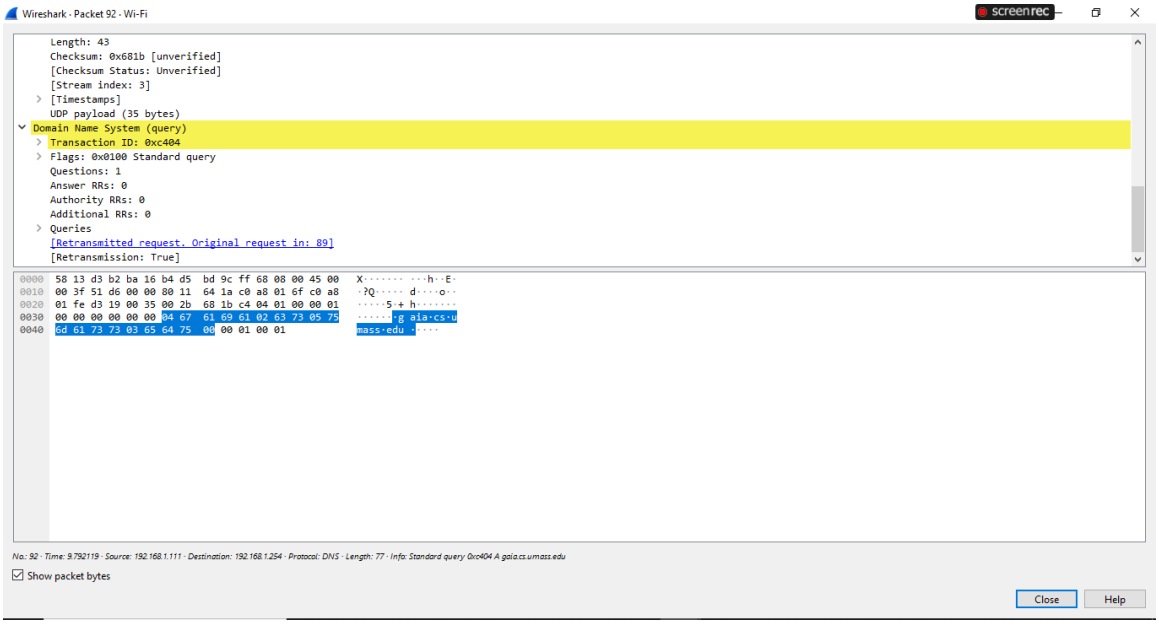

Chrome
chrome://settings/clearBrowserData
Settings
Clear browsing data
Basic
Advanced
Time range
All time
Browsing history
Clears history, including in the search box
Cookies and other site data
Signs you out of most sites
Cached images and files
Frees up 199 MB. Some sites may load more slowly on your next visit.
Search history and other forms of activity may be saved in your Google Account when you're signed in. You can delete them anytime.
Cancel
Clear data
Safe Browsing (protection from dangerous sites) and other security settings
Site settings

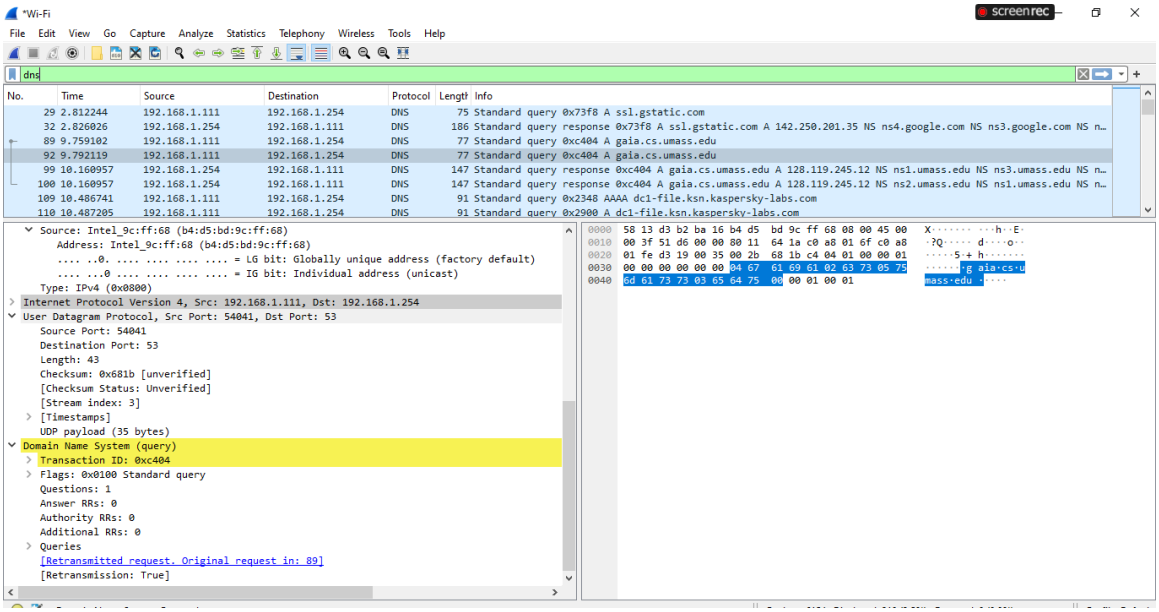

Clear browsing data
Basic
Advanced
Time range
All time
Browsing history
Clears history, including in the search box
Cookies and other site data
Signs you out of most sites
Cached images and files
Frees up 199 MB. Some sites may load more slowly on your next visit.
Cancel
Clear data
Safe Browsing (protection from dangerous sites) and other security settings

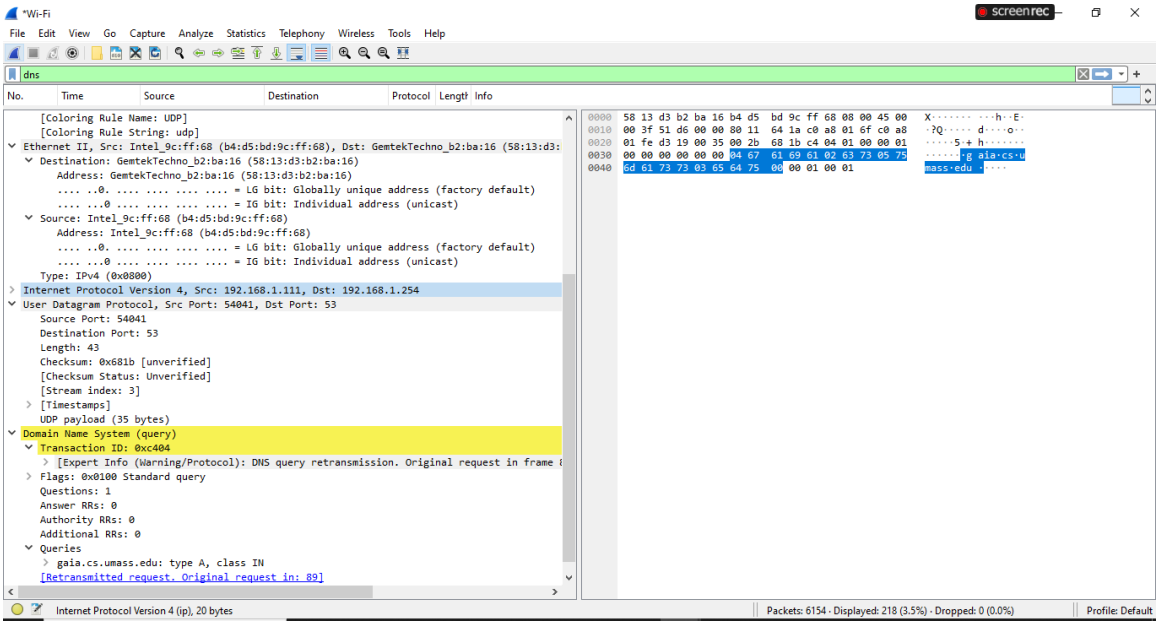

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.1.111 34.239.51.74 TLSv1.2 227 Application Data
2 0.003804 34.199.114.46 192.168.1.111 TCP 54 443 → 55138 [ACK] Seq=1 Ack=1 Win=130 Len=0
3 0.029608 fe80::1 fe80::b425:a3e4:406… ICMPv6 86 Neighbor Solicitation for fe80::b425:a3e4:406:f123 from 58:13:d3:b2:ba:16
4 0.029676 fe80::b425:a3e4:406… fe80::1 ICMPv6 86 Neighbor Advertisement fe80::b425:a3e4:406:f123 (sol, ovr) is at b4:d5:bd:9c:ff:68
5 0.130804 192.168.1.115 224.0.0.251 MDNS 136 Standard query 0x0000 ANY 17:b5:69:b2:4e:f0@EShare-2741._raop._tcp.local, "QU" question SRV 0 0 51040 loca…
6 0.147637 192.168.1.111 104.17.3.184 TCP 55 55129 → 443 [ACK] Seq=1 Ack=1 Win=260 Len=1 [TCP segment of a reassembled PDU]
7 0.169178 104.17.3.184 192.168.1.111 TCP 66 443 → 55129 [ACK] Seq=1 Ack=2 Win=10 Len=0 SLE=1 SRE=2
8 0.169693 34.199.114.46 192.168.1.111 TLSv1.2 512 Application Data
9 0.169827 34.239.51.74 192.168.1.111 TLSv1.2 113 Application Data
10 0.210528 192.168.1.111 34.199.114.46 TCP 54 55138 → 443 [ACK] Seq=1 Ack=459 Win=255 Len=0
11 0.210664 192.168.1.111 34.239.51.74 TCP 54 55137 → 443 [ACK] Seq=174 Ack=60 Win=259 Len=0
12 0.817701 192.168.1.111 169.150.215.48 TCP 55 53545 → 443 [ACK] Seq=1 Ack=1 Win=258 Len=1 [TCP segment of a reassembled PDU]
13 0.842807 192.168.1.115 224.0.0.251 MDNS 444 Standard query response 0x0000 TXT, cache flush PTR 17:b5:69:b2:4e:f0@EShare-2741._raop._tcp.local SRV, ca…
14 0.843775 169.150.215.48 192.168.1.111 TCP 54 443 → 53545 [ACK] Seq=0 Ack=2 Win=501 Len=0
15 0.843881 192.168.1.111 169.150.215.48 TCP 54 [TCP Dup ACK 12#1] [TCP ACKed unseen segment] 53545 → 443 [ACK] Seq=2 Ack=1 Win=258 Len=0
16 0.925568 169.150.215.48 192.168.1.111 TCP 66 [TCP Previous segment not captured] 443 → 53545 [ACK] Seq=1 Ack=2 Win=501 Len=0 SLE=1 SRE=2
17 1.456751 GemtekTechno_b2:ba:… Intel_9c:ff:68 ARP 60 Who has 192.168.1.111? Tell 192.168.1.254
18 1.456779 Intel_9c:ff:68 GemtekTechno_b2:ba:… ARP 42 192.168.1.111 is at b4:d5:bd:9c:ff:68
19 1.477870 192.168.1.111 34.199.114.46 TLSv1.2 364 Application Data
20 1.774573 192.168.1.115 255.255.255.255 UDP 93 48689 → 48689 Len=51
21 1.777103 34.199.114.46 192.168.1.111 TCP 54 443 → 55138 [ACK] Seq=459 Ack=311 Win=135 Len=0
22 1.777103 34.199.114.46 192.168.1.111 TLSv1.2 108 Application Data
23 1.778478 192.168.1.111 34.199.114.46 TLSv1.2 1055 Application Data
24 1.866474 192.168.1.115 224.0.0.251 MDNS 184 Standard query response 0x0000 SRV, cache flush 0 0 51040 localhost.local A, cache flush 192.168.1.115 NSE…
25 2.071092 34.199.114.46 192.168.1.111 TCP 54 443 → 55138 [ACK] Seq=513 Ack=1312 Win=205 Len=0
26 2.071655 34.199.114.46 192.168.1.111 TLSv1.2 512 Application Data
Source: Intel_9c:ff:68 (b4:d5:bd:9c:ff:68)
Address: Intel_9c:ff:68 (b4:d5:bd:9c:ff:68)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.1.111, Dst: 192.168.1.254
User Datagram Protocol, Src Port: 58601, Dst Port: 53
0000 58 13 d3 b2 ba 16 b4 d5 bd 9c ff 68 08 00 45 00
0010 00 3d 51 d4 00 00 80 11 64 1e c0 a8 01 6f c0 a8
0020 01 fe e4 e9 00 35 00 29 ef 62 73 f8 01 00 00 01
0030 00 00 00 00 00 00 03 73 73 6c 07 67 73 74 61 74
0040 69 63 03 63 6f 6d 00 00 01 00 01
Internet Protocol Version 4 (ip), 20 bytes
Packets: 6154 · Displayed: 6154 (100.0%) · Dropped: 0 (0.0%)
Profile: Default


Jim Kurose Homepage
gaia.cs.umass.edu/kurose_ross/index.php
HOME
ABOUT
RESOURCES (FOR EVERYONE)
INSTRUCTOR RESOURCES
MORE
Computer Networking: A Top-Down Approach
8th edition
Jim Kurose, Keith Ross
Authors' website
resources and information of interest to students, teachers, and readers alike.
Since the publication of the first edition 21 years ago, the book has been adopted at many hundreds of colleges and universities, translated into 14 languages, and used by literally millions students and practitioners worldwide. We've been overwhelmed by the positive response.
This textbook is for a first course on computer networking. It has been used in computer science and electrical engineering departments, information systems and informatics departments, in business schools, and elsewhere - at both the undergraduate and graduate levels. It should also be of interest to practitioners in industry as well. Find out more about the textbook here.
You can't buy a hard copy of the 8th edition, but instead can rent (and then choose/pay to keep the hardcopy if you want a hard copy book). You can rent a copy or subscribe to Pearson+ from our publisher, or rent a hard copy or purchase a Kindle version from Amazon, or rent a hard copy from VitalSource. The ISBNs are: Print rental: 9780136681557, Pearson+ access: 9780135928615.
We gratefully acknowledge the programming and problem design work of John Broderick (UMass '21), which has really helped to substantially improve this site.
Copyright © 2010-2024 J.F. Kurose, K.W. Ross
Comments welcome and appreciated: kurose@cs.umass.edu


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Protocol Length Info
29 2.812244 192.168.1.111 192.168.1.254 DNS 75 Standard query 0x73f8 A ssl.gstatic.com
32 2.826026 192.168.1.254 192.168.1.111 DNS 186 Standard query response 0x73f8 A ssl.gstatic.com A 142.250.201.35 NS ns4.google.com NS ns3.google.com NS n…
89 9.759102 192.168.1.111 192.168.1.254 DNS 77 Standard query 0xc404 A gaia.cs.umass.edu
92 9.792119 192.168.1.111 192.168.1.254 DNS 77 Standard query 0xc404 A gaia.cs.umass.edu
99 10.160957 192.168.1.254 192.168.1.111 DNS 147 Standard query response 0xc404 A gaia.cs.umass.edu A 128.119.245.12 NS ns1.umass.edu NS ns3.umass.edu NS n…
100 10.160957 192.168.1.254 192.168.1.111 DNS 147 Standard query response 0xc404 A gaia.cs.umass.edu A 128.119.245.12 NS ns2.umass.edu NS ns1.umass.edu NS n…
109 10.486741 192.168.1.111 192.168.1.254 DNS 91 Standard query 0x2348 AAAA dc1-file.ksn.kaspersky-labs.com
110 10.487205 192.168.1.111 192.168.1.254 DNS 91 Standard query 0x2900 A dc1-file.ksn.kaspersky-labs.com
111 10.495556 192.168.1.254 192.168.1.111 DNS 207 Standard query response 0x2348 AAAA dc1-file.ksn.kaspersky-labs.com CNAME ksn-dc1-file.geoksn.kaspersky.co…
112 10.495556 192.168.1.254 192.168.1.111 DNS 379 Standard query response 0x2900 A dc1-file.ksn.kaspersky-labs.com CNAME ksn-dc1-file.geoksn.kaspersky.com A…
170 15.560323 192.168.1.111 192.168.1.254 DNS 80 Standard query 0xd915 A beacons.gcp.gvt2.com
172 15.573132 192.168.1.254 192.168.1.111 DNS 249 Standard query response 0xd915 A beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com A 142.251.37.227 …
188 15.811583 192.168.1.111 192.168.1.254 DNS 76 Standard query 0xb78f A www.acunetix.com
189 15.846064 192.168.1.111 192.168.1.254 DNS 76 Standard query 0xb78f A www.acunetix.com
190 15.864722 192.168.1.254 192.168.1.111 DNS 162 Standard query response 0xb78f A www.acunetix.com A 104.18.16.171 A 104.18.17.171 NS seamus.ns.cloudflare.…
191 15.864914 192.168.1.254 192.168.1.111 DNS 162 Standard query response 0xb78f A www.acunetix.com A 104.18.16.171 A 104.18.17.171 NS dara.ns.cloudflare.co…
228 16.836145 192.168.1.111 192.168.1.254 DNS 77 Standard query 0xebb9 A beacons4.gvt2.com
229 16.841166 192.168.1.254 192.168.1.111 DNS 216 Standard query response 0xebb9 A beacons4.gvt2.com A 216.239.32.116 NS ns3.google.com NS ns1.google.com NS…
272 18.190121 192.168.1.111 192.168.1.254 DNS 77 Standard query 0xda1e A gaia.cs.umass.edu
273 18.190978 192.168.1.111 192.168.1.254 DNS 77 Standard query 0x49a8 HTTPS gaia.cs.umass.edu
275 18.197456 192.168.1.254 192.168.1.111 DNS 147 Standard query response 0xda1e A gaia.cs.umass.edu A 128.119.245.12 NS ns1.umass.edu NS ns2.umass.edu NS n…
283 18.679868 192.168.1.111 192.168.1.254 DNS 77 Standard query 0x45d9 A gaia.cs.umass.edu
284 18.685602 192.168.1.254 192.168.1.111 DNS 147 Standard query response 0x45d9 A gaia.cs.umass.edu A 128.119.245.12 NS ns3.umass.edu NS ns2.umass.edu NS n…
285 18.903959 192.168.1.111 192.168.1.254 DNS 77 Standard query 0x0e71 A business.bing.com
286 18.904435 192.168.1.111 192.168.1.254 DNS 77 Standard query 0x2280 HTTPS business.bing.com
287 18.910613 192.168.1.254 192.168.1.111 DNS 199 Standard query response 0x2280 HTTPS business.bing.com CNAME business-bing-com.b-0005.b-msedge.net CNAME b…
288 18.910613 192.168.1.254 192.168.1.111 DNS 194 Standard query response 0x0e71 A business.bing.com CNAME business-bing-com.b-0005.b-msedge.net CNAME b-000…
Frame 29: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NP
Ethernet II, Src: Intel_9c:ff:68 (b4:d5:bd:9c:ff:68), Dst: GemtekTechno_b2:ba:16 (58:13:d3:
Destination: GemtekTechno_b2:ba:16 (58:13:d3:b2:ba:16)
Source: Intel_9c:ff:68 (b4:d5:bd:9c:ff:68)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.1.111, Dst: 192.168.1.254
0000 58 13 d3 b2 ba 16 b4 d5 bd 9c ff 68 08 00 45 00
0010 00 3d 51 d4 00 00 80 11 64 1e c0 a8 01 6f c0 a8
0020 01 fe e4 e9 00 35 00 29 ef 62 73 f8 01 00 00 01
0030 00 00 00 00 00 00 03 73 73 6c 07 67 73 74 61 74
0040 69 63 03 63 6f 6d 00 00 01 00 01
Domain Name System: Protocol
Packets: 6154 · Displayed: 218 (3.5%) · Dropped: 0 (0.0%)
Profile: Default


Wireshark · Packet 92 · Wi-Fi
Length: 43
Checksum: 0x681b [unverified]
[Checksum Status: Unverified]
[Stream index: 3]
[Timestamps]
UDP payload (35 bytes)
Domain Name System (query)
Transaction ID: 0xc404
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
[Retransmitted request. Original request in: 89]
[Retransmission: True]
0000 58 13 d3 b2 ba 16 b4 d5 bd 9c ff 68 08 00 45 00
0010 00 3f 51 d6 00 00 80 11 64 1a c0 a8 01 6f c0 a8
0020 01 fe d3 19 00 35 00 2b 68 1b c4 04 01 00 00 01
0030 00 00 00 00 00 00 04 67 61 69 61 02 63 73 05 75
0040 6d 61 73 73 03 65 64 75 00 00 01 00 01
No.: 92 · Time: 9.792119 · Source: 192.168.1.111 · Destination: 192.168.1.254 · Protocol: DNS · Length: 77 · Info: Standard query 0xc404 A gaia.cs.umass.edu
Show packet bytes
Close
Help


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Protocol Length Info
29 2.812244 192.168.1.111 192.168.1.254 DNS 75 Standard query 0x73f8 A ssl.gstatic.com
32 2.826026 192.168.1.254 192.168.1.111 DNS 186 Standard query response 0x73f8 A ssl.gstatic.com A 142.250.201.35 NS ns4.google.com NS ns3.google.com NS n…
89 9.759102 192.168.1.111 192.168.1.254 DNS 77 Standard query 0xc404 A gaia.cs.umass.edu
92 9.792119 192.168.1.111 192.168.1.254 DNS 77 Standard query 0xc404 A gaia.cs.umass.edu
99 10.160957 192.168.1.254 192.168.1.111 DNS 147 Standard query response 0xc404 A gaia.cs.umass.edu A 128.119.245.12 NS ns1.umass.edu NS ns3.umass.edu NS n…
100 10.160957 192.168.1.254 192.168.1.111 DNS 147 Standard query response 0xc404 A gaia.cs.umass.edu A 128.119.245.12 NS ns2.umass.edu NS ns1.umass.edu NS n…
109 10.486741 192.168.1.111 192.168.1.254 DNS 91 Standard query 0x2348 AAAA dc1-file.ksn.kaspersky-labs.com
110 10.487205 192.168.1.111 192.168.1.254 DNS 91 Standard query 0x2900 A dc1-file.ksn.kaspersky-labs.com
Source: Intel_9c:ff:68 (b4:d5:bd:9c:ff:68)
Address: Intel_9c:ff:68 (b4:d5:bd:9c:ff:68)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.1.111, Dst: 192.168.1.254
User Datagram Protocol, Src Port: 54041, Dst Port: 53
Source Port: 54041
Destination Port: 53
Length: 43
Checksum: 0x681b [unverified]
[Checksum Status: Unverified]
[Stream index: 3]
[Timestamps]
UDP payload (35 bytes)
Domain Name System (query)
Transaction ID: 0xc404
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
[Retransmitted request. Original request in: 89]
[Retransmission: True]
0000 58 13 d3 b2 ba 16 b4 d5 bd 9c ff 68 08 00 45 00
0010 00 3f 51 d6 00 00 80 11 64 1a c0 a8 01 6f c0 a8
0020 01 fe d3 19 00 35 00 2b 68 1b c4 04 01 00 00 01
0030 00 00 00 00 00 00 04 67 61 69 61 02 63 73 05 75
0040 6d 61 73 73 03 65 64 75 00 00 01 00 01


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Protocol Length Info
[Coloring Rule Name: UDP]
[Coloring Rule String: udp]
Ethernet II, Src: Intel_9c:ff:68 (b4:d5:bd:9c:ff:68), Dst: GemtekTechno_b2:ba:16 (58:13:d3:
Destination: GemtekTechno_b2:ba:16 (58:13:d3:b2:ba:16)
Address: GemtekTechno_b2:ba:16 (58:13:d3:b2:ba:16)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Source: Intel_9c:ff:68 (b4:d5:bd:9c:ff:68)
Address: Intel_9c:ff:68 (b4:d5:bd:9c:ff:68)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.1.111, Dst: 192.168.1.254
User Datagram Protocol, Src Port: 54041, Dst Port: 53
Source Port: 54041
Destination Port: 53
Length: 43
Checksum: 0x681b [unverified]
[Checksum Status: Unverified]
[Stream index: 3]
[Timestamps]
UDP payload (35 bytes)
Domain Name System (query)
Transaction ID: 0xc404
[Expert Info (Warning/Protocol): DNS query retransmission. Original request in frame
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
gaia.cs.umass.edu: type A, class IN
[Retransmitted request. Original request in: 89]
0000 58 13 d3 b2 ba 16 b4 d5 bd 9c ff 68 08 00 45 00
0010 00 3f 51 d6 00 00 80 11 64 1a c0 a8 01 6f c0 a8
0020 01 fe d3 19 00 35 00 2b 68 1b c4 04 01 00 00 01
0030 00 00 00 00 00 00 04 67 61 69 61 02 63 73 05 75
0040 6d 61 73 73 03 65 64 75 00 00 01 00 01
Internet Protocol Version 4 (ip), 20 bytes
Packets: 6154 · Displayed: 218 (3.5%) · Dropped: 0 (0.0%)
Profile: Default