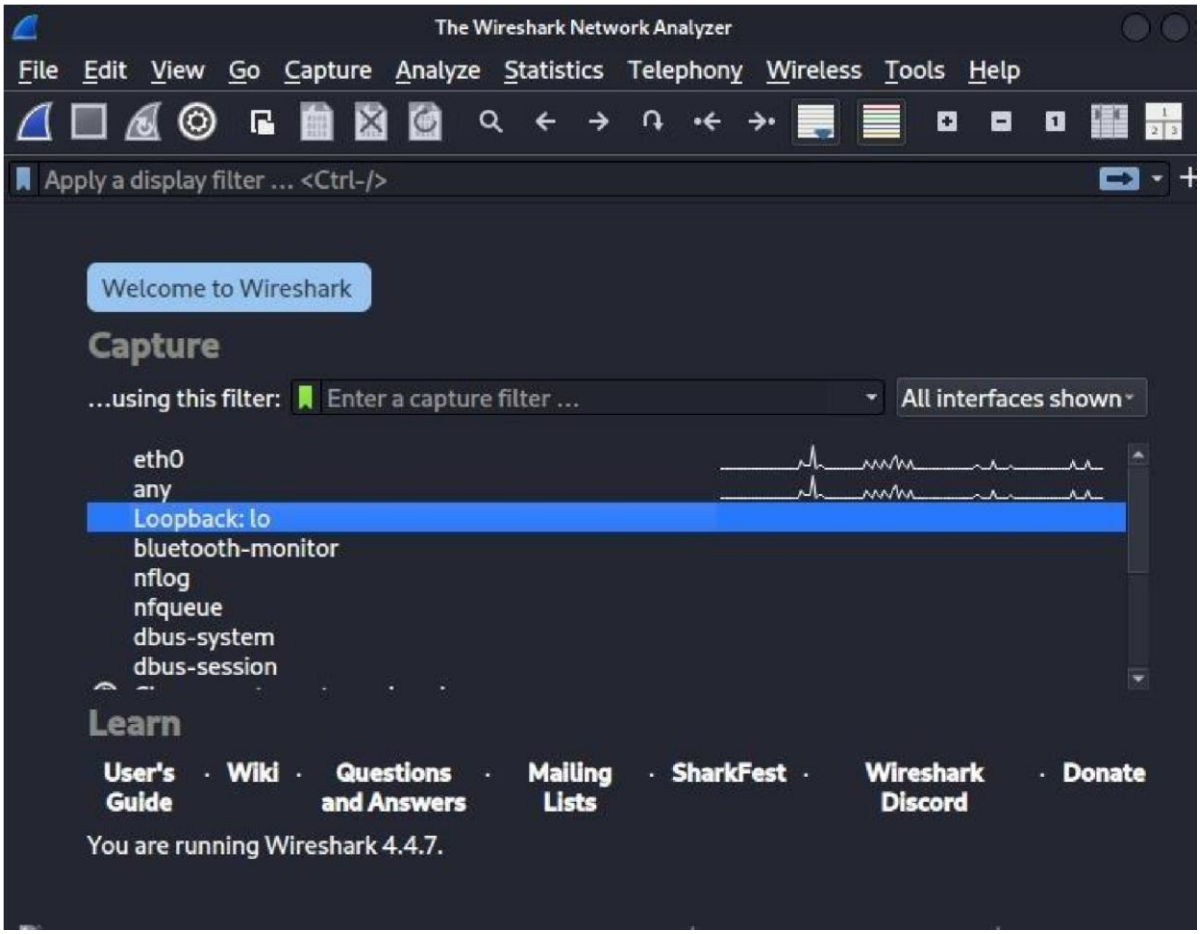
EXP N0 3: WIRESHARK (Password Capturing)

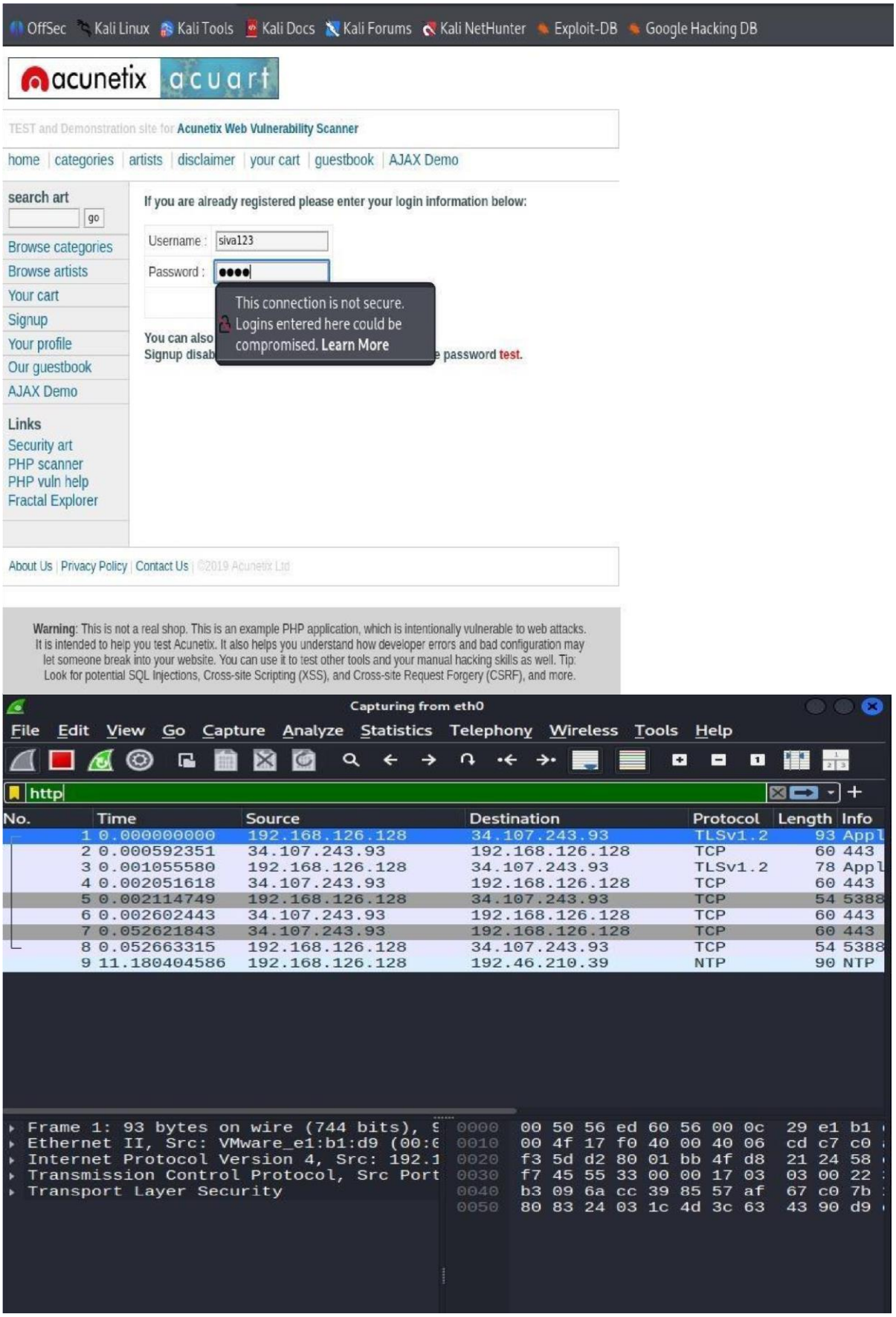
Aim :

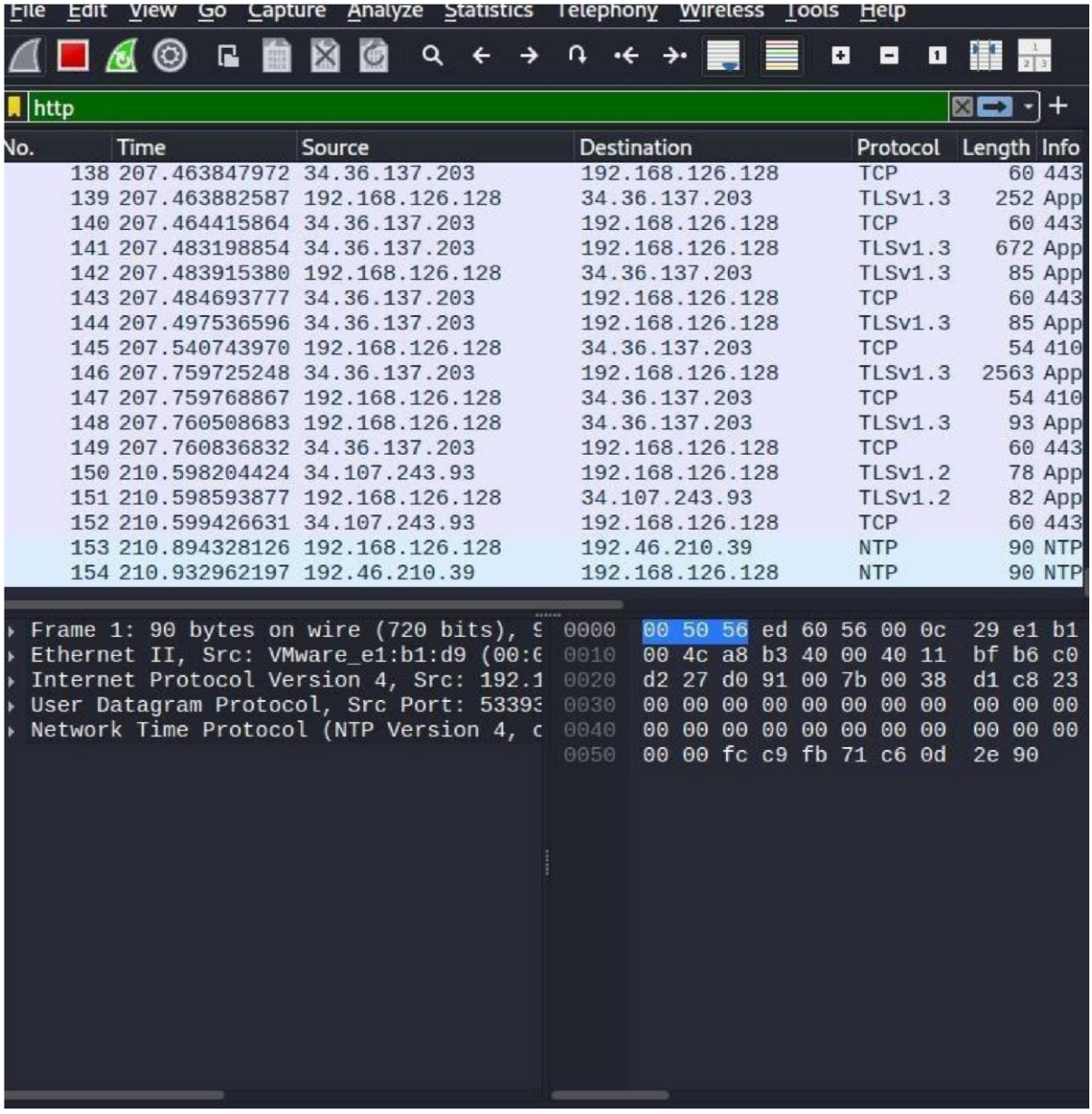
Use **Wireshark** to capture network traffic and locate plaintext credentials transmitted over insecure protocols (e.g., HTTP/FTP/Telnet).

Procedure :

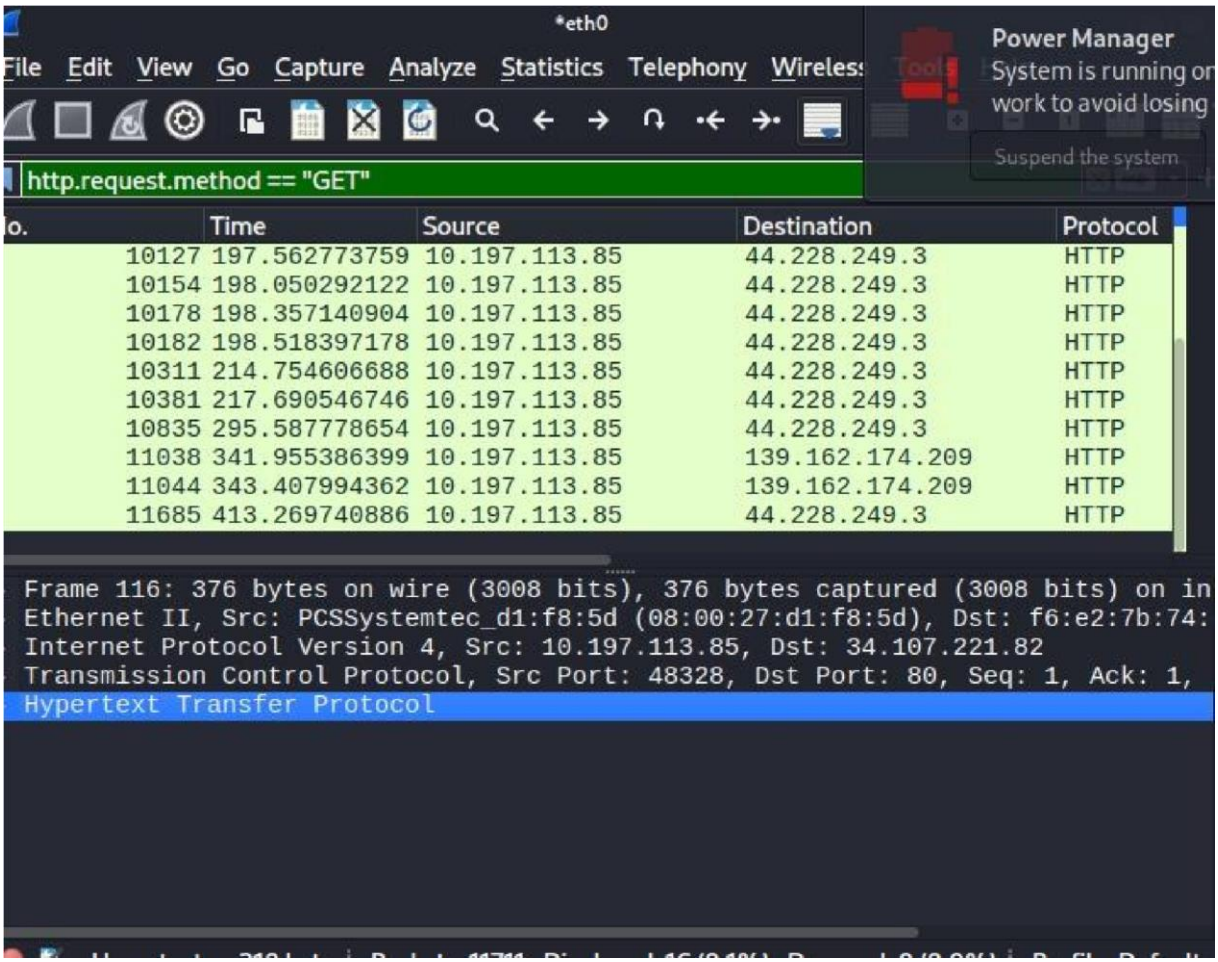
Start a capture on the correct interface, perform the login, filter for http and http.request.method=="POST", then inspect the **HTML form URL Encoded** fields to read uname/pass.
Important Only test on systems/networks you own or have explicit permission to test; capturing others' credentials is illegal and unethical.

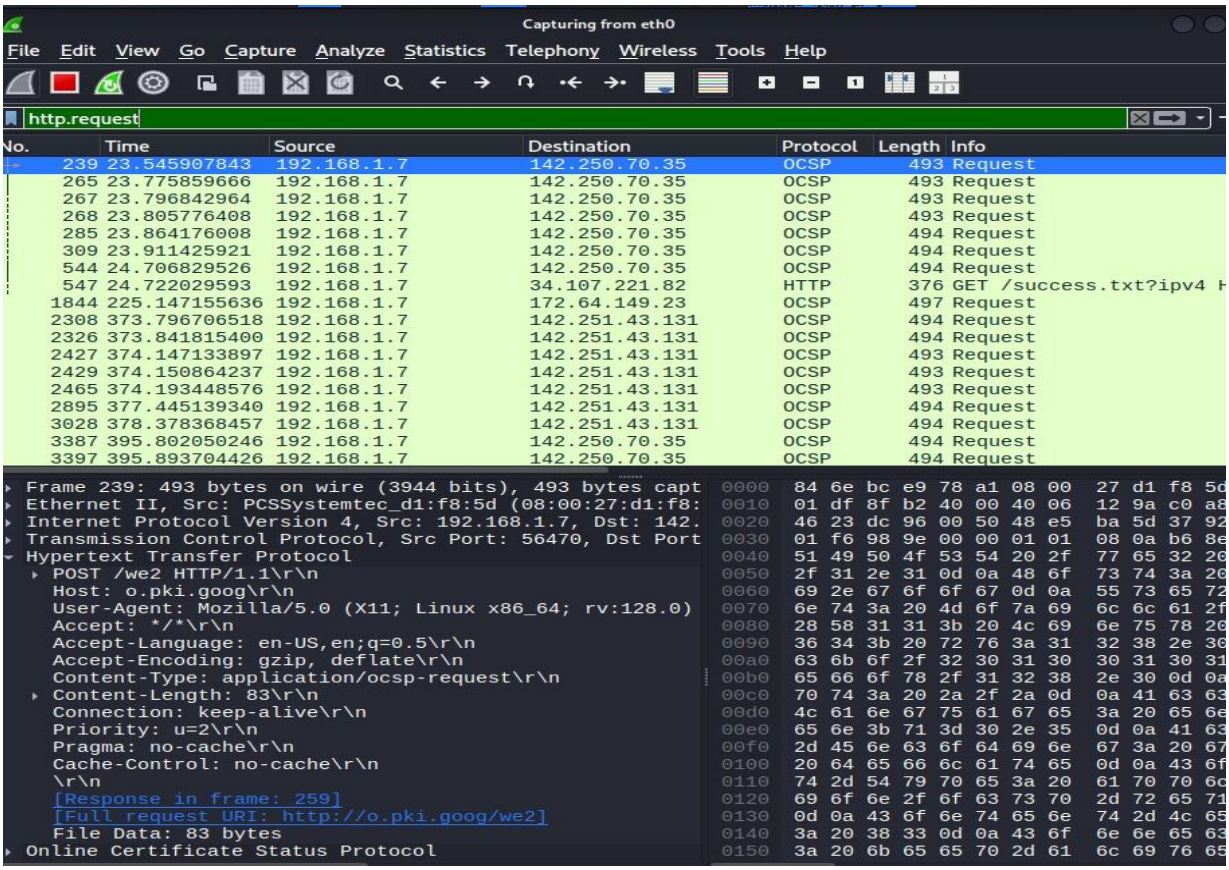



OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
If you are already registered please enter your login information below:
Username : siva123
Password : ••••
This connection is not secure. Logins entered here could be compromised. Learn More
You can also
Signup disab
e password test.
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: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
1 0.000000000 192.168.126.128 34.107.243.93 TLSv1.2 93 Appl
2 0.000592351 34.107.243.93 192.168.126.128 TCP 60 443
3 0.001055580 192.168.126.128 34.107.243.93 TLSv1.2 78 Appl
4 0.002051618 34.107.243.93 192.168.126.128 TCP 60 443
5 0.002114749 192.168.126.128 34.107.243.93 TCP 54 5388
6 0.002602443 34.107.243.93 192.168.126.128 TCP 60 443
7 0.052621843 34.107.243.93 192.168.126.128 TCP 60 443
8 0.052663315 192.168.126.128 34.107.243.93 TCP 54 5388
9 11.180404586 192.168.126.128 192.46.210.39 NTP 90 NTP
Frame 1: 93 bytes on wire (744 bits), 9
Ethernet II, Src: VMware_e1:b1:d9 (00:0
Internet Protocol Version 4, Src: 192.1
Transmission Control Protocol, Src Port
Transport Layer Security
0000 00 50 56 ed 60 56 00 0c 29 e1 b1
0010 00 4f 17 f0 40 00 40 06 cd c7 c0
0020 f3 5d d2 80 01 bb 4f d8 21 24 58
0030 f7 45 55 33 00 00 17 03 03 00 22
0040 b3 09 6a cc 39 85 57 af 67 c0 7b
0050 80 83 24 03 1c 4d 3c 63 43 90 d9


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protocol Length Info
138 207.463847972 34.36.137.203 192.168.126.128 TCP 60 443
139 207.463882587 192.168.126.128 34.36.137.203 TLSv1.3 252 App
140 207.464415864 34.36.137.203 192.168.126.128 TCP 60 443
141 207.483198854 34.36.137.203 192.168.126.128 TLSv1.3 672 App
142 207.483915380 192.168.126.128 34.36.137.203 TLSv1.3 85 App
143 207.484693777 34.36.137.203 192.168.126.128 TCP 60 443
144 207.497536596 34.36.137.203 192.168.126.128 TLSv1.3 85 App
145 207.540743970 192.168.126.128 34.36.137.203 TCP 54 410
146 207.759725248 34.36.137.203 192.168.126.128 TLSv1.3 2563 App
147 207.759768867 192.168.126.128 34.36.137.203 TCP 54 410
148 207.760508683 192.168.126.128 34.36.137.203 TLSv1.3 93 App
149 207.760836832 34.36.137.203 192.168.126.128 TCP 60 443
150 210.598204424 34.107.243.93 192.168.126.128 TLSv1.2 78 App
151 210.598593877 192.168.126.128 34.107.243.93 TLSv1.2 82 App
152 210.599426631 34.107.243.93 192.168.126.128 TCP 60 443
153 210.894328126 192.168.126.128 192.46.210.39 NTP 90 NTP
154 210.932962197 192.46.210.39 192.168.126.128 NTP 90 NTP
Frame 1: 90 bytes on wire (720 bits), 9
Ethernet II, Src: VMware_e1:b1:d9 (00:6
Internet Protocol Version 4, Src: 192.1
User Datagram Protocol, Src Port: 53393
Network Time Protocol (NTP Version 4, c
0000 00 50 56 ed 60 56 00 0c 29 e1 b1
0010 00 4c a8 b3 40 00 40 11 bf b6 c0
0020 d2 27 d0 91 00 7b 00 38 d1 c8 23
0030 00 00 00 00 00 00 00 00 00 00 00
0040 00 00 00 00 00 00 00 00 00 00 00
0050 00 00 fc c9 fb 71 c6 0d 2e 90

RESULT:


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless
Power Manager
System is running or
work to avoid losing
Suspend the system
http.request.method == "GET"
No. Time Source Destination Protocol
10127 197.562773759 10.197.113.85 44.228.249.3 HTTP
10154 198.050292122 10.197.113.85 44.228.249.3 HTTP
10178 198.357140904 10.197.113.85 44.228.249.3 HTTP
10182 198.518397178 10.197.113.85 44.228.249.3 HTTP
10311 214.754606688 10.197.113.85 44.228.249.3 HTTP
10381 217.690546746 10.197.113.85 44.228.249.3 HTTP
10835 295.587778654 10.197.113.85 44.228.249.3 HTTP
11038 341.955386399 10.197.113.85 139.162.174.209 HTTP
11044 343.407994362 10.197.113.85 139.162.174.209 HTTP
11685 413.269740886 10.197.113.85 44.228.249.3 HTTP
Frame 116: 376 bytes on wire (3008 bits), 376 bytes captured (3008 bits) on in
Ethernet II, Src: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d), Dst: f6:e2:7b:74:
Internet Protocol Version 4, Src: 10.197.113.85, Dst: 34.107.221.82
Transmission Control Protocol, Src Port: 48328, Dst Port: 80, Seq: 1, Ack: 1,
Hypertext Transfer Protocol


Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.request
No. Time Source Destination Protocol Length Info
239 23.545907843 192.168.1.7 142.250.70.35 OCSP 493 Request
265 23.775859666 192.168.1.7 142.250.70.35 OCSP 493 Request
267 23.796842964 192.168.1.7 142.250.70.35 OCSP 493 Request
268 23.805776408 192.168.1.7 142.250.70.35 OCSP 493 Request
285 23.864176008 192.168.1.7 142.250.70.35 OCSP 494 Request
309 23.911425921 192.168.1.7 142.250.70.35 OCSP 494 Request
544 24.706829526 192.168.1.7 142.250.70.35 OCSP 494 Request
547 24.722029593 192.168.1.7 34.107.221.82 HTTP 376 GET /success.txt?ipv4 H
1844 225.147155636 192.168.1.7 172.64.149.23 OCSP 497 Request
2308 373.796706518 192.168.1.7 142.251.43.131 OCSP 494 Request
2326 373.841815400 192.168.1.7 142.251.43.131 OCSP 494 Request
2427 374.147133897 192.168.1.7 142.251.43.131 OCSP 493 Request
2429 374.150864237 192.168.1.7 142.251.43.131 OCSP 493 Request
2465 374.193448576 192.168.1.7 142.251.43.131 OCSP 493 Request
2895 377.445139340 192.168.1.7 142.251.43.131 OCSP 494 Request
3028 378.378368457 192.168.1.7 142.251.43.131 OCSP 494 Request
3387 395.802050246 192.168.1.7 142.250.70.35 OCSP 494 Request
3397 395.893704426 192.168.1.7 142.250.70.35 OCSP 494 Request
Frame 239: 493 bytes on wire (3944 bits), 493 bytes capt
Ethernet II, Src: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:
Internet Protocol Version 4, Src: 192.168.1.7, Dst: 142.
Transmission Control Protocol, Src Port: 56470, Dst Port
Hypertext Transfer Protocol
POST /we2 HTTP/1.1\r\n
Host: o.pki.goog\r\n
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0)
Accept: */*\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Content-Type: application/ocsp-request\r\n
Content-Length: 83\r\n
Connection: keep-alive\r\n
Priority: u=2\r\n
Pragma: no-cache\r\n
Cache-Control: no-cache\r\n
\r\n
[Response in frame: 259]
[Full request URI: http://o.pki.goog/we2]
File Data: 83 bytes
Online Certificate Status Protocol
0000 84 6e bc e9 78 a1 08 00 27 d1 f8 5d
0010 01 df 8f b2 40 00 40 06 12 9a c0 a8
0020 46 23 dc 96 00 50 48 e5 ba 5d 37 92
0030 01 f6 98 9e 00 00 01 01 08 0a b6 8e
0040 51 49 50 4f 53 54 20 2f 77 65 32 20
0050 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20
0060 69 2e 67 6f 6f 67 0d 0a 55 73 65 72
0070 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f
0080 28 58 31 31 3b 20 4c 69 6e 75 78 20
0090 36 34 3b 20 72 76 3a 31 32 38 2e 30
00a0 63 6b 6f 2f 32 30 31 30 30 31 30 31
00b0 65 66 6f 78 2f 31 32 38 2e 30 0d 0a
00c0 70 74 3a 20 2a 2f 2a 0d 0a 41 63 63
00d0 4c 61 6e 67 75 61 67 65 3a 20 65 6e
00e0 65 6e 3b 71 3d 30 2e 35 0d 0a 41 63
00f0 2d 45 6e 63 6f 64 69 6e 67 3a 20 67
0100 20 64 65 66 6c 61 74 65 0d 0a 43 6f
0110 74 2d 54 79 70 65 3a 20 61 70 70 6c
0120 69 6f 6e 2f 6f 63 73 70 2d 72 65 71
0130 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65
0140 3a 20 38 33 0d 0a 43 6f 6e 6e 65 63
0150 3a 20 6b 65 65 70 2d 61 6c 69 76 65