Practical no:1

Aim : <u>Working with Sniffers for monitoring network communication</u>

Open the Wireshark



Click on the "Interfaces" button on the toolbar:

Check on the Ethernet Tab

And Click Start

4	Wireshark: Capture Inte	rfaces		-	□ ×
Device	Description	IP	Packets	Packets/s	;
🗌 进 VMware Network Adapter	VMnet1 VMware Virtual Ethernet Adapter	fe80::858f:9c93:318b:6039	0	0	<u>D</u> etails
💽 🔊 Ethernet	Realtek PCIe GBE Family Controlle	er fe80::51b9:24b1:434c:5bb	8 1224	88	<u>D</u> etails
🗌 🕂 VMware Network Adapter	VMnet8 VMware Virtual Ethernet Adapter	fe80::8d66:3a33:21e3:1eab	b 0	0	<u>D</u> etails
<u>H</u> elp	<u>S</u> tar	s <u>t</u> op	<u>O</u> ptions		<u>C</u> lose

You will get the List of all the packet arriver through your port

Capturing from Ethernet [Wireshark 1.10.8 (v1.10.8-2-g52a5244 from master-1.10)]	- 0 ×
Eile Edit View <u>Go</u> Capture Analyze Statistics Telephony <u>T</u> ools Internals <u>H</u> elp	
◎ ◎ ∡ ■ ∡ () == == ※ (2) 0, + + + + + + = = = 0, 0, 0, 17 ₩ ⊠ % % ₩	
Filter V Expression Clear Apply Save	
No. Time Source Destination Protocol Length Info	^
278 2.97793000 192.168.10.1 192.168.10.148 HTTP 1514 Continuation or non-HTTP traffic	
2/9 2.9//98400192.168.10.148 192.168.10.1 ICP 54 4929/ > nd1-aa5 [ACK] 564-1 ACK=183961 W1n=1024 Len=0	
281 2.97808700192.168.10.148 192.168.10.1 TCP 54 49297 > nd1-aas [AcK=185421 Win=1024 Len=0	
282 2.97813700 192.168.10.1 192.168.10.148 HTTP 1230 Continuation or non-HTTP traffic	
283 2.97816900 192.168.10.148 192.168.10.1 TCP 54 49297 > ndl-aas [ACK] Seq=1 Ack=186597 Win=1019 Len=0	
284 2.97896200192.168.10.1 192.168.10.148 HTTP 338 Continuation or non-HTTP traffic	
285 2.97900200 192 168 10.148 192 168 10.1 TCP 54 49297 > ndl-aas [ACK] Seq=1 Ack=186881 Win=1024 Len=0	
286 2.99910400 192.168.10.1 192.168.10.148 HTP 1514 Continuation or non-HTP traffic	
28/ 2.99918200192.108.10.148 192.108.10.1 ICP 34 4929/ > http://dx.j.sed=1 Ack=186341 Win=1024 Len=0	*
B Frame 1: 1)14 bytes on wire (12112 bits), 1)14 bytes captured (12112 bits) on interface 0 B Ethernet II, Src: bm_47:af:da (00:21:5e:47:af:da), bst: bell_09:81:11 (e3:1f:66:09:81:11)	
B Internet Protocol Version 4, Src: 192.168.10.1 (192.168.10.1), Dst: 192.168.10.148 (192.168.10.148)	
🗄 Transmission Control Protocol, Src Port: ndl-aas (3128), Dst Port: 49297 (49297), Seq: 1, Ack: 1, Len: 1460	
B Hypertext Transfer Protocol	
	^
0020 0a 94 0c 38 c0 91 77 cf eb 33 90 4b 43 0a 50 188.w3.KC.P.	
10030 T0 T5 / 6 0a 00 00 0b 14 a0 86 8/ 2/ 62 03 / 0 40	
0050 54 1d 84 ff 42 cl dd 87 ac 4a 55 00 21 6f 72 16 TB JU.!or.	
0060 98 1d 55 72 d7 bf 0b 02 c0 bb 55 c0 47 ef 24 0cur	
00/0 00 07 92 81 79 04 40 87 40 16 24 76 54 07 7.51 1.02	
0090 5a a9 77 4e e5 58 2c c3 c3 1d 9e c9 e0 99 57 df z.ww.x,w	
100a0 82 d5 tb 9e 10 ba t7 td b2 17 d1 cb 91 0e 83 60	
00c0 85 c9 82 04 07 25 f7 7f d0 5f bb d1 82 c0 fc le%	
00d0 d3 8c 26 a6 bc 37 57 3a ae d3 0e 4e ef a6 05 1cN	
100e0 tb b3 51 e2 c4 ad 7c b2 47 2d dc c0 at 3t 12 95, c,, G, G, c. L	
0100 f6 6f 89 7f 7f 20 31 7d 37 1f 1e 26 75 8f d4 07	
Dation c2 4b ft 65 47 7c 3b 7a 16 b7 0c b0 4t 12 35 52 v fc1 b0 ∰ (Ethernet (live capture in progress File CA	Profile: Default

Go to Filter Tab and enter "http"

Capturing	from Ethernet [Wireshark 1.10.8 (v1.10.8-2-g52a5244 from master-1.10)]	- 0 ×
<u>File Edit View Go Capture Analyze Statistics Telephony Tools Internal</u>	s <u>H</u> elp	
◎ ◎ ∡ ■ ∡ ⊨ ≞ × 2 ९ + + ⇒ ∓ ± ■ □	3] (Q, Q, 🖭 💥 🖄 🥵 🔆 💢	
Filter: http 🗸 Exp	ression Clear Apply Save	
No. Time Source Destination Pro	otocol Length Info	^
1 0.0000000 192.168.10.1 192.168.10.148 H ⁻	TTP 1514 Continuation or non-HTTP traffic	
3 0.00087100 192.168.10.1 192.168.10.148 HT	TTP 1514 Continuation or non-HTTP traffic	
5 0.00900800 192.168.10.1 192.168.10.148 HT	TTP 1514 Continuation or non-HTTP traffic	
7 0.02954600192.168.10.1 192.168.10.148 HT	TTP 1514 Continuation or non-HTTP traffic	
9 0.03041700 192.168.10.1 192.168.10.148 H	TTP 1514 Continuation or non-HTTP traffic	
11 0.03048000192.168.10.1 192.168.10.148 H	TTP 1230 Continuation or non-HTTP traffic	
13 0.03051400 192.168.10.1 192.168.10.148 H	IIP 338 Continuation or non-HITP traffic	
15 0.0345/000192.108.10.1 192.108.10.148 H	TTP 1514 Continuation or non-HITP traffic	
10 0 06740300102 168 10 1 102 168 10 148 H	TTP 1514 Continuation of hon-HTTP traffic	
19 0.00/49200192.108.10.1 192.108.10.148 H		
H Frame 1: 1514 bytes on wire (12112 bits), 1514 bytes cap	tured (12112 bits) on interface 0	
Ethernet II, SrC: Ibm_4/:ar:da (00:21:5e:4/:ar:da), Dst:	Dell_09381111 (c8:11:66:09381111)	
■ Internet Protocol Version 4, Src: 192.168.10.1 (192.168.	10.1), DSt: 192.108.10.148 (192.108.10.148)	
Hansmission Control Protocol	, DSC POLC. 49297 (49297), SEQ. 1, ACK. 1, LEN. 1400	
$\begin{array}{c} 0000 \\ 0010 \\ 05 \\ 0010 \\ 05 \\ 05 \\ 010 \\ 05 \\ 010 \\ 05 \\ 010 \\ 05 \\ 010 \\ 01$	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	~
🔵 🌌 Ethernet: <live capture="" in="" progress=""> File: C:\ Packets: 1917 · Displayed: 909 (4</live>	7.4%)	Profile: Default

Click on any of the http and Expand the "Data" tab

6	Capturing from Ethernet [Wireshark 1.10.8 (v1.10.8-2-g52a5244 from master-1.10)]	- 🗇 🗙
<u>File Edit View Go Capture Analyze Statistics Tel</u>	lephony <u>T</u> ools <u>I</u> nternals <u>H</u> elp	
● ● ∡ ■ ∠ ⊨ ≞ x 2 < + +	> 🐟 🚡 👱 🗐 🗟 Q, Q, Q, 🗹 👹 🖄 🥵 % 💢	
Filter: http	Expression Clear Apply Save	
No. Time Source Destin	nation Protocol Length Info	^
1 0.0000000 192.168.10.1 192.	.168.10.148 HTTP 1514 Continuation or non-HTTP traffic	
5 0 00900800 192 168 10 1 192	168.10.148 HTTP 1514 CONTINUATION OF NON-HTTP TRAFFIC	
7 0.02954600 192.168.10.1 192.	168.10.148 HTTP 1514 Continuation or non-HTTP traffic	
9 0.03041700 192.168.10.1 192.	.168.10.148 HTTP 1514 Continuation or non-HTTP traffic	
11 0.03048000 192.168.10.1 192.	.168.10.148 HTTP 1230 Continuation or non-HTTP traffic	
13 0.03051400 192.168.10.1 192.	.168.10.148 HTTP 338 Continuation or non-HTTP traffic	
15 0.03457000 192.168.10.1 192.	.168.10.148 HTTP 1514 Continuation or non-HTTP traffic	
19 0 06749200 192 168 10 1 192	108.10.148 HTTP 1514 CONTINUATION OF NON-HTTP traffic	
T Frame 1: 1514 bytes on wire (12112 bits	130. 1514 bits continued (1211) bits on interface 0	
Finance 1. 1914 bytes on whe (12112 bits Finance 1. 1914 bytes on whe (12112 bits Finance 1. 1914 bytes on whe (12112 bits	5, 1514 bytes captured (12112 bits) on interface o	
Internet Protocol Version 4, Src: 192.1	168.10.1 (192.168.10.1), Dst: 192.168.10.148 (192.168.10.148)	
Transmission Control Protocol, Src Port Ort O	t: ndl-aas (3128), Dst Port: 49297 (49297), Seq: 1, Ack: 1, Len: 1460	
Hypertext Transfer Protocol		
■ Data (1460 bytes)	17	
Data: 0014a08e8/2/e203/040110/0a884	+3aeer44earrr0eb4309	
[Length: 1400]		
0030 Td T5 /e 0a 00 00 p6 14 ad 8e 8/ 2 0040 11 07 6a 88 43 ae ef 44 ed ff f0 e		^
0050 54 1d 84 ff 42 c1 dd 87 ac 4a 55 0	00 21 6f 72 16 TBJU.!or.	
0060 98 1d 55 72 d7 bf 0b 02 c0 bb f5 c	20 47 ef 24 0c ur	
0080 8b 93 ba 93 67 20 32 7b ae c0 4d 8	$1 \le 24 + (\le 3a + 0)^2 + (3+1)^2 + (3+2)^2 + $	
0090 5a a9 77 4e e5 58 2c c3 c3 1d 9e c	e9 e0 99 57 df z.wN.xw.	
00a0 82 d5 fb 9e 10 ba f/ fd b2 1/ d1 c 00b0 cb 2c 35 6a 90 c9 4a 82 1f 08 4e 7	20 1 0 6 8 3 60	
00c0 85 c9 82 04 07 25 f7 7f d0 5f bb c	d1 82 c0 fc 1e%	
00d0 d3 8c 26 a6 bc 37 57 3a ae d3 0e 4	te ef a6 05 1c&7w:N	
00f0 e7 4a e5 41 67 ff a1 2e 3c 5f 5b a	$C(a_1, b_1, f_2, g_3, \dots, g_{n-1}, g_{n-1}, g_{n-1}, g_{n-1})$	
0100 f6 6f 89 7f 7f 20 31 7d 37 1f 1e 2	26 75 8f d4 07 1} 7&u	
0110 C2 4b f1 66 47 7C 3b 70 16 b7 0e b 0120 96 dd 23 09 b6 82 28 de 32 f7 03 6	かりの113 aa 52 、K.TGI; pR 55 R1 A8 55 R5 - 単(・2) 日 /	
0130 4b d1 16 d4 5e 74 2d 7c e6 96 54 8	57 86 c1 82 6a K^t]j	~
○ M Data (data), 1460 bytes	ets: 3100 · Displayed: 1459 (47.1%)	Profile: Default

Click on Hypertext Transfer Protocol

Click on Post

Canturing from Ethernet _ IWiresbark 110.8 (v1.10.8-2-o.5235244 from master-1.10)]	- 🗇 X	
Sile Site View Ge Castrie Ashine Statistic Telesheev Telesheeving Home Statistic Telesheeving Home Statistic Telesheeving Home		
Die Fair Jiew Zo Zebraie Brailze Stanzier, Leichioul Toole Interlage Tich		
🖲 🛞 🦼 📕 🔬 🔚 🔚 💥 💬 🔍 💠 💠 🌴 👱 🔜 🖼 😆 🔂 🔇 🔍 🔃 👹 🗺 😽 🙀		
Filter http v Expression Clear Apply Save		
No. Time Source Destination Protocol Length Info	^	
12 0.60620400 192.168.10.148 192.168.10.1 HTTP 1126 POST http://webres1.qheal.ctmail.com/SpamResolverNG/SpamResolverNG.dll?DoN	ewRequest HTTP/1.0	
22 0.94584200 192.168.10.148 192.168.10.1 HTTP 1043 POST http://webres1.qheal.ctmail.com/SpamResolverNG/SpamResolverNG.dll?DoN	ewRequest HTTP/1.0	
31 1.19350300 192.168.10.1 192.168.10.148 HTTP 116 HTTP/1.0 200 0K (text/html)		
38 1.35/3/30/TE80::295C:305/:4/aTT02::C S5DP 208 M-SEARCH * HITP/L1	allow Deguest UTTO /1 0	
47 2.0522740 192.106.10.146 192.106.10.1 mTP 1047 POST http://resolveri.dneat.ctmat.com/spamkesolverid/spamkesolveri	onewkequest HTTP/1.0	
59.2.2144450019216810148 192168101 HTTP 110 HTTP://oscilveri.dbal.ctmail.com/SpamPesolverMc/SpamPeso	ONewRequest HTTP/1 0	
64 2,47994800 192, 168, 10, 1 192, 168, 10, 148 HTTP 327 HTTP/1,0 200 0K (Text/html)	onemicquese mmy 110	
73 2,48340500 192,168,10.148 192,168,10.1 HTTP 1016 POST http://resolver1.gheal.ctmail.com/SpamResolverNG/SpamResolverNG.dl]?D	oNewRequest HTTP/1.0	
76 2.69309900 192.168.10.1 192.168.10.148 НТТР 990 НТТР/1.0 200 ок (text/html)	×	
Bypertext Transfer Protocol	^	
= POST http://webres1.qheal.ctmail.com/SpamResolverNG/SpamResolverNG.dll?DoNewRequest HTTP/1.0\r\n		
Expert Info (Chat/Sequence): POST http://webres1.qheal.ctmail.com/SpamResolverNG/SpamResolverNG.dll?DoNewRequest HTTP/1.0\r\n]		
[Message: POST http://webres1.qheal.ctmail.com/SpamResolverNG/SpamResolverNG.dll?DoNewRequest HTTP/1.0\r\n]		
[Severity level: Chat]		
[Group: Sequence]		
Request Method: POST		
Request URI: http://webresi.qheal.ctmail.com/spamkesolverNG/spamkesolverNG.dll?DoNewRequest		
Accept Language on USDA		
Accept: "/*//il		
Content-length: 785/r/n		
Host: webres1.oheal.ctmail.com\r\n		
Proxy-Authorization: Basic Oq==\r\n		
\r\n		
[Eull request HDT: http://webres1 dbes1 ctmsil comhttp://webres1 dbes1 ctmsil com/SnamDesolverNG/SnamDesolverNG dll?noNewDequest]	*	
0030 01 00 85 45 00 00 50 4f 53 54 20 68 74 74 70 3aE. PO ST http:	^	
0040 27 27 // 05 02 /2 05 /3 31 22 /1 08 05 01 05 22 //WeDFES 1.qneal.		
0060 65 73 6F 6c 76 65 72 4e 47 2F 53 70 61 6d 52 65 esolverN G/Spamke		
0070 73 6f 6c 76 65 72 4e 47 2e 64 6c 6c 3f 44 6f 4e solverNG .dll?DoN		
0080 05 // 52 05 /1 /5 05 /3 /4 20 48 54 54 50 27 51 eWkeddes t HTP/1		
00a0 61 67 65 3a 20 65 6e 2d 75 73 0d 0a 41 63 63 65 age: en- us. Acce		
00b0 70 74 3a 20 2a 2f 2a 0d 0a 55 73 65 72 2d 41 67 pt: */*. user-Ag		
UUCU b5 be /4 3a 20 40 bt /a b9 bc bc b1 2t 34 2e 30 ent; M02 111a/4,0 00d0 20 28 63 66 6d 70 61 74 69 62 6c 65 3b 20 57 69 (comma tible wi	~	
o to be to	ault	

🗖 Ca	pturing from Ethernet [Wireshark 1.10.8 (v1.10.8-2-g52a5244 from master-1.10)] – 🗖	x
Eile Edit View Go Capture Analyze Statistics Telephony Tools	Internals Help	
◎ ◎ ∡ ■ ∡ ⊨ ≞ x 2 < + + → 7 ±		
Filter: http	Expression Clear Apply Save	
No. Time Source Destination 12 0.60620400 192.168.10.148 192.168.10.1	Protocol Length Info HTTP 1126 POST http://webres1.qheal.ctmail.com/SpamResolverNG/SpamResolverNG.dll?DoNewRequest HTTP/1.0	^
22 0.94584200192.168.10.148 192.168.10.1 31 1.19350300192.168.10.1 192.168.10.148	<pre>HTTP 1043 POST http://webres1.qheal.ctmail.com/SpamResolverNG/SpamResolverNG.dll?DoNewRequest HTTP/1.0 HTTP 116 HTTP/1.0 200 0K (text/html)</pre>	
38 1.35737300 fe80::293c:5b67:47aff02::c 47 2.05527400 192.168.10.148 192.168.10.1	SSDP 208 M-SEARCH * HTTP/1.1 HTTP 1047 POST http://resolver1.qheal.ctmail.com/SpamResolverNG/SpamResolverNG.dll?DoNewRequest HTTP/1.0	
50 2.20731400192.168.10.1 192.168.10.148 59 2.21444500192.168.10.148 192.168.10.1	HTTP 116 HTTP/1.0 200 0K (text/html) HTTP 1016 POST http://resolver1.qheal.ctmail.com/SpamResolverNG/SpamResolverNG.dll?DoNewRequest HTTP/1.0	
64 2.47994800192.168.10.1 192.168.10.148 73 2.48340500192.168.10.148 192.168.10.1	HTTP 327 HTTP/1.0 200 0K (text/html) HTTP 1016 POST http://resolver1.qheal.ctmail.com/SpamResolverNG/SpamResolverNG.dll?DoNewRequest HTTP/1.0	
76 2.69309900 192.168.10.1 192.168.10.148	HTTP 990 HTTP/1.0 200 OK (text/html)	~
 Internet Protocol Version 4, Src: 192.168.10.148 (Transmission Control Protocol, Src Port: 49325 (49) 	192.168.10.148), Dst: 192.168.10.1 (192.168.10.1) 325), Dst Port: ndl-aas (3128), Sec: 1, Ack: 1, Len: 1072	^
Hypertext Transfer Protocol		
 POST http://webres1.gheal.ctmail.com/SpamResolve Accept-Language: en-us\r\n Accept: */*\r\n User-Agent: Mozilla/4.0 (compatible; win32; Comm Content-Length: 785\r\n Host: webres1.gheal.ctmail.com\r\n 	rNG/SpamResolverNG.dll?DoNewRequest HTTP/1.0\r\n touch Http Client)\r\n	
\r\n [Full request UPT: http://webrest.cheal.stmail.c	ombite://webcasi.ebcal.stmail.com/SpamBaselverNC/SpamBaselverNC.dll2DeNewBeguestl	
[HTTP request 1/1]	Unitel 2.7/web est great. Conart. Con/apanikeso rverwa/apanikeso rverwa, utr: Dokewkequese r	
🗉 Data (785 bytes)		
Data: 0117876543210500000011028c9a8a92629cd6a4 [Length: 785]	8a9a8aaa	~
0150 3d 0d 0a 0d 1 7 65 43 21 05 00 00 00 0160 02 8c 9a 8a 9c 9c 9c 6d a4 8a 9a 8a a6 9a 0170 9a f2 9c 88 9a 8c 6p 9c 8b 26 9c 8a 26 9c 8a 26 9c 8b 3c 2c 3c 3c 3c 3c 3	11 =	^
0180 e6 62 9c 88 ac 88 a2 aa 92 6a 9c f4 e8 8e a4 0190 b4 8e a4 d6 b4 8e a4 d4 e8 8e a4 d6 b4 8e a4 01a0 b4 8e a4 d4 e6 ee 9a 88 82 ee 9a 88 82 ee 9a	dē .b	
01b0 e6 f0 9e f4 82 ee 9a 88 82 ee 9a 80 60 60 60 7a 7	f4	
01e0 b4 8e a4 d6 b2 6e 9a a8 e6 ee 9a aa aa ee a2 01f0 ce ee 9a 88 e6 ee a2 a8 8a 64 9a 88 a2 ee 9e	d4n	~
🛑 💇 Data (data), 785 bytes 🛛 Packets: 24307 · Displa	red: 9615 (39.6%) Profile: Default	

Go to **Expression** Tab Near the Filter Tab

Click on "http.request - Request(True if HTTP request)"

Attp.proxy_authonzation - Proxy-Authonzation http.proxy_connect_host - Proxy-Connect-Hos http.proxy_connect_port - Proxy-Connect-Por http.referer - Referer (HTTP Referer) http.request - Request (TRUE if HTTP request) http.request.full_uri - Full request URI (The full http.request.method - Request Method (HTTP http.request.method - Request Method (HTTP http.request.uri - Request URI (HTTP Request- http.request.version - Request Version (HTTP F http.request in - Request in frame (This packer >		False Range (offset:length)
--	--	--------------------------------

Capturing from Ethernet [Wireshark 1.10.8 (v1.10.8-2-g52a5244 from master-1.10)] –	×
Eile Edit View <u>Go</u> <u>Capture</u> <u>Analyze</u> <u>Statistics</u> Telephony <u>Tools</u> <u>Internals</u> <u>H</u> elp	
● ◎ ∡ ■ ፈ ⊨ ≞ % 2 ੧ ቀ ቀ ∓ ½ ⊒ ⊒ ੧ ੧ ੧ ⊡ ¥ ⊠ ≅ % ⊒	
Filter http:request.method == POST v Expression Clear Apply Save	
No. Time Source Destination Protocol Length Info 2721 120.218121192.168.10.148 192.168.10.1 HTTP 1043 POST http://webres1.qheal.ctmail.com/SpamResolverNG/SpamResolverNG.dll?DoNewRequest HTTP/1.0 3332 224.276651 192.168.10.148 192.168.10.1 HTTP 1043 POST http://webres1.qheal.ctmail.com/SpamResolverNG/SpamResolverNG.dll?DoNewRequest HTTP/1.0 3712 242.822167 192.168.10.148 192.168.10.1 HTTP 1047 POST http://resolver1.qheal.ctmail.com/SpamResolverNG/SpamResolverNG.dll?DoNewRequest HTTP/1.0 3725 243.21586192.168.10.148 192.168.10.1 HTTP 1016 POST http://resolver1.qheal.ctmail.com/SpamResolverNG/SpamResolverNG.dll?DoNewRequest HTTP/1.0 3750 243.215186192.168.10.148 192.168.10.1 HTTP 1016 POST http://resolver1.qheal.ctmail.com/SpamResolverNG/SpamResolverNG.dll?DoNewRequest HTTP/1.0 3765 243.514823192.168.10.148 192.168.10.1 HTTP 1016 POST http://resolver1.qheal.ctmail.com/SpamResolverNG/SpamResolverNG.dll?DoNewRequest HTTP/1.0 4565 349.1868.10.148 192.168.10.1 HTTP 1016 POST http://resolver1.qheal.ctmail.com/SpamResolverNG/SpamResolverNG.dll?DoNewRequest HTTP/1.0 4565 549.2168.10.148 192.168.10.1 HTTP 1106 POST http://webres1.qheal.ctmail.com/SpamResolverNG/SpamResolverNG.dll?DoNewRequest HTTP/1.0	
 □ Internet Protocol Version 4, Src: 192.168.10.148 (192.168.10.148), Dst: 192.168.10.1 (192.168.10.1) □ Transmission Control Protocol, Src Port: 49582 (49582), Dst Port: ndl-aas (3128), Seq: 1, Ack: 1, Len: 1062 □ Hvpertext Transfer Protocol 	
○ POST http://webres1.qheal.ctmail.com/spamResolverNG/SpamResolverNG.dll?DoNewRequest HTTP/1.0\r\n	
[Expert Info (chat/Sequence): POST http://webres1.qheal.ctmail.com/SpamResolverNG/SpamResolverNG.dll?DoNewRequest HTTP/1.0\r\n] Request Mathod: POST	-
Request URI: http://webres1.gheal.ctmail.com/SpamResolverNG/SpamResolverNG.dll?DoNewRequest Request Version: HTTP/1.0 Accept-Language: en-uslr\n Accept: */%\r\n	
User-Adent: Mozilla/4.0 (compatible: Win32: Commtouch Http Client)\r\n	~
0000 00 21 5e 47 af de 65 11 06 00 45 00	· · · · · · · · · · · · · · · · · · ·
Frame (frame), 1116 bytes Packets: 10925. Displayed: 22.(0.2%)	

Enter this command **"http.request.method = = POST"** into Filter tab

Enter "http.host contains 123" in the Filter Tab

4	Capturing from Ethernet [Wireshark 1.10.8 (v1.10.8-2-g52a5244 from master-1.10)]	– 🗆 🗙
<u>File Edit View Go Capture Analyze Statistics Telephony</u>	iy Iools Internals Help	
● ● ▲ ■ ▲ ⊨ ≞ X 2 < + + →	春 👱 🗐 🖻 역, 역, 🥂 🗱 🔟 🥵 % 📆	
Filter: http.host contains 123	Expression Clear Apply Save	
No. Time Source Destination	Protocol Length Info	
8461 433.809048 192.168.10.148 192.168.1	10.1 HTTP 469 GET http://www.123greetings.com/ HTTP/1.1	
8517 434.292243 192.168.10.148 192.168.	10.1 HTP 3/3 GET http://www.i23greetings.com/Tavicon.tco HTP/1.1	
10404 045.705725 192.108.10.148 192.108.1	10.1 HTP 373 GET http://www.123greetings.com/ http/1.1	
Frame 8461: 469 bytes on wire (3752 bits), Frame 8461: 469	469 bytes captured (3752 bits) on interface 0	^
Ethernet II, SrC: Dell_09:81:11 (C8:17:66:0	19:81:11), DST: 10m_4/:aT:0a (00:21:50:4/:aT:0a) 10:148 (10:168 10:148), DFT: 10:169 10:1 (10:168 10:1)	
Transmission Control Protocol, Src Port: 49	30.149 (122.100.10.149), DSL 122.100.101 (122.100.101) 3002 (49602), DSL Port: ndl-aas (3128), Sen: 1, Ack: 1, Len: 415	
Hypertext Transfer Protocol	(4)(4)(4)(4)(4)(4)(4)(4)(4)(4)(4)(4)(4)(
GET http://www.123greetings.com/ HTTP/1.1	L\r\n	
Expert Info (Chat/Sequence): GET http:	//www.123greetings.com/ HTTP/1.1\r\n]	
Request Method: GET		
Request URI: http://www.123greetings.co	/m/	
Request Version: HTTP/1.1		
Host: www.i23greetings.com\r\n Broxy Connection: keen alive\r\r		
Accept: text/html application/vhtml+vml a	annlication/yml.g=0.9 image/webn */*·g=0.8/r/n	~
0000 00 21 5e 47 af da c8 1f 66 09 81 11 08		
0010 01 c7 21 39 40 00 80 06 42 12 c0 a8 0a	94 c0 a890 B	^
0020 0a 01 c1 c2 0c 38 91 74 14 cd 8a 0f 3d	36 50 188.t=6P.	
0030 01 00 C/ db 00 00 4/ 45 54 20 68 /4 /4 0040 2f 77 77 77 2e 31 32 33 67 72 65 65 74	/0 3a 2T6E T http://	
0050 73 2e 63 6f 6d 2f 20 48 54 54 50 2f 31	2e 31 0d s. com/ H TTP/1.1.	
0060 0a 48 6f 73 74 3a 20 77 77 77 2e 31 32	33 67 72 .Host: w Ww.123gr	
0080 78 79 2d 43 6f 6e 6e 65 63 74 69 6f 6e	3a 20 6b xx-connection: k	
0090 65 65 70 2d 61 6c 69 76 65 0d 0a 41 63	63 65 70 eep-aliv e. Accep	
UUAU /4 3a 20 74 65 78 74 2t 68 74 6d 6c 2c	61 /0 /0 I: text/ ntml,app	Y
Ethernet: Ethernet: Et	(61- Dieplayed: 4 (0.0%) Profile: Default	
		11:50 AM

Enter "http.request.uri contains 123" in the Filter Tab

EVE Lat Yew Go Capture Analyze Subjics: Telephony Look Internal: Holp Image: State Control (State Control	۵	Capturing from Ethernet [Wireshark 1.10.8 (v1.10.8-2-g52a5244 from master-1.10)] – 🗖 💌	
• • • • • • • • • • • • • • • • • • •	<u>File Edit View Go Capture Analyze Statistics Telephony To</u>	ols Internals Help	
Filte: https://www.i23greetings.com/ HTTP/1.1 B451 433.00048 192.168.10.148 192.168.10.1 HTTP 323 647 Http://www.i23greetings.com/ HTTP/1.1 10255 443.00048 192.168.10.148 192.168.10.1 HTTP 323 647 Http://www.i23greetings.com/ HTTP/1.1 10255 443.00048 192.168.10.148 192.168.10.1 HTTP 323 647 Http://www.i23greetings.com/ HTTP/1.1 10555 443.00048 192.168.10.148 192.168.10.1 HTTP 373 647 Http://www.i23greetings.com/favicon.ico HTTP/1.1 10555 443.00048 192.168.10.148 192.168.10.1 HTTP 373 647 Http://www.i23greetings.com/favicon.ico HTTP/1.1 10555 643.00048 192.168.10.148 192.168.10.1 HTTP 373 647 Http://www.i23greetings.com/favicon.ico HTTP/1.1 10555 643.00048 192.168.10.148 192.168.10.148 (00:21:56:47.31) HTTP 373 647 Http://www.i23greetings.com/favicon.ico HTTP/1.1 1055 643.00048 192.168.10.148 (00:22:56:10.1) HTTP 373 647 Http://www.i23greetings.com/favicon.ico HTTP/1.1 1055 643.00048 192.168.10.148 (00:22:56:10.168.10.1 (192.156:10.1) HTTP 373 647 Http://www.i23greetings.com/favicon.ico HTTP/1.1 105 647 647 647 647 647 647 647 647 647 647	● ● ◢ ■ ◢ ⊨ ⊨ ⊨ ₩ ≈ । < + + ⇒ ∓ ;	👱 🔲 📾 🔍 Q, Q, 🔯 👹 🕺 🎋 💢	
No. Time Source Detination Protocol Length Info 8461 835048192.168.10.148 192.168.10.1 HTTP 373 GET http://www.123greetings.com//HTTP/1.1 10464 645.70725192.168.10.148 192.168.10.1 HTTP 373 GET http://www.123greetings.com//favicon.ico HTTP/1.1 10525 645.898444 192.168.10.1 HTTP 373 GET http://www.123greetings.com//favicon.ico HTTP/1.1 10525 645.898444 192.168.10.1 HTTP 373 GET http://www.123greetings.com/favicon.ico HTTP/1.1 10525 645.898444 192.168.10.148 192.168.10.1 HTTP 373 GET http://www.123greetings.com/favicon.ico HTTP/1.1 10525 645.898444 192.168.10.148 192.168.10.148 192.168.10.148 10525 645.898444 192.168.10.148 192.168.10.148 192.168.10.148 10 Externent II, src: bell_09:81:11 psr: bm.47:8fdd (002.21:5e:47:8f':da) 10 Intramsingsion control Protocol, src bort: 49602 (49602), pst rot: nd-as (122.168.10.148) 11 Intramsingsion control Protocol, src bort: 49602 (49602), pst rot: nd-as (122.168.10.19)	Filter: http.request.uri contains 123	Expression Clear Apply Save	
B Frame 8461: 469 bytes on wire (3752 bits), 469 bytes captured (3752 bits) on interface 0 B Ethernet II, 5rc: bell_09:81:11 (c8:1f:66:09:81:11), Dst: Ibm_47:af:da (00:21:5e:47:af:da) B Internet Protocol Version 4, Src: 192.168.10.148 (192.168.10.148), Dst: 192.168.10.1 (192.168.10.1) B Tranmission control Protocol, Src Port: 49602 (49602), Dst Port: ndl-ass (3128), Seq: 1, Ack: 1, Len: 415 B Hypertext Transfer Protocol G Ethernet II: for (chat/sequence): GET http://www.123greetings.com/ HTTP/1.1\r\n] Request Version: HTTP/1.1 M Hot: Wh: 123greetings.com/(r\n) Proxy-connection: keep-alive\r\n Accent: text/fram.aonlication/xml:o=0.9.imaop/webn.*/*:n=0.8\r\n Cond 0 1 21: 5e 47 af da c8 1f 66 09 81 11 08 00 45 00 1.^6 f6t. Coll 0 1 21: 5e 47 af da c8 1f 66 09 81 11 08 00 45 00 1.^6 f6t. Coll 0 1 21: 5e 47 af da c8 1f 66 09 81 11 08 00 45 00 1.^6 f6t. Coll 0 1 21: 5e 47 af da c8 1f 66 09 81 11 08 00 45 00 1.^6 f6t. Coll 0 1 21: 5e 47 af da c8 1f 66 09 81 11 08 00 45 00 1.^6 f6t. Coll 0 1 21: 5e 47 af da c8 1f 66 09 81 11 08 00 45 00 1.^6 f6t. Coll 0 1 21: 5e 47 af da c8 1f 66 09 81 11 08 00 45 00 1.^6 f6t. Coll 0 1 21: 5e 47 af da c8 1f 66 09 81 11 08 00 45 00 1.^6 f6t. Coll 0 1 21: 5e 47 af da c8 1f 66 09 81 11 08 00 45 00 1.^6 f6t. Coll 0 1 21: 5e 47 af da c8 1f 66 09 81 10 08 00 61 18t. t6t. Coll 0 21: 5e 47 af da c8 1f 66 09 81 11 08 00 45 00 18t. t6t. Coll 0 21: 5e 47 af da c8 1f 66 09 81 11 08 00 45 00 18t. t6t. Coll 0 21: 5e 47 af da c8 1f 66 09 81 11 08 00 45 00 18t. t6t. Coll 0 21: 5e 47 af da c8 1f 66 09 81 10 08 00 64 12: 20 08 06 04 12: 20 08 06 04 12: 20 08 06 04 12: 20 08 06 04 12: 20 08 06 04 12: 20 08 06 04 10: 20 08 06 04 10: 20 08 06 04 10: 20 08 06 04 10: 20 08 06 04 12: 20 08 06 04 10: 20 08 06 04 10: 20 08 06 04 1	No. Time Source Destination 8461 433.809048 192.168.10.148 192.168.10.1 81317 434.292243 192.168.10.148 192.168.10.1 10464 645.70575 192.168.10.148 192.168.10.1 10525 645.898444 192.168.10.148 192.168.10.1	Protocol Length Info HTTP 469 GET http://www.123greetings.com/HTTP/1.1 HTTP 373 GET http://www.123greetings.com/favicon.ico HTTP/1.1 HTTP 469 GET http://www.123greetings.com/HTTP/1.1 HTTP 373 GET http://www.123greetings.com/favicon.ico HTTP/1.1	
Request Wethod: GET Request Version: HTTP/1.1 Host: www.123greetings.com/r Prost: www.123greetings.com/r prost: www.123greetings.com/r more than the than	 Brame 8461: 469 bytes on wire (3752 bits), 469 Ethernet II, src: pell_09:81:11 (c8:1f:66:09:81 Internet Protocol Version 4, src: 192.168.10.14 Transmission Control Protocol, src port: 49602 Hypertext Transfer Protocol GET http://www.123greetings.com/ HTTP/1.1\r\n Breppert Info (chat/sequence): GET http://ww 	bytes captured (3752 bits) on interface 0 :11), Dst: Ibm.47:af:da (00:21:5e:47:af:da) & (192.168.10.148), Dst: 192.168.10.1 (192.168.10.1) (49602), Dst Port: ndl-aas (3128), Seq: 1, Ack: 1, Len: 415 w.123greetings.com/ HTTP/1.1\r\n]	
0000 00 21 5e 47 af da c8 1f 66 09 81 11 08 00 45 00 .!^Ac fE. 0010 01 c1 c2 0c 38 91 74 14 cd 8a 0f 3d 36 50 18 98c B 0020 0a 11 c1 c2 0c 38 91 74 14 cd 8a 0f 3d 36 50 18 98c8t.t6P. 0030 01 c1 c2 0c 38 91 74 14 cd 8a 0f 3d 36 50 18 8t.t6P. 0030 01 c1 c2 0c 38 91 74 14 cd 8a 0f 3d 36 50 18 8t.t6P. 0030 01 c1 c2 0c 38 91 74 14 cd 8a 0f 3d 36 50 18 8t.t6P. 0030 01 c1 c2 0c 38 91 74 14 cd 8a 0f 3d 36 50 18 8t.t6P. 0030 01 c1 c2 0c 38 91 74 14 cd 8a 0f 3d 36 50 18 8t.t6P. 0030 01 c1 c2 0c 38 91 74 14 cd 8a 0f 3d 36 50 18 8t.t6P. 0030 01 c1 c2 0c 38 91 74 14 cd 8a 0f 3d 36 50 18 8t.t6P. 0030 72 ze 63 ef 6d 2f 20 48 54 54 50 2f 31 2e 31 0d s.com/ H TTP/1.1 0060 0a 48 6f 73 74 2e 63 36 f 6d 0d 0a 50 72 6f eetings.comPro 0080 78 79 2d 43 6f 6e 6e 56 56 3d 74 69 6e 63 72 66 32 00 6b xy-come ction: k eep-aliy eecep 0090 65 65 70 2d 61 6c 69 76 65 0d 0d 41 63 63 65 70 eep-aliy eecep ecep 0080 78 78 78 74 2f 68 74 6d 6c 26 61 77 04 74 74 74 74 74 74 74 74 74 74 74 74 74	Request Method: GET Request URI: http://www.123greetings.com/ Request Version: htTP/1.1 Host: www.123greetings.com/r\n Proxy-Connection: keep-alive\r\n Accept: text/html.application/xhml+xml.application/xml:p=0.9.image/webp.*/%:p=0.8\r\n		
	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	45 00 .!^G fE. coas90s. 50 18	

Enter http.referer contains 123 "simple2" in the Filter Tab



Enter "**http.response.code** == **404**" in the Filter Tab

Capturing from Ethernet [Wireshark 1.10.8 (v1.10.8-2-g52a5244 from master-1.10)]	- • ×
<u>File Edit View Go C</u> apture <u>A</u> nalyze <u>Statistics</u> Telephony <u>I</u> ools <u>I</u> nternals <u>H</u> elp	
● ◎ ∡ ■ △ ⊨ ⊨ % 2 ੧, + + • • 7 ± ⊟ ⊑ 0, 0, 0, 17 ¥ ⊠ 5, % 12	
Filter: http://expression Clear Apply Save	
No. Time Source Destination Protocol Length Info 14243 1020.77753 192.168.10.1 192.168.10.148 HTTP 60 HTTP/1.0 404 Not Found (text/html)	
⊕ Frame 14243: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0	
B Ethernet II, Src: Ibm_47:af:da (00:21:5e:47:af:da), Dst: Dell_09:81:11 (c8:1f:66:09:81:11)	
■ Internet Protocol Version 4, Src: 192.168.10.1 (192.168.10.1), Dst: 192.168.10.148 (192.168.10.148)	
Infansmission control Protocol, SrC Port: nol-ads (s120), DSt Port: 49091 (49091), Seq: 020, ACK: 340, Len: 0 Is passembled Trp segments (625 bytes): #14240(235) #14241(201)	
Hyperset transfer Protocol	
HTTP/1.0 404 Not Found\r\n	
Expert Info (Chat/Sequence): HTTP/1.0 404 Not Found\r\n]	
Request Version: HTTP/1.0	
Status Code: 404	
Response Phrase: Not Found	
Date: Fr1, 07 Nov 2014 06:20:52 GMT/r\n	
Server: Abache/L.3.31 (UD1X) PHP/4.3.9 mon Lavout/3.0.3\r\n 10000 c8 1f 66 09 81 11 00 21 5e 47 af da 08 00 45 00f! ^GE.	
0010 00 28 3d 37 40 00 80 06 27 b3 c0 a8 0a 01 c0 a8 . (=7@ ' 0020 0a 94 0c 38 c2 1b b3 3e b0 0c 98 df bc 3d 50 11	
0030 TE ab 94 8a 00 00 00 00 00 00 00 00	
Emps (60 h day) Descrambled T/D (675 h day)	
Institution and the fore action and the fore action and the fore action and the fore action a	
Ethernet: https://www.capture.in.progress-File Displayed: 1(0.0%)	Profile: Default 11-57 AM

Enter http.content_type == ''image/gif'' in the Filter Tab

Capturing from Ethernet [Wireshark 1.10.8 (v1.10.8	-2-g52a5244 from master-1.10)] 🛛 – 🗇 🗙
<u>Eile Edit View Go Capture Analyze Statistics Telephony Iools Internals H</u> elp	
● ● ◢ ■ ∡ ⊨ ⊨ ≍ ≈ । ੧ + + + + 7 ± ⊟ ⊑ 9 9 9 11 ₩ ⊠ % ₩	
Filter: http:content_type == "image/gif" Expression Clear Apply Save	
No. Time Source Destination Protocol Length Info	~
 □ Frame 14787: 230 bytes on wire (1840 bits), 230 bytes captured (1840 bits) on interface 0 □ Ethernet II, Src: Ibm_47:af:da (00:21:5e:47:af:da), DSt: Dell_09:81:11 (Cslf:66:09:81:11) □ Internet Protocol Version 4, Src: 192.168.10.1 (192.168.10.1), DSt: 192.168.10.148 (192.168 □ Transmission control Protocol, Src Port: ndl-aas (3128), DSt Port: 49692 (49692), Seq: 882, □ [2 Reasembled TCP Segments (Cs2 bytes): #14786(449), #14787(176)] □ HTTP/1.0 200 GK\r\n □ [Expert Info (Chat/Sequence): HTTP/1.0 200 GK\r\n] Request Version: HTTP/1.0 Status Code: 200 Response Phrase: 0K 	.10.148) Ack: 1245, Len: 176
Date: Fri, 07 Nov 2014 06:21:05 GMT/r/n	~
Server: ADACHE/L.S.SI (UNIX) PHP/4.S.9 mod TAVOUT/S.O.S\F\D	
Output Column Column <thcolumn< <="" td=""><td>~</td></thcolumn<>	~

Frame (230 bytes) Reassembled TCP (625 bytes)

● 🛃 Ethernet: live capture in progress> File: C:\... Packets: 19691 · Displayed: 1 (0.0%)

Profile: Default

Practical no: 2

Aim : Using open SSL for web server - browser communication

- Install apache if it is not installed
- Install openssl if it is not installed

Generate the RSA Key

openssl genrsa -des3 -out server.key 2048 [enter a password] [confirm your password]

😣 🗖 🔲 🛛 root@chiya-VirtualBox: /etc/apache2/ssl chiya@chiya-VirtualBox:~\$ openssl genrsa -des3 -out server.key 1024 Generating RSA private key, 1024 bit long modulus . . . + + + + + + + e is 65537 (0x10001) Enter pass phrase for server.key: Verifying - Enter pass phrase for server.key: chiya@chiya-VirtualBox:~\$ openssl req -new -key server.key -out server.csr Enter pass phrase for server.key: You are about to be asked to enter information that will be incorporated into your certificate request. What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank For some fields there will be a default value, If you enter '.', the field will be left blank. Country Name (2 letter code) [AU]:IN State or Province Name (full name) [Some-State]:maha Locality Name (eg, city) []:mum Organization Name (eg, company) [Internet Widgits Pty Ltd]:sies Organizational Unit Name (eg, section) []:sies Common Name (e.g. server FQDN or YOUR name) []:sies Email Address []:sies.mscit2013@gmail.com

Certificate Signing Request (CSR)

openssl req –new -key server.key -out server.csr [enter your private key password] [enter your two character country code] [enter your full state or province name] [enter your city name] [enter your company name] [enter your organizational unit or leave it blank] [enter your common name or fqdn] [enter your admin email address] [leave the rest of the attributes blank]



Sign Your Certificate Signing Request

openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt

[enter your private key password]

```
root@chiya-VirtualBox:~# openssl x509 -req -days 365 -in /etc/apache2/ssl/server
.csr -signkey /etc/apache2/ssl/server.key -out /etc/apache2/ssl/server.crt
Signature ok
subject=/C=IN/ST=maha/L=mum/O=sies/OU=sies/CN=sies/emailAddress=sies.mscit2013@g
mail.com
Getting Private key
Enter pass phrase for /etc/apache2/ssl/server.key:
root@chiya-VirtualBox:~#
```

Remove the PassPhrase From Your Private Key

cp server.key server.key.secure openssl rsa -in server.key.secure -out server.key [enter your private key password]

```
root@chiya-VirtualBox:~
root@chiya-VirtualBox:~# cp /etc/apache2/ssl/server.key /etc/apache2/ssl/server.key.secure
root@chiya-VirtualBox:~# openssl rsa -in /etc/apache2/ssl/server.key.secure -out
/etc/apache2/ssl/server.key
Enter pass phrase for /etc/apache2/ssl/server.key.secure:
writing RSA key
root@chiya-VirtualBox:~#
```

Set file permissions



Configure SSL setting in apache server

- make sure all cryptography files exists in /etc/apache2/ssl
- create sites-available folder in /etc/apache2
- create default-ssl file in path /etc/apache2/sites-available/default-ssl

😣 🖨 🗊 root@chiya-VirtualBox: /etc/apache2/sites-available
chiya@chiya-VirtualBox:~\$ sudo -s [sudo] password for chiya: root@chiya-VirtualBox:~# cd /etc/apache2/ root@chiya-VirtualBox:/etc/apache2# dir apache2.conf envvars mods-available ports.conf sites-enabled conf.d magic mods-enabled sites-available ssl root@chiya-VirtualBox:/etc/apache2# cd ssl root@chiya-VirtualBox:/etc/apache2/ssl# ls server.crt server.csr server.key server.key.secure root@chiya-VirtualBox:/etc/apache2/ssl#
root@chiya-VirtualBox:/etc/apache2/ssl# cd /etc/apache2/sites-available/ root@chiya-VirtualBox:/etc/apache2/sites-available# ls default default-ssl default-ssl~ root@chiya-VirtualBox:/etc/apache2/sites-available# root@chiya-VirtualBox:/etc/apache2/sites-available# gedit /etc/apache2/sites-ava ilable/default-ssl

default-ssl confuration file



open a website hosted inside apache server



now change the protocol to https in the address bar

Mozilla F	irefox			
	(http://127.0.1.1/	Ŧ		
Q	https://127.0.1.1/	,	7	
	Tt			

Apache server has denied the un-identified https connection



View the connection security details

Firefox Web Browser	↑ ↓ ●)) 10:3	1AM 🔱
▶ Page Info - https://127.0.1.1/		
General Media Security	्रि 🕶 🕐 🚷 🕶 Google	۹ 🏠
Website Identity		_
Website: 127.0.1.1		
Owner: This website does not supply ownership information.		
Privacy & History		
Have I visited this website prior to today?	ı permissible length.	
Is this website storing information (cookies) on my computer? No View Cookies		
Have I saved any passwords for this website? No View Saved Passwords	se the authenticity of the	
Technical Details		
Connection Not Encrypted The website 127.0.1.1 does not support encryption for the page you are viewing. Information sent over the Internet without encryption can be seen by other people	is problem. Alternatively, broken site.	
while it is in transit.	J	

Practical no: 3

Aim : <u>Using GNU PGP</u>

Kleopatra



Click on File --> New Certificate or press Ctrl+N

C. Mary Carliforday Taola Catting Minday	Kleopatra	- 0 ×
New Certificate Ctrl+N	edsplay 🐼 Stop Operation 🍂 Lookup Certificates on Server Clipboard	
Lookup Certificates on Server Ctrl+Shift+I Import Certificates Ctrl+I	rticates	My Certificates
Export Certificates Ctrl+E	Valid Until Details Key-ID	
Export Secret Keys Export Certificates to Server Ctrl+Shift+E		
 Decrypt/Verify Files Sign/Encrypt Files 		
Create Checksum Files Verify Checksum Files		
😮 Close Ctrl+W		
Quit Ctrl+Q		
🗧 ⋵ 🚞 횓 🧕	A A R A A A A A A A A A A A A A A A	P 🔛 记 🕕 12:37 PM 11/7/2014

Choose "Create a Personal OpenPGP key Pair" --> Next



Enter the details Name, Email, Comment --> Next

		?	×
© 🙃	Certificate Creation Wizard		
Enter D	etails		
Please ente parameters	er your personal details below. If you want more control over the certi s, click on the Advanced Settings button.	ficate	:
Na <u>m</u> e:	siesmsc	(re	quired)
<u>E</u> Mail:	sies.mscit2013@gmail.com	(re	quired)
<u>C</u> omment:	rac	(op	tional)
	siesmsc (rac) <sies.mscit2013@gmail.com></sies.mscit2013@gmail.com>		
	Advanced	Setti	ngs
	Next	Can	cel.

Select Create Key

				?
	Certificate Creation W	/izard		
Review	/ Certificate Paran	neters		
Please rev	view the certificate param	neters before procee	ding to create the certi	ficate.
Name: Email Ac Commer	siesmsc Idress: sies.mscit2013@gi nt: rac	mail.com		
, <u>S</u> how	all details			
			<u>C</u> reate Key	Cancel
Show	all details		<u>Create Key</u>	Cance

INFORMATION SECURITY

MSc.IT- sem 3 [2014-15]

You will see details of your key

 Certificate Creation Wizard
Review Certificate Parameters Please review the certificate parameters before proceeding to create the certificate.
Name: siesmsc Email Address: sies.mscit2013@gmail.com Comment: rac Key Type: RSA Key Strength: 2,048 bits Certificate Usage: Sign, Encrypt
Cancel

Enter Passphrase(password)

1	pinentry ×					
Enter passphrase						
	Passphrase					
	Quality:	i	.00%			
		<u>O</u> K	<u>C</u> ancel			

Re-enter the password

pinentry				×
	Please re-en Passphrase	ter this pass	phrase <u>C</u> ancel	

Key Pair Successfully Created

Click Finish

? 🗙
📀 👩 Certificate Creation Wizard
Key Pair Successfully Created
Your new key pair was created successfully. Please find details on the result and some suggested next steps below.
Result
Certificate created successfully. Fingerprint: 6F2EF617939A996632B67D4FAAF6B61C0B88D048
Next Steps
Make a Backup Of Your Key Pair
Send Certificate By EMail
Upload Certificate To Directory Service
Einish

You will see Overview of your Certificate in Overview Tab

Kleopatra ?	×
Overview User-IDs & Certifications Technical Details Chain Dump	
This certificate is currently valid. User-ID: siesmsc (rac) <sies.mscit2013@gmail.com> Validity: from 2014-11-07 12:40 until forever Certificate type: 2,048-bit RSA (secret key available) Certificate usage: Signing EMails and Files, Encrypting EMails and Files, Certifying other Certificates Key-ID: 0B88D048 Fingerprint: 6F2EF617939A996632B67D4FAAF6B61C0B88D048 Ownertrust: ultimate Stored: on this computer</sies.mscit2013@gmail.com>	
Photo At the moment, Kleopatra does not support photos in certificates. It has no support for adding, nor for displaying them. This is for the following reasons: Photos give a false sense of security. Photos increase the size of certificates. Actions Change Passphrase Change Expiry Date	
Close 🔯 Help	,

•				Kleopatra	9		?	×
ļ	<u>Overview</u>	<u>U</u> ser-I	Ds & Certifications	Technical Details	Ch <u>a</u> in Dump	1		
	Name		EMail	Valid From	Valid Until	Statu	User-IDs	
	siesms	c (rac) <	sies.mscit2013@g	mail.com>			Certify	
	•					►		
			Load	Certifications (may	take a while)			
						80	jose 🔯	Help

You will see User Id and Certification of your Certificate in User-Ids & Certifications

Click on Technical Details to see subkeys Details

Click on Close

		Kleop	atra			?	×
ſ	Qverview User-IDs & Certification	ns <u>T</u> echnical Det	ails 🛛 🔿	h <u>a</u> in <u>D</u> ump			_
	ID Type Valid	From Valid Until	Status	Strength			
	AAF6B61C0B88D048 RSA 2014-	11-07	good	2048			
					😢 Close	🙋 н	elp

Click on "Export Certificates"

•						Kle	
<u>File View</u> <u>Certificates</u>	<u>T</u> ools <u>S</u> ettin	gs <u>W</u> indow <u>H</u> el	р				
Import Certificates Export Certificates Certificates Certificates Stop Operation							
Search <alt+q></alt+q>	Search <alt+q> Export Certificates</alt+q>						
My Certificates	Trusted Certific	ates Other Certi	ficates				
Name ∇	E-Mail	Valid From	Valid Until	Details	Key-ID		
siesmsc (rac) sie	s.mscit2013	2014-11-07		OpenPGP	0B88D048		

Export the File

	Export Certificat	es			×
€ ⋺ - ↑ 🖡	→ This PC → Desktop →	~ ¢	Search Desktop		Q
Organize 👻 Ne	w folder			•== •	0
☆ Favorites	^ Name		Date modified	Туре	
Desktop	DDJDPCDSZAzaqSZ		10/16/2014 2:01 PM	File folder	
鷆 Downloads	ISM .		11/5/2014 12:33 PM	File folder	
🔚 Recent places	🌗 sam		10/7/2014 12:39 PM	File folder	
	Tor Browser		10/20/2014 12:16	File folder	
💻 This PC					
📔 Desktop					
Documents					
鷆 Downloads					
Music					
📔 Pictures					
📔 Videos	~ <				>
File <u>n</u> ame:	6F2EF617939A996632B67D4FAAF6B61C0B88D04	18			~
Save as <u>t</u> ype:	OpenPGP Certificates (*.asc *.gpg *.pgp)				~
) Hide Folders			<u>S</u> ave	Cancel	

On the Desktop Key Exported





Click Sign & Encrypt(OpenPGP only) radio button --> Next

? ×								
📀 👩 Sign/Encrypt Files								
What do you want to do?								
Please select here whether you want to sign or encrypt files.								
• C:/Users/msclab/Desktop/6F2EF617939A996632B67D4FAAF6B61C0B88D048.asc								
Archive files with: TAR (PGP®-compatible)								
Archive name (OpenPGP): ====617939A996632B67D4==AA==661C0B88D048.asc.tar 🔇								
Archive name (S/MIME): 17939A996632B67D4FAAF6B61C0B88D048.asc.tar.gz 🕢 🔛								
Sign and Encrypt (OpenPGP only)								
C Encrypt								
C Sign								
 Text output (ASCII armor) Remove unencrypted original file when done 								
Next Cancel								

				?	×
🕞 👩 Sign/Encn	/pt Files				
For whom do	ou want to end	crypt?			
Please select for who own certificates.	m you want the files	to be encrypted. Do	not forge	t to pick one	of your
Search		All C	ertificates	s	-
Name 🗸	E-Mail	Valid I	From	Valid Un	til
siesmsc (rac)	sies.mscit2013@gı	mail.com 2014-11	-07		C
•					
<u> </u>	₩ <u>A</u> dd	▲ <u>R</u> emove			
Name ∇	E-Mail	Valid From	Valio	d Until	De
4					
<u> </u>					
			Next	Car	ncel

			? ×
🗧 👩 Sign/Encrypt F	iles		
For whom do you	want to encrypt	2	
Please select for whom yo own certificates.	ou want the files to be en	ncrypted. Do not forge	t to pick one of your
Search		All Certificates	s 💌
Name 🗸	E-Mail	Valid From	Valid Until
-	▼ <u>A</u> dd	▲ <u>R</u> emove	Þ
Name 🗸	E-Mail	Valid From	Valid Until
siesmsc (rac) sies	.mscit2013@gmail.co	om 2014-11-07	C
•		1	

Select file name --> Add --> Next

Check "Remeber this" --> Sign & Encrypt

	?	×
📀 👩 Sign/Encrypt Files		
Who do you want to sign as?		
Please choose an identity with which to sign the data.		
✓ Sign with OpenPGP		
Sign with S/ <u>M</u> IME		
OpenPGP Signing Certificate:		
siesmsc (rac) <sies.mscit2013@gmail.com> (0B88D048)</sies.mscit2013@gmail.com>		-
$\boxed{\mathbf{R}}$ Remember these as default for future operations		
Sign & Encrypt	Cano	cel

Enter Passphrase(Password)

pinentry
Please enter the passphrase to unlock the secret key for the OpenPGP certificate: "siesmsc (rac) <sies.mscit2013@gmail.com>" 2048-bit RSA key, ID 0B88D048, created 2014-11-07.</sies.mscit2013@gmail.com>
Passphrase
<u>OK</u> <u>C</u> ancel

Click FInish

? ×
😑 👩 Sign/Encrypt Files
Results
Status and progress of the crypto operations is shown here.
OpenPGP: All operations completed.
6F2EF617939A996632B67D4FAAF6B61C0B88D048.asc → 6F2EF617939A996632B67D4FAAF6B61C0B88D048.asc.gpg: Signing and encryption succeeded.
, Keep open after operation completed
<u>F</u> inish <u>C</u> ancel

Key will create on Desktop

Right Click on Key-- Decrypt and verify

0526501		Open with
44331616612 415/AVA1616		Decrypt and verify
DEHSIBD.O-	8	More GpgEX options
	0	Quick Heal Internet Security Scan PowerISO
		Share with Add to archive Add to archive Add to "6F2EF617939A996632B67D4FAAF6B61C0B88D048.rar" Compress and email Compress to "6F2EF617939A996632B67D4FAAF6B61C0B88D048.rar" and email
		Send to 🕨
A		Cut Copy
(C		Create shortcut Delete Rename
		Properties
		→ 💽 🏴 🏔 😭 🐠 11248 PM 11/7/2014

INFORMATION SECURITY

MSc.IT- sem 3 [2014-15]

Select file to decrypt --> Decrypt/verify

•	Decrypt/Verify File	es	? ×
Choose operations to be performed Here you can check and, if needed, override the op	erations Kleopatra dete	cted for the input given.	
Input file: C:/Users/msclab/Desktop/6F2EF61	939A996632B67D4FAAF	F6B61C0B88D048.asc	
Signed data: C:/Users/msclab/Desktop/demo.tx	:		🛛 🔛
☐ Input file is <u>a</u> n archive; unpack with: TAR (GP @-compatible)		~
Create all output files in a single folder			
Output folder: C:/Users/msclab/Desktop			🛯 🎴
		Back Decrypt/Verify	Ca <u>n</u> cel

Practical no: 4

Aim : Performance evaluation of various cryptographic algorithms

- Install g++ if not already installed
- Install crpto++ if not already installed

Prog.cpp

```
include <iostream>
#include <iomanip>
```

```
#include "crypto++/modes.h"
#include "crypto++/aes.h"
#include "crypto++/filters.h"
```

```
int main(int argc, char* argv[]) {
```

```
//
```

```
// Key and IV setup
```

```
byte key[ CryptoPP::AES::DEFAULT_KEYLENGTH ], iv[CryptoPP::AES::BLOCKSIZE ];
memset( key, 0x00, CryptoPP::AES::DEFAULT_KEYLENGTH );
memset( iv, 0x00, CryptoPP::AES::BLOCKSIZE );
```

```
//
// String and Sink setup
//
std::string plaintext = "Now is the time for all good men to come to the aide...";
std::string ciphertext;
std::string decryptedtext;
```

```
//
// Dump Plain Text
//
std::cout << "Plain Text (" << plaintext.size() << " bytes)" <<std::endl;
std::cout << plaintext;
std::cout << std::endl << std::endl;
//
// Create Cipher Text
//
CryptoPP::AES::Encryption aesEncryption(key,
CryptoPP::AES::DEFAULT_KEYLENGTH);
CryptoPP::CBC_Mode_ExternalCipher::Encryption cbcEncryption(
aesEncryption, iv );</pre>
```

```
CryptoPP::StreamTransformationFilter
                                                      stfEncryptor(cbcEncryption,
                                                                                               new
CryptoPP::StringSink( ciphertext ) );
  stfEncryptor.Put( reinterpret_cast<const unsigned char*>(
plaintext.c_str() ), plaintext.length() + 1 );
  stfEncryptor.MessageEnd();
  //
  // Dump Cipher Text
  //
  std::cout << "Cipher Text (" << ciphertext.size() << " bytes)" <<std::endl;</pre>
  for( int i = 0; i < ciphertext.size(); i++ ) {</pre>
     std::cout << "0x" << std::hex << (0xFF & static_cast<byte>(ciphertext[i])) << " ";</pre>
  }
  std::cout << std::endl << std::endl;</pre>
  //
  // Decrypt
  //
  CryptoPP::AES::Decryption aesDecryption(key,
CryptoPP::AES::DEFAULT_KEYLENGTH);
  CryptoPP::CBC_Mode_ExternalCipher::Decryption cbcDecryption(
aesDecryption, iv );
  CryptoPP::StreamTransformationFilter
                                                      stfDecryptor(cbcDecryption,
                                                                                               new
CryptoPP::StringSink( decryptedtext ) );
  stfDecryptor.Put( reinterpret_cast<const unsigned char*>(
ciphertext.c str()), ciphertext.size());
  stfDecryptor.MessageEnd();
  //
  // Dump Decrypted Text
  //
  std::cout << "Decrypted Text: " << std::endl;</pre>
  std::cout << decryptedtext;</pre>
  std::cout << std::endl << std::endl;</pre>
  return 0;
}
```

To compile use the following command:

g++ -g3 -ggdb -o0 -Wall -Wextra -unused -o AesOutput aesexample.cpp -lcryptopp

😣 🗐 🗊 chiya@chiya-VirtualBox: -	~			
<pre>chiya@chiya-VirtualBox:~\$ g+ pp -lcryptopp prog.cpp: In function 'int m prog.cpp:48:41: warning: com ons [-Wsign-compare] prog.cpp: At global scope: prog.cpp:8:5: warning: unuse prog.cpp:8:5: warning: unuse chiva@chiva-VirtualBox:~S di</pre>	+ -g3 -ggd ain(int, c parison be d paramete r	b -o0 -Wall har**)': tween signed r 'argc' [-W r 'argv' [-W	-Wextra -unused -o and unsigned integ unused-parameter] unused-parameter]	prog prog.c ger expressi
code.cpp~ Downloads Desktop examples.desktop Documents Music chiya@chiya-VirtualBox:~\$	Pictures prog prog.cpp	prog.cpp~ Public server.crt	server.key server.key.secure Templates	Videos

To execute use the following command

./prog

😣 🗖 🔲 chiya@chiya-VirtualBox: ~

chiya@chiya-VirtualBox:~\$./prog Plain Text (55 bytes) Now is the time for all good men to come to the aide...

Cipher Text (64 bytes)

0x7f 0xf8 0xb3 0xea 0x8a 0x2 0xb3 0x7a 0x3d 0x28 0x66 0x9c 0x97 0x13 0xa7 0xb3 0 xf 0xa2 0x50 0x25 0x80 0xd5 0xd2 0x32 0xce 0xe8 0xa 0x57 0x33 0xef 0x70 0xff 0x4 8 0xe9 0xe8 0x4 0x98 0xa9 0x4 0xc2 0x5e 0xa7 0xb0 0x40 0x43 0xa1 0xfc 0x23 0xb1 0xa1 0xeb 0x1e 0xb2 0xf6 0x97 0x62 0x70 0xa1 0x81 0xca 0x6e 0x78 0x80 0x90

Decrypted Text: Now is the time for all good men to come to the aide...

chiya@chiya-VirtualBox:~\$

Practical No: 5

Aim : Configuring S/MIME for e-mail communication

Some settings to you gmail account

https://mail.google.com/mail/u/0/#settings/fwdandpop

➢ Enable pop



Enable app settings

https://www.google.com/settings/security/lesssecureapps



Configure MS outlook by providing the required credentials

Add New E-mai	il Account
Choose E-r	mail Service
۲	Microsoft Exchange, POP3, IMAP, or HTTP Connect to an e-mail account at your Internet service provider (ISP) or your organization's Microsoft Exchange server.
C	<u>O</u> ther
	Connect to a server type shown below.
	Outlook Mobile Service (Text Messaging)
	< Back Next > Cancel

Add New E-mail Accou	nt	×
Auto Account Setu	IP	×,
Your Name:	MSc IT Example: Barbara Sankovic	
<u>E</u> -mail Address:	sies.mscit2013@gmail.com Example: barbara@contoso.com	
Password:	******	
Retype Password:	*******	
Manually configure	Type the password your Internet service provider has given you.	
	< Back Next > Car	ncel

Choose E-n	nail Service	×
۲	Internet E-mail	
	Connect to your POP, IMAP, or HTTP server to send and receive e-mail messages.	
0	<u>M</u> icrosoft Exchange	
	Connect to Microsoft Exchange for access to your e-mail, calendar, contacts, faxes and voice mail.	
0	<u>O</u> ther	
	Connect to a server type shown below.	
	Outlook Mobile Service (Text Messaging)	
	< <u>B</u> ack <u>N</u> ext > Ca	ancel

Add New E-mail Account		
Internet E-mail Settings Each of these settings ar	e required to get your e-mail accou	unt working.
User Information		Test Account Settings
Your Name:	MSc IT	After filling out the information on this screen, we
E-mail Address:	sies.mscit2013@gmail.com	button below. (Requires network connection)
Server Information		Tech Associate Certificate
Account Type:	POP3	Lest Account Settings
Incoming mail server:	pop.gmail.com	
Outgoing mail server (SMTP):	smtp.gmail.com	
Logon Information		
<u>U</u> ser Name:	sies.mscit2013@gmail.com	
Password:	******	
I E	emember password	
🕅 Reguire logon using Secure	Password Authentication (SPA)	More Settings
		< Back Next > Cancel

More settings

Internet E-mail Settings	x
General Outgoing Server Connection Advanced	
Mail Account	_
Type the name by which you want to refer to this account. For example: "Work" or "Microsoft Mail Server"	
sies.mscit2013@gmail.com	
Other User Information	_
Organization:	
Reply E-mail:	
1	
OK Cance	el 🚽
Internet E-mail Settings	
General Outgoing Server Connection Advanced	1
Server Port Numbers	
Incoming server (POP3): 995 Use Defaults	
Outgoing server (SMTP): 465	
Use the following type of encrypted connection: SSL	
Server Timeouts	
Short - Long 1 minute	
Delivery	
Remove from server after 10 days	
Remove from server when deleted from 'Deleted Items'	
OK Cancel	

INFORMATION SECURITY

Test account settings

Test Account Settings		
Congratulations! All tests completed successfully. Cli	ick Close to continue.	Stop
		Close
Tasks Errors		
Tasks	Status	
✓ Log onto incoming mail server (POP3)	Completed	
✓ Send test e-mail message	Completed	

- Click Next
- Click Finsih.

Open Trust Center



Click on Get a Digital ID.



Open Comodo website

B Digital ID - Windows Internet Explorer		
🖉 🖉 🔹 🚺 https://support.office.com/en-us/article/Digital-ID-b06cfc76-56a1-4a74-b2dd-91a55de79cdf?ui=en-US&rs=en-US&rad=US	🗕 🔄 🗙 O Astromenda	+ م
x Google View Share More >		Sign In 🔌 🕶
👷 Favorites 🛛 🎭 🙋 Suggested Sites 👻 🙋 Web Slice Gallery 🕶		
1 Digital ID	🚹 🕶 🔝 👻 🚍 🖶 🛨 <u>P</u> age 🕶 <u>S</u> a	fety ▼ T <u>o</u> ols ▼ @ ▼ [≫]
		^ ^
	Search 🔎	
Digital ID		
Digital IDs help to validate your identity, and they can be used to sign important documents electronically. To find services that issue digital IDs for your use, or services that complement Office and use digital IDs, check out the services listed here.		
ARX CoSign® Digital Signatures To learn more, download a free trial, and start digitally signing your documents, visit the ARX website.		=
Avoco secure2trust To learn more and purchase secure2trust, visit the Avoco website.		1
ChosenSecurity ® Digital ID To learn more, visit the ChosenSecurity website.		
Comodo To learn more and download the Free Email Certificate, visit the Comodo website.		
GlobalSign To learn more about GlobalSign digital signatures, visit the GlobalSign website.		
My Credential [™] from GeoTrust, Inc. To learn more, visit the GeoTrust website.		
VeriSign To learn more about digital IDs, visit the VeriSign website.		
Visit the Office Store for other services that work with Microsoft Office.		
Applies To: Access 2013, Access 2007, Access 2010, Excel 2013, Excel 2007, Excel 2010, OneNote 2007, OneNote 2010, Outlook 2013, Outlook 2 Project 2007, Project 2010, Publisher 2013, Publisher 2007, Publisher 2010, Visio 2013, Visio 2007, Visio 2010, Word 2013, Word 2007, Word 2011 Standard, Visio Standard 2010, OneNote 2013, PowerPoint 2013, Project Professional 2013, Project Standard 2013, Visio Professional 2013	007, Outlook 2010, PowerPoint 2007, PowerPoint 2010, Project 2007 Standard, Project 2010 Standard, Visio 2007	-
lone	Internet Protected Mode: On	🖓 🔻 🍕 100% 💌



And click "Yes" if Pop up occurs



Clikc on Ok



And click "Yes" if Pop up occurs





GO to your gmail account and open the then click on Install







Certificate × General Details Certification Path Show: <All> -Field ~ Value Valid from 10 November 2014 AM 05:30:00 Valid to 11 November 2015 AM 05:29:59 Subject bhalke.sachin1@gmail.com Ξ authority Key Identifier KeyID=82 af 6c 8c f8 c5 fe 96... 🛐 Subject Key Identifier 65 b1 9f 99 df f0 b4 1b 5b 04 ... 🛐 Enhanced Key Usage Secure Email (1.3.6.1.5.5.7.3.... Netscape Cert Type SMIME (20)

 30
 82
 01
 0a
 02
 82
 01

 ec
 56
 bb
 ac
 2b
 8d
 6a

 fd
 b2
 7b
 ba
 da
 97
 07

 81
 c7
 52
 74
 df
 7f
 de

 ae
 7c
 79
 f3
 4f
 3c
 94

 09
 d2
 ae
 58
 a9
 d4
 4c

 c6
 2a
 32
 a0
 ac
 58
 c3

 26
 cd
 45
 42
 ce
 ae
 52

 f6
 1a
 ff
 c7
 ba
 b9
 ab

 01 00 c2 8b 82 b6 e7 02 ea 86 0c bc f8 56 fa 8c 10 0b a9 9e 9b 6a 5a 41 24 26 55 04 76 2a bf f5 73 74 42 64 59 3e 36 7f 10 b1 1a af 65 44 0b 23 93 ed 32 c4 c8 e9 ab 85 ad 79 55 97 = c9 8a Edit Properties... Copy to File... Learn more about certificate details OK

Click on "Detail" . Then Select "Public key" . Then "Copy to file"

Click next



Click Yes and next

ertificate Export Wizard	3
Export Private Key	
You can choose to export the private key with the certificate.	
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.	
Do you want to export the private key with the certificate?	
Yes, export the private key	
No, do not export the private key	
Learn more about exporting private keys	
	5
< <u>B</u> ack Next > Cancel	

Click Next and Create password

Certificate Export Wizard	-
Password	
To maintain security, you must protect the private key by using a password.	
Type and confirm a password.	
Password:	
Type and confirm password (mandatory):	
••••••	
	1
< Back Next > Cancel	J

Next \rightarrow Then Browse data to store \rightarrow Finish

 \rightarrow Repeat above same step using different gmail account(Reciever)

Now configure that Certificate to your outlook account

Go to Tools \rightarrow Trust center \rightarrow Email Security \rightarrow click on Import /export

Trust Center	
Trust Center Trusted Publishers Add-ins Privacy Options E-mail Security Attachment Handling Automatic Download Macro Security Programmatic Access	Encrypted e-mail
	ОК Сапсе

Browse your Digital Certificate here

Import/Export Digita	al ID
Import existing I Import the Digital I password you enter	Digital ID from a file ID from the file to your computer. You must use the ered while exporting the certificate to this file.
Import <u>F</u> ile:	C:\Users\Jitu\Documents\sa1.pfx
Password:	•••••
Digital ID Name:	sa
 Export your Digital I Export the Digital I this information. 	tal ID to a file ID information into a file. Enter a password to help protect
Digital ID;	<u>S</u> elect
Eilename:	Browse
Passwo <u>r</u> d:	
<u>⊂</u> onfirm:	
<u>Microsoft Inter</u>	net Explorer 4.0 Compatible (low-security)
Delete Digital II	O from system
	OK Cancel

→click "OK"

- → Create new message
- \rightarrow And send to Reciever



Download the attached file(Public key)→open if not directly open(open with "Crypto Shell Extensions")

Google	✓ Q	sdhsawant1@g
Gmail -	Click here to enable desktop notifications for Gmail. Learn more Hide	4 of 156 < >
COMPOSE	🗞 Google Adwords™ - Show up on Google - Official Free Support from Google™. Start Now and Save Up to Rs.5000	v
Inbox (122) Starred Important Sent Mail Drafts More • Search people sdhsawant	(no subject) □ Intox × Sachin Bhalke <sachin.darkhart@gmail.com></sachin.darkhart@gmail.com>	GOOGLE ADWORDS ¹⁴ Show up on Official Free Support fro Google ¹⁴⁷ . Start Now an Up to Re. 5000 Get Your Cloud Togg Start Here to Get Softla in-One, Highly Tuned Cl www.softlayer.com/integ
	Srinath G Social Error Surged from Coople Ads - Unit May and Social Lip to Dr. 5000 Ads - Unit May the 36th France Surged from Coople Ads - Unit	Sanesh am ID ha maam Call mobile +91982096247

🚡 certmgr - [Certificates - Current User]	× V 😫 enable using app in gr × V M (no subject) - sdhsaw: × V II Downloads ×	
File Action View Help		☆ =
	bot/fb_bot.php a	
Certificates - Current User CulusERS.VITU/DOWNLOADS\SMIME (1).P75	1	Î
	Open down	loads folder <u>Clear all</u>
	le8tri	
	78vi	
	1	
	ew=	
< <u> </u>	Σ	
ESOb.pdf http://muresults.net/itacademic/MSc3/Q8/ES.pdf Show in folder Remove from list	-	
smime.p?s https://mail-attachment.googleusercontent.com/attachment/?ui=2&ik=c2de708ea7 Show in folder Remove from list	78criew=	
wisetup-web.exe http://wildisenvice.microsoft.com/download/C/1/B/C18A42D6-6A50-4A4A-90E5-FA9 Show in folder Remove from list	9347£936	
Outlookexpress-setup.exe http://files4.mirror1.info/download/694637/dl?bc=694637&pid=tucows&brand=tuc Show in folder Remove from list	cows.com	
	▲ (()) 😽 😭 🛛 PM 07:16

Click on Certificates

🚡 certmgr - [Certificates - Current U	ser\C:\USERS\JITU\DOWNLOADS\SMIM	ME (1).P7S\Certificat	
<u>File Action View H</u> elp			
🗢 🔿 🙋 🖬 🧟 🗟 ד			
Certificates - Current User	Issued To	Issued By	Ex
C:\USERS\JITU\DOWNLOADS	🔄 AddTrust External CA Root	AddTrust External CA Root	30
Certificates	COMODO RSA Certification Au	AddTrust External CA Root	30
	COMODO RSA Client Authentic	COMODO RSA Certification Auth	10
	sdhsawant1@gmail.com	COMODO RSA Client Authenticat	10
	<		-
C:\USERS\JITU\DOWNLOADS\SMIME	(1).P7S store contains 4 certificates.		

Double click on the" Recievers Public key"(Issued To →email address) Details→Copy to files→Save

Certificate		×
General Details Certification Path]	
Show: <a>	▼	
Field	Value	<u>^</u>
Version Serial number Signature algorithm Signature hash algorithm Sissuer Valid from Valid to Subject	V3 Of f2 15 30 26 77 f4 b9 aa f0 sha256RSA sha256 COMODO RSA Client Authenti 09 November 2014 AM 05:30:00 10 November 2015 AM 05:29:59 sdhsawant1@gmail.com	
Learn more about <u>certificate details</u>	lit Properties	
		к

Now Address book \rightarrow File \rightarrow New Entry \rightarrow

Address Book: Contact:		
File Edit Tools		
Search: Name only	More columns Address Book	✓ Adyanced Find
Name	Display Name	E-mail Address
S bhal S sac S sace	sachin.darkhart@gmail.com sdhsawant@gmail.com sdhsawant1@gmail.com	sachin.darkhart@gm sdhsawant@gmail.co sdhsawant1@gmail.c
•		4

Enter name and	Email	Address((receivers)
----------------	-------	----------	-------------

	÷) ÷	sac - Contac	t	
Contact Ins	ert Format Text			0
Save & New * Save & Send * Close X Delete Actions	General Details	E-mail Meeting Call Communicate	Task ige Business Picture Categorize Follow Card Up Options	ABC Spelling Proofing OneNote
Full Name Company: Job țitle: Filg as: Internet Display as:	sac sac sdhsawant@qmail.com;		sac	
Web page address:		Notes		-
IM address:				
Phone numbers				
Business				
Home				
Business Fax				
Mobile				
Addresses				=
This is the mailing add <u>r</u> ess				
				⇒ s

Click on Certificate→Import Certificate(Recievers Public key)

	9044	÷		sac - Contact	and an extension				- 🗆 <mark>- X</mark> -
	Contact Inser	t Format Text							0
Save & Close	Save & New -	General Details	E-mail Meeting Call	🛃 Assign Task 🔊 Web Page 修 Map	Business Picture C Card	ategorize Follow	😤 Private 🔝 Address Book & Check Names	ABC Spelling	Contact Notes
	Actions	Show	Communio	cate		Options		Proofing	OneNote
Outlood You can <u>C</u> ertifica	c will use one of thes get a certificate by re ttes (Digital IDs):	e certificates to send encrypted mai ecceiving digitally signed mail from th	to this contact. Is contact or by importin	g a certificate file f	or this contact.				Properties Set as <u>D</u> efault Import Export <u>R</u> emove

INFORMATION SECURITY MSc.I

Locate Certificate		Contraction of the local division of the loc	X
		🗸 🍕 Search sa	٩
Organize 🔻 New	folder	8≡ ▼ 🗍	0
😡 Microsoft Offic	Name	Date modified Type	S
	MACOSX	05-11-2010 AM 10 File folder	
🚖 Favorites	<u>]]</u> 2	31-07-2014 PM 08: File folder	
📃 Desktop	12	21-09-2014 AM 04 File folder	
🐌 Downloads 🗏	🌗 cssmenu	29-07-2014 AM 04 File folder	
📃 Recent Place	퉬 key	10-11-2014 AM 02 File folder	
	🌗 logowebsite	20-09-2014 PM 10: File folder	
🥃 Libraries	🌗 New folder	31-07-2014 PM 08: File folder	
Documents	🌗 sexyddmenu-source	06-10-2011 PM 09: File folder	
J Music	🌗 templates websites	01-10-2014 PM 04: File folder	
📔 Pictures	🛱 123	10-11-2014 AM 03 Security Certif	icate
📑 Videos			
🖳 Computer 🔍 🔻	•	III	÷.
F	File <u>n</u> ame: 123	✓ Digital ID Files Too <u>l</u> s ✓ Open ✓ Canc	• el

Click "Ok"

Then Create New message \rightarrow select "To" \rightarrow Select contact name \rightarrow Enable on" Sign " and "Encrypt" \rightarrow send

📭 🖬 🤊 🗠 🕹	. *) ₹	-	-	sd - Message (H	TML)			_ 0 <mark>_</mark> ×
Message	Insert Options	Format Text						
Paste S Format Pair Clipboard		▲ A [*] A [*] H = T H = T A [*] 2 • <u>A</u> • E = E = F = F = F = F = F = F = F = F =	Address Check Book Names	ach Attach Business Calenda le Item Card • Include	r Signature	Permission ~ High Importance	ABC Spelling Proofing	
This message will be se	ent via sies.mscit2013@	gmail.com.						
То	sdhsawant@gmail.c	<u>:om;</u>					\sim	
<u>S</u> end <u>C</u> c								
Account - Subject:	sd							
sdfsd								

Practical No: 6

Aim : Understanding buffer overflow & format string attacks

- make sure u have gedit or equivalent text editer
- Use gedit file.c to create the code file •

Source code

{

}

#include <stdio.h> #include <string.h> #include <stlib.h>

```
int main (int argc, char **argv)
       char buf [100]
       int x = 1
       snprintf ( buf, size of buf, argv [1] );
       buf [ size of buf -1 ] = 0
       printf ( "Buffer size is: (%d) \nData input: %s \n", strlen (buf), buf);
       printf ("X equals: %d/ in hex: %\#x\nMemory address for x: (%p) \n", x, x,&x);
       return 0;
```

Compile using the following command

gcc fileName.c -o fileName

This is format string vulnerability. If the format string parameter "%x %x" is inserted in the input string, when the format function parses the argument, the

output will display the name Bob, but instead of showing the %x string, the application will show the contents of a memory address.

```
🔰 ubuntu@ubuntu: ~
       fer size is: (5)
input: value
juals: 1/ in hex: 0x1
bry address for x: (0xbfcca1f4)
buntu@ubuntu:~$
buntu@ubuntu:~$
buntu@ubuntu:~$
uffer size is: (17)
ata input: b7695269 bfee52cf
equals: 1/ in hex: 0x1
emory address for x: (0xbfee52a4)
buntu@ubuntu:~$
          .
u@ubuntu:
```

Source code

```
#include <stdio.h>
#include <string.h>
int main(void)
       char buff[15];
       int pass = 0;
       printf("\n Enter the password : \n");
       gets(buff);
       if(strcmp(buff, "thegeekstuff"))
       {
               printf ("\n Wrong Password \n");
       }
       else
       {
               printf ("\n Correct Password \n");
               pass = 1;
       if(pass)
/* Now Give root or admin rights to user*/
               printf ("\n Root privileges given to the user \n");
       }
       return 0;
}
```

Compile using the following command

gcc fileName.c -o fileName

There is a logic behind the output above. What attacker did was, he/she supplied an input of length greater than what buffer can hold and at a particular length of input the buffer overflow so took place that it overwrote the memory of integer 'pass'. So despite of a wrong password, the value of 'pass' became non zero and hence root privileges were granted to an attacker.

Selection States and Selection States and Selection States and Selection States and Selection Selection States and Selection Selecti

1

enter pwd abcd rightroot priv given to uubuntu@ubuntu:~\$ ubuntu@ubuntu:~\$./buff

INFORMATION SECURITY MSc.IT

MSc.IT- sem 3 [2014-15]

Practical No: 7

Aim : <u>Using Nmap/Zenmap</u>

Open Nmap Target --> **''localhost''** Select **''Scan''** --> Select Profile **''Intense Scan''**



Select Host Tab

 Zenmap 				-	-	of Females Suffrage Suffrage		l	- 0	X
Sc <u>an T</u> ools <u>P</u> rofile <u>H</u> el	p									
Target: localhost					▼ Profile	: Intense scan		-	Scan	Cancel
Command: nmap -T4 -A	-v localhost									
Hosts Services	Nman Out	out Ports / I	Hosts Topology Host Detai	ails Scans						
	4 Port	Protocol	State Senvice	1 Version						4 .
OS Host	• 1	tcp	unknown tcpmux	resion						
Incamost (127.0.0.1)	• 3	tcp	unknown compressnet							i
	• 4	tcp	unknown unknown							
	6	tcp	unknown unknown							
	• 7	tcp	unknown echo							
	9	tcp	unknown discard							
	• 13	tcp	unknown daytime							
	• 17	tcp	unknown gotd							
	• 19	tcp	unknown chargen							
	• 20	tcp	unknown ftp-data							
	• 21	tcp	unknown ftp							
	• 22	tcp	unknown ssh							
	• 23	tcp	unknown telnet							
	• 24	tcp	unknown priv-mail							
	• 25	tcp	unknown smtp							
	9 26	tcp	unknown rsftp							
	9 30	tcp	unknown unknown							
	9 32	tcp	unknown unknown							
	9 33	tcp	unknown dsp							
	9 37	tcp	unknown time							
	• 42	tcp	unknown nameserver							
	e 43	tcp	unknown whois							
	🔴 49	tcp	unknown tacacs							
< III >	53	tcp	unknown domain							_
Filter Hosts										Ŧ

INFORMATION SECURITY

MSc.IT- sem 3 [2014-15]

Open Topology Tab

🔹 Zenmap		Annual Manual New Yorks States Name	
Scan <u>T</u> ools <u>P</u> rofile <u>H</u> el	2		
Target: localhost		Profile: Intense scan	▼ Scan Cancel
Command: nmap -T4 -A -	v localhost		
Hosts Services	Nmap Output Ports / Hosts Topology Host Details Scans		
OS 4 Host A	Hosts Viewer Fisheye Controls		Save Graphic
		Connect (127 do 1)	
Filter Hosts			

Open Host Details

 Zenmap 			and Property in the Association Property lies of the Association P		- 0	×
Sc <u>an T</u> ools <u>P</u> rofile <u>H</u> elp						
Target: localhost		▼ Profi	e: Intense scan	•	Scan	Cancel
Command: nmap -T4 -A -v	localhost					
Hosts Services	Nmap Output Ports / Hosts Topology Host Details Scans					
OS 4 Host A Iocalhost (127.0.0.1	[localhost (127.0.0.1) [Host Status					
	Open ports: 0					
	Closed ports: 0 Scanned ports: 1000					
	Up time: Not available Last boot: Not available					
	□ Addresses IPv4: 127.0.0.1 IPv6: Not available					
	MAC: Not available					
	Hostnames					
	Name - Type: localhost - PTR					
Filter Hosts						

Target --> "google.com"

Select "Scan" --> Select Profile "Intense Scan"

Select Host Tab --> Nmap Output



Go to Ports/Hosts tab

👁 Zenmap		states - The state of some rest at a family	
Sc <u>an T</u> ools <u>P</u> rofile <u>H</u> el	lp		
Target: google.com		Profile: Intense scan	▼ Scan Cancel
Command: nmap -T4 -A -	-v google.com		
Hosts Services	Nmap Output Ports / Hosts Topology Host Details	Scans	
OS 4 Hart	Port Protocol State Service	 Version 	•
(1) google.com (74.12)	😑 80 tcp open http	Google httpd 2.0 (GFE)	
M localhost (127.0.0.1	🔵 443 tcp open http	Google httpd 2.0 (GFE)	
<			
Filter Hosts			

Go to Host Viewer

Go		to	General				
∞ Hosts Viewer		and the first sector with					
Hosts	General Services	Traceroute					
localhost (127.0.0.1)	General information						
	Address:	[ipv4] 74.125.296.100	•				
	Hostname:	[user] google.com	•				
	Operating System	stem					
	Used ports:	80/tcp open	•				
	Match Cla	uss Fingerprint					
	% • Nam	e 4 DB Line	•				
	100 Linu:	(2018 - 2022 - 0					
<►	Sequences						

	General Se	rvices Trav	eroute				
e.com (74.125.236.1	General Se		lerodic			-	
ost (127.0.0.1)	Ports (2)	Extraports (998) Special	fields			
	Port	Protocol	State 4	Service 4	Method	_	
	B 80	tcp	open	http	probed		
	80	state	reason_ip				
	80	state	state	open			
	80	state	reason				
	80	state	reason_ttl				
	80	service	product	Google httpd			
	80	service	name	http			
	80	service	extrainfo	GFE			
	80	service	version	2.0			
	80	service	conf	10			
	80	service	method	probed			
	= 443	tcp	open	http	probed		
	443	3 state	reason_ip				
	443	3 state	state	open			
	443	3 state	reason				
	44	3 state	reason_ttl				
	44	3 service	product	Google httpd			
	443	3 service	name	http			
	443	3 service	extrainfo	GFE			
	443	3 service	version	2.0			
	443	3 service	conf	10			
	443	3 service	method	probed			

Go to Service

Go	То	Traceroute		
	* (* * * * * * * * * * * * * * * * * *			
Hosts google.com (74.125.236.1 localhost (127.0.0.1)	General Services Traceroute TTL RTT IP Hostname 1 2.00 74.125.236.100 bom03s01-in-f4.1e100.net			
Image: Image	Traceroute on port 443/tcp totalized 1 known hops.			

Go to Zenmap --> Select "Hosts"

INFORMATION SECURITY MSc.IT- sem 3 [2014-15]



Select Host Details

🗢 Zenmap	and a second	
Sc <u>an T</u> ools <u>P</u> rofile <u>H</u> elp	p	
Target: google.com	Profile: Intense scan	▼ Scan Cancel
Command: nmap -T4 -A -v	v google.com	
Hosts Services	Nmap Output Ports / Hosts Topology Host Details Scans	
OS 4 Host	G google.com (74125.226.100)	A
V locelhost (127.0.0.1	Not status State: up Open ports: 2 Filtered ports: 998 Closed ports: 0 Scanned ports: 1000 Up time: Not available Last boot: Not available PAvi: 74125266.00 IPv6: Not available MAC: Not available Name - Type: google.com - user Name - Type: bom03:001-in-f41.Le100.net - PTR	E
	Comparing System Name: Linux 2.6.18 - 2.6.22 Linux 2.6.18 - 2.6.22 Comparing the second seco	
< Ⅲ ► Filter Hosts	general purpose Linux Linux 2.6.X	

Target "scanme.nmap.org" --> Profile Intense Scan

 Zenmap 	And the first th		×	
Scan <u>T</u> ools <u>P</u> rofile <u>H</u> e	ip			
Target: sacnme.nmap.or	Profile: Intense scan -	Scan	Cance	j
Command: nmap -T4 -A	-v sacnme.nmap.org			
Hosts Services	Nmap Output Ports / Hosts Topology Host Details Scans			
OS 4 Host	nmap -T4 -A -v sacnme.nmap.org	-	Details	;]
 google.com (74.12! localhost (127.0.0.1) 	Consider submitting a service fingerprint. _Rum withscript-args http-server-header.skip http.ttp.(/ Pawision 33700 /)		*	
3 sacnme.nmap.org (<pre>[</pre>			
	Amerissive OS messes: Linux 2.6.18 (93%), Linux 2.6.18 - 2.6.22 (98%), Linux 2.6.15 - 2.6.26 (Likely embedded) (97%), Linux 3.2 - 3.6 (87%), Linux 3.5 (87 Netgear ReadyNAS Duo NMS device (RAIDiator 4.1.4) (87%), Linux 2.6.32 - 2.6.39 (86%), Linux 3.2.0 (85%), Vyatta router (Linux 2.6.26) (85%), Linux 2.6.28 (No exact OS matches for host (test conditions non-ideal). Uptime muess: 0.841 days (since Sat Nov 00 12:09:20 2014) Network Distance: 15 host (fully=256 (Good Luck!) <u>TP ID Sequence Generation</u> ; All zeros	6), 35%)		
	TRACEROUTE (using port 113/tcp) HOP RT ADDR55 1 1.00 ms 122.169.0.254 2 17.00 ms segment-110:226.51fy.net (119.226.13.193) 3 17.00 ms 221-134-204-217.sify.net (221.134.204.217) 4, 6			
	7 35.00 ms segment-124-7.sify.net (124.7.237.85) 8 77.00 ms 61.8.59.9 9 100.00 ms be2.wr2.sin0.asianetcom.net (61.14.157.185) 1011			
	12 238.00 % 109651.00053.7%1.016.0%1 (5.48.102.133) 12 735.00 % 1096551.00053.7%1.016.0%1 (6.48.105.22.13) 14 735.00 % 10965673.7%1.10006.0%0 (6.54.04.105.22.13) 15 282.00 % map.org (173.255.243.189)		ш	
	N <u>SE:</u> Script Post-scanning. Initiating NSE at 13:08 Completed NSE at 13:08, 0.00s elapsed <u>Read data files from:</u> C:\Program Files (x86)\Nmap			
4 III >	US and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ . <u>Nmap done:</u> 1 IP address (1 host up) scanned in 365.00 seconds Raw packets ser: 3138 (142.562KB) Rcvd: 102 (5.574KB)			
Filter Hosts			-	

Select Host --> Select Topology



Practical No: 8

Aim : Socket Programming

Socket program Client class

```
import java.io.DataInputStream;
import java.io.DataOutputStream;
import java.io.IOException;
import java.io.InputStream;
import java.io.OutputStream;
import java.net.Socket;
public class GreetingClient {
       public static void main(String[] args) {
              String serverName = args[0];
              int port = Integer.parseInt(args[1]);
              try
              {
                      System.out.println("Connecting to " + serverName + " on port "
                                    + port);
                      Socket client = new Socket(serverName, port);
                      System.out.println("Just connected to "
                                    + client.getRemoteSocketAddress());
                      OutputStream outToServer = client.getOutputStream();
                      DataOutputStream out = new DataOutputStream(outToServer);
                     out.writeUTF("Hello from " + client.getLocalSocketAddress());
                      InputStream inFromServer = client.getInputStream();
                      DataInputStream in = new DataInputStream(inFromServer);
                      System.out.println("Server says " + in.readUTF());
                      client.close();
              }
                      catch (IOException e)
                      e.printStackTrace();
              }
       }
}
```

Socket program Server class

import java.io.DataInputStream; import java.io.DataOutputStream; import java.io.IOException; import java.net.ServerSocket; import java.net.Socket; import java.net.SocketTimeoutException;

```
INFORMATION SECURITY
```

MSc.IT- sem 3 [2014-15]

```
public class GreetingServer extends Thread {
       private final ServerSocket serverSocket;
       public GreetingServer(int port) throws IOException {
              serverSocket = new ServerSocket(port);
              serverSocket.setSoTimeout(10000);
       }
       @Override
       public void run() {
              while (true) {
                      try {
                             System.out.println("Waiting for client on port "
                                            + serverSocket.getLocalPort() + "...");
                             Socket server = serverSocket.accept();
                             System.out.println("Just connected to "
                                            + server.getRemoteSocketAddress());
                             DataInputStream in = new DataInputStream(
                                            server.getInputStream());
                             System.out.println(in.readUTF());
                             DataOutputStream out = new DataOutputStream(
                                            server.getOutputStream());
                             out.writeUTF("Thank you for connecting to "
                                            + server.getLocalSocketAddress() + "\nGoodbye!");
                             server.close();
                      } catch (SocketTimeoutException s) {
                             System.out.println("Socket timed out!");
                             break;
                      } catch (IOException e) {
                             e.printStackTrace();
                             break;
                      }
               }
       }
       public static void main(String[] args) {
              int port = Integer.parseInt(args[0]);
              try {
                      Thread t = new GreetingServer(port);
                      t.start();
               } catch (IOException e) {
                      e.printStackTrace();
       }
}
```

Run at command prompt

Java GreetingServer 6066



Java GreetingClient localhost 6066

