International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-6, Issue-8)

Research Article | **August 2017**

Forensic Analysis of Asterisk-FreePBX based VoIP Server

Hardik Tandel, Parag H. Rughani, Ph. D.*
IFS, Gujarat Forensic Sciences University,
Gujarat, India

Abstract—

VoIP – Voice over IP is becoming an important aspect of communication. With invention of high speed Internet together with mobile phones has made it possible to utilize this highly important technology for voice communication. International calls are now possible with VoIP at compatible rates compared to past. The trend made people develop applications based on VoIP not only for private IP PBX but for subscribed users from all over the world. The dependency in whole technology is its VoIP Server, which is not directly exposed to end users, but if can be compromsed then can affect all the connected users. Looking at increasing popularity of VoIP, attackers are now targeting these VoIP servers for various purposes like stealing information or using service to make free calls. It is always difficult to prevent such attacks but investigation may always help in solving such attacks and preventing future attacks with similar modus operandi. These work focuses on forensic analysis of VoIP server asterisk and discusses important artifacts which can be retrieved from affected VoIP server.

Keywords— VoIP Forensics, Asterisk Forensics, FreePBX Forensics, Asterisk Analysis, VoIP Analysis, VoIP Attacks, VoIP related crimes

I. INTRODUCTION

VoIP is a revolutionary word that has changed ways of communication. It is one of the most crucial invention Internet users are utilizing but are least aware about it. People are enjoying VoIP calling but are not technically aware about change it has brought in the communication industry. Some of the interesting findings show interesting facts. It has been observed that companies switching to VoIP save between 50 to 70 percent [1], Unified Communications saves around 115 minutes a day per employee [2], the market of Global VoIP Services to Surge from USD 83 Billion in 2015 to USD 140 Billion by 2021 [3], telecoms are losing an average of 700,000 landline customers per month [4], By 2018, 42 percent of firms will send 100 percent of their traffic over SIP trunks [5], and much more [6].

The VoIP is certainly a very useful medium of communication but is it secure enough to communicate and store personal information? The answer is of course a subjective statement and it would vary based on the security implementation. However, it has been observed in most of the cases that companies implementing VoIP do not customize default solutions and do not emphasize on security. Main reason could be lack of awareness about possibilities of cyber attacks on this technology. Nevertheless, this is also not an untouched area and attacks have already been observed on VoIP setups.

Researchers have already warned about increasing attacks on VoIP [7][8], some of the authors have found and explored common vulnerabilities in VoIP environment [9]. This is one of the expected things which happen in the cyber world, as soon as new technology become popular, attackers start targeting it. Due to lack of awareness and security experts it is difficult to stop the attacks on VoIP environment. But, proper investigation is required to make sure criminals are punished. As the technology is emerging, very few forensic investigators are well versed in handling cases related to VoIP. The work mentioned in this paper is carried out to assist such forensic investigators in solving VoIP related crimes.

II. RELATED WORK

As being an old concept, sufficient research is done on VoIP technology, security and forensics. Some of the relevant articles are cited here. Some researchers worked on VoIP client [10], while some researchers focused on VoIP networks [11][12], some focused on attack patterns [13][14], while some emphasized on forensics aspects [15][16]. However, different researchers worked on enhancing security and forensics practice for VoIP attacks, there is still much to do in this field. This article is based on forensic analysis of Asterisk and FreePBX to make forensic investigators understand important artifacts, which can be retrieved from a VoIP environment.

III. EXPERIMENT

This section discusses experiment carried out to achieve objective. Asterisk server is selected at the core for setting up VoIP environment. The reasons behind selecting asterisk server are its openness, power and popularity [17]. The server as being open source allows all sorts of customization in setting up private IP PBX in any enterprise [18]. Front end is required to manage asterisk server which comes as a module with asterisk is FreePBX[19]. The solution offered by asterisk with FreePBX can allow any small to large organization to setup a low cost private IP PBX with minimum inputs. FreePBX provides a reach and user friendly GUI to asterisk, which makes it easy for administrators to configure VoIP Server as per the requirement[21].

After setting up the server, various users had been created to see real time communication. Soft Phone Zoiper [22] was used as a client. Calls were made to different extensions to create log entries at server. A custom shell script to use tcpdump[23] for capturing packets was written and same was used for network traffic interception. After sufficient entries, Forensic Falcon disk imager [24] was used to create image of the Server Hard Disk having Asterisk. EnCase Forensic [25] was used to analyze image and understand important artifacts from the disk. Observations are discussed in following section.

IV. RESULTS

Crucial artifacts were found while analyzing hard disk dump using encase. Some of the important artifacts are mentioned below:

A. List of users [Extensions and Passwords] were retrieved from the dump.

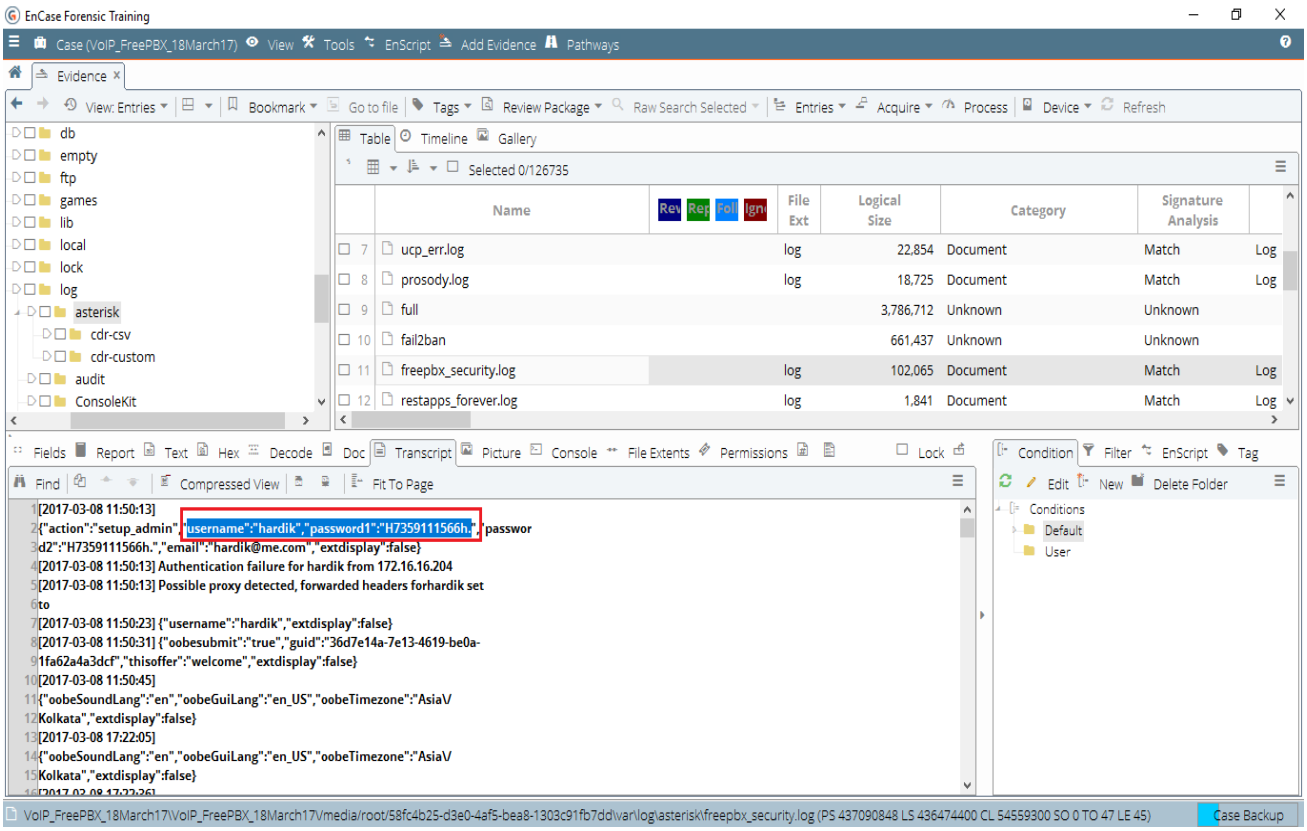
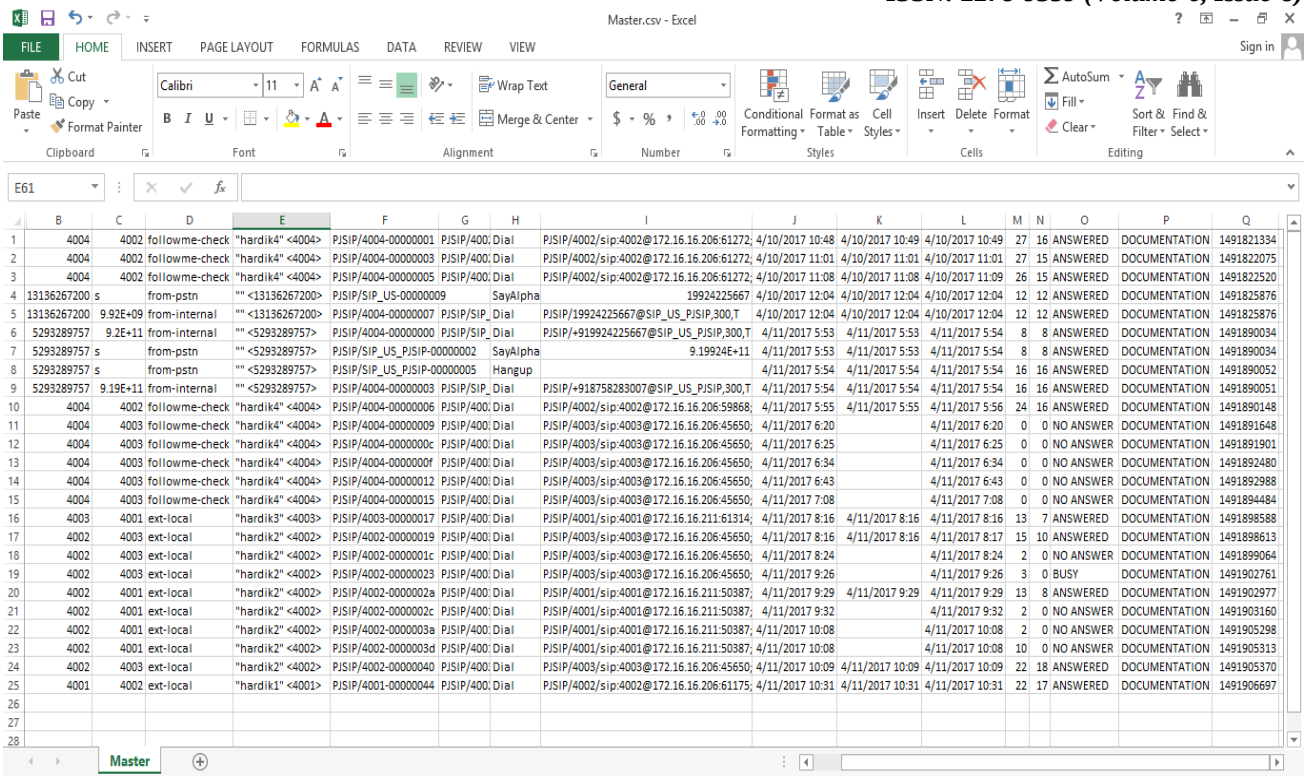


Fig. 4.1 Users and Passwords

Above detail is very useful in getting basic idea about various users who had been created to access the asterisk server. Apart from username and password it also shows email ID and other account related details. However, only user detail is not sufficient in investigating a case. There is need to identify calls related details. CDR details plays a crucial role in investigating a crime, fortunately we could find following details related to calls made using asterisk.

B. CDR Details were recovered from a comma separated file called Master.csv located on /var/log/asterisk/cdr-csv as shown below:

The detail shown in above figure gives a complete insight about calls made using asterisk server. The csv file includes majority of critical information including username, extension, duration of the call, status of the call and much more.



	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	4004	4002	followme-check	"hardik4" <4004>	PJSIP/4004-00000001	PJSIP/400	Dial	PJSIP/4002/sip:4002@172.16.16.206:61272;	4/10/2017 10:48	4/10/2017 10:49	4/10/2017 10:49	27	16	ANSWERED	DOCUMENTATION	1491821334
2	4004	4002	followme-check	"hardik4" <4004>	PJSIP/4004-00000003	PJSIP/400	Dial	PJSIP/4002/sip:4002@172.16.16.206:61272;	4/10/2017 11:01	4/10/2017 11:01	4/10/2017 11:01	27	15	ANSWERED	DOCUMENTATION	1491822075
3	4004	4002	followme-check	"hardik4" <4004>	PJSIP/4004-00000005	PJSIP/400	Dial	PJSIP/4002/sip:4002@172.16.16.206:61272;	4/10/2017 11:08	4/10/2017 11:08	4/10/2017 11:09	26	15	ANSWERED	DOCUMENTATION	1491822520
4	13136267200	s	from-pstn	"" <13136267200>	PJSIP/SIP_US-00000009		SayAlpha	19924225667	4/10/2017 12:04	4/10/2017 12:04	4/10/2017 12:04	12	12	ANSWERED	DOCUMENTATION	1491825876
5	13136267200	9.92E+09	from-internal	"" <13136267200>	PJSIP/4004-00000007	PJSIP/SIP_	Dial	PJSIP/19924225667@SIP_US_PJSIP,300,T	4/10/2017 12:04	4/10/2017 12:04	4/10/2017 12:04	12	12	ANSWERED	DOCUMENTATION	1491825876
6	5293289757	9.2E+11	from-internal	"" <5293289757>	PJSIP/4004-00000000	PJSIP/SIP_	Dial	PJSIP/+919924225667@SIP_US_PJSIP,300,T	4/11/2017 5:53	4/11/2017 5:53	4/11/2017 5:54	8	8	ANSWERED	DOCUMENTATION	1491890034
7	5293289757	s	from-pstn	"" <5293289757>	PJSIP/SIP_US_PJSIP-00000002		SayAlpha	9.19924E+11	4/11/2017 5:53	4/11/2017 5:53	4/11/2017 5:54	8	8	ANSWERED	DOCUMENTATION	1491890034
8	5293289757	s	from-pstn	"" <5293289757>	PJSIP/SIP_US_PJSIP-00000005		Hangup		4/11/2017 5:54	4/11/2017 5:54	4/11/2017 5:54	16	16	ANSWERED	DOCUMENTATION	1491890052
9	5293289757	9.19E+11	from-internal	"" <5293289757>	PJSIP/4004-00000003	PJSIP/SIP_	Dial	PJSIP/+918758283007@SIP_US_PJSIP,300,T	4/11/2017 5:54	4/11/2017 5:54	4/11/2017 5:54	16	16	ANSWERED	DOCUMENTATION	1491890051
10	4004	4002	followme-check	"hardik4" <4004>	PJSIP/4004-00000006	PJSIP/400	Dial	PJSIP/4002/sip:4002@172.16.16.206:59868;	4/11/2017 5:55	4/11/2017 5:55	4/11/2017 5:56	24	16	ANSWERED	DOCUMENTATION	1491890148
11	4004	4003	followme-check	"hardik4" <4004>	PJSIP/4004-00000009	PJSIP/400	Dial	PJSIP/4003/sip:4003@172.16.16.206:45650;	4/11/2017 6:20		4/11/2017 6:20	0	0	NO ANSWER	DOCUMENTATION	1491891648
12	4004	4003	followme-check	"hardik4" <4004>	PJSIP/4004-0000000c	PJSIP/400	Dial	PJSIP/4003/sip:4003@172.16.16.206:45650;	4/11/2017 6:25		4/11/2017 6:25	0	0	NO ANSWER	DOCUMENTATION	1491891901
13	4004	4003	followme-check	"hardik4" <4004>	PJSIP/4004-0000000f	PJSIP/400	Dial	PJSIP/4003/sip:4003@172.16.16.206:45650;	4/11/2017 6:34		4/11/2017 6:34	0	0	NO ANSWER	DOCUMENTATION	1491892480
14	4004	4003	followme-check	"hardik4" <4004>	PJSIP/4004-00000012	PJSIP/400	Dial	PJSIP/4003/sip:4003@172.16.16.206:45650;	4/11/2017 6:43		4/11/2017 6:43	0	0	NO ANSWER	DOCUMENTATION	1491892988
15	4004	4003	followme-check	"hardik4" <4004>	PJSIP/4004-00000015	PJSIP/400	Dial	PJSIP/4003/sip:4003@172.16.16.206:45650;	4/11/2017 7:08		4/11/2017 7:08	0	0	NO ANSWER	DOCUMENTATION	1491894484
16	4003	4001	ext-local	"hardik3" <4003>	PJSIP/4003-00000017	PJSIP/400	Dial	PJSIP/4001/sip:4001@172.16.16.211:61314;	4/11/2017 8:16	4/11/2017 8:16	4/11/2017 8:16	13	7	ANSWERED	DOCUMENTATION	1491898588
17	4002	4003	ext-local	"hardik2" <4002>	PJSIP/4002-00000019	PJSIP/400	Dial	PJSIP/4003/sip:4003@172.16.16.206:45650;	4/11/2017 8:16	4/11/2017 8:16	4/11/2017 8:17	15	10	ANSWERED	DOCUMENTATION	1491898613
18	4002	4003	ext-local	"hardik2" <4002>	PJSIP/4002-0000001c	PJSIP/400	Dial	PJSIP/4003/sip:4003@172.16.16.206:45650;	4/11/2017 8:24		4/11/2017 8:24	2	0	NO ANSWER	DOCUMENTATION	1491899064
19	4002	4003	ext-local	"hardik2" <4002>	PJSIP/4002-00000023	PJSIP/400	Dial	PJSIP/4003/sip:4003@172.16.16.206:45650;	4/11/2017 9:26		4/11/2017 9:26	3	0	BUSY	DOCUMENTATION	1491902761
20	4002	4001	ext-local	"hardik2" <4002>	PJSIP/4002-0000002a	PJSIP/400	Dial	PJSIP/4001/sip:4001@172.16.16.211:50387;	4/11/2017 9:29	4/11/2017 9:29	4/11/2017 9:29	13	8	ANSWERED	DOCUMENTATION	1491902977
21	4002	4001	ext-local	"hardik2" <4002>	PJSIP/4002-0000002c	PJSIP/400	Dial	PJSIP/4001/sip:4001@172.16.16.211:50387;	4/11/2017 9:32		4/11/2017 9:32	2	0	NO ANSWER	DOCUMENTATION	1491903160
22	4002	4001	ext-local	"hardik2" <4002>	PJSIP/4002-0000003a	PJSIP/400	Dial	PJSIP/4001/sip:4001@172.16.16.211:50387;	4/11/2017 10:08		4/11/2017 10:08	2	0	NO ANSWER	DOCUMENTATION	1491905298
23	4002	4001	ext-local	"hardik2" <4002>	PJSIP/4002-0000003d	PJSIP/400	Dial	PJSIP/4001/sip:4001@172.16.16.211:50387;	4/11/2017 10:08		4/11/2017 10:08	10	0	NO ANSWER	DOCUMENTATION	1491905313
24	4002	4003	ext-local	"hardik2" <4002>	PJSIP/4002-00000040	PJSIP/400	Dial	PJSIP/4003/sip:4003@172.16.16.206:45650;	4/11/2017 10:09	4/11/2017 10:09	4/11/2017 10:09	22	18	ANSWERED	DOCUMENTATION	1491905370
25	4001	4002	ext-local	"hardik1" <4001>	PJSIP/4001-00000044	PJSIP/400	Dial	PJSIP/4002/sip:4002@172.16.16.206:61175;	4/11/2017 10:31	4/11/2017 10:31	4/11/2017 10:31	22	17	ANSWERED	DOCUMENTATION	1491906697
26																
27																
28																

Fig. 4.2 CDR Details

After getting call details, it is required to understand and learn about the VoIP client and content of the call. As mentioned earlier a custom shell script based on tcpdump was created to intercept packets from asterisk server. Packets captured using this script was analyzed using wireshark and it was possible for us to find out client details and listen the communication carried out by user through asterisk based VoIP.

C. VoIP Client detail was retrieved from the captured packet. The analysis was done using wireshark as shown below. As mentioned earlier zoiper was used to make the calls. Detailed analysis of the packet allowed us to find out IP address from where the call was made, related time stamps and client details as shown in following figure.

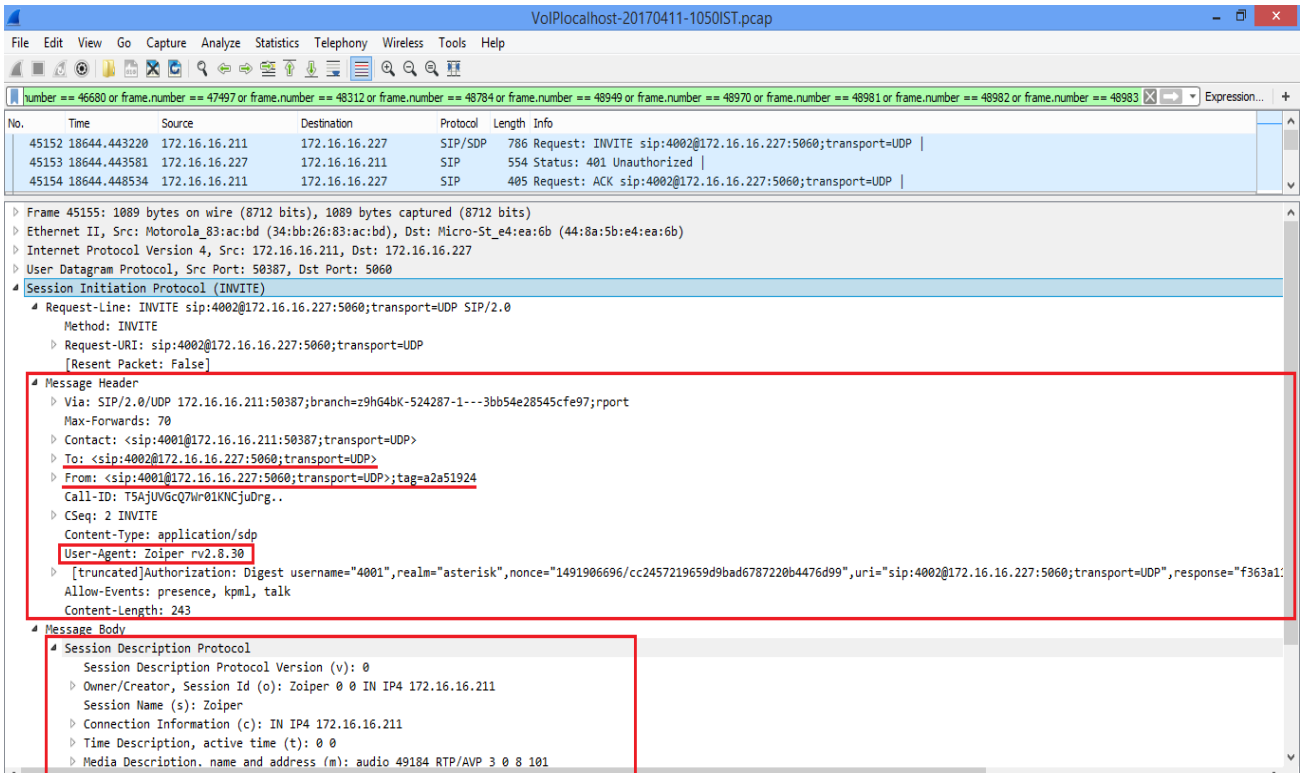


Fig. 4.3 VoIP Client Details

D. After getting VoIP client details, we focused on finding out voice data communicated over VoIP. The captured packets helped in achieving this as shown below.

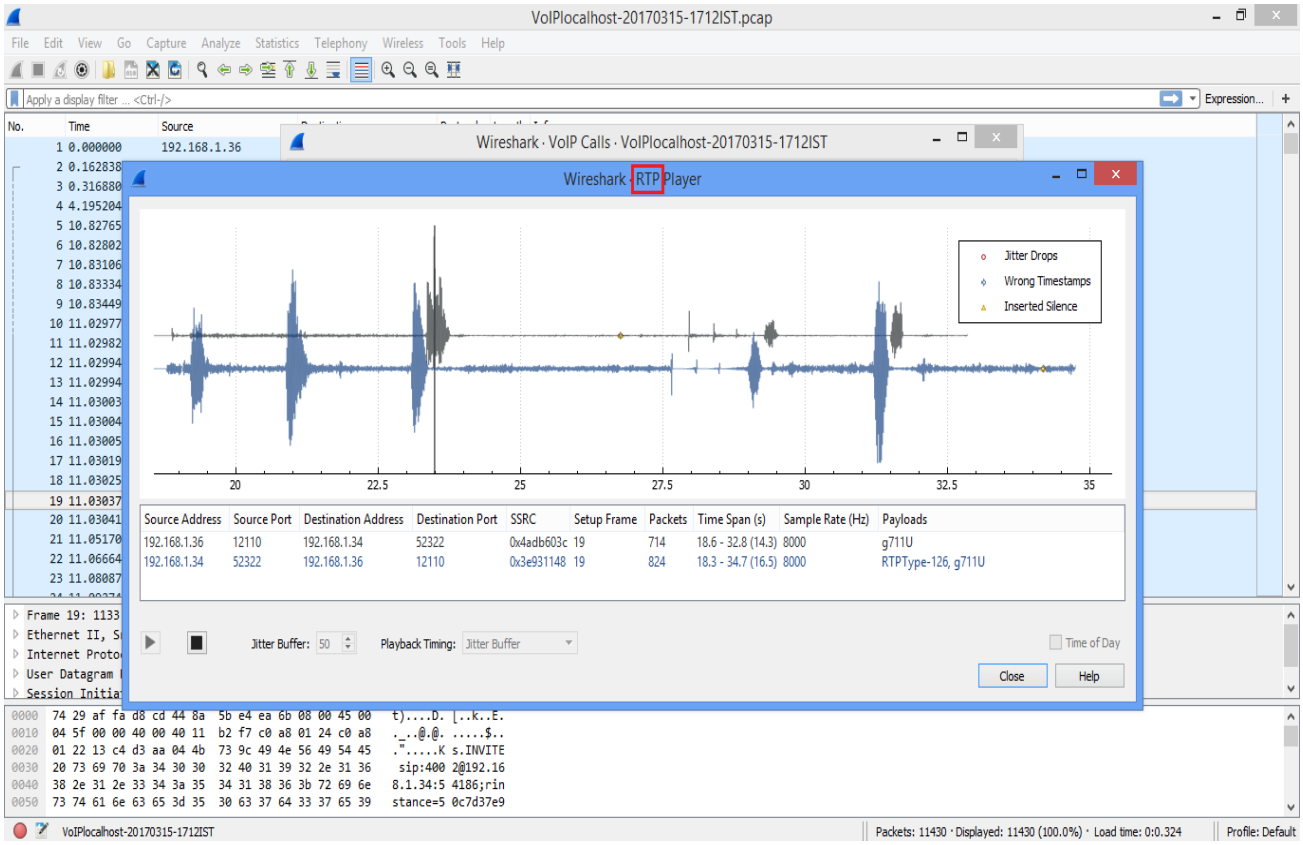


Fig. 4.4 Voice Content – RTP

Next, we could retrieve crucial logs related to access and error. However, it is common to analyze these logs in routine computer forensics, but in case of VoIP related crimes, these log files can reveal much more. These logs play crucial role when a VoIP server was attacked remotely or a compromised VoIP server was used to change certain system level settings or credentials.

E. Access Logs are very important in understanding who accessed web server at what time and from where. Following screen depicts part of access log retrieved from our experiment.

```
172.16.16.204 - - [08/Mar/2017:17:19:22 +0530] "GET /admin HTTP/1.1" 301 314 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chro
172.16.16.204 - - [08/Mar/2017:17:19:22 +0530] "GET /admin/ HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome
172.16.16.204 - - [08/Mar/2017:17:19:22 +0530] "GET /admin/config.php HTTP/1.1" 200 15255 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like
172.16.16.204 - - [08/Mar/2017:17:19:22 +0530] "GET /admin/assets/css/bootstrap-3.3.5.min.css?load_version=13.0.190.19 HTTP/1.1" 200 122540 "http://172.16.16.203/
172.16.16.204 - - [08/Mar/2017:17:19:23 +0530] "GET /admin/assets/css/typehead.js-bootstrap3-0.2.3.css?load_version=13.0.190.19 HTTP/1.1" 200 6546 "http://172.16
172.16.16.204 - - [08/Mar/2017:17:19:23 +0530] "GET /admin/assets/css/bootstrap-table-reorder-rows.css?load_version=13.0.190.19 HTTP/1.1" 200 820 "http://172.16.
172.16.16.204 - - [08/Mar/2017:17:19:23 +0530] "GET /admin/assets/css/bootstrap-table-1.9.0.css?load_version=13.0.190.19 HTTP/1.1" 200 6654 "http://172.16.16.203/
172.16.16.204 - - [08/Mar/2017:17:19:23 +0530] "GET /admin/assets/css/font-awesome.min-4.5.0.css?load_version=13.0.190.19 HTTP/1.1" 200 27466 "http://172.16.16.2
172.16.16.204 - - [08/Mar/2017:17:19:23 +0530] "GET /admin/assets/css/jquery-ui-1.10.3.custom.css?load_version=13.0.190.19 HTTP/1.1" 200 59756 "http://172.16.16.
172.16.16.204 - - [08/Mar/2017:17:19:23 +0530] "GET /admin/assets/js/outdatedbrowser.min.js?load_version=13.0.190.19 HTTP/1.1" 200 3176 "http://172.16.16.203/adm
172.16.16.204 - - [08/Mar/2017:17:19:23 +0530] "GET /admin/assets/css/outdatedbrowser.min.css?load_version=13.0.190.19 HTTP/1.1" 200 1066 "http://172.16.16.203/a
172.16.16.204 - - [08/Mar/2017:17:19:23 +0530] "GET /admin/assets/js/jquery-1.11.3.min.js?load_version=13.0.190.19 HTTP/1.1" 200 95957 "http://172.16.16.203/admi
172.16.16.204 - - [08/Mar/2017:17:19:23 +0530] "GET /admin/assets/js/selector-set-1.0.6.js?load_version=13.0.190.19 HTTP/1.1" 200 11183 "http://172.16.16.203/adm
172.16.16.204 - - [08/Mar/2017:17:19:23 +0530] "GET /admin/assets/less/cache/lessphp_5bb5fb9369f168b338710b81b71ecf8bb4796422.css HTTP/1.1" 200 93269 "http://172
172.16.16.204 - - [08/Mar/2017:17:19:23 +0530] "GET /admin/assets/js/jquery.selector-set-0.1.8.js?load_version=13.0.190.19 HTTP/1.1" 200 4054 "http://172.16.16.2
172.16.16.204 - - [08/Mar/2017:17:19:23 +0530] "GET /admin/assets/js/class.js?load_version=13.0.190.19 HTTP/1.1" 200 1911 "http://172.16.16.203/admin/config.php"
172.16.16.204 - - [08/Mar/2017:17:19:23 +0530] "GET /admin/assets/js/jquery-migrate-1.2.1.js?load_version=13.0.190.19 HTTP/1.1" 200 16621 "http://172.16.16.203/a
172.16.16.204 - - [08/Mar/2017:17:19:23 +0530] "GET /admin/assets/js/jed.js?load_version=13.0.190.19 HTTP/1.1" 200 37240 "http://172.16.16.203/admin/config.php"
172.16.16.204 - - [08/Mar/2017:17:19:23 +0530] "GET /admin/assets/js/modgettext.js?load_version=13.0.190.19 HTTP/1.1" 200 2281 "http://172.16.16.203/admin/config
172.16.16.204 - - [08/Mar/2017:17:19:23 +0530] "GET /admin/assets/js/modernizr.js?load_version=13.0.190.19 HTTP/1.1" 200 13110 "http://172.16.16.203/admin/config
172.16.16.204 - - [08/Mar/2017:17:19:23 +0530] "GET /admin/assets/js/tableExport.min.js?load_version=13.0.190.19 HTTP/1.1" 200 14161 "http://172.16.16.203/admin/
172.16.16.204 - - [08/Mar/2017:17:19:23 +0530] "GET /admin/assets/js/jquery.tablednd.min.js?load_version=13.0.190.19 HTTP/1.1" 200 9316 "http://172.16.16.203/adm
172.16.16.204 - - [08/Mar/2017:17:19:23 +0530] "GET /admin/assets/js/bootstrap-3.3.4.custom.min.js?load_version=13.0.190.19 HTTP/1.1" 200 34488 "http://172.16.16.
172.16.16.204 - - [08/Mar/2017:17:19:23 +0530] "GET /admin/assets/fonts/opensans-bold-webfont.woff2 HTTP/1.1" 200 52788 "http://172.16.16.203/admin/assets/less/c
172.16.16.204 - - [08/Mar/2017:17:19:23 +0530] "GET /admin/assets/fonts/opensans-regular-webfont.woff2 HTTP/1.1" 200 50876 "http://172.16.16.203/admin/assets/les
172.16.16.204 - - [08/Mar/2017:17:19:23 +0530] "GET /admin/assets/js/bootstrap-table-locale/bootstrap-table-en-US.js?load_version=13.0.190.19 HTTP/1.1" 200 1244
172.16.16.204 - - [08/Mar/2017:17:19:23 +0530] "GET /admin/assets/js/bootstrap-table-1.9.0.js?load_version=13.0.190.19 HTTP/1.1" 200 94113 "http://172.16.16.203/
172.16.16.204 - - [08/Mar/2017:17:19:23 +0530] "GET /admin/assets/js/bootstrap-table-cookie.js?load_version=13.0.190.19 HTTP/1.1" 200 13135 "http://172.16.16.203/
172.16.16.204 - - [08/Mar/2017:17:19:23 +0530] "GET /admin/images/sangoma-horizontal_thumb.png HTTP/1.1" 200 11362 "http://172.16.16.203/admin/config.php" "Mozil
172.16.16.204 - - [08/Mar/2017:17:19:23 +0530] "GET /admin/images/freepbx_small.png?load_version=13.0.190.19 HTTP/1.1" 200 7438 "http://172.16.16.203/admin/confi
172.16.16.204 - - [08/Mar/2017:17:19:23 +0530] "GET /admin/images/tango.png HTTP/1.1" 200 2555 "http://172.16.16.203/admin/config.php" "Mozilla/5.0 (Windows NT 6
172.16.16.204 - - [08/Mar/2017:17:19:23 +0530] "GET /admin/assets/js/bootstrap-table-mobile.js?load_version=13.0.190.19 HTTP/1.1" 200 3849 "http://172.16.16.203/
```

Fig. 4.5 Access Logs

F. Similar to access logs, error logs are equally important as they log all the errors raised on the server. Following screen is a part of error log retrieved from our experiment.

```
[Wed Mar 15 16:47:02 2017] [notice] Digest: generating secret for digest authentication ...
[Wed Mar 15 16:47:02 2017] [notice] Digest: done
[Wed Mar 15 16:47:02 2017] [notice] Apache/2.2.15 (Unix) DAV/2 PHP/5.3.28 mod_ssl/2.2.15 OpenSSL/1.0.1e-fips configured -- resuming normal operations
[Wed Mar 15 16:51:23 2017] [notice] caught SIGTERM, shutting down
[Wed Mar 15 16:52:24 2017] [notice] suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Wed Mar 15 16:52:25 2017] [notice] Digest: generating secret for digest authentication ...
[Wed Mar 15 16:52:25 2017] [notice] Digest: done
[Wed Mar 15 16:52:28 2017] [notice] Apache/2.2.15 (Unix) DAV/2 PHP/5.3.28 mod_ssl/2.2.15 OpenSSL/1.0.1e-fips configured -- resuming normal operations
Error opening Certificate /etc/pki/tls/certs/localhost.crt
140448361289544:error:0200100D:system library:fopen:Permission denied:bss_file.c:398:fopen('/etc/pki/tls/certs/localhost.crt','r')
140448361289544:error:20074002:BIO routines:FILE_CTRL:system lib:bss_file.c:400:
unable to load certificate
[Wed Mar 15 17:16:55 2017] [notice] SIGHUP received.  Attempting to restart
httpd: Could not reliably determine the server's fully qualified domain name, using localhost.localdomain for ServerName
[Wed Mar 15 17:16:55 2017] [notice] Digest: generating secret for digest authentication ...
[Wed Mar 15 17:16:55 2017] [notice] Digest: done
[Wed Mar 15 17:16:55 2017] [notice] Apache/2.2.15 (Unix) DAV/2 PHP/5.3.28 mod_ssl/2.2.15 OpenSSL/1.0.1e-fips configured -- resuming normal operations
[Wed Mar 15 17:22:47 2017] [notice] caught SIGTERM, shutting down
[Wed Mar 15 17:23:50 2017] [notice] suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Wed Mar 15 17:23:51 2017] [notice] Digest: generating secret for digest authentication ...
[Wed Mar 15 17:23:51 2017] [notice] Digest: done
[Wed Mar 15 17:23:53 2017] [notice] Apache/2.2.15 (Unix) DAV/2 PHP/5.3.28 mod_ssl/2.2.15 OpenSSL/1.0.1e-fips configured -- resuming normal operations
[Wed Mar 15 17:31:54 2017] [notice] caught SIGTERM, shutting down
[Wed Mar 15 17:33:16 2017] [notice] suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Wed Mar 15 17:33:16 2017] [notice] Digest: generating secret for digest authentication ...
[Wed Mar 15 17:33:16 2017] [notice] Digest: done
[Wed Mar 15 17:33:18 2017] [notice] Apache/2.2.15 (Unix) DAV/2 PHP/5.3.28 mod_ssl/2.2.15 OpenSSL/1.0.1e-fips configured -- resuming normal operations
[Wed Mar 15 17:34:06 2017] [notice] caught SIGTERM, shutting down
[Fri Mar 17 16:18:18 2017] [notice] suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Fri Mar 17 16:18:19 2017] [notice] Digest: generating secret for digest authentication ...
[Fri Mar 17 16:18:19 2017] [notice] Digest: done
[Fri Mar 17 16:18:21 2017] [notice] Apache/2.2.15 (Unix) DAV/2 PHP/5.3.28 mod_ssl/2.2.15 OpenSSL/1.0.1e-fips configured -- resuming normal operations
[Fri Mar 17 16:21:40 2017] [notice] caught SIGTERM, shutting down
[Fri Mar 17 16:22:30 2017] [notice] suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Fri Mar 17 16:22:31 2017] [notice] Digest: generating secret for digest authentication ...
[Fri Mar 17 16:22:31 2017] [notice] Digest: done
[Fri Mar 17 16:22:34 2017] [notice] Apache/2.2.15 (Unix) DAV/2 PHP/5.3.28 mod_ssl/2.2.15 OpenSSL/1.0.1e-fips configured -- resuming normal operations
```

Fig. 4.6 Error Logs

The observations shown above are few related to basic analysis of a crime committed using or targeting an asterisk server. They include almost all the basic things an investigator should know for investigating such crimes. The details mentioned in this article makes forensic investigator familiar about important artifacts of asterisk server.

V. CONCLUSION

Outcome of the work will assist forensic investigators who are not very comfortable with VoIP server investigation. It is worth as most of the VoIP solutions - commercial or free - have asterisk at their core. This article will act as a basic guideline for the investigators and they can take help of findings of this paper to speed up their investigation.

REFERENCES

[1] Chu D., The Cost Benefits of Switching to a VoIP Service, telzio 2014 [https://telzio.com/blog/cost-benefits-switching-voip-service/]
[2] Pruitt B., Why Unified Communications? (NEW Infographic Explains), Digium, 2012
[3] Global VoIP Services Market Poised to Surge from USD 83 Billion in 2015 to USD 140 Billion by 2021, Market Research Store, 2016
[4] Kowalke M., VoIP by the Numbers, TMC Net, 2013
[5] SIP trunking statistics that show how fast IT managers are making the transition, ExpertIT, 2013
[6] Vorodi S., Just the Facts, Please: Your Go-To List of Cold, Hard VoIP Statistics, The VoIP Report, 2017
[7] Cooney M., IBM warns of rising VoIP cyber-attacks, Network World, 2016
[8] VOIP Attacks On The Rise, Nettitude, 2015
[9] Steffen C., 6 Common Ways to Suffer a VoIP Attack, VoIP Innovations, 2015
[10] Sgaras, C., Kechadi, M. T., & Le-Khac, N. A. (2015). Forensics acquisition and analysis of instant messaging and VoIP applications. In Computational forensics (pp. 188-199). Springer, Cham.
[11] Pelaez, J. C., & Fernandez, E. B. (2009, August). Voip network forensic patterns. In Computing in the Global Information Technology, 2009. ICCGI'09. Fourth International Multi-Conference on (pp. 175-180). IEEE.
[12] Hsu, H. M., Sun, Y., & Chen, M. (2008). A collaborative forensics framework for VoIP services in multi-network environments. Intelligence and Security Informatics, 260-271.
[13] Yen, Y. S., Lin, I. L., & Wu, B. L. (2011). A study on the forensic mechanisms of VoIP attacks: Analysis and digital evidence. Digital Investigation, 8(1), 56-67.
[14] Ibrahim, M., Abdullah, M. T., & Dehghantanha, A. (2012, June). VoIP evidence model: A new forensic method for investigating VoIP malicious attacks. In Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on (pp. 201-206). IEEE.

[15] Fernandez, E., Pelaez, J., & Larrondo-Petrie, M. (2007). Attack patterns: A new forensic and design tool. Advances in digital forensics III, 345-357.
[16] Slay, J., & Simon, M. (2008, January). Voice over IP forensics. In Proceedings of the 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop (p. 10). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).
[17] Montoro, P., & Casilari, E. (2009, July). A comparative study of VoIP standards with asterisk. In Digital Telecommunications, 2009. ICDT'09. Fourth International Conference on (pp. 1-6). IEEE.
[18] Qadeer, M. A., & Imran, A. (2008, December). Asterisk voice exchange: An alternative to conventional EPBX. In Computer and Electrical Engineering, 2008. ICCEE 2008. International Conference on (pp. 652-656). IEEE.
[19] Rober, A. (2009). FreePBX Powerful Telephony Solutions.
[20] Giripunje, S. D., & Sonaskar, S. (2011). Low Cost IP Private Branch Exchange (PBX). International Journal of Computer Applications, 23(3), 12-14.
[21] SETTHAWONG, P., & VANNIJA, V. (2010). Improving the IP-PBX Administration and Management Process by Utilizing the EZY IP-PBX Frontend to augment FreePBX. Journal of Global Management Research (JGMR), Issue, 6(1), 47-56.
[22] Zoiper - https://www.zoiper.com/
[23] TCPDump - http://www.tcpdump.org/
[24] Forensic Falcon - https://www.logicube.com/shop/falcon/?v=c86ee0d9d7ed
[25] EnCase Forensic - https://www.guidancesoftware.com/encase-forensic

