Hunting Threats with Wireshark Plugins

Nishant Sharma, Jeswin Mathai and Shivam Bathla
PentesterAcademy.com & AttackDefense.com

About Me

Me, **Nishant Sharma**

- R&D Manager and Lead Trainer, Pentester Academy
- Firmware developer, Enterprise WiFi APs and WIPS Sensors, Mojo Networks (Acquired by Arista Networks)
- Masters degree in Infosec
- Published research at Blackhat US/Asia, DEF CON USA/China, HITB Amsterdam and other venues
- Conducted trainings in HITB, OWASP NZ day and for multiple private clients

About Us

Jeswin Mathai,

- Security Researcher
- Published research at Blackhat US/Asia, DEF CON USA and other venues
- Conducted trainings for multiple private clients

Shivam Bathla

- Security Researcher
- Newest member of the team ☺

Security Research/Trainer at Hacker Cons

OWASP
NEW ZEALAND DAY
2019

HITB

DEF CON

black hat

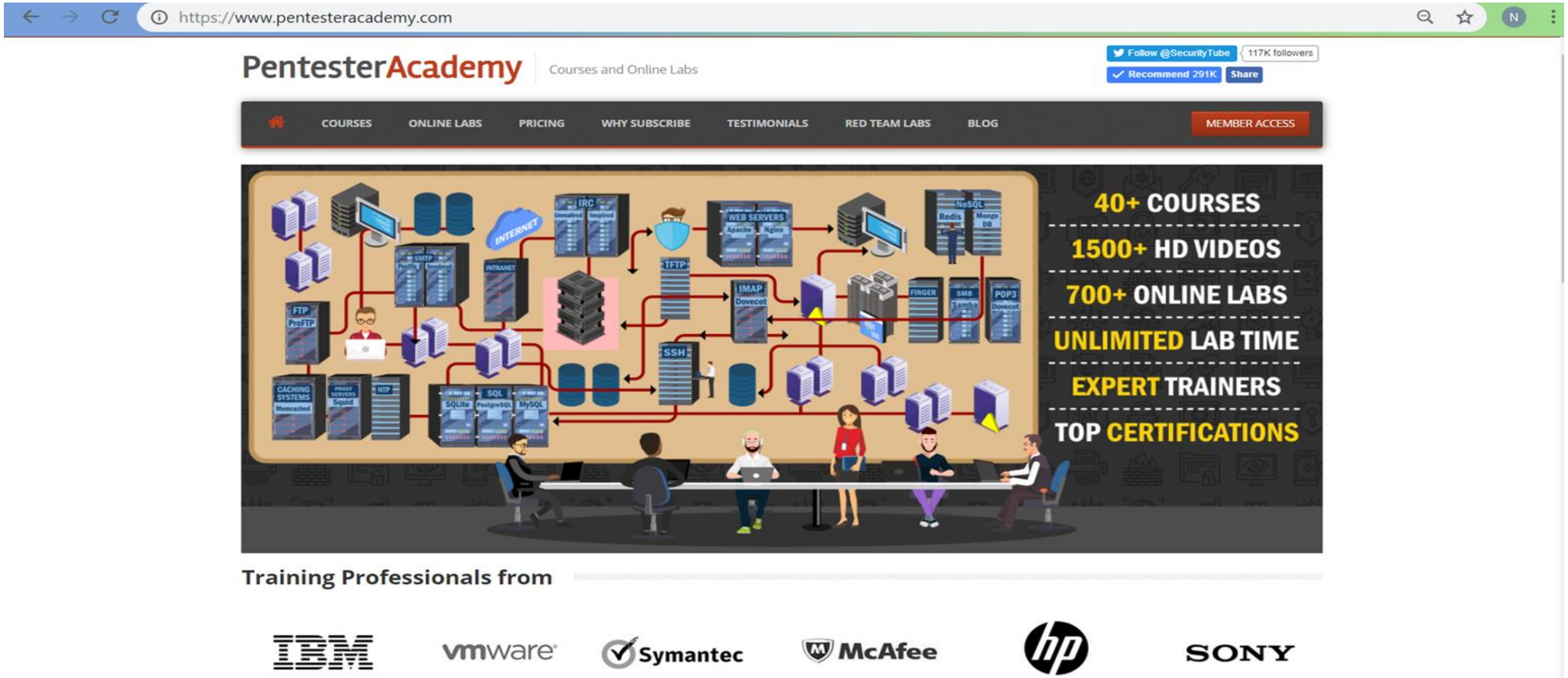
WALL OF SHEEP

WIRELESS VILLAGE

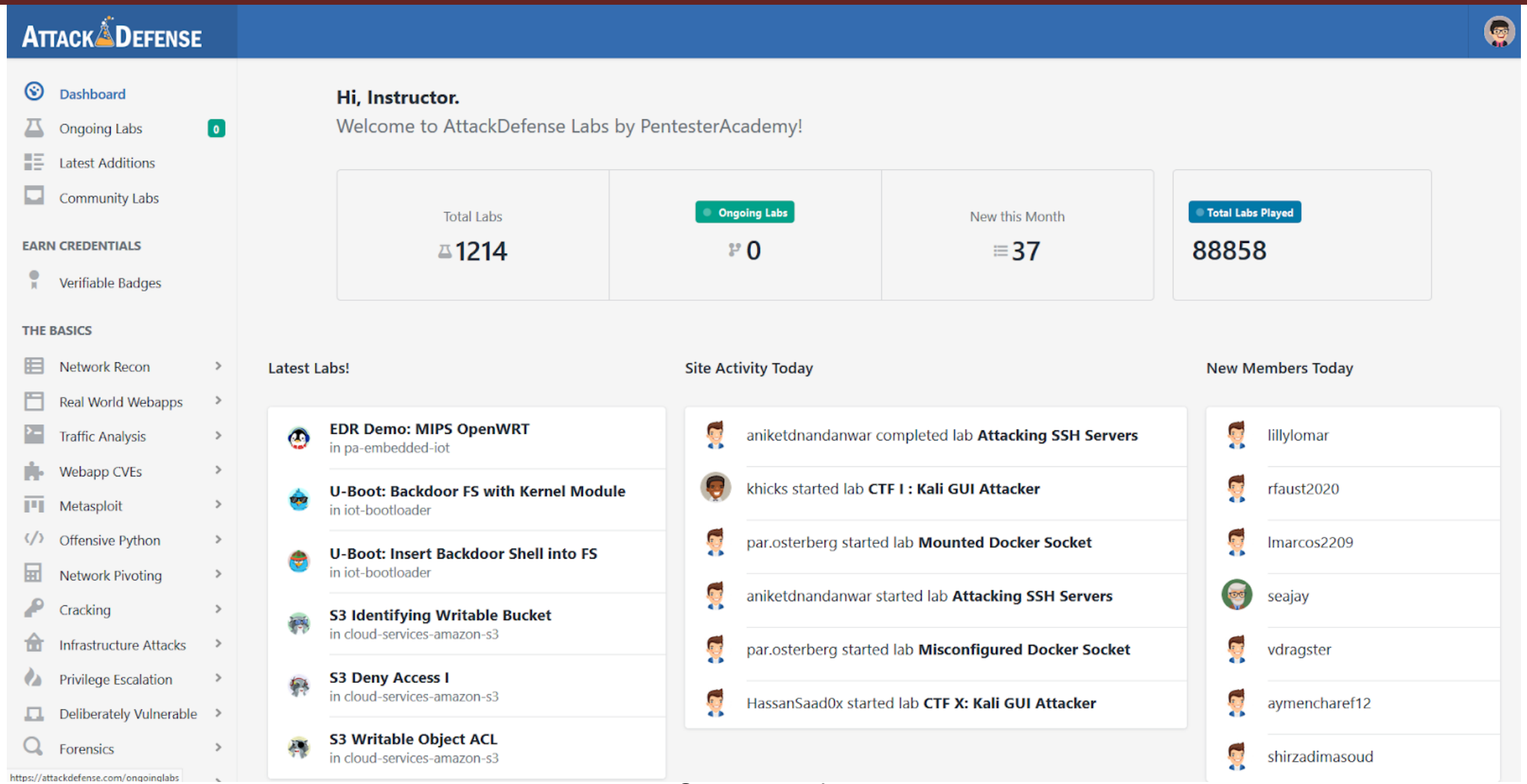
IoT VILLAGE
DEFCON

ROOTCON
Hacker Conference

PentesterAcademy.com



AttackDefense.com



Dedicated Instances, No VPN, Only Web browser

attackdefense.com:1 (root)

Not secure | s5z0m22bx9zv3f6majd5b43gn.us-west1.attackdefenselabs.com/#/client/a2FsaQBjAG5vYXV0aA==

LXTerminal

File Edit Tabs Help

```
root@attackdefense:~# ip a
1025: eth0@if1026: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueu
e state UP group default
    link/ether 02:42:0a:01:01:04 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.4/24 brd 10.1.1.255 scope global eth0
       valid_lft forever preferred_lft forever
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
```

README

Monitor Settings

README

Terminal

KALI L

"the quieter you become, the r

wifi-capture.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	GuangLia_05:9c:97	Broadcast	802.11	264	Beacon frame, SN=1
2	0.001824	GuangLia_05:9c:97	HonHaiPr_a5:19:c9	802.11	258	Probe Response, SN
3	0.001858		GuangLia_05:9c:97 (…	802.11	58	Acknowledgement, F
4	0.002160	GuangLia_05:9c:97	HonHaiPr_a5:19:c9	802.11	258	Probe Response, SN
5	0.002188		GuangLia_05:9c:97 (…	802.11	58	Acknowledgement, F
6	0.021797	HonHaiPr_a5:19:c9	Broadcast	802.11	112	Probe Request, SN=
7	0.023416	GuangLia_05:9c:97	HonHaiPr_a5:19:c9	802.11	258	Probe Response, SN
8	0.023466		GuangLia_05:9c:97 (…	802.11	58	Acknowledgement, F

```
▸ Frame 1: 264 bytes on wire (2112 bits), 264 bytes captured (2112 bits)
▸ Radiotap Header v0, Length 48
▸ 802.11 radio information
▸ IEEE 802.11 Beacon frame, Flags: ........
▸ IEEE 802.11 wireless LAN
```

```
0000  00 00 30 00 2f 40 10 a0  20 08 00 a0 20 08 00 00   ··0·/@·· ····· ····
0010  17 6b 2e 45 00 00 00 00  00 0c 3c 14 40 01 de 00   ·k.E···· ··<·@···
0020  00 00 00 00 13 e5 01 00  0c 00 00 00 de 00 b7 02   ····· ····· ·····
0030  80 00 00 00 ff ff ff ff  ff ff e4 95 6e 45 9c 97   ····· ····· ····nE··
0040  e4 95 6e 45 9c 97 70 6c  6e d9 99 28 00 00 00 00   ··nE··pl n··(····
0050  64 00 21 00 00 15 43 6f  75 72 61 67 65 54 68 65   d·!···Co urageThe
0060  43 6f 77 61 72 64 6c 79  44 6f 67 01 08 8c 12 98   Cowardly Dog·····
0070  24 b0 48 60 6c 03 01 24  05 04 01 02 00 00 07 0a   $·H`l··$ ·····
0080  55 53 20 24 04 17 95 05  1e 00 0b 05 00 00 49 00   US $···· ·····I·
0090  00 3b 02 80 00 2d 1a 6f  09 1b ff 00 00 00 00 00   ·;···-·o ·····
```

wifi-capture.pcap Packets: 80065 · Displayed: 80065 (100.0%) Profile: Default

wifi-capture.pcap LXTerminal 05:51

Talk Overview

- Motivation
- Why Wireshark
- Wireshark Plugins and Plugins type
- What all we can do
  - Macro Analysis
  - Modifying Traffic
  - Attack Detection
  - Tool Detection
- Conclusion

Motivation

- Macro analysis
- Custom/Proprietary protocols
- Scaling detection logic (i.e. automating detection)
- Easy to get and operate

Why Wireshark Plugins?

- Plug and play
- Plugins can be
  - Lua scripts
  - Compiled C/C++ code
- Harnessing power of Wireshark
- OS independent
- Large user base

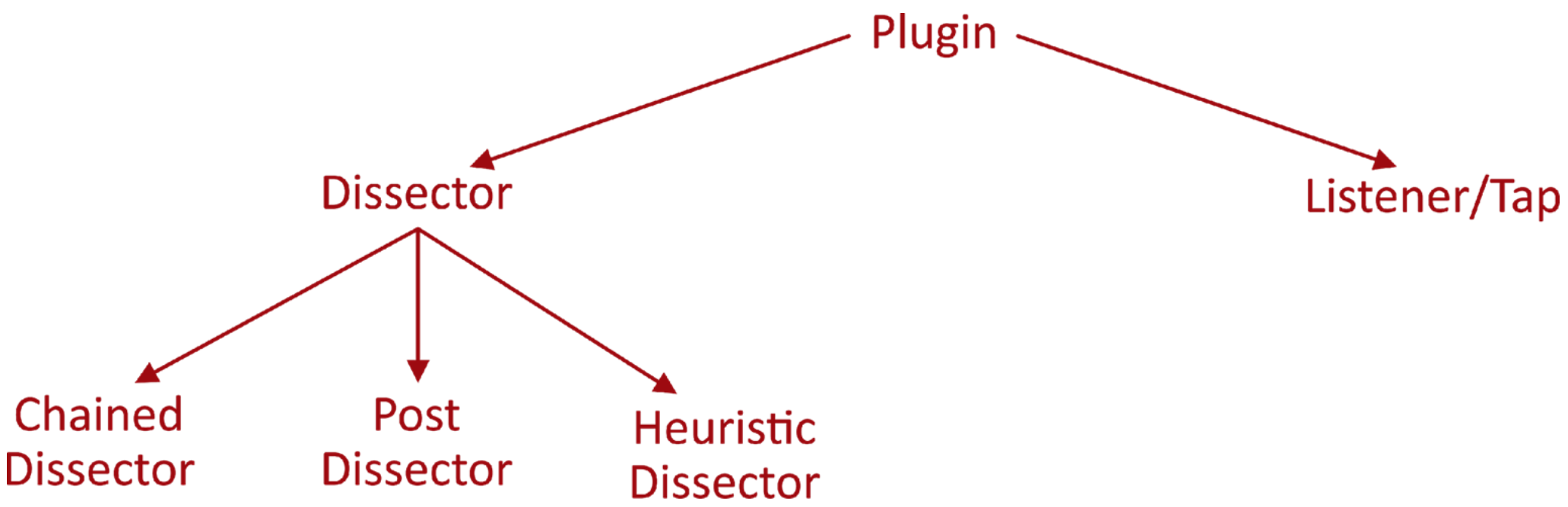
Wireshark Plugins

- plugins for various purposes
- Plugins can be
  - Lua scripts
  - Compiled C/C++ code

Why Lua?

- User friendly
- No Compilation

Wireshark Plugins Types



Tap/Listener

- To read the packet and summarizing the information
- Macro Analysis

Sample Tap/Listener

Wireshark · List of urls

Client: 192.168.252.128

S.NO	Domain	IP address	Packets exchanged	Data exchanged	%age packets	Duration
1	googleads.g.doubleclick.net	216.58.220.2	1	216	0.46296296296296	111.99859
2	accounts.google.com	216.58.220.13	1	216	0.46296296296296	69.583764
3	d1y6jrbzotnyjg.cloudfront.net	52.84.108.196	1	216	0.46296296296296	101.5861
4	ads.yahoo.com	106.10.198.33	1	216	0.46296296296296	115.369101
5	www.google.com	216.58.199.132	2	432	0.46296296296296	47.025383
6	syndication.twitter.com	199.59.148.85	1	216	0.46296296296296	148.854945
7	cdn.optimizely.com	23.52.64.131	2	432	0.46296296296296	25.334201
8	platform.twitter.com	199.96.57.6	2	360	0.55555555555556	125.473812
9	www.google.co.in	216.58.199.131	6	1296	0.46296296296296	47.195543

Highlight:

Reset Search Close

Dissector

- To interpret the payload data
- Decodes its part of the protocol and passes the payload to next

Example Dissection Flow

Sample Dissector: Before

Complete_normal_call.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... + torrent cleanup_own_ssid cleanup_probe

No.	Time	Source	Destination	Protocol	Length	Sequence nu	Info
366	23.539017	192.168.20.1	192.168.20.130	RTP	214		PT=ITU-T G.711 PCMU, SSRC=0x294823, Seq=5229, Time=11200
367	23.540170	192.168.20.130	192.168.20.132	RTP	214		PT=ITU-T G.711 PCMU, SSRC=0xAFD8AB5, Seq=20595, Time=11200
368	23.540675	192.168.20.132	192.168.20.130	RTP	214		PT=ITU-T G.711 PCMU, SSRC=0x43572C47, Seq=29428, Time=11200
369	23.540996	192.168.20.130	192.168.20.1	RTP	214		PT=ITU-T G.711 PCMU, SSRC=0x3C988166, Seq=25721, Time=11200
370	23.558827	192.168.20.1	192.168.20.130	RTP	214		PT=ITU-T G.711 PCMU, SSRC=0x294823, Seq=5230, Time=11360
371	23.559261	192.168.20.130	192.168.20.132	RTP	214		PT=ITU-T G.711 PCMU, SSRC=0xAFD8AB5, Seq=20596, Time=11360
372	23.560761	192.168.20.132	192.168.20.130	RTP	214		PT=ITU-T G.711 PCMU, SSRC=0x43572C47, Seq=29429, Time=11360
373	23.561106	192.168.20.130	192.168.20.1	RTP	214		PT=ITU-T G.711 PCMU, SSRC=0x3C988166, Seq=25722, Time=11360
374	23.578996	192.168.20.1	192.168.20.130	RTP	214		PT=ITU-T G.711 PCMU, SSRC=0x294823, Seq=5231, Time=11520
375	23.579711	192.168.20.130	192.168.20.132	RTP	214		PT=ITU-T G.711 PCMU, SSRC=0xAFD8AB5, Seq=20597, Time=11520
376	23.581088	192.168.20.132	192.168.20.130	RTP	214		PT=ITU-T G.711 PCMU, SSRC=0x43572C47, Seq=29430, Time=11520
377	23.581450	192.168.20.130	192.168.20.1	RTP	214		PT=ITU-T G.711 PCMU, SSRC=0x3C988166, Seq=25723, Time=11520

```
▷ Frame 370: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits)
▷ Ethernet II, Src: Vmware_c0:00:08 (00:50:56:c0:00:08), Dst: Vmware_f8:0d:44 (00:0c:29:f8:0d:44)
▷ Internet Protocol Version 4, Src: 192.168.20.1, Dst: 192.168.20.130
▷ User Datagram Protocol, Src Port: 4000, Dst Port: 15674
▷ Real-Time Transport Protocol
```

Sample Dissector: After

Complete_normal_call.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression... + torrent cleanup_own_ssid cleanup_probe

No.	Time	Source	Destination	Protocol	Length	Sequence nu	Hello World	Info
365	23.520490	192.168.20.130	192.168.20.1	RTP	214		✓	PT=ITU-T G.711 PCMU, SSRC=0x3C988166, Seq=25720, Time=1
366	23.539017	192.168.20.1	192.168.20.130	RTP	214		✓	PT=ITU-T G.711 PCMU, SSRC=0x294823, Seq=5229, Time=1120
367	23.540170	192.168.20.130	192.168.20.132	RTP	214		✓	PT=ITU-T G.711 PCMU, SSRC=0xAFD8AB5, Seq=20595, Time=11
368	23.540675	192.168.20.132	192.168.20.130	RTP	214		✓	PT=ITU-T G.711 PCMU, SSRC=0x43572C47, Seq=29428, Time=1
369	23.540996	192.168.20.130	192.168.20.1	RTP	214		✓	PT=ITU-T G.711 PCMU, SSRC=0x3C988166, Seq=25721, Time=1
370	23.558827	192.168.20.1	192.168.20.130	RTP	214		✓	PT=ITU-T G.711 PCMU, SSRC=0x294823, Seq=5230, Time=1136
371	23.559261	192.168.20.130	192.168.20.132	RTP	214		✓	PT=ITU-T G.711 PCMU, SSRC=0xAFD8AB5, Seq=20596, Time=11
372	23.560761	192.168.20.132	192.168.20.130	RTP	214		✓	PT=ITU-T G.711 PCMU, SSRC=0x43572C47, Seq=29429, Time=1
373	23.561106	192.168.20.130	192.168.20.1	RTP	214		✓	PT=ITU-T G.711 PCMU, SSRC=0x3C988166, Seq=25722, Time=1
374	23.578996	192.168.20.1	192.168.20.130	RTP	214		✓	PT=ITU-T G.711 PCMU, SSRC=0x294823, Seq=5231, Time=1152
375	23.579711	192.168.20.130	192.168.20.132	RTP	214		✓	PT=ITU-T G.711 PCMU, SSRC=0xAFD8AB5, Seq=20597, Time=11

```
Frame 372: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits)
Ethernet II, Src: Vmware_3a:a6:0f (00:0c:29:3a:a6:0f), Dst: Vmware_f8:0d:44 (00:0c:29:f8:0d:44)
Internet Protocol Version 4, Src: 192.168.20.132, Dst: 192.168.20.130
User Datagram Protocol, Src Port: 4000, Dst Port: 16912
Real-Time Transport Protocol
Hello World
    Hello World: Hello
```

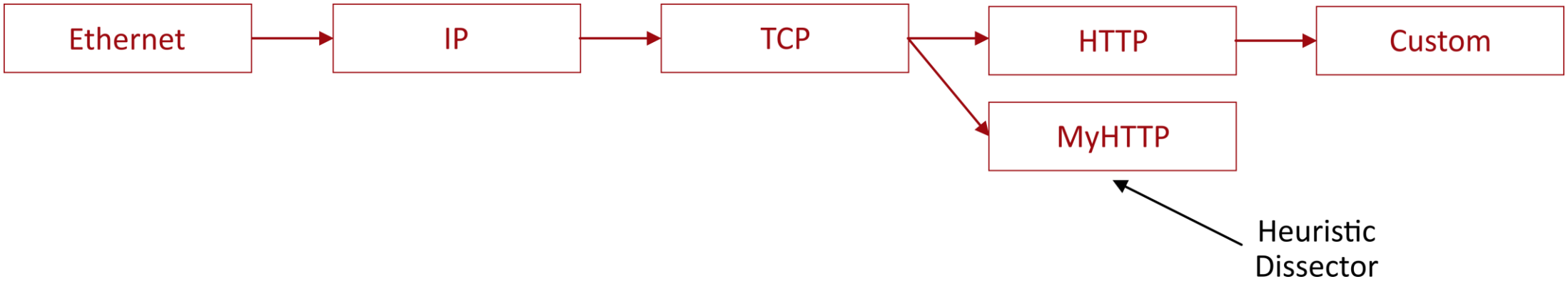
This one

Heuristic Dissector

- Identifies the protocol on the basis of heuristics
- Heuristics can be
  - Average size or size range of the packets
  - Specific codes or strings in the header or the payload
- Useful when port based detection fails i.e. protocols operating on non standard ports (e.g. DNS server running on port 8089)

Heuristic Dissector

Example Dissection Flow



Note: The heuristic dissector will only give result if no existing dissector is able to identify the packet

Example: DNS heuristic dissector

Lua File: dns_dissector.lua

File Source:
https://wiki.wireshark.org/Lua/Examples?action=AttachFile&do=get&target=dissector.lua

Heuristic Dissector: DNS Server on Port 8089

DNS_traffic_server port_8089.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Protocol	Destination	Length	Info
11	4.555392055	192.168.1.16	SSDP	239.255.255.250	216	M-SEARCH * HTTP/1.1
12	5.114518734	192.168.1.115	DB-LS…	192.168.1.255	188	Dropbox LAN sync Discovery Protocol
13	5.462842742	192.168.1.33	UDP	192.168.1.104	74	46191 → 8089 Len=32
14	5.463360963	192.168.1.104	UDP	192.168.1.33	90	8089 → 46191 Len=48

```
▷ Frame 13: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
▷ Ethernet II, Src: HewlettP_4b:06:c9 (48:0f:cf:4b:06:c9), Dst: CompalIn_4b:c4:4d (f8:a9:63:4b:c4:4d)
▷ Internet Protocol Version 4, Src: 192.168.1.33, Dst: 192.168.1.104
◢ User Datagram Protocol, Src Port: 46191, Dst Port: 8089
    Source Port: 46191
    Destination Port: 8089
    Length: 40
    Checksum: 0xf239 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 7]
◢ Data (32 bytes)
    Data: 26da0100000100000000000003777777706676f6f676c6503...
    [Length: 32]
```

```
0000  f8 a9 63 4b c4 4d 48 0f  cf 4b 06 c9 08 00 45 00   ..cK.MH. .K....E.
0010  00 3c cb 4f 00 00 40 11  2b 88 c0 a8 01 21 c0 a8   .<.O..@. +....!..
0020  01 68 b4 6f 1f 99 00 28  f2 39 26 da 01 00 00 01   .h.o...( .9&.....
0030  00 00 00 00 00 00 03 77  77 77 06 67 6f 6f 67 6c   .......w ww.googl
0040  65 03 63 6f 6d 00 00 01  00 01                     e.com... ..
```

Heuristic Dissector: Identifying DNS Traffic

DNS_traffic_server port_8089.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

mydns

No.	Time	Source	Protocol	Destination	Length	Info
13	5.462842742	192.168.1.33	MYDNS	192.168.1.104	74	Query (9946) www.google.com
14	5.463360963	192.168.1.104	MYDNS	192.168.1.33	90	Response (9946) www.google.com
15	5.463688094	192.168.1.33	MYDNS	192.168.1.104	74	Query (40285) www.google.com
16	5.565232771	192.168.1.104	MYDNS	192.168.1.33	102	Response (40285) www.google.com

```
▷ Frame 13: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
▷ Ethernet II, Src: HewlettP_4b:06:c9 (48:0f:cf:4b:06:c9), Dst: CompalIn_4b:c4:4d (f8:a9:63:4b:c4:4d)
▷ Internet Protocol Version 4, Src: 192.168.1.33, Dst: 192.168.1.104
◢ User Datagram Protocol, Src Port: 46191, Dst Port: 8089
    Source Port: 46191
    Destination Port: 8089
    Length: 40
    Checksum: 0xf239 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 7]
  [Heuristic dissector used]
◢ MyDNS Protocol
    Transaction ID: 9946
  ▷ Flags: 0x0100
    Number of Questions: 1
    Number of Answer RRs: 0
    Number of Authority RRs: 0
    Number of Additional RRs: 0
  ▷ Queries
```

What all can be done?

- Macro Analysis
- Modifying Traffic
- Attack Detection
- Attack Tool Detection

Macro Analysis

- **HTTP**
  - Downloaded Files
  - GET Requests With Details
  - POST Requests With Details
- **HTTPS**
  - List of urls
- **WiFi**
  - Overview

Macro Analysis: HTTP

- Downloaded Files

Wireshark · Downloaded Files

S.no	Host	User Agent	Path	Content Type	Content Length
1	ecx.images-amazon.com	Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.8.0	/images/I/41wuVnAeedL._AC_SY200_.jpg	image/jpeg	7751
2	ecx.images-amazon.com	Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.8.0	/images/I/41O1oRMP6pL._AC_SY200_.jpg	image/jpeg	6424
3	ecx.images-amazon.com	Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.8.0	/images/I/412maSA0fuL._AC_SY200_.jpg	image/jpeg	4978
4	ecx.images-amazon.com	Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0	/images/I/316zh6kkqML._AC_SY200_.jpg	image/jpeg	4044

Highlight:

Reset Search Close

Macro Analysis: HTTP

- GET Requests With Details

Wireshark · GET Requests With Details

S.no	Host	User Agent	Path	Parameters
1	www.amazon.in	Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko /20100101 Firefox/31.0 Iceweasel/31.8.0	/	
2	ecx.images-amazon.com	Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko /20100101 Firefox/31.0 Iceweasel/31.8.0	/images/I/412maSA0fuL._AC_SY200_.jpg	
3	ecx.images-amazon.com	Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko /20100101 Firefox/31.0 Iceweasel/31.8.0	/images/I/41wuVnAeedL._AC_SY200_.jpg	
4	ecx.images-amazon.com	Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko /20100101 Firefox/31.0 Iceweasel/31.8.0	/images/I/412OwlOMxPL._AC_SY200_.jpg	

Highlight:

Reset Search Close

Macro Analysis: HTTP

- GET Requests With Details

Wireshark · GET Requests With Details

		Iceweasel/31.8.0		
60	aax-eu.amazon-ads ystem.com	Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko /20100101 Firefox/31.0 Iceweasel/31.8.0	/x/getad	c=100&pc=301128&pt=Gateway&u= http%3A%2F%2Fwww.amazon.in&sr c=501&sz=300x250&ad-sid=0101c 66c5eeb112791056302b3670d179c 19f083ced67d91b5d063276932661 1c071&pj=%7B%22prid%22%3A%220 101642030409d906ca37d77d5be4b 68593e93b53a79f250f176e4ebbd5 54fcea7b1%22%2C%22bn%22%3A%22 301128%22%7D&slot=right-7
61	www.amazon.in	Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko /20100101 Firefox/31.0 Iceweasel/31.8.0	/gp/product/B01DDP7UQ0/ref=br_a sw_pdt-3/278-7381968-4337153/ue data/unsticky/278-7381968-43371 53/Detail/ntpoffrw	ul&v=0.501.0&id=0XGJXTGHGWS34 MQJAXRV&ctb=1&m=1&sc=0XGJXTGH GWS34MQJAXRV&pc=1342633&tc=-4 07&hob=1&hoe=3&ul=1342633&t=1 466408318624&pty=Detail&spty= Glance&pti=B01DDP7UQ0&tid=0JA E5VRXPMH77731K1TX&aftb=1
62	googleads.g.doubl eclick.net	Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko	/pagead/viewthroughconversion/9 84527532/	value=0&label=r_58CJXm0gIQw9i z3gM&guid=ON&script=0&data=ec

Highlight:

Reset Search Close

Macro Analysis: HTTP

- POST Requests With Details

Wireshark · POST Requests With Details

S.no	Host	User Agent	Path	Parameter
1	fls-eu.amazon.in	Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko /20100101 Firefox/31.0 Iceweasel/31.8.0	/1/batch/1/OE/	
2	fls-eu.amazon.in	Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko /20100101 Firefox/31.0 Iceweasel/31.8.0	/1/action-impressions/1/OP/csm/action/csm-features:impression-tracking?requestId=1VD546T6JFGBNYWW1R8W&marketplaceId=A21TJRUUN4KGV&session=278-7381968-4337153&csm=1	
3	fls-eu.amazon.in	Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko /20100101 Firefox/31.0 Iceweasel/31.8.0	/1/batch/1/OE/	

Highlight:

Reset Search Close

Macro Analysis: HTTPS

- List of URLs

Wireshark · List of urls

Client: 192.168.252.128

S.NO	Domain	IP address	Packets exchanged	Data exchanged	%age packets	Duration
1	googleads.g.doubleclick.net	216.58.220.2	1	216	0.46296296296296	111.99859
2	accounts.google.com	216.58.220.13	1	216	0.46296296296296	69.583764
3	d1y6jrbzotnyjg.cloudfront.net	52.84.108.196	1	216	0.46296296296296	101.5861
4	ads.yahoo.com	106.10.198.33	1	216	0.46296296296296	115.369101
5	www.google.com	216.58.199.132	2	432	0.46296296296296	47.025383
6	syndication.twitter.com	199.59.148.85	1	216	0.46296296296296	148.854945
7	cdn.optimizely.com	23.52.64.131	2	432	0.46296296296296	25.334201
8	platform.twitter.com	199.96.57.6	2	360	0.55555555555556	125.473812
9	www.google.co.in	216.58.199.131	6	1296	0.46296296296296	47.195543

Highlight:

Reset Search Close

Macro Analysis: WiFi

- WiFi Networks Overview

Wireshark · Overview

S.no	SSID	BSSID	Channel	Data Count	Managment Count	% Packets	Security	Key Managment	WPS
1	Destek	20:a6:80:b7:53:3d	3	746	384	7.43	WPA/WPA2 Personal	PSK	Enabled
2	Board room	f4:f2:6d:47:1c:a6	1	1101	163	44.22	WPA2 Personal	PSK	Enabled
3	NWPUNE	c8:3a:35:55:54:20	6	27	504	1.13	WPA/WPA2 Personal	PSK	Disabled
4	HIDER-2	f4:f2:6d:46:dd:6a	7	14	310	0.93	WPA2 Personal	PSK	Enabled
5	HP-Print-52-Deskjet 3540 series	f0:92:1c:fc:de:52	6	0	419	0.00	WPA2 Personal	PSK	
6	PA_NET	50:c7:bf:c8:2a:1b	6	151	647	11.28	WPA/WPA2 Personal	PSK	
7	HP-Print-96-LaserJet Pro MFP	40:49:0f:b9:9d:96	6	0	268	0.00	No-Encryption		
8	eFinserve	74:da:da:17:da:ef	2	4	60	0.00	WPA/WPA2 Personal	PSK	

Highlight:

Reset Search Close

Modifying Traffic

- **Example Case:**
  - Decrypting encrypted SRTP Traffic
  - Exporting call as audio file

- Extending Wireshark

RTP Packets

Complete_normal_call.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

rtp

Expression... torrent

No.	Time	Source	Destination	Protocol	Length	Ta	Info
3103	37.140222	192.168.20.1	192.168.20.130	RTP	214		PT=ITU-T G.711 PCMU, SSRC=0x294823, Seq=5909, Time=120000
3104	37.141062	192.168.20.130	192.168.20.132	RTP	214		PT=ITU-T G.711 PCMU, SSRC=0xAFD8AB5, Seq=21275, Time=120000
3105	37.143728	192.168.20.132	192.168.20.130	RTP	214		PT=ITU-T G.711 PCMU, SSRC=0x43572C47, Seq=30108, Time=120000
3106	37.144098	192.168.20.130	192.168.20.1	RTP	214		PT=ITU-T G.711 PCMU, SSRC=0x3C988166, Seq=26401, Time=120000
3110	37.160340	192.168.20.1	192.168.20.130	RTP	214		PT=ITU-T G.711 PCMU, SSRC=0x294823, Seq=5910, Time=120160

```
▷ Frame 3106: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits)
▷ Ethernet II, Src: Vmware_f8:0d:44 (00:0c:29:f8:0d:44), Dst: Vmware_c0:00:08 (00:50:56:c0:00:08)
▷ Internet Protocol Version 4, Src: 192.168.20.130, Dst: 192.168.20.1
▷ User Datagram Protocol, Src Port: 15674, Dst Port: 4000
◢ Real-Time Transport Protocol
  ▷ [Stream setup by SDP (frame 37)]
    10.. .... = Version: RFC 1889 Version (2)
    ..0. .... = Padding: False
    ...0 .... = Extension: False
    .... 0000 = Contributing source identifiers count: 0
    0... .... = Marker: False
    Payload type: ITU-T G.711 PCMU (0)
    Sequence number: 26401
    [Extended sequence number: 91937]
    Timestamp: 120000
    Synchronization Source identifier: 0x3c988166 (1016627558)
    Payload: 5f5f606265696b6c6e70777b7d7d7e7d7a797efaf8fb7e7d...
```

Recovered VoIP Calls

Wireshark · VoIP Calls · Complete_normal_call

Start Time	Stop Time	Initial Speaker	From	To	Protocol	Duration	Packets	State	Comments
17.478218	38.752328	192.168.20.132	<sip:1111@192.168.20.130	<sip:2222@192.168.20.130	SIP	00:00:21	10	COMPLETED	INVITE 200
17.598013	38.757037	192.168.20.130	"Bob" <sip:1111@192.168.20.130	<sip:2222@192.168.20.1;ob	SIP	00:00:21	7	COMPLETED	INVITE 200

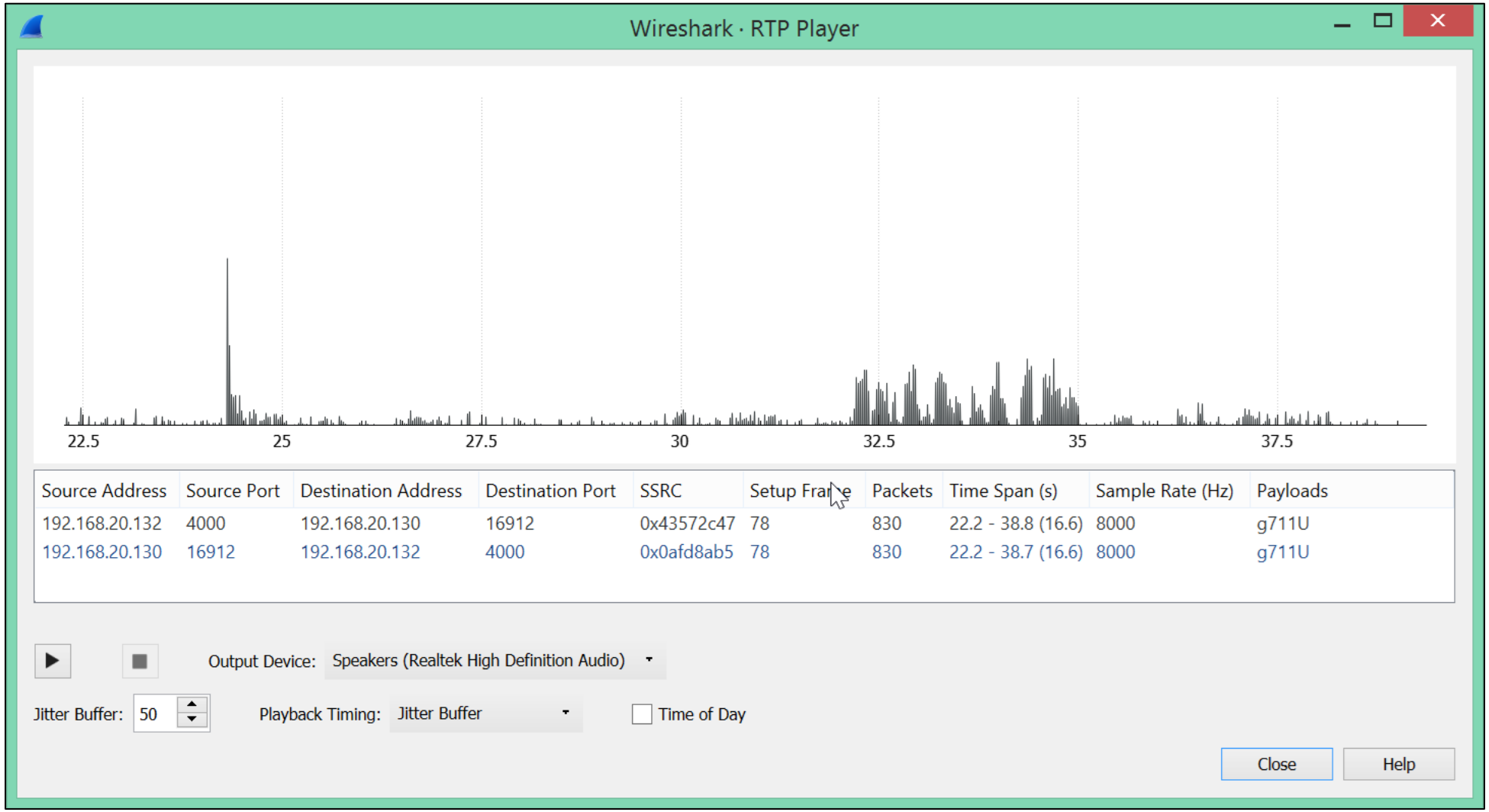
Time of Day

OK | Cancel | Prepare Filter | Flow Sequence | Play Streams | Copy | Help

Flow Sequence

Time	192.168.20.132		192.168.20.130		192.168.20.1	Comment
17.478218	58655	INVITE SDP (opus g711A g711U telephon... →	5060			SIP INVITE From: <sip:1111@192.168.20.130 To:...
17.485438	58655	← 100 Trying	5060			SIP Status 100 Trying
17.597307	58655	← 180 Ringing	5060			SIP Status 180 Ringing
17.598013			5060	INVITE SDP (g711U g711A GSM G726-32 t... →	52987	SIP INVITE From: "Bob" <sip:1111@192.168.20.1...
17.603920			5060	← 100 Trying	52987	SIP Status 100 Trying
17.604301			5060	← 180 Ringing	52987	SIP Status 180 Ringing
17.605610	58655	← 180 Ringing	5060			SIP Status 180 Ringing
22.145095			5060	← 200 OK SDP (g711U telephone-event)	52987	SIP Status 200 OK
22.148286			5060	ACK →	52987	SIP Request INVITE ACK 200 CSeq:28747
22.150650	58655	← 200 OK SDP (g711U g711A telephone-eve...	5060			SIP Status 200 OK
22.156664	58655	ACK →	5060			SIP Request INVITE ACK 200 CSeq:20778
22.158359	58655	UPDATE SDP (g711U telephone-event) →	5060			SIP UPDATE From: <sip:1111@192.168.20.130 To...
22.160190			15674	← RTP (g711U)	4000	RTP, 830 packets. Duration: 16.581s SSRC: 0x294...
22.160191	4000	← RTP (g711U)	16912			RTP, 830 packets. Duration: 16.581s SSRC: 0xAFD...
22.161608	58655	← 200 OK SDP (g711U telephone-event)	5060			SIP Status 200 OK
22.161703	4000	RTP (g711U) →	16912			RTP, 830 packets. Duration: 16.588s SSRC: 0x435...
22.162308			15674	RTP (g711U) →	4000	RTP, 830 packets. Duration: 16.589s SSRC: 0x3C9...
38.751436	58655	BYE →	5060			SIP Request BYE CSeq:20780
38.752328	58655	← 200 OK	5060			SIP Status 200 OK

Reconstructed Call



Possible Configurations

- SIP + RTP
- SIP over TLS + RTP
- **SIP + SRTP**
- SIP over TLS + SRTP

SRTP key in SDP packet

Normal_Call_two_parties.pcap

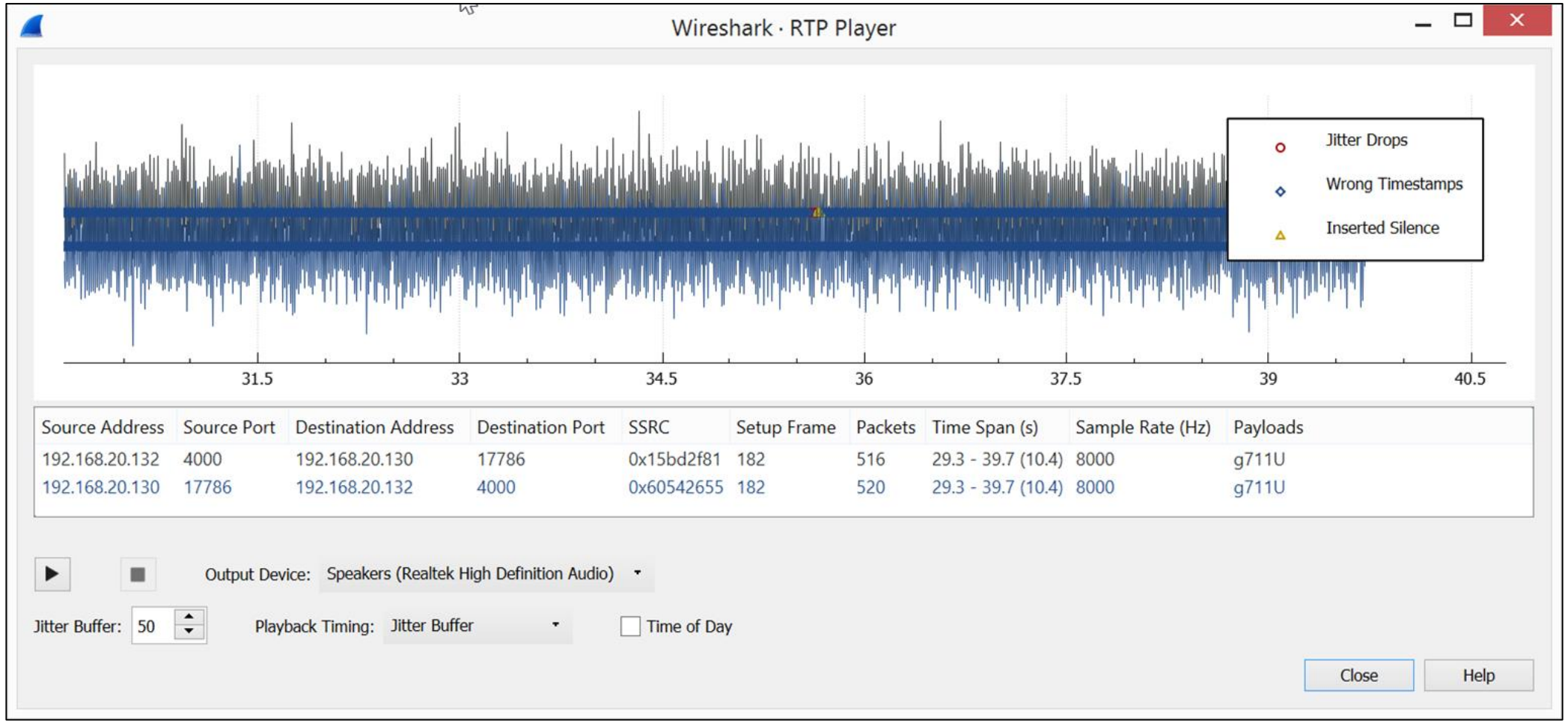
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

sdp

No.	Time	Source	Destination	Protocol	Length	Ta	Info
128	27.128753	192.168.20.132	192.168.20.130	SIP/SDP	278		Request: INVITE sip:2222@192.168.20.130
131	27.301506	192.168.20.130	192.168.20.1	SIP/SDP	1174		Request: INVITE sip:2222@192.168.20.1:60168;ob
173	29.293203	192.168.20.1	192.168.20.130	SIP/SDP	1101		Status: 200 OK
178	29.314263	192.168.20.130	192.168.20.132	SIP/SDP	1131		Status: 200 OK

```
Internet Protocol Version 4, Src: 192.168.20.1, Dst: 192.168.20.130
User Datagram Protocol, Src Port: 60168, Dst Port: 5060
Session Initiation Protocol (200)
  Status-Line: SIP/2.0 200 OK
  Message Header
  Message Body
    Session Description Protocol
      Session Description Protocol Version (v): 0
      Owner/Creator, Session Id (o): - 3730471310 3730471311 IN IP4 192.168.5.114
      Session Name (s): pjmedia
      Bandwidth Information (b): AS:84
      Time Description, active time (t): 0 0
      Session Attribute (a): X-nat:0
      Media Description, name and address (m): audio 4000 RTP/SAVP 0 101
      Connection Information (c): IN IP4 192.168.5.114
      Bandwidth Information (b): TIAS:64000
      Media Attribute (a): rtcp:4001 IN IP4 192.168.5.114
      Media Attribute (a): sendrecv
      Media Attribute (a): rtpmap:0 PCMU/8000
      Media Attribute (a): rtpmap:101 telephone-event/8000
      Media Attribute (a): fmtp:101 0-16
      Media Attribute (a): ssrc:965767637 cname:66bf37b000942b74
      Media Attribute (a): crypto:1 AES_CM_128_HMAC_SHA1_80 inline:2stvabBcXXf3HtaHCSsB8WACeRBst9f7lwLqlzqE
```

Encrypted Call



Decrypting SRTP: SRTP Packets

Normal_Call_two_parties.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

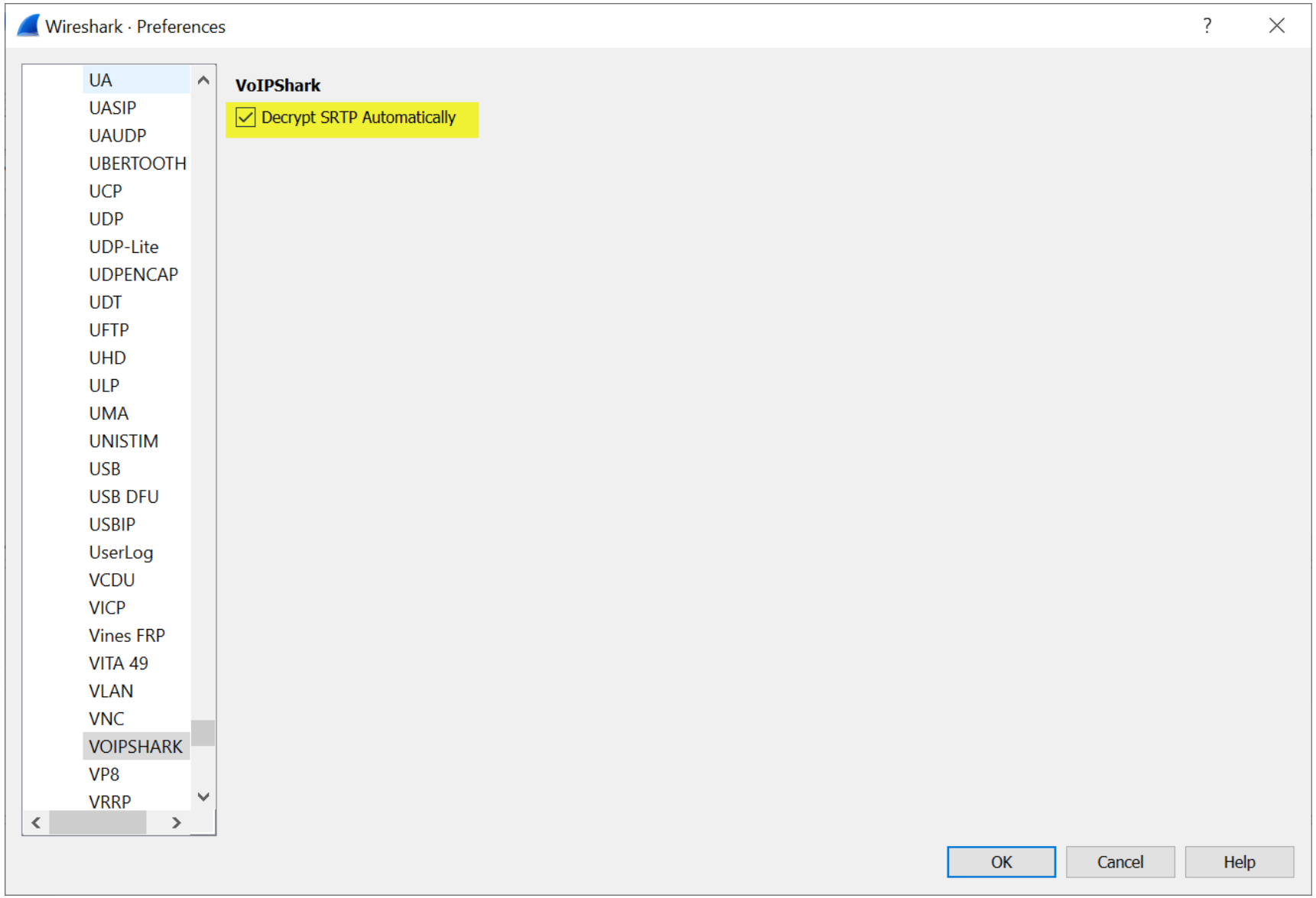
rtp

Expression...

No.	Time	Source	Destination	Protocol	Length	SSID	Sequence number	Info
177	29.311833	192.168.20.1	192.168.20.130	SRTP	224			PT=ITU-T G.711 PCMU, SSRC=0x3
183	29.316949	192.168.20.130	192.168.20.132	SRTP	224			PT=ITU-T G.711 PCMU, SSRC=0x6
189	29.332471	192.168.20.1	192.168.20.130	SRTP	224			PT=ITU-T G.711 PCMU, SSRC=0x3
190	29.333063	192.168.20.130	192.168.20.132	SRTP	224			PT=ITU-T G.711 PCMU, SSRC=0x6
191	29.334585	192.168.20.132	192.168.20.130	SRTP	224			PT=ITU-T G.711 PCMU, SSRC=0x1
192	29.334904	192.168.20.130	192.168.20.1	SRTP	224			PT=ITU-T G.711 PCMU, SSRC=0x4
193	29.352961	192.168.20.1	192.168.20.130	SRTP	224			PT=ITU-T G.711 PCMU, SSRC=0x3
194	29.353301	192.168.20.130	192.168.20.132	SRTP	224			PT=ITU-T G.711 PCMU, SSRC=0x6
195	29.354843	192.168.20.132	192.168.20.130	SRTP	224			PT=ITU-T G.711 PCMU, SSRC=0x1
196	29.355005	192.168.20.130	192.168.20.1	SRTP	224			PT=ITU-T G.711 PCMU, SSRC=0x4
197	29.372665	192.168.20.1	192.168.20.130	SRTP	224			PT=ITU-T G.711 PCMU, SSRC=0x3
198	29.372952	192.168.20.130	192.168.20.132	SRTP	224			PT=ITU-T G.711 PCMU, SSRC=0x6
199	29.375160	192.168.20.132	192.168.20.130	SRTP	224			PT=ITU-T G.711 PCMU, SSRC=0x1

```
> Frame 177: 224 bytes on wire (1792 bits), 224 bytes captured (1792 bits)
> Ethernet II, Src: Vmware_c0:00:08 (00:50:56:c0:00:08), Dst: Vmware_ff:65:9b (00:0c:29:ff:65:9b)
> Internet Protocol Version 4, Src: 192.168.20.1, Dst: 192.168.20.130
> User Datagram Protocol, Src Port: 4000, Dst Port: 16450
> Real-Time Transport Protocol
```

Decrypting SRTP: Enabling Auto Decryption



Decrypting SRTP: Decrypted SRTP (RTP)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

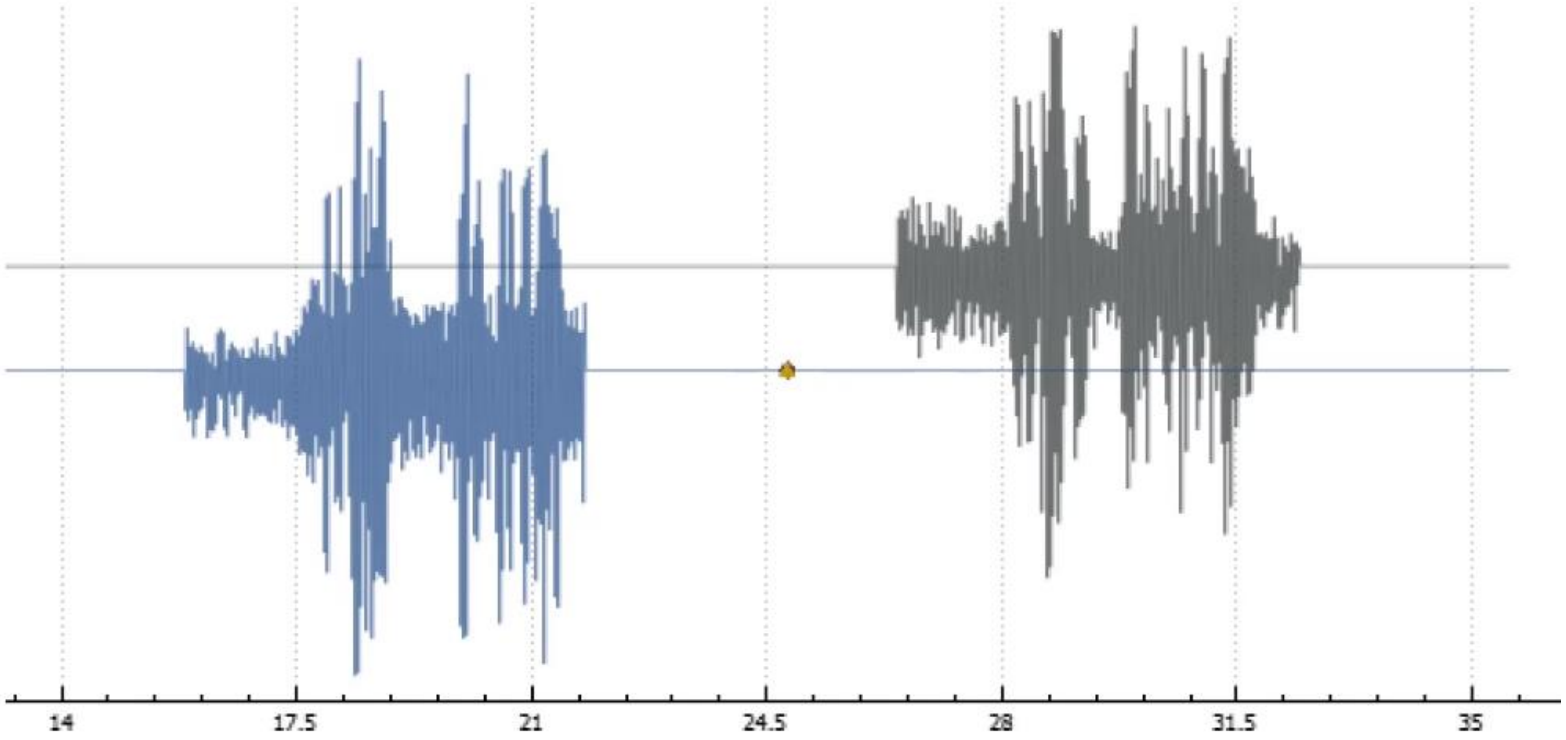
rtp

Expression...

No.	Time	Source	Destination	Protocol	Length	SSID	Sequence number	Info
177	29.311833	192.168.20.1	192.168.20.130	RTP	224			PT=ITU-T G.711 PCMU, SSRC=0x3
183	29.316949	192.168.20.130	192.168.20.132	RTP	224			PT=ITU-T G.711 PCMU, SSRC=0x6
189	29.332471	192.168.20.1	192.168.20.130	RTP	224			PT=ITU-T G.711 PCMU, SSRC=0x3
190	29.333063	192.168.20.130	192.168.20.132	RTP	224			PT=ITU-T G.711 PCMU, SSRC=0x6
191	29.334585	192.168.20.132	192.168.20.130	RTP	224			PT=ITU-T G.711 PCMU, SSRC=0x1
192	29.334904	192.168.20.130	192.168.20.1	RTP	224			PT=ITU-T G.711 PCMU, SSRC=0x4
193	29.352961	192.168.20.1	192.168.20.130	RTP	224			PT=ITU-T G.711 PCMU, SSRC=0x3
194	29.353301	192.168.20.130	192.168.20.132	RTP	224			PT=ITU-T G.711 PCMU, SSRC=0x6
195	29.354843	192.168.20.132	192.168.20.130	RTP	224			PT=ITU-T G.711 PCMU, SSRC=0x1
196	29.355005	192.168.20.130	192.168.20.1	RTP	224			PT=ITU-T G.711 PCMU, SSRC=0x4
197	29.372665	192.168.20.1	192.168.20.130	RTP	224			PT=ITU-T G.711 PCMU, SSRC=0x3
198	29.372952	192.168.20.130	192.168.20.132	RTP	224			PT=ITU-T G.711 PCMU, SSRC=0x6
199	29.375160	192.168.20.132	192.168.20.130	RTP	224			PT=ITU-T G.711 PCMU, SSRC=0x1

```
> Frame 177: 224 bytes on wire (1792 bits), 224 bytes captured (1792 bits)
> Ethernet II, Src: Vmware_c0:00:08 (00:50:56:c0:00:08), Dst: Vmware_ff:65:9b (00:0c:29:ff:65:9b)
> Internet Protocol Version 4, Src: 192.168.20.1, Dst: 192.168.20.130
> User Datagram Protocol, Src Port: 4000, Dst Port: 16450
> Real-Time Transport Protocol
```

Decrypted call



Source Address	Source Port	Destination Address	Destination Port	SSRC	Setup Frame	Packets	Time Span (s)	Sample Rate
192.168.20.1	4000	192.168.20.130	14904	0x00294823	4294967295	1135	12.8 - 35.5 (22.7)	8000
192.168.20.130	14904	192.168.20.1	4000	0x1edaa6cf	4294967295	1135	12.8 - 35.5 (22.7)	8000

VoIPShark: Exporting Call Audio

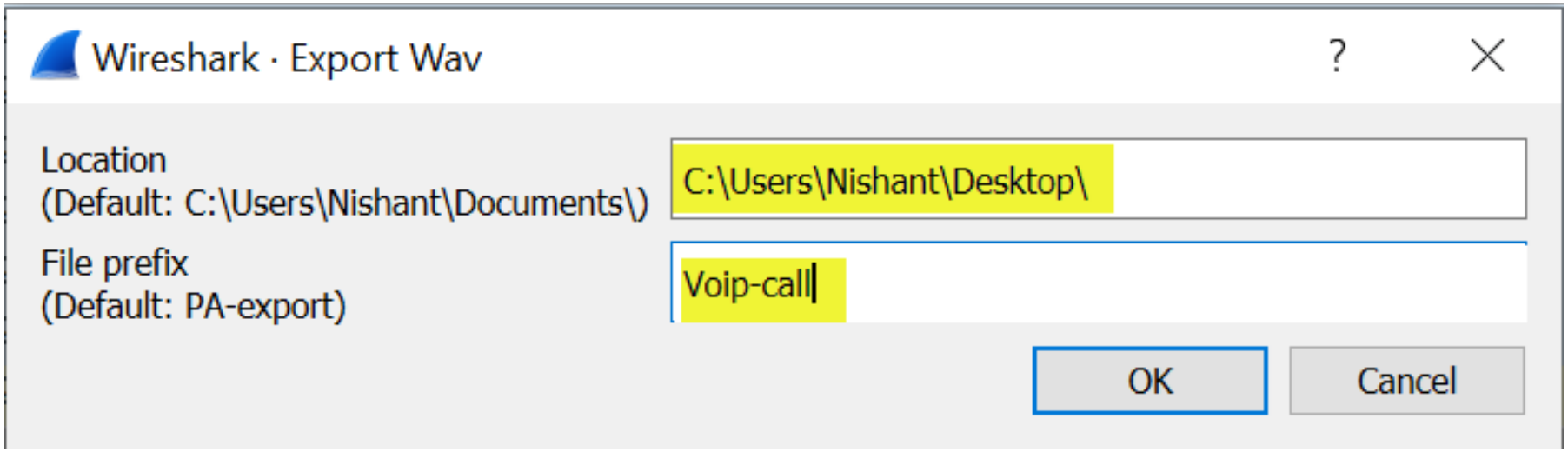
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

rtp

No.	Time	Source	Destination	Protocol	Sequence numb
177	29.311833	192.168.20.1	192.168.20.130	RTP	
183	29.316949	192.168.20.130	192.168.20.132	RTP	
189	29.332471	192.168.20.1	192.168.20.130	RTP	224
190	29.333063	192.168.20.130	192.168.20.132	RTP	224
191	29.334585	192.168.20.132	192.168.20.130	RTP	224
192	29.334904	192.168.20.130	192.168.20.1	RTP	224
193	29.352961	192.168.20.1	192.168.20.130	RTP	224
194	29.353301	192.168.20.130	192.168.20.132	RTP	224
195	29.354843	192.168.20.132	192.168.20.130	RTP	224

Tools:
- Firewall ACL Rules
- Lua ▸
- VOIP ▸
  - Export Wav
  - SIP Information Gathering ▸
  - VOIP Attack Detection ▸

Exporting Call Audio: Specifying Location and File name



Exporting Call Audio: Exported Streams

Wireshark · Export Wav

```
Streams Found: 4

Stream 1 Exported Successfully!
Please Check: C:\Users\Nishant\Desktop\Voip-call-192.168.20.130-192.168.20.1-0x4efa778b.wav

Stream 2 Exported Successfully!
Please Check: C:\Users\Nishant\Desktop\Voip-call-192.168.20.130-192.168.20.132-0x60542655.wav

Stream 3 Exported Successfully!
Please Check: C:\Users\Nishant\Desktop\Voip-call-192.168.20.132-192.168.20.130-0x15bd2f81.wav

Stream 4 Exported Successfully!
Please Check: C:\Users\Nishant\Desktop\Voip-call-192.168.20.1-192.168.20.130-0x399071d5.wav
```

Highlight:

Close

Attack Detection

- **WiFi Attacks**
  - Beacon Flood Detection
  - Deauth Disassoc Flooding
  - Possible Handshake Cracking
  - Evil Twin Detector
- SIP Invite Flood
- MiTM Attempts
- Dictionary Attack

Attack Detection: WiFi

- Beacon Flood Detection

Wireshark · Beacon Flood Detection

S.no	SSID	BSSID	Channel	Security	Beacons Sent	Detection Code
1	9TlDHTwmUu2f1	fc:d9:7a:96:09:2c	2	WEP	154	1,2
2	GYzH_T_p2 yW	fb:38:a8:4e:a6:14	4	WEP	85	1,2
3	IShBccMqCbqIl8	0f:d9:68:f4:d9:3c	9	WEP	90	1,2
4	GFKIQRwt8gNzv	83:42:17:e7:a3:39	12	WEP	86	1,2
5	vn9AIOBkh0dQH	91:9c:7a:41:17:18	11	WEP	60	1,2
6	cVDaV7cyqe0O	06:7a:33:70:97:d7	11	WEP	58	1,2
7	mRZ9q6vX0F5hVT	a9:e6:ab:aa:39:bf	11	WEP	59	1,2
8	16lMovg6FB	3c:47:78:39:47:c7	2	WEP	68	1,2
9	ITGneAwyT36MrQ	75:5f:41:b8:d5:38	12	WEP	84	1,2
10	rNFq1FWw6aWOSN	62:0f:86:75:55:74	5	WEP	75	1,2

Highlight:

Reset Search Close

Attack Detection: WiFi

- Deauth Disassoc Flooding

Wireshark · Deauth Disassoc Flooding

S.no	Source	Target	Statistics
1	50:c7:bf:c8:2a:1b	ff:ff:ff:ff:ff:ff	Deauth Count: 25600 Deauth per sec: 1706.4846416428 DisAssoc Count: 0 DisAssoc per sec: 0 Data after Deauth/Disassoc: true
2	50:c7:bf:c8:2a:1b	94:65:2d:ce:d4:55	Deauth Count: 25545 Deauth per sec: 1651.5276630719 DisAssoc Count: 0 DisAssoc per sec: 0 Data after Deauth/Disassoc: true
3	50:c7:bf:c8:2a:1b	94:14:7a:4b:fd:88	Deauth Count: 9 Deauth per sec: 0.27805509482513 DisAssoc Count: 0 DisAssoc per sec: 0 Data after Deauth/Disassoc: false

Highlight:

Reset Search Close

Attack Detection: WiFi

- Possible Handshake Cracking

Wireshark · Possible Handshake Cracking

S.no	Access Point	Station	Available Hanshakes For Breaking
1	50:c7:bf:c8:2a:1b	94:65:2d:ce:d4:55	1,2,3,4
2	f0:92:1c:fc:de:52	4c:80:93:94:d8:92	1,2,3,4
3	50:c7:bf:c8:2a:1b	44:80:eb:7a:22:61	1,2
4	50:c7:bf:c8:2a:1b	cc:61:e5:b7:57:cd	1,2,3,4
5	f4:f2:6d:4e:b6:24	30:75:12:08:f4:21	1,2,3,4
6	f4:f2:6d:4e:9b:38	d0:04:01:67:94:59	1,2
7	f4:f2:6d:4e:b6:24	60:8e:08:92:f3:c0	1,2,3,4

Highlight:

Reset Search Close

Attack Detection: WiFi

- Evil Twin Detector

Wireshark · Evil Twin Detector

S.no	SSID	Attack Detected	BSSID	Channel	Security	Key Managment
1	PA_NET	Evil twin suspicious sequence	50:c7:bf:c8:2a:1b	6	WPA/WPA2 Personal	PSK
			2d:cf:46:29:04:b4	5	WEP	
			d8:68:a7:ff:3f:2b	6	WEP	
			fc:d9:7a:96:09:2c	2	WEP	
			7b:be:90:16:89:9d	7	WEP	
			77:c6:2f:26:98:88	6	WEP	
			b4:30:d4:34:9d:3a	6	WEP	
			0f:bd:2f:a1:f7:0f	6	WEP	
			68:f4:d9:3c:a8:35	10	WEP	
			5b:1b:a3:2a:82:88	5	WEP	
			a4:e9:57:db:5e:20	4	WEP	
			38:a8:4e:a6:14:93	10	WEP	
			56:24:44:df:59:8d	8	WEP	
			8f:2a:cd:c2:40:c1	12	WEP	
			57:74:64:c4:af:15	1	WEP	
			52:71:6a:72:29:23	5	WEP	

Highlight:

Reset Search Close

Attack Detection: SIP

- Invite Flooding

Wireshark · Invite Flooding

S.no	Attacker Machine	Attacker Extension	Target Extension	Target Machine	Invites Sent	Invites Per second
1	192.168.20.134	PentesterAcademy	1111	192.168.20.132	14	0.22

Highlight:

Reset Search Close

Attack Detection: MiTM

Wireshark · MITM Attempts

S.no	Call Source	Call Destination	Source Mac	Destination Mac	Attacker Mac
1	192.168.1.60	192.168.1.71	00:0c:29:9c:2f:3f ,48:0f:cf:4b:06:c9	48:0f:cf:4b:06:c9 ,f8:a9:63:4b:c4:4d	48:0f:cf:4b:06:c9

Highlight:

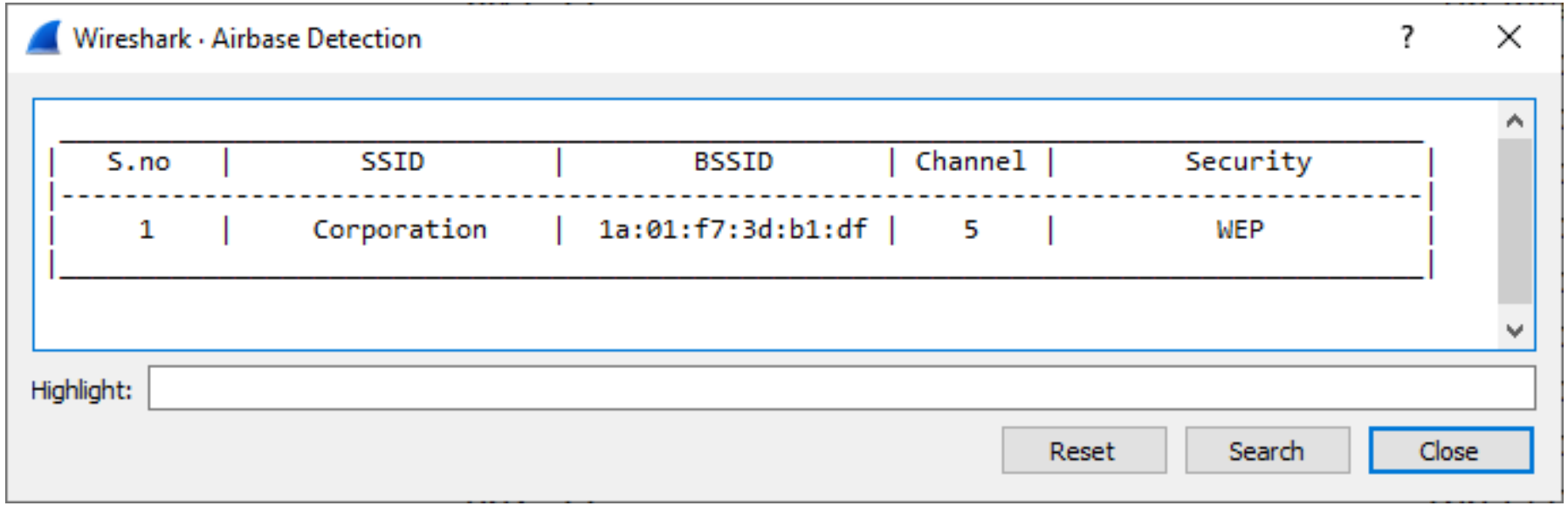
Reset Search Close

Attack Tool Detection

- **Example Case:** Airbase Detection
- Airbase: Tool to create Honeypots and Evil Twins

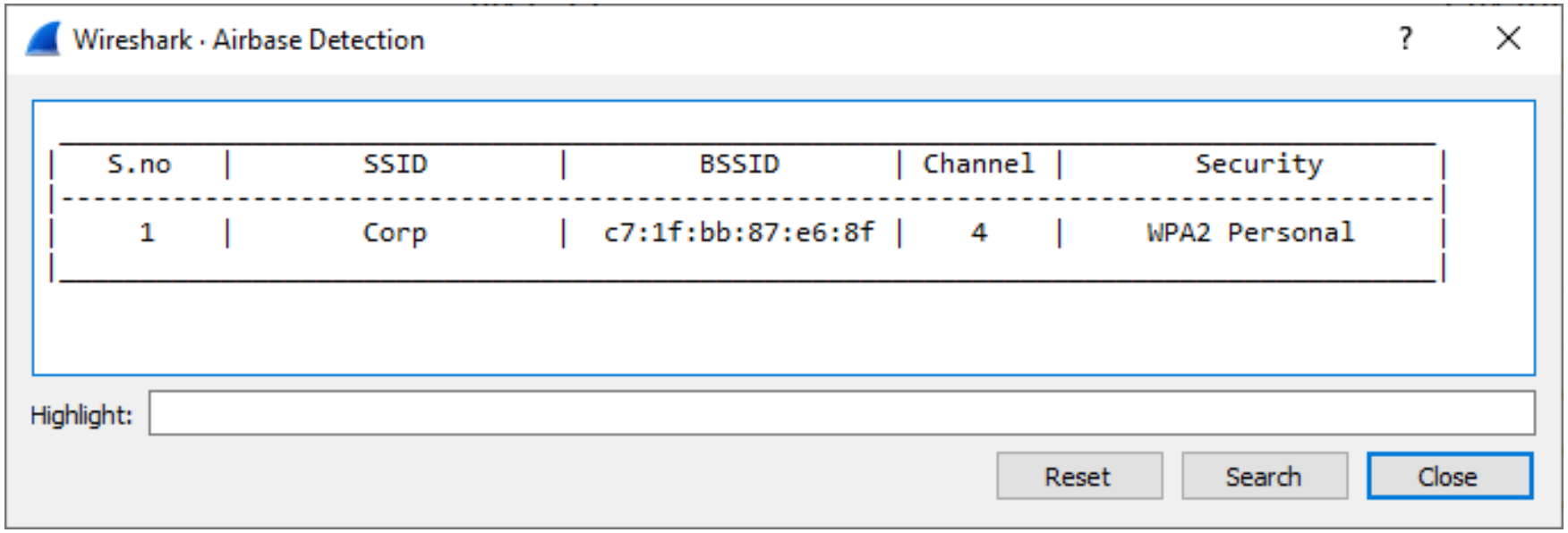
Attack Tool Detection

- Airbase Detection - WEP



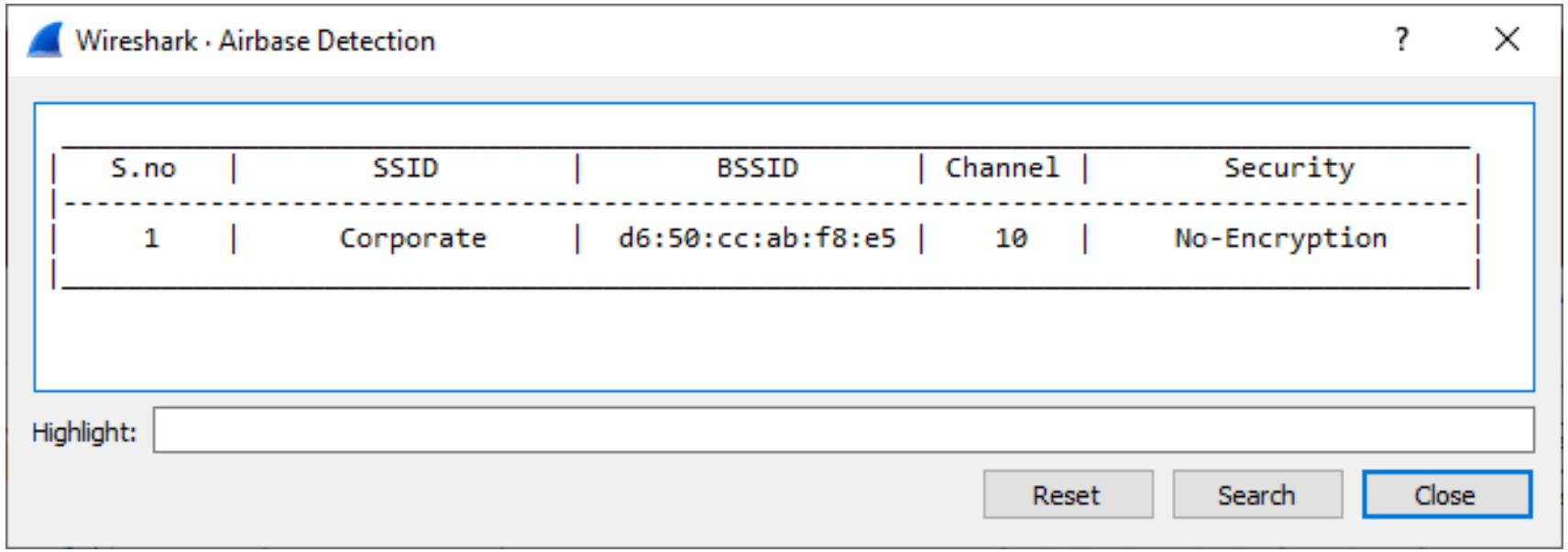
Attack Tool Detection

- Airbase Detection – WPA2-Personal



Attack Tool Detection

- Airbase Detection – No-Encryption



Demo

PAToolkit

- Collection of Wireshark plugins to perform
  - Macro analysis
  - Providing summary or overview
  - Dissecting unknown protocols
  - Detecting attacks/threats
- Coveres WiFi, DNS, DHCP, HTTP, HTTPS

- GitHub: http://www.github.com/pentesteracademy/patoolkit

VoIPShark

- Collection of Wireshark plugins to
  - Decrypt VoIP calls
  - Export call audio
  - Overview of traffic (Extensions, SMS, DTMF)
  - Common VoIP attacks

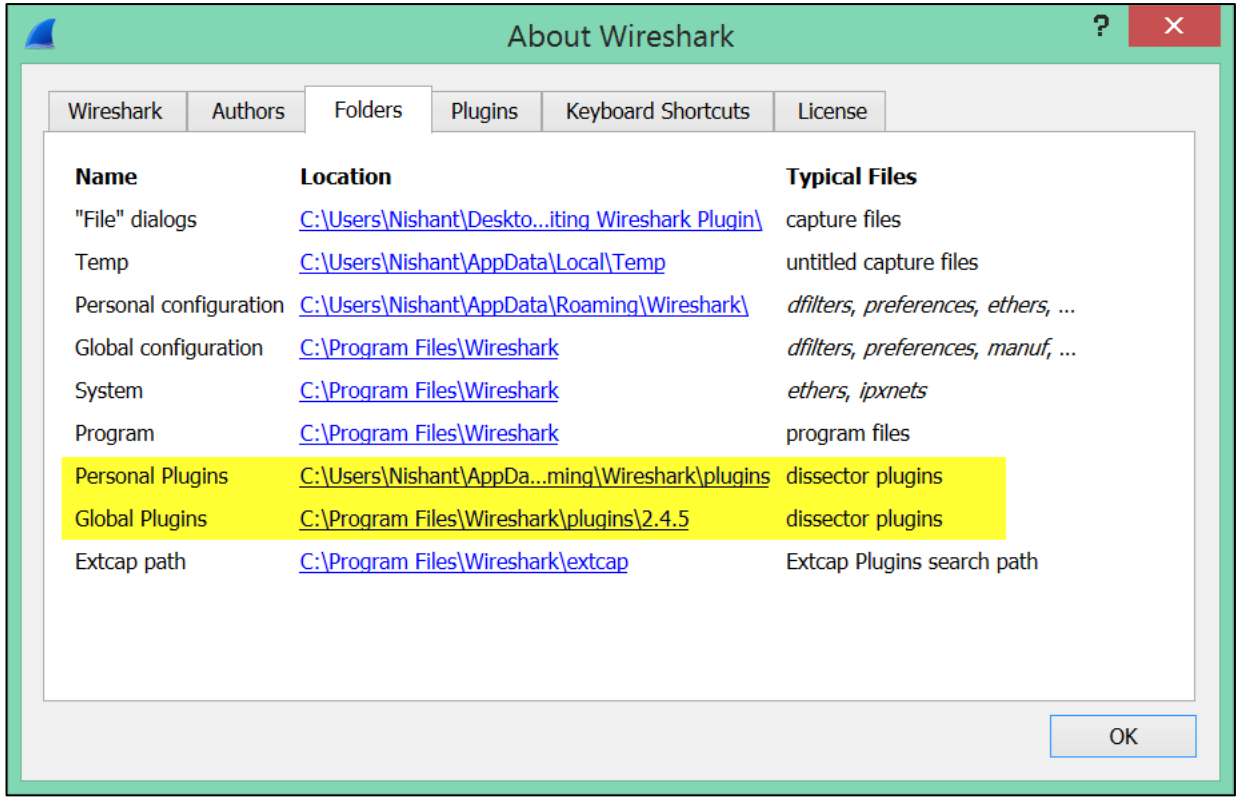
- GPL just like Wireshark

- Github: http://www.github.com/pentesteracademy/voipshark

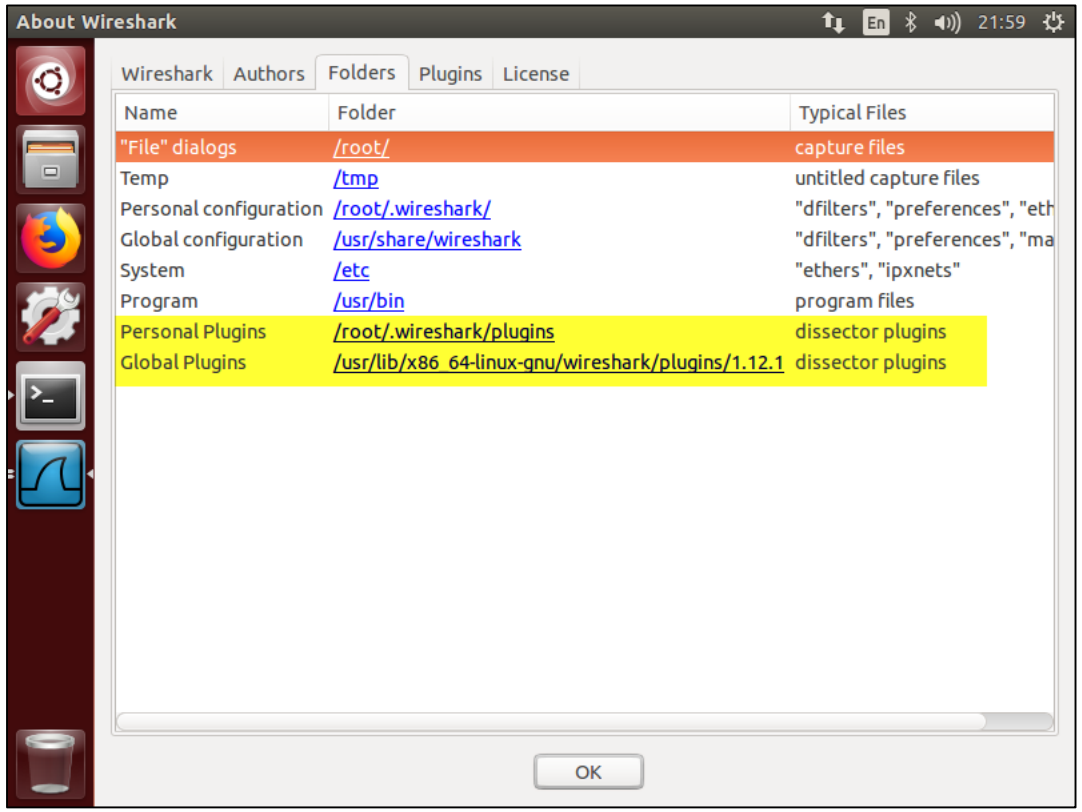
Plugins locations

- Check Help > About Wireshark > Folders

Windows



Ubuntu



Q & A

nishant@attackdefense.com