THE UNIVERSITY OF WAIKATO
*Te Whare Wānanga o Waikato*

University of Waikato
Network Research Group

openLI

# Running a VoIP Intercept

## OpenLI Training: Chapter Twelve


Shane Alcock
University of Waikato
New Zealand
shane.alcock@waikato.ac.nz

# VoIP Intercepts

- We've used the REST API to configure our first VoIP intercept

- Normally that would be the end of our job
  - Mirrored SIP + RTP traffic already appears at the collectors
  - Any future calls for our target will get intercepted

# VoIP Intercepts

- The training lab is a bit different
  - Not tapping an operational VoIP network
  - We have to generate our own traffic for testing

# tracereplay

- Libtrace tool that can replay pcaps onto a network interface
  - IP addresses, ports, packet content unchanged
  - Replays packets at same rate as they were captured
    - `-X` option can be used to increase rate
  - Perfect for controlled testing of OpenLI

```
tracereplay <pcap file> ring:<interface name>
```

# tracereplay

- Collector container has a directory: `pcaps/`
  - There you will find some replayable traffic for the training lab

- Use tracereplay to replay the traffic on to interface `eth2`
  - You'll remember this as our capture interface
  - Don't worry -- the replayed traffic will go nowhere
    - It will be capturable on the sending interface, though

# Experiment Checklist

- ❑ Provisioner service is running on openli-provisioner
- ❑ Collector service is running on openli-collector
- ❑ Mediator service is running on openli-mediator
- ❑ tracepktdump for HI2 is running on openli-agency
- ❑ tracepktdump for HI3 is running on openli-agency

# Replaying VoIP Traffic

- On the collector container, run:

```
tracereplay /home/openli-coll/pcaps/tcpsip_voip.pcap ring:eth2
```

- Be patient -- the call will take a minute to complete

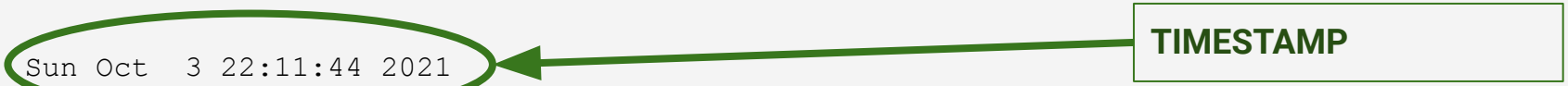
# Examining HI2 Output

- Switch to your terminals on openli-agency
  - Let's look at the tracepktdump output for HI2 first
  - I'll walk you through the **last** displayed record
    - The output is large, so I'll do it in several parts
    - Feel free to scroll back further and examine others as well

# Examining HI2 Output

```
Sun Oct  3 22:11:44 2021
 Capture: Packet Length: 735/735 Direction Value: -1
 ETSILI: pS-PDU:
 ETSILI:   PSHeader:
 ETSILI:     li-psDomainId: 0.4.0.2.2.5.1.17.0
 ETSILI:     lawfulInterceptionIdentifier: TESTVOIP001
 ETSILI:     authorizationCountryCode: NZ
 ETSILI:     communicationIdentifier:
 ETSILI:       networkIdentifier:
 ETSILI:         operatorIdentifier: WAND
 ETSILI:         networkElementIdentifier: openli-lab
 ETSILI:       communicationIdentityNumber: 1796335989
 ETSILI:       deliveryCountryCode: NZ
 ETSILI:     sequenceNumber: 7
 ETSILI:     interceptionPointID: col001
 ETSILI:     microSecondTimeStamp:
 ETSILI:       seconds: 1633299104
 ETSILI:       microSeconds: 441138
 ETSILI:     timeStampQualifier: timeOfInterception
```

# Examining HI2 Output



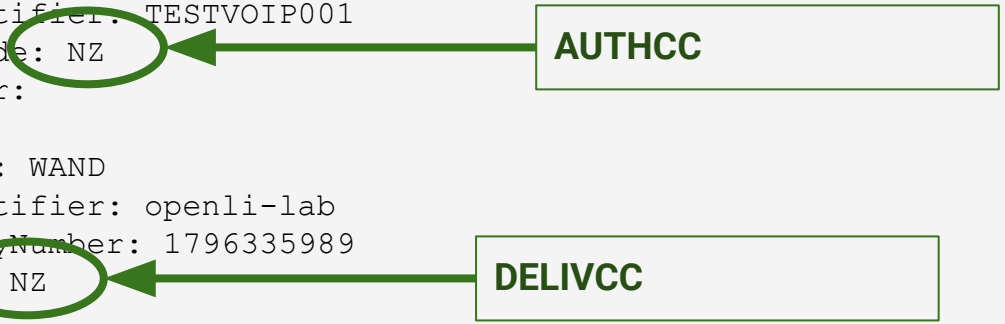

```
Sun Oct  3 22:11:44 2021
Capture: Packet Length: 735/735 Direction Value: -1
ETSILI: pS-PDU:
ETSILI:   PSHeader:
ETSILI:     li-psDomainId: 0.4.0.2.2.5.1.17.0
ETSILI:     lawfulInterceptionIdentifier: TESTVOIP001
ETSILI:     authorizationCountryCode: NZ
ETSILI:     communicationIdentifier:
ETSILI:       networkIdentifier:
ETSILI:         operatorIdentifier: WAND
ETSILI:         networkElementIdentifier: openli-lab
ETSILI:       communicationIdentityNumber: 1796335989
ETSILI:       deliveryCountryCode: NZ
ETSILI:     sequenceNumber: 7
ETSILI:     interceptionPointID: col001
ETSILI:     microSecondTimeStamp:
ETSILI:       seconds: 1633299104
ETSILI:       microSeconds: 441138
ETSILI:     timeStampQualifier: timeOfInterception
```

# Examining HI2 Output

```
Sun Oct  3 22:11:44 2021
 Capture: Packet Length: 735/735 Direction Value: -1
 ETSILI: pS-PDU:
 ETSILI:   PSHeader:
 ETSILI:     li-psDomainId: 0.4.0.2.2.5.1.17.0
 ETSILI:     lawfulInterceptionIdentifier: TESTVOIP001
 ETSILI:     authorizationCountryCode: NZ
 ETSILI:     communicationIdentifier:
 ETSILI:       networkIdentifier:
 ETSILI:         operatorIdentifier: WAND
 ETSILI:         networkElementIdentifier: openli-lab
 ETSILI:       communicationIdentityNumber: 1796335989
 ETSILI:       deliveryCountryCode: NZ
 ETSILI:     sequenceNumber: 7
 ETSILI:     interceptionPointID: col001
 ETSILI:     microSecondTimeStamp:
 ETSILI:       seconds: 1633299104
 ETSILI:       microSeconds: 441138
 ETSILI:     timeStampQualifier: timeOfInterception
```

# Examining HI2 Output

```
Sun Oct  3 22:11:44 2021
 Capture: Packet Length: 735/735 Direction Value: -1
 ETSILI: pS-PDU:
 ETSILI:   PSHeader:
 ETSILI:     li-psDomainId: 0.4.0.2.2.5.1.17.0
 ETSILI:     lawfulInterceptionIdentifier: TESTVOIP001
 ETSILI:     authorizationCountryCode: NZ
 ETSILI:     communicationIdentifier:
 ETSILI:       networkIdentifier:
 ETSILI:         operatorIdentifier: WAND
 ETSILI:         networkElementIdentifier: openli-lab
 ETSILI:       communicationIdentityNumber: 1796335989
 ETSILI:       deliveryCountryCode: NZ
 ETSILI:     sequenceNumber: 7
 ETSILI:     interceptionPointID: col001
 ETSILI:     microSecondTimeStamp:
 ETSILI:       seconds: 1633299104
 ETSILI:       microSeconds: 441138
 ETSILI:     timeStampQualifier: timeOfInterception
```

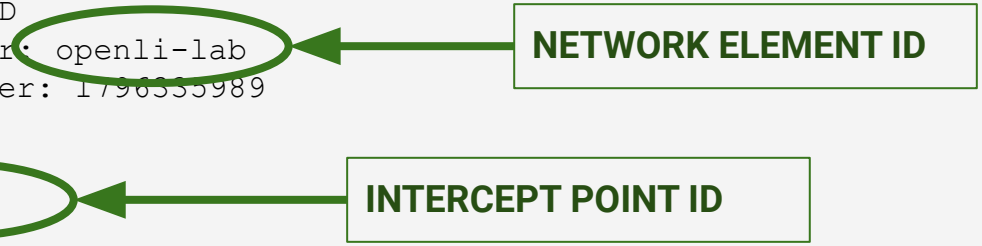


# Examining HI2 Output

```
Sun Oct  3 22:11:44 2021
 Capture: Packet Length: 735/735 Direction Value: -1
 ETSILI: pS-PDU:
 ETSILI:   PSHeader:
 ETSILI:     li-psDomainId: 0.4.0.2.2.5.1.17.0
 ETSILI:     lawfulInterceptionIdentifier: TESTVOIP001
 ETSILI:     authorizationCountryCode: NZ
 ETSILI:     communicationIdentifier:
 ETSILI:       networkIdentifier:
 ETSILI:         operatorIdentifier: WAND
 ETSILI:         networkElementIdentifier: openli-lab
 ETSILI:       communicationIdentityNumber: 1796335989
 ETSILI:       deliveryCountryCode: NZ
 ETSILI:     sequenceNumber: 7
 ETSILI:     interceptionPointID: col001
 ETSILI:     microSecondTimeStamp:
 ETSILI:       seconds: 1633299104
 ETSILI:       microSeconds: 441138
 ETSILI:     timeStampQualifier: timeOfInterception
```

# Examining HI2 Output

```
Sun Oct  3 22:11:44 2021
 Capture: Packet Length: 735/735 Direction Value: -1
 ETSILI: pS-PDU:
 ETSILI:   PSHeader:
 ETSILI:     li-psDomainId: 0.4.0.2.2.5.1.17.0
 ETSILI:     lawfulInterceptionIdentifier: TESTVOIP001
 ETSILI:     authorizationCountryCode: NZ
 ETSILI:     communicationIdentifier:
 ETSILI:       networkIdentifier:
 ETSILI:         operatorIdentifier: WAND
 ETSILI:         networkElementIdentifier: openli-lab
 ETSILI:       communicationIdentityNumber: 1796335989
 ETSILI:       deliveryCountryCode: NZ
 ETSILI:     sequenceNumber: 7
 ETSILI:     interceptionPointID: col001
 ETSILI:     microSecondTimeStamp:
 ETSILI:       seconds: 1633299104
 ETSILI:       microSeconds: 441138
 ETSILI:     timeStampQualifier: timeOfInterception
```



# Examining HI2 Output

```
Sun Oct  3 22:11:44 2021
 Capture: Packet Length: 735/735 Direction Value: -1
 ETSILI: pS-PDU:
 ETSILI:   PSHeader:
 ETSILI:     li-psDomainId: 0.4.0.2.2.5.1.17.0
 ETSILI:     lawfulInterceptionIdentifier: TESTVOIP001
 ETSILI:     authorizationCountryCode: NZ
 ETSILI:     communicationIdentifier:
 ETSILI:       networkIdentifier:
 ETSILI:         operatorIdentifier: WAND
 ETSILI:         networkElementIdentifier: openli-lab
 ETSILI:       communicationIdentityNumber: 1796335989
 ETSILI:       deliveryCountryCode: NZ
 ETSILI:     sequenceNumber: 7
 ETSILI:     interceptionPointID: col001
 ETSILI:     microSecondTimeStamp:
 ETSILI:       seconds: 1633299104
 ETSILI:       microSeconds: 441138
 ETSILI:     timeStampQualifier: timeOfInterception
```

# Examining HI2 Output

```
Sun Oct  3 22:11:44 2021
 Capture: Packet Length: 735/735 Direction Value: -1
 ETSILI: pS-PDU:
 ETSILI:   PSHeader:
 ETSILI:     li-psDomainId: 0.4.0.2.2.5.1.17.0
 ETSILI:     lawfulInterceptionIdentifier: TESTVOIP001
 ETSILI:     authorizationCountryCode: NZ
 ETSILI:     communicationIdentifier:
 ETSILI:       networkIdentifier:
 ETSILI:         operatorIdentifier: WAND
 ETSILI:         networkElementIdentifier: openli-lab
 ETSILI:       communicationIdentityNumber: 1796335989
 ETSILI:       deliveryCountryCode: NZ
 ETSILI:     sequenceNumber: 7
 ETSILI:     interceptionPointID: col001
 ETSILI:     microSecondTimeStamp:
 ETSILI:       seconds: 1633299104
 ETSILI:       microSeconds: 441138
 ETSILI:     timeStampQualifier: timeOfInterception
```

# Examining HI2 Output

```
Sun Oct  3 22:11:44 2021
 Capture: Packet Length: 735/735 Direction Value: -1
 ETSILI: pS-PDU:
 ETSILI:   PSHeader:
 ETSILI:     li-psDomainId: 0.4.0.2.2.5.1.17.0
 ETSILI:     lawfulInterceptionIdentifier: TESTVOIP001
 ETSILI:     authorizationCountryCode: NZ
 ETSILI:     communicationIdentifier:
 ETSILI:       networkIdentifier:
 ETSILI:         operatorIdentifier: WAND
 ETSILI:         networkElementIdentifier: openli-lab
 ETSILI:       communicationIdentityNumber: 1796335989
 ETSILI:       deliveryCountryCode: NZ
 ETSILI:     sequenceNumber: 7
 ETSILI:     interceptionPointID: col001
 ETSILI:     microSecondTimeStamp:
 ETSILI:       seconds: 1633299104
 ETSILI:       microSeconds: 441138
 ETSILI:     timeStampQualifier: timeOfInterception
```

**TIMESTAMP (again)**

# Examining HI2 Output

- Now let’s look at the IRI Payload

# Examining HI2 Output

```
ETSILI:   Payload:
ETSILI:     iRIPayloadSequence:
ETSILI:       IRIPayload:
ETSILI:       iRIType: IRI-Report
ETSILI:       iRIContents:
ETSILI:            iPMMIRI:
ETSILI:            iPMMIRIObjId: .5.5.6.1
ETSILI:            iPMMIRIContents:
ETSILI:              sIPMessage:
ETSILI:                ipSourceAddress:
ETSILI:                  iP-type: IPv4
ETSILI:                  iP-value:
ETSILI:                    iPBinaryAddress: 10.100.50.65
ETSILI:                  iP-assignment: Not Known
ETSILI:                  iPv4SubnetMask: 255.255.255.255
ETSILI:                ipDestinationAddress:
ETSILI:                  iP-type: IPv4
ETSILI:                  iP-value:
ETSILI:                    iPBinaryAddress: 192.168.1.73
ETSILI:                  iP-assignment: Not Known
ETSILI:                  iPv4SubnetMask: 255.255.255.255
```

# Examining HI2 Output

```
ETSILI:   Payload:
ETSILI:     iRIPayloadSequence:
ETSILI:       IRIPayload:
ETSILI:       iRIType: IRI-Report
ETSILI:       iRIContents:
ETSILI:            iPMMIRI:
ETSILI:            iPMMIRIObjId: .5.5.6.1
ETSILI:            iPMMIRIContents:
ETSILI:              sIPMessage:
ETSILI:                ipSourceAddress:
ETSILI:                  iP-type: IPv4
ETSILI:                  iP-value:
ETSILI:                    iPBinaryAddress: 10.100.50.65
ETSILI:                  iP-assignment: Not Known
ETSILI:                  iPv4SubnetMask: 255.255.255.255
ETSILI:                ipDestinationAddress:
ETSILI:                  iP-type: IPv4
ETSILI:                  iP-value:
ETSILI:                    iPBinaryAddress: 192.168.1.73
ETSILI:                  iP-assignment: Not Known
ETSILI:                  iPv4SubnetMask: 255.255.255.255
```

# Examining HI2 Output

```
ETSILI:   Payload:
ETSILI:     iRIPayloadSequence:
ETSILI:       IRIPayload:
ETSILI:       iRIType: IRI-Report
ETSILI:       iRIContents:
ETSILI:            iPMMIRI:
ETSILI:            iPMMIRIObjId: .5.5.6.1
ETSILI:            iPMMIRIContents:
ETSILI:              sIPMessage:
ETSILI:                ipSourceAddress:
ETSILI:                  iP-type: IPv4
ETSILI:                  iP-value:
ETSILI:                    iPBinaryAddress: 10.100.50.65
ETSILI:                  iP-assignment: Not Known
ETSILI:                  iPv4SubnetMask: 255.255.255.255
ETSILI:                ipDestinationAddress:
ETSILI:                  iP-type: IPv4
ETSILI:                  iP-value:
ETSILI:                    iPBinaryAddress: 192.168.1.73
ETSILI:                  iP-assignment: Not Known
ETSILI:                  iPv4SubnetMask: 255.255.255.255
```

# Examining HI2 Output

- Lastly, there is the SIP payload itself
  - Too much to fit on a slide nicely
- SIP is a textual protocol, so you can interpret yourself

# Examining HI2 Output

- Some things to look out for in this example
  - Commands and reply codes
    - INVITE, BYE, REGISTER, 200 OK
  - Target phone number: 12345678910
  - The other participant: 0800000000
  - The realm: example.com
  - IP addresses and port numbers in the SDP content
  - When Call ID changes, so does the CIN in the header

# Examining HI3 Output

- Now let’s take a look at the HI3 CCs we received
  - Again, we’re going to focus on the **last** record

# Examining HI3 Output

```
Sun Oct  3 22:11:38 2021
 Capture: Packet Length: 332/332 Direction Value: -1
 ETSILI: pS-PDU:
 ETSILI:   PSHeader:
 ETSILI:     li-psDomainId: 0.4.0.2.2.5.1.17.0
 ETSILI:     lawfulInterceptionIdentifier: TESTVOIP001
 ETSILI:     authorizationCountryCode: NZ
 ETSILI:     communicationIdentifier:
 ETSILI:       networkIdentifier:
 ETSILI:         operatorIdentifier: WAND
 ETSILI:         networkElementIdentifier: openli-lab
 ETSILI:       communicationIdentityNumber: 138071930
 ETSILI:       deliveryCountryCode: NZ
 ETSILI:     sequenceNumber: 3949
 ETSILI:     interceptionPointID: col001
 ETSILI:     microSecondTimeStamp:
 ETSILI:       seconds: 1633299098
 ETSILI:       microSeconds: 131200
 ETSILI:     timeStampQualifier: timeOfInterception
```

# Examining HI3 Output

```
Sun Oct  3 22:11:38 2021
 Capture: Packet Length: 332/332 Direction Value: -1
 ETSILI: pS-PDU:
 ETSILI:   PSHeader:
 ETSILI:     li-psDomainId: 0.4.0.2.2.5.1.17.0
 ETSILI:     lawfulInterceptionIdentifier: TESTVOIP001
 ETSILI:     authorizationCountryCode: NZ
 ETSILI:     communicationIdentifier:
 ETSILI:       networkIdentifier:
 ETSILI:         operatorIdentifier: WAND
 ETSILI:         networkElementIdentifier: openli-lab
 ETSILI:       communicationIdentityNumber: 138071930
 ETSILI:       deliveryCountryCode: NZ
 ETSILI:     sequenceNumber: 3949
 ETSILI:     interceptionPointID: col001
 ETSILI:     microSecondTimeStamp:
 ETSILI:       seconds: 1633299098
 ETSILI:       microSeconds: 131200
 ETSILI:     timeStampQualifier: timeOfInterception
```

# Examining HI3 Output

```
Sun Oct  3 22:11:38 2021
 Capture: Packet Length: 332/332 Direction Value: -1
 ETSILI: pS-PDU:
 ETSILI:   PSHeader:
 ETSILI:     li-psDomainId: 0.4.0.2.2.5.1.17.0
 ETSILI:     lawfulInterceptionIdentifier: TESTVOIP001
 ETSILI:     authorizationCountryCode: NZ
 ETSILI:     communicationIdentifier:
 ETSILI:       networkIdentifier:
 ETSILI:         operatorIdentifier: WAND
 ETSILI:         networkElementIdentifier: openli-lab
 ETSILI:       communicationIdentityNumber: 138071930
 ETSILI:       deliveryCountryCode: NZ
 ETSILI:     sequenceNumber: 3949
 ETSILI:     interceptionPointID: col001
 ETSILI:     microSecondTimeStamp:
 ETSILI:       seconds: 1633299098
 ETSILI:       microSeconds: 131200
 ETSILI:     timeStampQualifier: timeOfInterception
```

# Examining HI3 Output

- The CC Payload
  - Not a lot interesting going on here, but for the sake of completion

# Examining HI3 Output

```
ETSILI:   Payload:
ETSILI:     cCPayloadSequence:
ETSILI:       CCPayload:
ETSILI:       payloadDirection: toTarget
ETSILI:       cCContents:
ETSILI:            iPMMCC:
ETSILI:            iPMMCCObjId: .5.5.6.2
ETSILI:            frameType: ipFrame
ETSILI:            mMCCprotocol: rTP
ETSILI:              mMCCContents: ...
```

# Examining HI3 Output

```
ETSILI:   Payload:
ETSILI:     cCPayloadSequence:
ETSILI:       CCPayload:
ETSILI:       payloadDirection: toTarget
ETSILI:       cCContents:
ETSILI:            iPMMCC:
ETSILI:            iPMMCCObjId: .5.5.6.2
ETSILI:            frameType: ipFrame
ETSILI:            mMCCprotocol: rTP
ETSILI:              mMCCContents: ...
```

# Examining HI3 Output

```
ETSILI:   Payload:
ETSILI:     cCPayloadSequence:
ETSILI:       CCPayload:
ETSILI:       payloadDirection: toTarget
ETSILI:       cCContents:
ETSILI:            iPMMCC:
ETSILI:            iPMMCCObjId: .5.5.6.2
ETSILI:            frameType: ipFrame
ETSILI:            mMCCprotocol: rTP
ETSILI:              mMCCContents: ...
```

# Examining HI3 Output

- The captured RTP content itself
  - Includes IP / UDP headers, plus application payload
  - RTP is binary encoded, so we won't be able to interpret that

# Examining HI3 Output

```
 IP: Header Len 20 Ver 4 DSCP 00 ECN 0 Total Length 200
 IP: Id 20428 Fragoff 0 DONT_FRAG
 IP: TTL 55 Proto 17 Checksum 62658
 IP: Source 10.100.50.65 Destination 192.168.1.73
 UDP: Source 47854 Dest 5000
 UDP: Len 180 Checksum 44083
unknown protocol udp/5000
 Unknown Protocol: 5000
  80 08 87 06 4a 47 fa 12 14 a5 00 12 d5 d5 55 55      ....JG........UU
  55 55 55 55 d5 d5 55 55 55 55 55 55 d5 d5 55 55      UUUU..UUUUUU..UU
  55 55 55 55 55 55 55 55 55 55 55 55 55 55 d5 d5      UUUUUUUUUUUUUU..
  55 55 55 55 55 55 55 55 55 55 55 55 54 54 54 54      UUUUUUUUUUUUTTTT
  54 54 55 55 55 55 d5 d5 55 55 55 55 55 55 55 55      TTUUUU..UUUUUUUU
  55 55 55 55 55 55 d5 d5 d5 d5 55 55 d5 d5 d5 d5      UUUUUU....UU....
  55 55 d5 d5 d5 d5 55 55 54 54 55 55 55 55 d5 d5      UU....UUTTUUUU..
  d5 d5 55 55 54 54 54 54 54 54 54 54 55 55 54 54      ..UUTTTTTTTTUUTT
  55 55 54 54 55 55 55 55 54 54 54 54 54 54 54 54      UUTTUUUUTTTTTTTT
  55 55 55 55 55 55 55 55 55 55 55 55 d5 d5 55 55      UUUUUUUUUUUU..UU
  55 55 55 55 d5 d5 d5 d5 55 55 d5 d5                  UUUU....UU..
```

# Examining HI3 Output

```
 IP: Header Len 20 Ver 4 DSCP 00 ECN 0 Total Length 200
 IP: Id 20428 Fragoff 0 DONT_FRAG
 IP: TTL 55 Proto 17 Checksum 62650
 IP: Source 10.100.50.65 Destination 192.168.1.73
 UDP: Source 47854 Dest 5000
 UDP: Len 180 Checksum 44083
unknown protocol udp/5000
 Unknown Protocol: 5000
  80 08 87 06 4a 47 fa 12 14 a5 00 12 d5 d5 55 55      ....JG........UU
  55 55 55 55 d5 d5 55 55 55 55 55 55 d5 d5 55 55      UUUU..UUUUUU..UU
  55 55 55 55 55 55 55 55 55 55 55 55 55 55 d5 d5      UUUUUUUUUUUUUU..
  55 55 55 55 55 55 55 55 55 55 55 55 54 54 54 54      UUUUUUUUUUUUTTTT
  54 54 55 55 55 55 d5 d5 55 55 55 55 55 55 55 55      TTUUUU..UUUUUUUU
  55 55 55 55 55 55 d5 d5 d5 d5 55 55 d5 d5 d5 d5      UUUUUU....UU....
  55 55 d5 d5 d5 d5 55 55 54 54 55 55 55 55 d5 d5      UU....UUTTUUUU..
  d5 d5 55 55 54 54 54 54 54 54 54 54 55 55 54 54      ..UUTTTTTTTTUUTT
  55 55 54 54 55 55 55 55 54 54 54 54 54 54 54 54      UUTTUUUUTTTTTTTT
  55 55 55 55 55 55 55 55 55 55 55 55 d5 d5 55 55      UUUUUUUUUUUU..UU
  55 55 55 55 d5 d5 d5 d5 55 55 d5 d5                  UUUU....UU..
```

**IP ADDRESSES AND PORTS**

# Wrap Up

- We can perform intercepts on the training lab
  - Use tracereplay to replicate traffic from pcaps
  - Use tracepktdump to receive / dump encoded ETSI records

- Explored some ETSI records for VoIP intercepts
  - Confirmed our configuration has been applied
  - Identified the “useful” record content for debug / validation

# Next Time

- Configuring an IP intercept
  - Mostly similar to VoIP, but a few key differences