Uživatelská dokumentace k Prototypu mikrosondy (uSondy) pro monitorování IPv6 provozu

Brno, 2015

# Obsah

Protokoly pro export zachycené komunikace
Formát dat exportovaných přes TCP 3
Formát dat exportovaných přes UDP 3
Formát Direct export protokolu 3
Vstupní Ethernet II rámec 4
Výstupní Ethernet II rámec 4
Čelní panel uSondy
Zapojení 4
Zapojení - TCP export
Zapojení - UDP/Direct export
Nastavení IP adresy po spuštění6
Nastavení uSondy
Nastavení času
Konfigurace módu7
Konfigurace SLIS režimu
Konfigurace TCP exportu
Konfigurace UDP exportu
Uložení výchozí konfigurace
Nastavení odposlechů 10
Statistiky
LED diody na čelním panelu
Tlačítko na čelním panelu12
Zachycení dat z uSondy
Příklady použití
Topologie
Příklad 1 - zachycení veškeré komunikace, export přes TCP13
Konfigurace14
Export do PCAPu15
Prozkoumání zachycené komunikace15
Příklad 2 - zachycení konkrétní IP17

Konfigurace	
Export do PCAPu	
Prozkoumání zachycené komunikace	19
Příklad 3 - zachycení veškeré komunikace, export přes UDP	20
Konfigurace	20
Export do PCAPu	21
Prozkoumání zachycené komunikace	22

# Protokoly pro export zachycené komunikace

Komunikaci lze exportovat 3 způsoby. Prvním je export přes TCP spojení, které zajistí, že veškeré exportované pakety budou doručeny na ukládací zařízení. Druhým způsobem je export UDP protokolem, zde hrozí možnost, že exportované pakety budou po cestě zahozeny, nebo dorazí v jiném pořadí než byly odeslány. Třetí možností je tzv. Direct export, v tomto případě jsou pakety exportovány téměř beze změny a tedy ukládací zařízení musí být připojeny přímo k uSondě, jinak exportované pakety vůbec nedorazí.

Protokol	Rychlost	Překročení MTU	Ztráta paketu	Poznámka
ТСР	300Mb/s	NE	NE	Vhodné při záchytu filtrované komunikace
UDP	1Gb/s	ANO	ANO	Vhodné při záchytu veškeré komunikace na lince
Direct Export	1Gb/s	NE	NE	Úložné zařízení musí být připojeno přímo k uSondě

## Formát dat exportovaných přes TCP

Před každý zachycený paket je vložena INI3 hlavička:

0	1	2	3	1	
Blob	Size   Timest Timest	Interface amp_0 (unix) amp_1 (ns p	+   Reserved řesnost)	+     	
RID	_0	RII	_1	I	
Blob Size	Velił	cost zachyce	ného rámce		(2 bytes)
Interface	Rozhi	aní na ktere	ém byl příc	hozí rámec zachycen	(1 bytes)
Reserved	Rezei	vováno pro l	oudoucí pou	žití	(1 bytes)
Timestamp	Časov	vá značka př:	ichodu pake	tu ze sítě na rozhraní	(4 + 4 bytes)
RID 0/1	Ident	ifikátor pra	avidla, pod	le kterého byl paket vybrán pro export	(2 + 2 bytes)

INI3 hlavička + zachycený paket tvoří tzv. superpaket. Několik superpaketů je následně spojeno dohromady a odesláno přes TCP jako aplikační data. Pozn. může dojít k situaci, kdy v 1 TCP paketu je několik superpaketů, kde poslední superpaket není celý. Zbytek tohoto superpaketu je odeslán v následujícím TCP paketu.

### Formát dat exportovaných přes UDP

Před každý zachycený paket je vložena INI3 hlavička jako v případě exportu přes TCP. Následně každý odeslaný UDP paket obsahuje právě 1 superpaket. Pokud je velikost původního zachyceného paketu + velikost INI3 hlavičky větší než MTU cesty, přes kterou UDP paket musí projít, pak ho nějaký síťový prvek po cestě zahodí.

## Formát Direct export protokolu

U exportovaných paketů je nahrazena zdrojová a cílová MAC adresa MACINI3 hlavičkou. Kvůli tomu je potřeba připojit ukládací zařízení přímo k mikrosondě.

## Vstupní Ethernet II rámec

+----+ | DA | SA | Type | Data | FCS | ---+----+----+ +---+---+--Destination MAC Address (6 bytes) DA Source MAC Address (6 bytes) SA Protocol Type (2 bytes) Туре Data Protocol Data (46 - 1500 bytes) FCS Frame Checksum (4 bytes)

## Výstupní Ethernet II rámec

+++   INI3   T +++ / \   \	++ ype   Data   FCS   +			
	MACINI3			
++-   0   ++-	1   2	3	+	
Sequence n   	umber   Interface Timestamp_0 (unix) Timestamp_1 (ns pře	Reserved snost)		
Sequence numbe Interface Reserved Timestamp	r 16B neznaménkové č Rozhraní na kterém Rezervováno pro bu Časová značka příc	íslo, označu byl příchoz doucí použit hodu paketu	uje pořadové číslo zachyceného rámce zí rámec zachycen tí ze sítě na rozhraní	(2 bytes) (1 bytes) (1 bytes) (4 + 4 bytes)

# Čelní panel uSondy



Obrázek 1: Čelní panel

#### Administrační port (Neoznačený port) Výstupní port (A) Odposlechové vstupní porty (C,D)

Po připojení napájecího napětí pomocí externího zdroje se uSonda spustí a zhruba do 30 sekund nabootuje operační systém a automaticky se spustí všechny potřebné služby.

# Zapojení

Konfigurace uSondy se provadí přes **Administrační port**. Odposlouchávaná linka je vždy připojena přes ethernetový TAP do portů **C,D**. Způsob připojení zařízení, na které se odchycená komunikace bude ukládat, záleží na nastavení uSondy.

# Zapojení - TCP export



**Obrázek 2: TCP export** 

Zapojení - UDP/Direct export



**Obrázek 3: UDP/Direct export** 

# Nastavení IP adresy po spuštění

Na SD kartě uSondy je soubor **settings**, ve kterém je možné nastavit IP adresu, která se přiřadí **Administračnímu portu (Neoznačený port)**. Výchozí obsah souboru:

```
#This option set default IP adress
# Examples
# IPADDRESS=10.10.10.10/24 - after boot on ETH1 will be set IP 10.10.10.10 255.255.255.0
# IPADDRESS=dhcp - after boot IP adress on ETH1 will be received from DHCP server
IPADDRESS=dhcp
```

Pozn. řádky začínající # jsou komentáře a na funkčnost nemají vliv

Položku **IPADRESS** je možné nastavit na řetězec dhcp, kdy IP adresa se získá přes dhcp protokol. Alternativně je možné nastavit konkrétní IP adresu s délkou prefixu (např. 192.18.0.1/24)

# Nastavení uSondy

uSonda má dostupné webové rozhraní přes na **Administračním portu**. IP adresa tohoto portu je nastavitelná viz Nastavení IP adresy po spuštění.

Přístupové údaje na webové rozhraní:

```
Uživatelské jméno: admin
Heslo: R6sataJpuj
```

Konfigurace způsobu exportování a nastavení času na uSondě se provádí v nabídce **Configure**. Nastavení filtrovacích pravidel pro záchyt komunikace je dostupné na stránce **Interceptions**.

## Nastavení času

Po zapnutí je potřeba nastavit aktuální čas, tak aby časová razítka, která se přidělují zachyceným paketům, odpovídali skutečnosti. Všechny časové údaje, které uSonda používá jsou v **UTC+0**.

Čas je možné nastavit 3 způsoby:

- Manuální (Manually) Ruční nastavení data a času
- **NTP** Čas se získá ze vzdáleného NTP serveru (vyžaduje funkční připojení k Internetu skrz port neoznačený port)
- Automatické (Get from configuration PC) Použije se aktuální čas, který je nastaven na počítači, ze kterého se právě uSonda konfiguruje

Nastavení se provede stiskem tlačítka Set time.

Time settings	
Time source: Manually ด NTP ດ Get from configuration PC ∩ <sup>require enabled</sup> JavaScript	
Set time	
Date: 10.1.2015 Format DD.MM.YYYY	
Time: 12:48:00 Format HH:MM:SS	
Set time	

#### Obrázek 4: Příklad manuálního nastavení data a času

## Konfigurace módu

uSonda lze nakonfigurovat do jednoho ze 3 režimů.

- **Standalone** Zachycení komunikace, která odpovídá nakonfigurovaným filtrovacím pravidlům. Konfigurace filtrovacích pravidel se provádí přímo na uSondě.
- **SLIS** uSonda se připojí k systému SLIS, na kterém jsou nakonfigurovány odposlechy. uSonda zachycená data odešle na zpracování zpět na server se SLISem.
- **Packet capture** U zachycené komunikace neprobíhá filtrování a tedy veškerý zachycený síťový provoz je vyexportován na úložné zařízení.

Každý mód umožňuje export pomocí protokolů TCP a UDP. Direct export je možný použít pouze v režimu Standalone a Packet capture.

### Konfigurace SLIS režimu

Mode select:	Standalone 🔿	SLIS 💿	Packet capture 🔿
--------------	--------------	--------	------------------

CCCI connection	
CCCI Host IP:	10.11.10.71
CCCI Host port:	21105

#### Obrázek 5: Úkázka nastavení režimu SLIS

V tomto režimu je zapotřebí nakonfigurovat spojení se systém SLIS.

CCCI connection - Toto spojení slouží pro získávání filtrovacích pravidel od systému SLIS

- CCCI Host IP IP adresa, na které je SLIS přístupný
- CCCI Host port TCP port, na kterém SLIS naslouchá pro příchozí spojení

#### Konfigurace TCP exportu

Mode configuration
Mode select: Standalone ด SLIS 🔿 Packet capture 🔿
Export protocol select: TCP <ul> <li>UDP <ul> <li>Direct Export </li> </ul> </li> </ul>
Primary TCP export configuration
Destination IP: fe80::201:80ff:fe79:d386
Destination port: 21103
Secondary TCP export: Nothing C All 💿 Fallback C
Secure connection:
SSH port: 5715
Secondary TCP export configuration
Destination IP: 10.11.10.71
Destination port: 21112
Save configuration

#### Obrázek 6: Úkázka nastavení pro komunikaci přes TCP

**Primary TCP export configuration** - Primární nastavení TCP exportu, kam bude zachycená komunikace odesílána

- Destination IP IP adresa zařízení, které bude komunikaci ukládat
- Destination port TCP port, na kterém ukládací zařízení naslouchá
- Secondary TCP export
  - Nothing sekundární ukládání je vypnuto
  - All kopie dat, které se zasílají do SLISu, jsou odeslána na nastavený HDD (konfigurace HDD exportu je stejná jako u režimu Standalone a Packet capture)
  - Fallback na nastavený HDD se začnou odesílat zachycené rámce pouze pokud dojde ke ztrátě spojení s SLISem
- Secure connection vytvoří zabezpečené spojení se serverem, na který se odesílají zachycená data

- Na serveru je potřeba mít uživatele slis
- Uživatel slis umožňuje vzdálené přihlášení pomocí SSH certifikátů
- Soubor /home/slis/.ssh/authorized\_keys obsahuje záznam s dodaným veřejným klíčem

**Secondary TCP export configuration** - Sekundární nastavení TCP exportu, kam bude zachycená komunikace odesílána (aktivace se odvíjí od nastavení *Secondary TCP export* 

- Destination IP IP adresa zařízení, které bude komunikaci ukládat
- Destination port TCP port, na kterém ukládací zařízení naslouchá

### Konfigurace UDP exportu

Mode configuration		
Mode select: Sta	ndalone 💿 SLIS C	Packet capture C
Export protocol sele	ect: TCP O UDP 🖲	Direct Export C
UDP export configuratio	n	
Source IP:	fe80::201:80ff:fe79:f386	
Source port:	20100	
Source MAC:	00:01:80:13:18:AB	
Destination IP:	fe80::201:80ff:fe79:d386	
Destination port:	21103	
Destination MAC:	00:01:80:79:D3:86	
Save configuration		

Obrázek 7: Úkázka nastavení pro komunikaci přes UDP

#### **UDP** export configuration

- Source IP IP adresa, která bude ve výstupním paketu uvedena jako zdrojová
- Source port UDP port, který bude ve výstupním paketu uveden jako zdrojový
- Source MAC MAC adresa, která bude ve výstupním paketu uvedena jako zdrojová
- Destination IP IP adresa zařízení, které bude komunikaci ukládat
- Destination port UDP port, na kterém ukládací zařízení naslouchá
- Destination MAC MAC adresa následujícího síťového zařízení, který leží na cestě k úložnému zařízení

# Uložení výchozí konfigurace

Po zapnutí uSondy je vždy načtena výchozí konfigurace. Pro úpravu této konfigurace slouží tlačítko **Save active configuration as default** na stránce **Configure**. Po stisknutí tohoto tlačítka se uloží aktuálně používaná konfigurace jako výchozí.

Default configuration
Save active configuration as default |

Obrázek 8: Tlačítko pro uložení výchozí konfigurace

# Nastavení odposlechů

Nastavení odposlechů se provádí na stránce Interceptions.

### Přidání odposlechu

- Lawful Interception Identifier textový identifikátor odposlechu (nesmí se shodovat s již probíhajícími, či naplánovanými odposlechy)
- Network Identifier IPv4/IPv6 adresa (případně rozsah zadaný pomocí masky) určující, které pakety budou zachyceny
- Interception start time datum a čas, od kdy bude odposlech se zadanou IPv4/IPv6 adresou platný (formát dd.mm.rrrr [hh:mm])
- Interception end time datum a čas, kdy zadané pravidlo pozbude platnosti a odposlech bude ukončen (formát dd.mm.rrrr [hh:mm])
- **Pozor**: předpokládá se čas zadaný v **UTC+0**

### Odstranění odposlechu

 Nahoře na stránce s odposlechy je možné vidět aktivní odposlechy, případně odposlechy čekající na aktivaci, pro odstranění takového odposlechu stačí kliknout na ikonu křížku ve sloupci Remove

### **Current interceptions**

#### Active interceptions

LIID	NID	Start	End	Remove
Odposlech	'10.11.10.0/24'	Sat Jan 10 00:00:00 2015	Sun Jan 11 00:00:00 2015	×

#### Waiting interceptions

LIID	NID	Start	End	Remove
Neaktivni odposlech	'192.168.7.8'	Sat Jan 10 14:00:00 2015	Sat Jan 10 15:00:00 2015	×

## Add new interception

Lawful Interception Identifier (LIID)	Novy odposlech
Network Identifier (NID)	10.11.10.2 See dedicated page for more details
Interception start time	10.1.2015 14:00 Format: dd.mm.yyyy [HH:MM].
Interception end time	11.1.2015 Format: dd.mm.yyyy [HH:MM]. Note that this time specifies open end of the interception interval, i.e. data from this time will not be intercepted.
	Insert

Obrázek 9: Ukázka nastavení odposlechů

# **Statistiky**

Na stránce Statistics jsou dvě kategorie statistik:

Ethernet statistics - Informuje o počtu přijatých/odeslaných rámců

- Interface 0 = D
- Interface 1 = C
- Output Interface = A

Filter statistics - Udává počet paketů, které zpracovával filtr

- Allowed počet paketů, které byly vyexportováný
- Denied pakety, které byly vyfiltrovány
- Total počet všech paketů, které vstoupily do filtru

# **Ethernet statistics**

Interface 0		Interface 1		Output	
	Received bytes	76390	Received bytes	60650592480	Received
	Received frames	1067	Received frames	882538637	Received
	Send bytes	0	Send bytes	0	Send by
	Send frames	0	Send frames	0	Send fra

Output interface		
Received bytes	0	
Received frames	0	
Send bytes	60653038893	
Send frames	882575286	

## **Filter statistics**

Interfac	e 0	Interface 1		
Allowed	1067	Allowed	882613410	
Denied	0	Denied	0	
Total	1067	Total	882613410	

Obrázek 10: Ukázka statistik

# LED diody na čelním panelu

LED	Funkce

- 0 uSonda je nastavena
- 1 uSonda se nastavuje
- 2 uSonda je nastavena
- 3 uSonda se nastavuje
- 4 uSonda je nastavena
- 5 uSonda se nastavuje
- 6 uSonda je nastavena
- 7 uSonda se nastavuje
- 8 uSonda je nastavena
- 9 uSonda se nastavuje

# Tlačítko na čelním panelu

Při podržení tlačítka cca 10s dojde k restartování uSondy.

# Zachycení dat z uSondy

Pokud je export uSondy nastaven v režimu Direct export, je možné na rozhraní **A** připojit PC a pomocí Wiresharku zobrazit/uložit rámce, které uSonda exportuje. Pro lepší zobrazení a analýzu zachycených paketů je možno využít také plug-in o programu Wireshark. Dostupný je zde: <u>http://www.fit.vutbr.cz/research/view\_product.php?id=398</u>

# Příklady použití

Použité nástroje:

- uSonda verze 1.2
- PC+Linux
- Wireshark 1.12 (<u>https://www.wireshark.org/</u>)
  - INI3 plugin (<u>http://www.fit.vutbr.cz/research/prod/index.php?id=398</u>)
  - INI3SEQ plugin (<u>http://www.fit.vutbr.cz/research/prod/index.php?id=398</u>)
- INI3 dump (<u>http://www.fit.vutbr.cz/research/prod/index.php?id=398</u>)

# Topologie



Obrázek 11: Topologie sítě

# Příklad 1 - zachycení veškeré komunikace, export přes TCP

V tomto příkladu bude ukázáno jak zachytit veškerý provoz, který je do uSondy poslán. Provoz bude uložen na připojeném počítači ve formě pcapu včetně INI3 hlaviček. Export bude prováděn za použití TCP.



Obrázek 12: Zapojení uSondy

## Konfigurace

Po zapnutí uSondy se připojíme na webové rozhraní. Na stránce **Configuration** pokud není vybráno **Get from configuration PC**, tak ho zvolíme a klikneme na tlačítko **Set time**. Nyní je na uSondě nastaven aktuální čas.

Stále na stránce **Configuration** v sekci **Mode configuration** zvolíme **Packet capture**. Tato volba zajistí, exportování veškeré příchozí komunikace. Aby bylo možné navázat TCP spojení s PC, na kterém bude síťový provoz uložen, Export protokol vybereme TCP. Do pole **Destination IP** vložíme 192.168.0.139 a **Destination port** nastavíme na 21112. Secondary TCP export a SSH tunelovaní necháme vypnuté. Nyní klikneme na tlačítko **Save configuration**.

# Configuration

Time settings
Time source: Manually C NTP C Get from configuration PC require enabled JavaScript
Set time
Mode configuration
Mode select: Standalone 🔿 SLIS 🔿 Packet capture ด
Export protocol select: TCP 💿 UDP 🔿 Direct Export 🔿
Primary TCP export configuration
Destination IP: 192.168.0.139
Destination port: 21112
Secondary TCP export: Nothing 💿 All 🔿 Fallback 🔿
Secure connection:
Save configuration
Default configuration Save active configuration as default

#### Obrázek 13: Nastavení uSondy

#### **Export do PCAPu**

Na konfiguračním stroji spustíme nástroj ini3\_dump:

./ini3\_dump -p 21112 -f provoz

Parametr -p aktivuje příjem zachycené komunikace z uSondy na TCP portu 21112 (tento port byl nastaven v konfiguraci uSondy). Parametr -f zajistí, že komunikace bude uložena do souboru *provoz.pcap*. Když máme odchycen dostatek paketů, aplikaci ukončíme stisknutím Ctrl+C.

#### Prozkoumání zachycené komunikace

Protože zachycená komunikace je uložena včetně INI3 hlaviček není možné tento pcap otevřít běžnými nástroji. Pro tento případ byl vytvořen plugin do Wiresharku, který umožňuje takto vytvořený soubor otevřít a zpracovat. Pokud je již ve Wiresharku plugin nainstalován, soubor stačí přímo otevřít bez dalších kroků.

Při vybrání libovolného paketu lze v podrobnostech vidět jednotlivé položky INI3 hlavičky následovaný původním rámcem.

	provez.gcop (Wireshark 3.12.5 (Sit Rev University International)					
	The Edit View Go Capture Analyse Statistics Telephony Tools Internals Help					
Pitteri		* Expre	sional clear in	2 de la companya de l		
No. Time 27 3 220020	Searce	Destination	Protocal	Longth Info 80 BTT Book = 4000/07/00-04-08-14-4a-30 Cook = 30000 Dock = 0x8005		
28 4.735600	ExtremeN_ld:de:30	Broadcast	INES	76 who has 1d7.229.1d.207 Tell 1d7.229.1d.1		
29 4,100299	147.229.14.184	147.229.14.255	INES	76 Source pert: 1534 Destination pert: 1534		
30 4.162300	ExtremeN_ld:de:30	Broadcast	INER	76 Who has 147.229.14.1007 Tell 147.229.14.1		
31 4,173983	147.229.14.228 Estrembli Mirder 20	147,229,14,255 Broadcast	INCO	108 Name guery N8 CH84N00-JUE CH410*		
33 4.480009	Extremely 1d:de:30	Broadcast	INES	70 who has 147.220.14.207 [01] 147.220.14.1 76 who has 147.220.14.1097 [01] 147.200.14.1		
34 4.662310	fe80::3838:971:89c8:2	4402::c	INCO	224 N-SEARCH * HTTP/1.1		
35 5.732206	fe80::204:96ff:fe1d:6	ff02::1:ff35:6a1f	INES	102 Meighbar Solicitation for 2001:67c:1220:80e:cb:b23e:9525:6alf from 00:04:96:1d:4e:30		
36 4,884528	ExtremeN_1d:4e:30	Broadcast	INES	78 Who has 147,229,14,287 Tell 147,229,14,1		
37 5.012412	147.229.14.226	147.229.14.255	INES	100 Name quary HB (MBWHQ2-JUNCOR-LC>		
38 5.162259	147.229.14.138 Extremely 1d:do:30	147,229,14,295	TAE 3	102 Source parts SHEL Destination parts SHEL TO Who has 147 250 14 1077 Tell 147 250 14 1		
40 5,566906	ExtremeN_ld:de:30	Broadcast	INE 3	76 who has 147,229.14.1007 Tell 147,229.14.1		
41 5,682267	147.229.14.217	147,229,14,255	INCO	98 Source pert: 53338 Destination pert: 1947		
42 6,732228	Hewlett79:7e:e5					
43 5.827269	ExtremeN_1d:4e:30	Broadcast	INES	76 Who has 147,229.14.287 Tell 147,229.14.1		
44 6.155368	ExtremeN_1d:4e:30	Broadcast	INED	76 Who has 147,229,14,1077 Tell 147,229,14,1		
45 6.162201	Extremely_10:00:30 147.729.14.228	Broadcast 147, 229, 14, 295	THE 3	78 WTO DBS 147.229-14.207 Tell 147.229.14.1 102 Serve and 152721 S2721 Destination and 152721		
47 6,232302	feBD::70ac:dlld:cedc:	1102:20	INER	220 N-SEARCH + HTTP/1		
AR # #10010	Petromate tal-do-ten	Revaluant	TAPS	ד אז מקר דאו וומד ידחו אר מרר דאר אלא אד		
<ul> <li>Frame 20: 76 byte</li> <li>Internal Network</li> </ul>	s on wire [608 bats], 7 Interface 3	6 bytes captured (60	9 bitej			
Interface: 1						
Reserved: 0x00						
Timestamp [unix]	): Jan 1, 1970 00:05:0	6.464973422 UTC				
MID O: Dx0000						
RID 1: Dx0000	Between the second land	name bet as such as	. mendener M	1.44.44.44.44.44		
- CUMPREX 21, OFCI DELEMENT_DIALEDIAL UNIVERSITE HER DAY, USUS OF BADGARS CONTROLLEDIAL DIALEDIAL DIALEDIAL DIALEDIALEDIALEDIALEDIALEDIALEDIALEDIALE						
· Post and Party Caller	in Figures (Ladeans)					
0000 2: 00 01 02 3	2 01 00 00 fe es b6 lb	00.00.00.002		1488.14		
0050 H H H H H		OR 05 00 01	ND			
0020 08 00 06 04 0	0 01 00 04 95 14 4e 30 0 00 93 e5 0e 4e 00 00	93 e5 0e 01				
0040 00 00 00 00 0						
🖯 🕺 Frame (frame),	76 bytes Pad	iets: 500 - Displayed: 50	0 (100.0%) · Lea	5 time: 0.00.005	Profile: Default	

Obrázek 14: Screenshot wiresharku se zachycenými daty

# Příklad 2 - zachycení konkrétní IP

V tomto případě bude uložen jen vybraný provoz, který bude určen IP adresou odposlouchávaného. Zachycená komunikace bude exportována v protokolem **Direct export**.



Obrázek 15: Zapojení uSondy

#### Konfigurace

Po zapnutí uSondy se připojíme na webové. Na stránce **Configuration** pokud není vybráno **Get from configuration PC**, tak ho zvolíme a klikneme na tlačítko **Set time**. Nyní je na uSondě nastaven aktuální čas.

Stále na stránce **Configuration** v sekci **Mode configuration** zvolíme **Standalone**. Tato volba zajistí, exportování pouze takové komunikace, která je nastavena. **Export protocol** bude **Direct export**. Nyní klikneme na tlačítko **Save configuration**.

# Configuration

Time settings
Time source: Manually C NTP C Get from configuration PC c require enabled JavaScript
Set time
Mode configuration
Mode select: Standalone 🖲 SLIS 🔿 Packet capture 🔿
Export protocol select: TCP C UDP C Direct Export 💿
Save configuration
Default configuration Save active configuration as default
Save active configuration as default

Obrázek 16: Nastavení uSondy

Lawful Interception Identifier (LIID)	Odposlech
Network Identifier (NID)	147.229.14.208       See dedicated page for more details
Interception start time	15.6.2015 Format: dd.mm.yyyy [HH:MM].
Interception end time	15.6.2015 10:00 Format: dd.mm.yyyy [HH:MM]. Note that this time specifies open end of the interception interval, i.e. data from this time will not be intercepted.
	Insert

Obrázek 17: Nastavení odposlechu na uSondě

# Export do PCAPu

Na konfiguračním stroji spustíme nástroj ini3\_dump:

./ini3\_dump -d eth1 -f provoz

Parametr -d aktivuje ukládání všech paketů, které přijdou na rozhraní eth1. Předpokládá se, že uSonda je přímo připojen k PC (bez použití switche/routeru). Parametr -f zajistí, že komunikace bude uložena do souboru provoz.pcap. Když máme odchycen dostatek paketů, aplikaci ukončíme stisknutím Ctrl+C.

#### Prozkoumání zachycené komunikace

V režimu Direct export jsou exportované pakety mírně upraveny, tak že původní MAC adresy jsou přepsány speciální INI3 hlavičkou (detailně viz dokumentace uSondy). I když je teoreticky možné vytvořený soubor otevřít normálními nástroji, které pracují s PCAP soubory, doporučuje se zkoumat soubor otevřený ve Wiresharku s pluginem INI3SEQ. Pokud je již ve Wiresharku plugin nainstalován, soubor stačí přímo otevřít bez dalších kroků.

Při vybrání libovolného paketu lze v podrobnostech vidět jednotlivé položky INI3 hlavičky následovaný původním rámcem.

			provoz,gcap [Wirschark 1.12.5 (Git Rev Unknown from unknown]]	
File Edt View Go Capture Analyze	Statistics Telephony Too	la internala M		
		soonal tare	dual pre-	
In Tom Searce	Destination Annuals an and	Pretocal	Langth Info Nor Millsmöd Levin Belgigert Humania Burrado Leving (Ster-Dobusci Sect-Descu	
107 -1417572982 147.229.14.209	147,229,14,100	TOP	BB 62139-00 (ACK) Segm2477 ArXin8544 Winnet55 Lenno TSwalm10860986 TSecrit24225	
108 1417572932 147.229.14.100	147.229.14.206	TOP	71 80-43130 (PSH, ACK) 540-8544 Adx-2477 Min-411 Lan-5 TSuA-434216 TSuC-1880399	
109 -1417572932 147.229.14.209	147.229.14,100	TCP	- Bit 40139-40 (AX) Segr2477 Actre540 stretts Lared Tsra1+L080581 Tsec+44226 (8) (327 distribution dis VTD) 1	
111 -1417572932 147,229,54,100	147, 229, 14, 200	TOP	500 300-3110 (ACK) 556-550 (ACK) 560-550 (Acrosta Larve TSval+34270 TSecret/60050)	
112 -1417572932 147.229.14.100	147.229.14.208	TOP	222 (TOP segment of a reassestived POU)	
113 -1417572932 147,229,14,298	147.229.14.100	TOP	08. 43139-80 (ACX) 5wg-2891 Ack-8705 Win-677 Len-0 T5wil-1580507 T5wir-34272	
114 -1417572932 147.229.14.100	147,229,14,209	TOP	68 (TOP segment of a reassant)ad POU)	
115 -1417572932 147.229.14.100	147,229,14,298.	TOP	The LTCP segment of a reasonabled POUL	
117 -1417572012 147.229.14.100	147,229,14,208	HTR	on the segment of a reasonable pour	
118 -1417572932 147, 229, 14, 208	147,229,14,100	TCP	51 (1977) 213 400 91 (1982) 2010 10 (1987) 10 (1987) 10 (1977) 10	
119 -1417572932 147.229.14.209	147.229.14,100	TOP	88 40139-80 (ACK) Segr2886 Ack:9718 Winn077 Lenco TSval:1682509 TSecr:04072	
120 -1417572082 147.229.14.208	147.229.14.100	TOP	68 43139-80 [ACK] 5eg-2801 Ack-8720 VGr-877 Len-0 T5val-1580500 T5ecr-34272	
121 -1417572932 147.229.14.208	147.228.14,100	TCP	68 40139-00 (ACX) Segn2891 Ack+0725 Win+677 Len+0 TSval+1588509 TSecr+04272	
122 -1417572932 147.229.14.100	147.229.14.208	TOP	88 80-43128 [FIN, ACK] Sequi Ackul Wirod28 Lerod Texal=34288 TSecTu1072789	
123 -1417572939 147.229.14.100	147,229,14,200	TOP	18 60-41130 (FIN, AK) Sep-1 Ark-1 atm-241 Lam-0 Tsuit-14208 Tsucr-15/2709	
126 - LAUTOTADAY 147 228, 34, 258	147.229.14.100	TOP	(a) GALM-MD (AV) BEDI AND MINDER LETU GVALUERADI DECEMBER (B) GALM-MD (AV) BEDI DECEMBER (DOC) DECEMBER (DOC) (D) CONTRACT (D) CONTR	
126 -1417572934 147,229,14,209	147,229,14,225	NENS	50 Name garry Ne MCROD-Not-	
127 -1417572934 147.229.14.191	147,229,14,208	NEMI	104 None guery response 98 147.228 14.101	
Timestamp (unis): An (5, 2015 Ge Ethermat 33, Sec) 70:05:00;66:02 Transmit Second General Protocol, Sec P	05:120 05:12004204040 UTC (7e:55:e0:05:10:21), De (7:225:14.500 1147.229.1 Nort: 00 1850, Det Perti	t: af:23:00:01 4.100), Det: 1 43139 (43136)	legies (a/i25:00:01:0=001 d7:250:10.250 (147:250:14:200) ;901:0500, ¥(ki:2002; Luni 150	
000         af         30         00         1         50         10<	8         21         66         00         45         00         .4         10           64         65         66         56         .5          2           64         65         66         50         0         18             65         66         20         30         30         20         18             73         32         30         30         30         31         35              76         82         30         30         32         24   <	<ul> <li>H</li></ul>		
000         rf         320         001         445         600         76         56         600         157           000         64         66         72         46         100         66         71         100         <	6 27 06 00 45 00	50 / .6. 8.8 d. 3 d. 3 d. 1.200 C ter Men, 15 201 5 061081 C. Server: chu vo.2 C tha vo.2. c t		

Obrazek 18: Screenshot wiresharku se zachycenymi daty

# Příklad 3 - zachycení veškeré komunikace, export přes UDP

V tomto příkladu bude ukázáno jak zachytit veškerý provoz, který je do uSondy poslán. Provoz bude uložen na připojeném počítači ve formě pcapu **bez** INI3 hlaviček. Export bude prováděn za použití UDP.



Obrázek 19: Zapojení uSondy

## Konfigurace

Po zapnutí uSondy se připojíme na webové rozhraní. Na stránce **Configuration** pokud není vybráno **Get from configuration PC**, tak ho zvolíme a klikneme na tlačítko **Set time**. Nyní je na uSondě nastaven aktuální čas.

Stále na stránce **Configuration** v sekci **Mode configuration** zvolíme **Packet capture**. Tato volba zajistí, exportování veškeré příchozí komunikace. **Export protocol** bude UDP. Jednotlivá pole nastavíme stejně jako na obrázku a konfiguraci uložíme.

# Configuration

Time settings					
Time source: Manually C NTP C Get from configuration PC 💿 require enabled JavaScript					
Set time	Set time				
Mode configuration					
Mode select: Sta	ndalone 🔿 SLIS 🔿 Packet capture ด				
Export protocol sele	ect: TCP o UDP © Direct Export o				
UDP export configuratio	n				
Source IP:	192.168.0.129				
Source port:	20100				
Source MAC:	00:01:80:13:18:AB				
Destination IP:	192.168.0.139				
Destination port:	21112				
Destination MAC:	00:01:80:13:18:CD				
Save configuration					
Default configuration					
Save active configuration as	default				

#### Obrázek 20: Nastavení uSondy

#### **Export do PCAPu**

Na konfiguračním stroji spustíme nástroj ini3\_dump:

./ini3\_dump -u -p 21122 -f provoz -m

Kombinace Parametrů -u a -p aktivuje příjem zachycené komunikace z uSondy na UDP portu 21122 (tento port byl nastaven v konfiguraci uSondy). Parametr -f zajistí, že komunikace bude uložena do souboru *provoz.pcap*. Parametr -m zapíná oříznutí INI3 hlaviček a tedy vytváří standardní PCAP soubor. Když máme odchycen dostatek paketů, aplikaci ukončíme stisknutím Ctrl+C.

# Prozkoumání zachycené komunikace

Soubor *provoz.pcap* normální soubor typu PCAP a tedy je možné jej otevřít běžně dostupnými nástroji, jako je například Wireshark.

						provoz,pcap [Wirschark 1,12.6 (Gilt Rev Unknown from unknown)]	
File			o Capture Analyze Stati	istics Telephony Tools	Internals Help		
۲	0	4 🔳		2. • •			
Fite	4			* Express	ilon <sub>er</sub> Clear Apply	Sive	
No.	Tis	me .	Searce	Destination	Protocal Le	agth Info	
	05 2.	925274	ExtremeN_ld:4e:30	Broadcast	APP	60 Who has 147.229.14.2267 Tell 147.229.14.1	
	80 2.	9202/8	Tesu::/dac:dild:cedc:	104.14.177.7	360P	200 M-MARCH * MINYLLL 115 JUNE 4000 (AND SALES AND SALES AND SALES AND TANK AND TAKEN AND TAKEN AND TAKEN AND TAKEN AND TAKEN AND TAKEN	
	99 2.	958153	Extremely 1d:de:30	Broadcast	APP	50 Who has 107,252,14,927 Tell 147,292,14,1	
	89 3.	926484	2001167(11220180e1613	2001+67c+1220+808++9	8 046	98 Standard query Oxdffa - A graph.facebook.com	
	90 3.	209265	2001:67c:1220:00e:613	2001:67c:1220:000::9	0 045	90 Standard query Ox8665 AAAA graph.facebook.com	
	91 4,	127860	2001:67::1220:808::93	2001:67c:1220:80e:61	3 046	229 Standard query response dxdffa _GMMME apl.facebook.com GMMME star.cl0r.facebook.com A 60.171.290.5	
	92 3.	296450	194.14.177.2	147.229.14.208	TCP	66 4070-39905 [AOX] Sept. Ack-075 Win-102 Lan-0 TS+81-34624023 TSect-3000620	
	90 J.	310.00	107.229.10.209	191.10.177.2	TOP	Jar and Sector (1994, AC) begins acti initian Lentzi initian territari sector and activity and activity and activity in the sector and and activity in the sector activity in the sec	
	94 J. 95 J.	306002	147.229.14.209	194, 14, 177, 2	TCP	20 40/0-39900 [PSY, MAL SEPT. ACHEO'S BLF-10: LITH-10: LITH-2/ 1944/-96042020 [SET-5000820] 85 S007-4070 [ALT] Sam-50: Ark-50 Min-1444 [Lith-11:2017] [Sun-1500920] TSET-5000820	
	96 3.	328118	2001167:112201808:193	2001+67c+1220+80e+61	8 DNS	255 Standard query response DaBbd5 OMAME asi.facebook.com CMAME star.cl0r.facebook.com AAAA 2003(2880)1111f00(faceb000c00)	
	97 3.	320100	2001:67c:1220:00e:513	2e03:2000:11:1f04:fa	C TOP	94 44165-443 [STN] Seg=0 Win=20800 Len=0 PES=1440 SACK_PERM=1 TSval=3000833 TSecr=0 WS=128	
	98 3,	329959	194.14.177.2	147.229.14.208	TCP	147 4070-39905 [PS-L ACK] Sequ20 Ack:996 Win=182 Len=81 TSval:346242633 TSecr:3000829	
	99 J.	330015	147.229.14.208	194.14.177.2	TCP	56 35905-4070 [ACK] 5eq-996 Ack=L09 VGn=L444 Len=0 T5val=3000840 T5ecr=345242633	
1	00 3.	224649	ExtremeN_ld:4e:30	Broadcast	APP	60 Who has 147,229,14,2367 Tell 147,229,14.1	
1	01 31	304716	2001200011111041100 2001:07:1220:00:00:013	2001167(112201806161	S TOP	bit 443-44100 [DTK, 4KH] Degro Ackel Kinel2000 Leneo ROD-1410 Deka_rEDML ToreLASSOC207 Tech-SCOODL KO-226 DE 4410-442 [AV] Send Ackel Kinel2000 Leneo ROD-1410 Deka_rEDML ToreLASSOC207 Tech-SCOODL KO-226	
1	08 3.	300003	2001:67c:1220:00e:613	2w09:2880:11:1f04:fa	TLSv1.2	de Cient Hello	
1	04 3.	458177	ExtremeN_1d:4e:30	Broadcast	APP	50 Who has 147,229,14,1707 Tell 147,229,14,1	
1	05 3.	494795	2x09:2990:11:1f04:fac	2001:67c:1220:80e:61	3 TCP	96 643-64166 [ACK] Sequi Ackm323 Winm15104 Lenno TSvalm383052518 TSecrm3000871	
⊨ Use ⊨ Dom	r Data ain Ne	agran Pro	rteol, Src Porti 53 (58)	0, Det Perti 19964 [∐	3364)		
0000 0010 0020 0040 0050 0050 0050 0090 0090 0090 009	00 01 00 00 01 00 01 44 81 80 08 69 00 01 70 65 04 72 00 01 47 00	1 80 77 a 0 0 a9 1 0 20 a9 0 a 88 4a 2 0 00 01 0 5 61 63 6 1 60 0c 0 2 74 61 7 1 00 00 0 1 00 01 4 0 02 00 0	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	96         dd         60         00<			
•₹	Fée	"provoz.pi	ap" 29 k8 00:00 Pack	oets: 168 - Displayed: 168	(100.0%) · Load time	0.00.003	Profile: Default

Obrázek 21: Screenshot wiresharku se zachycenými daty