

# Špijunaža

Andrej Šavikin

Matematička gimnazija

13. 05. 2024.

**1. Špijunaža kroz istoriju**

**2. Elektromagnetni talasi**

**3. Eksperiment**

# Šta je špijunaža?



- Prikupljanje informacija
- Neprimetno
- Sa kojim ciljem?
  - Stvaranja strateške prednosti
  - Zaštita interesa
  - Omišljanje i produbljivanje ciljeva
  - Kontrola mase ljudi
  - Zabava(?)



Planiranje

Prikupljanje

Obrada

Prenos

Zaštita



- Poznavanje mete špijuniranja
- Poznavanje medijuma koji se špijunira
- Poznavanje vreme prenosa informacije
- Osmišljanje pristupa informaciji
- Osmišljanje prenosa prikupljene informacije

Planiranje

Prikupljanje

Obrada

Prenos

Zaštita



- Najčešće na neprijateljskoj teritoriji
- Najviše prilika da nešto pođe po zlu
- U moderno vreme su otvorena vrata cyber špijunaži
- Najzanimljiviji deo 😄
- Potreban veliki set veština da se izvede

- Da li mora da bude na neprijateljskoj teritoriji?
- Radio komunikacije koje neprijatelj obavlja se čuju do nas, ali da li možemo to da iskoristimo?



Teufelsberg  
Đavolje brdo  
Berlin

Planiranje

Prikupljanje

Obrada

Prenos

Zaštita



- Kako od prikupljenih informacija znamo šta je nama zapravo potrebno?
- Koliko informacija možemo da odbacimo a da se ne izgubi srž?
- Da li moramo da odbacimo informacije?
- Kako da dešifrujemo poruku?

Planiranje

Prikupljanje

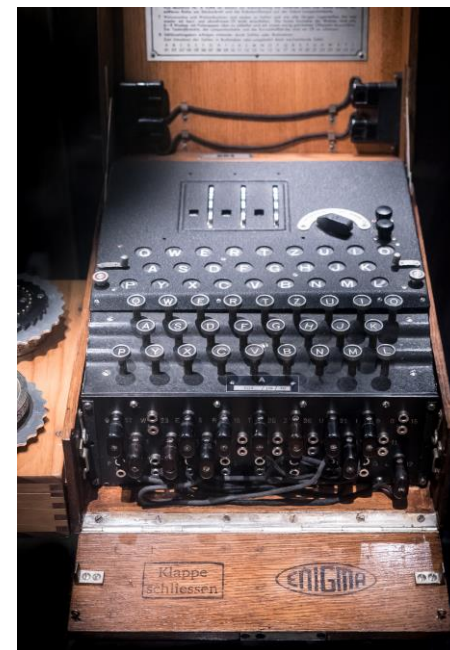
Obrada

Prenos

Zaštita



- Kako poruku iz neprijateljske teritorije da prenesemo u domaću?
- Kako da ne špijuniraju nas dok je prenosimo?
- U eksperimentalnoj postavci ne moramo da brinemo o ovome





Planiranje

Prikupljanje

Obrada

Prenos

Zaštita



- Kako da se zaštitimo od špijunaže?
- Da li možemo da predvidimo sve tipove špijunaže?
- Da li je lakše špijunirati ili zaštititi se od špijunaže?

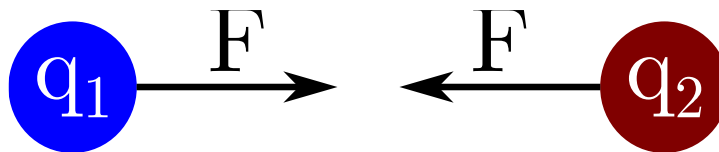
**1. Špijunaža kroz istoriju**

**2. Elektromagnetni talasi**

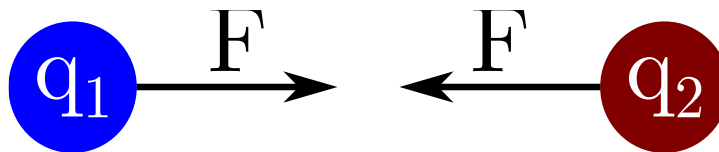
**3. Eksperiment**

- Ok, želimo da špijuniramo. Šta sada?
- Svi uređaji zrače elektromagnetne talase, hajde da iskoristimo to
- Zašto svi uređaji zrače elektromagnetne talase?
- Da li je nama kao špijunima uvek korisna informacija sadržana u elektromagnetnim talasima?
- Šta su zapravo elektromagnetni talasi?

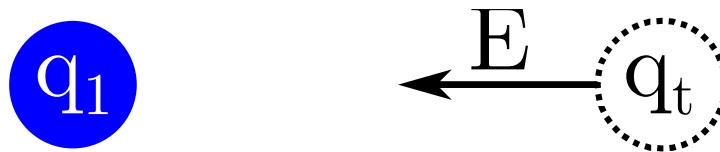
- Znamo da naelektrisanja žele da se privlače ili odbijaju u zavisnosti od svog znaka
- $F = k_e \frac{q_1 q_2}{r^2}$
- Da bi mogli da izračunamo ovu silu, potrebna su nam dva poznata naelektrisanja
- Umesto da znamo dva naelektrisanja gde se nalaze i koliki je njihov intenzitet, krenućemo od jednog naelektrisanja poznate vrednosti i zapitati se šta bi se desilo kada bi dodali još jedno naelektrisanje negde u prostoru



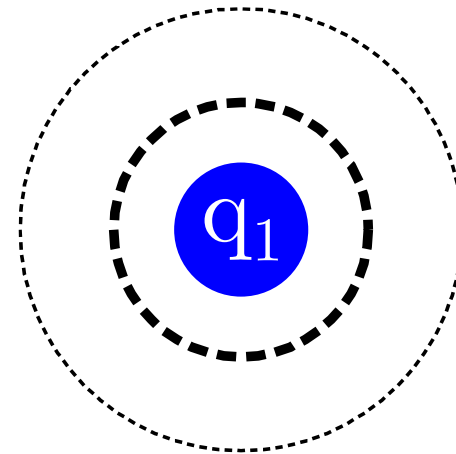
- Znamo da naelektrisanja žele da se privlače ili odbijaju u zavisnosti od svog znaka
- $F = k_e \frac{q_1 q_2}{r^2}$
- Da bi mogli da izračunamo ovu silu, potrebna su nam dva poznata naelektrisanja
- Umesto da znamo dva naelektrisanja gde se nalaze i koliki je njihov intenzitet, krenućemo od jednog naelektrisanja poznate vrednosti i zapitati se šta bi se desilo kada bi dodali još jedno naelektrisanje negde u prostoru



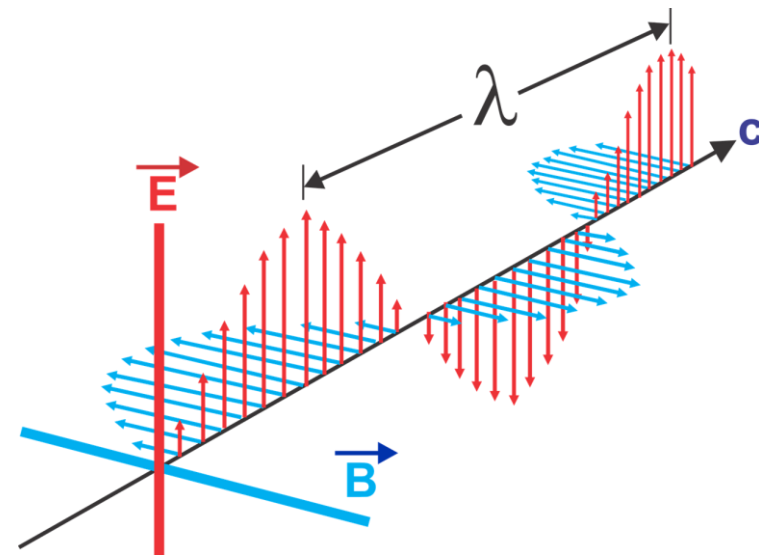
- Ne možemo više da definišemo silu, pošto ona zavisi i od drugog nepostojećeg elektrisanja
- Uvešćemo neko poznato naelektrisanje  $q_t$ , izračunati silu pa zatim podeliti dobijenu silu sa vrednošću tog poznatog naelektrisanja da dobijemo jačinu električnog polja
- Ovo nam dozvoljava da stavimo naelektrisanje bilo koje vrednosti na to mesto, uradimo prosto skalarno množenje i dobijemo silu koja će delovati nad tim naelektrisanjem
- $\vec{F} = q\vec{E}$



- S obzirom da je intenzitet sile jednaka po kružnici oko naelektrisanja, zaključujemo da je polje takođe
- Možemo da nacrtamo linije po kojima je intenzitet sile, tj. polja jednak
- Primećuje se da su ove linije u svim tačkama prostora
- Mi možemo da slušamo polje i u nekoj tački prostora koja nije originalno planirana za to



- Uz električne talase postoje i magnetni talasi
- Ovi talasi se formiraju oko provodnika kroz koje teče struja
- Bez gubitka suštine, možemo da za naše potrebe analiziramo ponašanje električnih talasa, a da magnetne talase zanemarimo u analizi





- Nama zgodna činjenica je da se oko svih provodnika formiraju elektromagnetni talasi
- Zanimljivo je da se energija kroz provodnik ne prenosi kretanjem elektrona u provodniku, već polijma koji okružuju provodnik
- Kablovi su često oklopljeni, što smanjuje količinu izračenih elektromagnetnih talasa, ali i dalje se dosta talasa rasipa na konektorima

1. Špijunaža kroz istoriju
2. Elektromagnetni talasi
3. Eksperiment

- Koji su nam pogodni izvori elektromagnetnih talasa kod jednog računarskog sistema?
- Da li možemo da oslušujemo baš bilo koju žicu ili imamo dodatna ograničenja?
- Odakle zapravo možemo da dobijemo korisnu informaciju?

- Jedan zanimljiv izvor talasa je veza između računara i ekrana
- U moderno vreme se najčešće koristi HDMI, ali nije retko da se vidi VGA za prenos informacija
- U navedenom eksperimentu je uspešno rekonstruisana slika i sa HDMI i sa VGA, ali teorija rekonstrukcije signala sa HDMI prevazilazi vreme dostupno za ovu prezentaciju
- VGA je pogodan za snimanje pošto prenosi signal analogno (kroz naponske nivoe) i dosta je lakše posle dešifrovati informaciju
- Jedno od ograničenja ovakvog sistema je da ne vidi konstantne naponske nivoe, već samo promene naponskih nivou

- **Koji se provodnici nalaze unutar ovog konektora?**
  - Par za plavu boju
  - Par za crvenu boju
  - Par za zelenu boju
  - Horizontalna i vertikalna sinhronizacija
  - GND
  - Pomoćni konektori koji nam nisu od interesa



- Šta nam je potrebno za snimanje elektromagnetnih talasa i rekonstrukciju slike?

\$1000



Laptop

\$10



Antena

\$2817



Softverski definisan  
radio

- **A šta je Softverski Definisan Radio?**
- **Primopredajnik koji može da se isprogramira računarski da snima određene signale**
- **Dosta savremene telekomunikacije koristi uređaje koji funkcionišu slično SDRovima**
- **Može da radi demodulaciju množenjem snimljenog signala sa signalom generisanim unutar SDRa**

- Prvi korak: snimimo elektromagnetne talase
  - Pazimo da je rezultujući intenzitet zbir intenziteta pojedinačnih boja
  - Pazimo da antena snima samo izvod promene intenziteta polja
- Drugi korak: odredimo gde počinje svaka linija piksela i gde počinje jedan frejm
  - Najčešće se slika iscrtava red po red sa leva na desna
- Treći korak: odrediti vrednosti pojedinačnih piksela i iscrtati ih



- GNU Radio
- Dozvoljava nam da direktno hvatamo signal sa SDRa, i radimo obradu nad njim
- FOSS program
- Veliki learning curve
- Graficki interfejs za programiranje
- gr-tempest projekat

# Ekspériment



GRC - Editing: /Users/andrew/sw/gr/grc/examples/audio/b\_flat\_scale.grc.xml

File Edit Execute Options Help

untitled\* b\_flat\_scale.grc.xml

**About**  
Title: The Famous Phone Tones  
Author: Josh Blum

**Note**  
Note: 350 hz + 440 hz + AWGN

```
graph LR; S1[Signal Source] --> A[Add]; S2[Signal Source] --> A; N[Noise Source] --> A; A --> MC[Multiply Constant]; MC --> SS[Scope Sink]; MC --> AS[Audio Sink]; MC --> FTS[FFT Sink];
```

**Signal Source**  
Sampling Rate: 32000  
Wave Form: Cosine  
Frequency: 350  
Amplitude: 1  
Offset: 0

**Signal Source**  
Sampling Rate: 32000  
Wave Form: Cosine  
Frequency: 440  
Amplitude: 1  
Offset: 0

**Noise Source**  
Noise Type: Gaussian  
Amplitude: 0.01  
Seed: 71

**Add**

**Multiply Constant**  
Constant: 0.1

**Scope Sink**  
Title: Scope  
Sampling Rate: 32000  
Frame Decimation: 1  
Vertical Scale: 0  
Time Scale: 0.001  
Marker: Line

**Audio Sink**  
Sampling Rate: 32kHz

**FFT Sink**  
Title: FFT  
Sampling Rate: 32000  
Y per dB: 20  
Reference Level: 20  
FFT Size: 512  
FFT Rate: 15  
Options: Off

Variables				
Variable	Default	Min	Max	Step
samp_rate	32e3			
volume	.1	0	.5	0.005
noise	.01	0	.1	0.001

+ Add - Remove

**Signal Blocks**

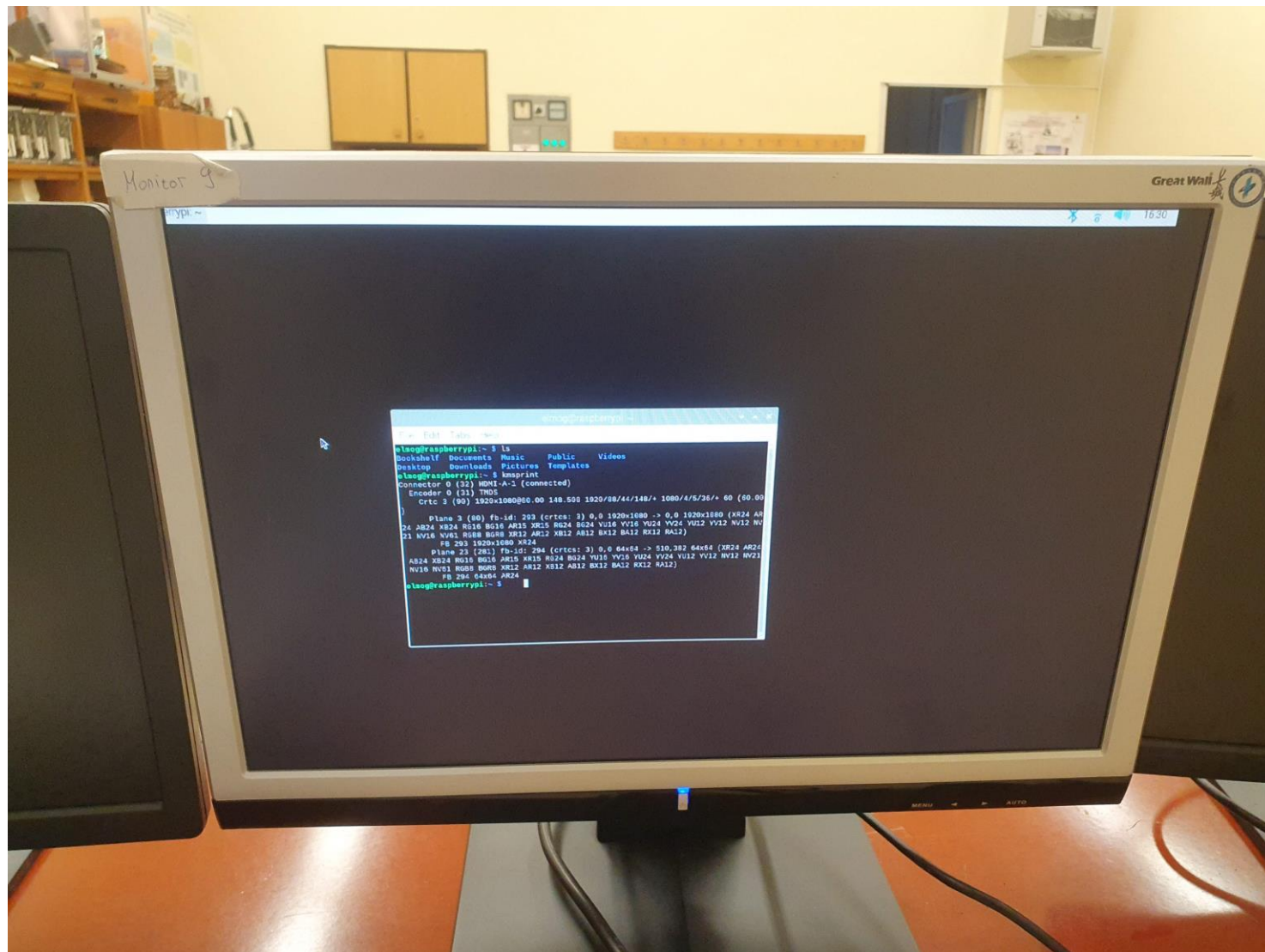
Category

- Sources
  - Signal Source
  - Noise Source
  - Vector Source
  - Random Source
  - Null Source
  - File Source
  - UDP Source
  - Audio Source
  - USRP Source
  - USRP Dual Source
- Sinks
  - Graphical Sinks
  - Operators
  - Conversions
  - Generic Filters
  - Filters
  - Modulators
  - Coders
  - Trellis
  - Misc

+ Add

Showing: "/Users/andrew/sw/gr/grc/examples/audio/b\_flat\_scale.grc.xml"  
Showing: ""  
Showing: "/Users/andrew/sw/gr/grc/examples/audio/b\_flat\_scale.grc.xml"





The screenshot displays a LabVIEW application window titled "gr\_tempest\_v2-0-0\_HDMI\_fs\_50MHz\_fc\_148.5MHz.grc - /home/sava/tempest\_2/gr-tempest/examples". The main workspace shows a signal processing flowchart with the following components:

- Device Arguments:** Configured with `re_ed=127`, `Sync: Unknown PPS`, `Samp rate (Sps): 50M`, `Ch0: Center Freq (Hz): 148.5M`, `Ch0: AGC: Default`, and `Ch0: Gain Value: 50`.
- Sync Detector:** Parameters include `Nacreen: 646`, `Vacreen: 1.0lik`, `Hblanking: 94`, and `Vblanking: 45`.
- Delay:** Set to `Delay: 740`.
- Complex to Mag:** Converts the complex signal to its magnitude.
- Normalize Flow:** Parameters include `Minimum: 1.0`, `Maximum: 245`, `Window: 740`, `Alpha: exp(1.0m)`, and `Update probe: 100m`.
- Other blocks:** `orrelation` (9771.5M), `sampling_sync`, and `me Sink` (1.04825M).

A control panel titled "Manual Tempest Example" is overlaid on the right side, showing the "Autocorrelation Plot Tab" with the following settings:

- Vertical resolution (total): 1125
- Refresh Rate (Hz): 60
- Inverted colors?:  Yes,  No
- Harmonic: 5.0
- 'DroppedFrames': 5
- 'DelaySyncDetector': 740
- Horizontal resolution (total): 2200
- Ratio Finder toggle: ON or OFF (FFT peaks).

At the bottom of the interface, a console window displays the following text:

```
[FFT_peak_finder] Ratio = 0.966656, d_accumulator = 304908.000000,
[FFT_peak_finder] warning: FFT peak finder: Non-PMT type received, expecting Boolean PMT
Imports
import_0 from math import pi
Variables
```



Photo Courtesy of General Dynamics Corporation

**Hvala na pažnji!**

**Pitanja?**