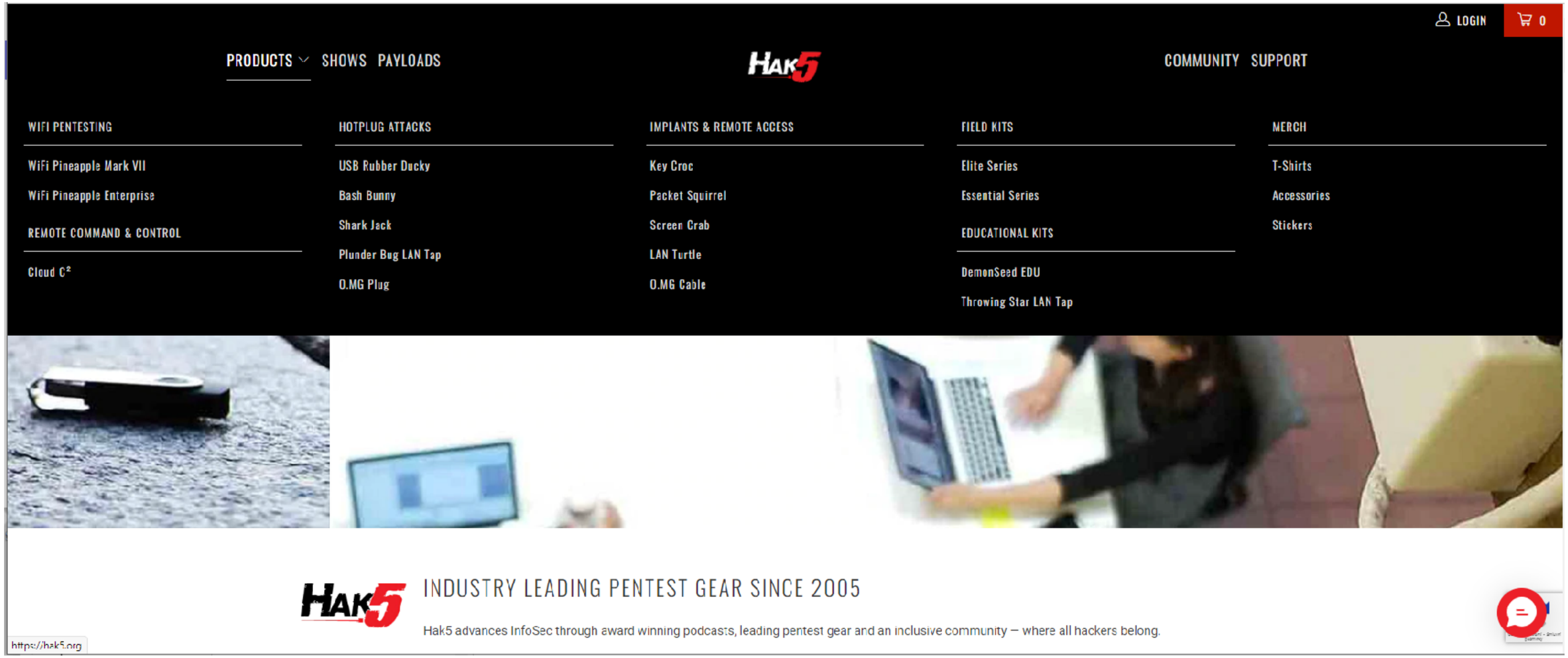
Electronic Attack on Computer Interfaces

Tomáš Rosa
Cryptology and Biometrics Competence Centre of Raiffeisen Bank International
Department of Algebra, Faculty of Mathematics and Physics, Charles University in Prague

HW versus SW Security Disparity

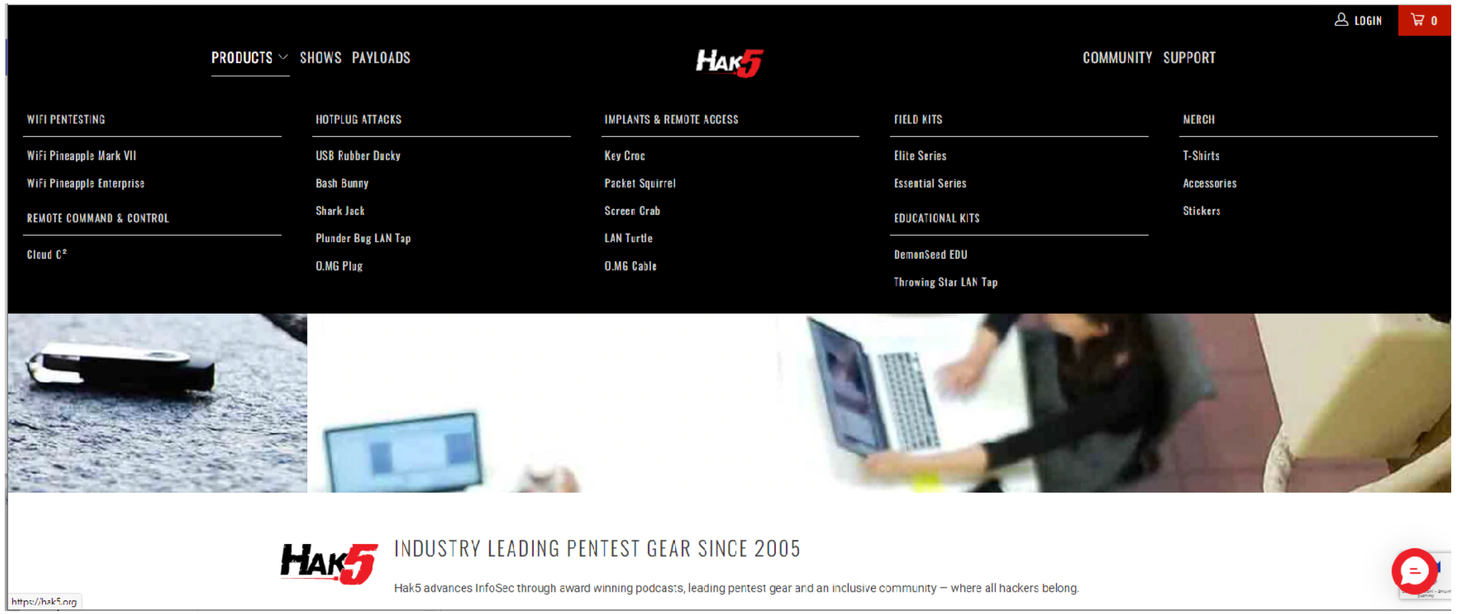
- When it comes to an assessment of physical or hardware-based attack vectors, there is often a lack of experience to perform a risk analysis meaningfully – ***hence, it is usually not performed at all***
  - 802.1X with or without integrity protection on L2?
  - DMA attacks – „This is a problem of unattended computers only, isn't it?“
  - USB 2.0 – a bit dated and will hardly improve anymore, *but its exploitations are recent and getting better each day*
  - PCIe through thunderbolt – DMA attacks and SSD hot plug is just the beginning
  - USB-C – confusing even for its developers; USB 4.0 meant to clean up, but it actually brings further complications
  - Digital video signals – „They are too complex to be attacked, right?“

Ongoing Evaluation – Popular Red Team Toolbox Gadgets



Debriefing Analysis Report Viewpoint

1. Plausibility of the suggested scenarios
2. Technology limits
3. Detection
4. Countermeasures



Display Data

Preview: Screen Crab

Screen grabber for HDMI, based on Lontium chipset for signal bridging and conversion

Captures either single frames or video, results stored locally on SD card and possibly also at C2 cloud

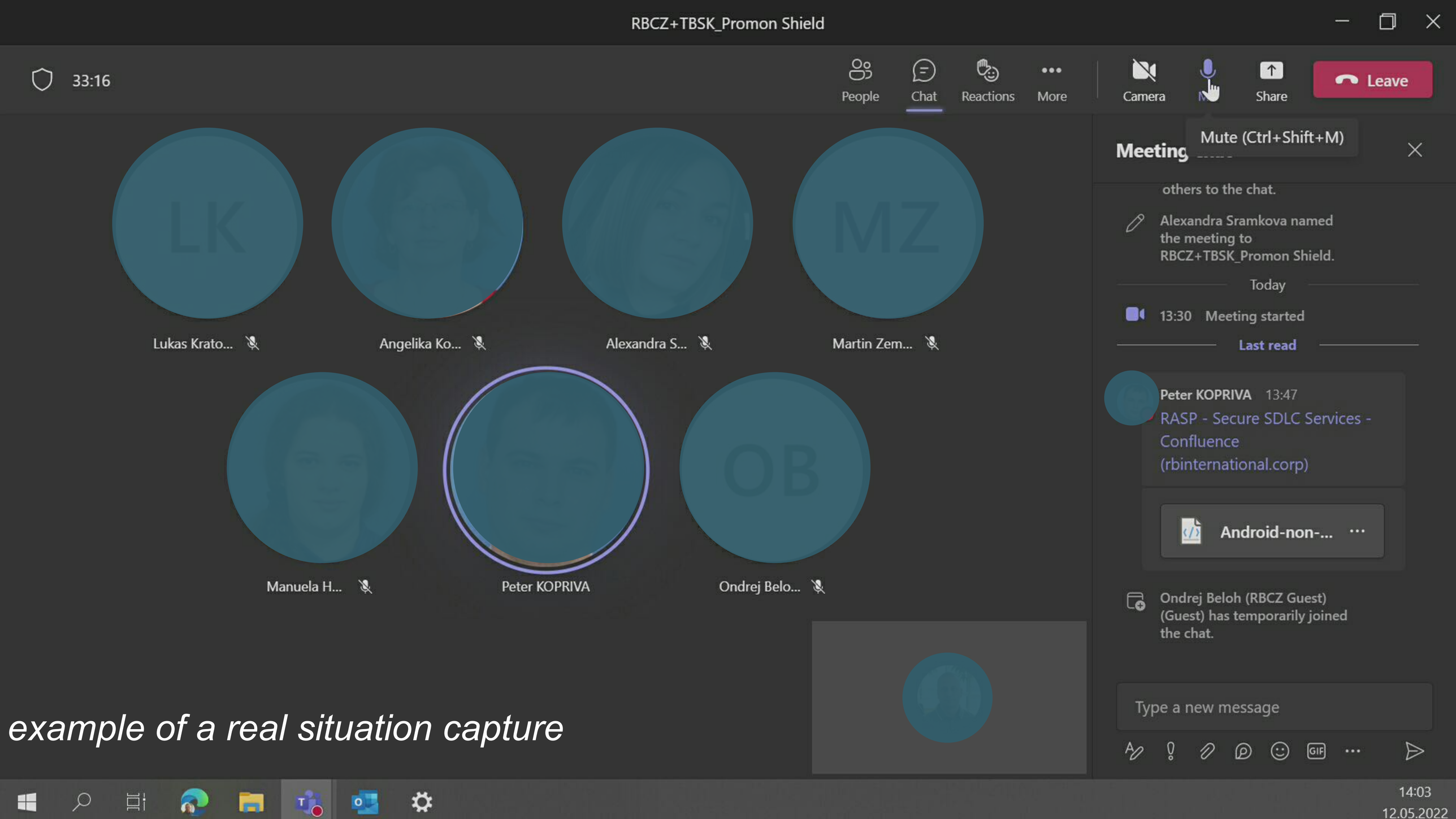
Remote management via C2 cloud

Debriefing Analys

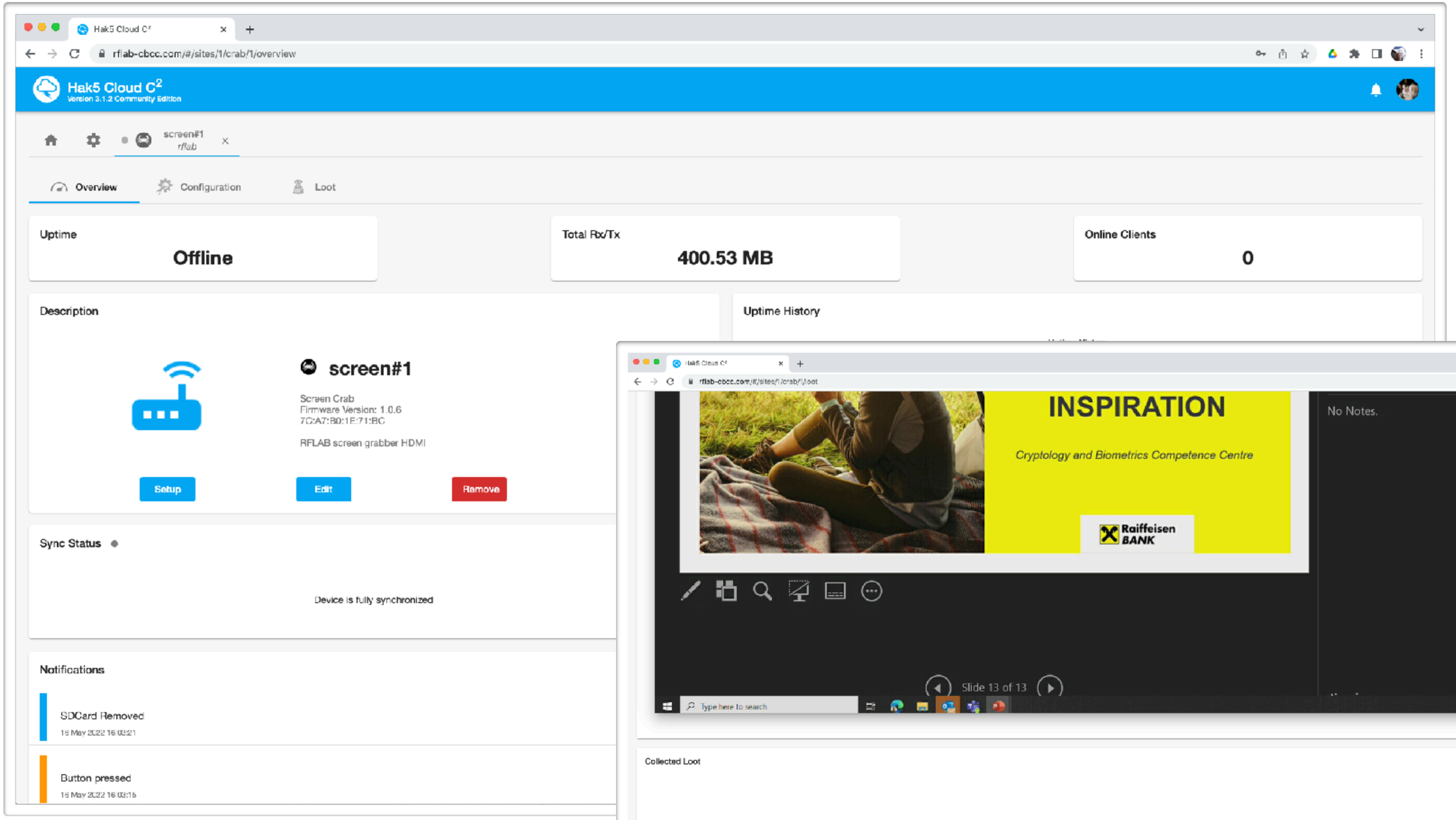
1. Plausible with small operational issues
2. HDMI signal is generally unprotected, certain limits are imposed by available chipsets
3. Can be detected as LONTIUM adapter
4. Consider encrypted video links for highly sensitive areas. Regular physical inspection of highly exposed links. *Sealed ports*?

screen crab

original parts



example of a real situation capture


Hak5 Cloud C²
rflab-cbcc.com/#/sites/1/crab/1/overview
Hak5 Cloud C²
Version 3.1.2 Community Edition
screen#1
rflab
Overview
Configuration
Loot
Uptime
Offline
Total Rx/Tx
400.53 MB
Online Clients
0
Description
screen#1
Screen Crab
Firmware Version: 1.0.6
7C:A7:B0:1E:71:BC
RFLAB screen grabber HDMI
Setup
Edit
Remove
Uptime History
Sync Status
Device is fully synchronized
Notifications
SDCard Removed
16 May 2022 16:03:21
Button pressed
16 May 2022 16:03:15

INSPIRATION
Cryptology and Biometrics Competence Centre
Raiffeisen BANK
No Notes.
Slide 13 of 13
Collected Loot
Filter
Delete All
Export
Name
Date
Size
Download
Remove
View
5871.jpg
30d 17h ago
557468
Download
Remove
View
5872.jpg
30d 17h ago
557381
Download
Remove
Chat

The World of USB

USB 1.0
12mbps

Type A

Type B

Mini-A

Mini-B

Micro-A

Micro-B

USB 2.0
480mbps

Type A

Type B

Mini-A

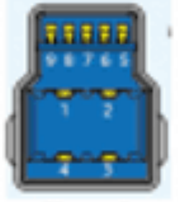
Mini-B

Micro-A

Micro-B

USB 3.1
Gen1
(Previously 3.0)
5gbps

Type A



Type B

Mini-B

Micro-B

USB 3.1
Gen2
10gbps

Type A

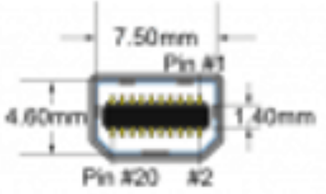
Type-C

USB 3.2
20gbps

Type-C

Thunderbolt
2
20gbps

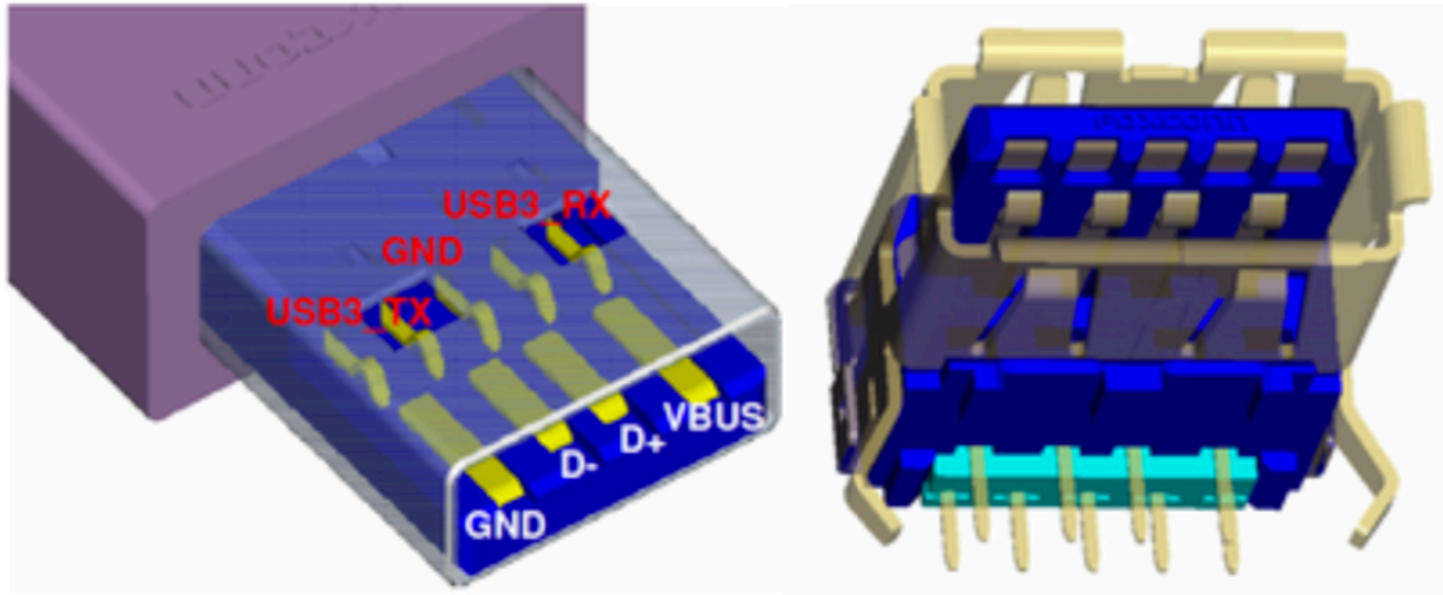
Mini DisplayPort
Connector



Thunderbolt
3
40gbps

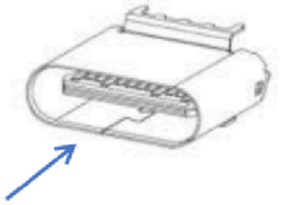
Type-C

Connector Stacking - USB 3.0/3.1 Example



USB Type-C® – Functional Model

- USB 3.2 / *USB4™* data bus
  - Two sets of TX/RX pin pairs, supports x1 and x2 operation
- USB 2.0 data bus
  - Two pin sets on host, one set on device – strapped together within the host and device
- Two power buses
  - VBUS and VCONN
- Two sideband pins (SBU1/SBU2)
  - *SBTX / SBRX for USB4*
- CC – Configuration Channel
  - Two CC pins in connector
  - One CC wire in cable



Looking into the product receptacle:

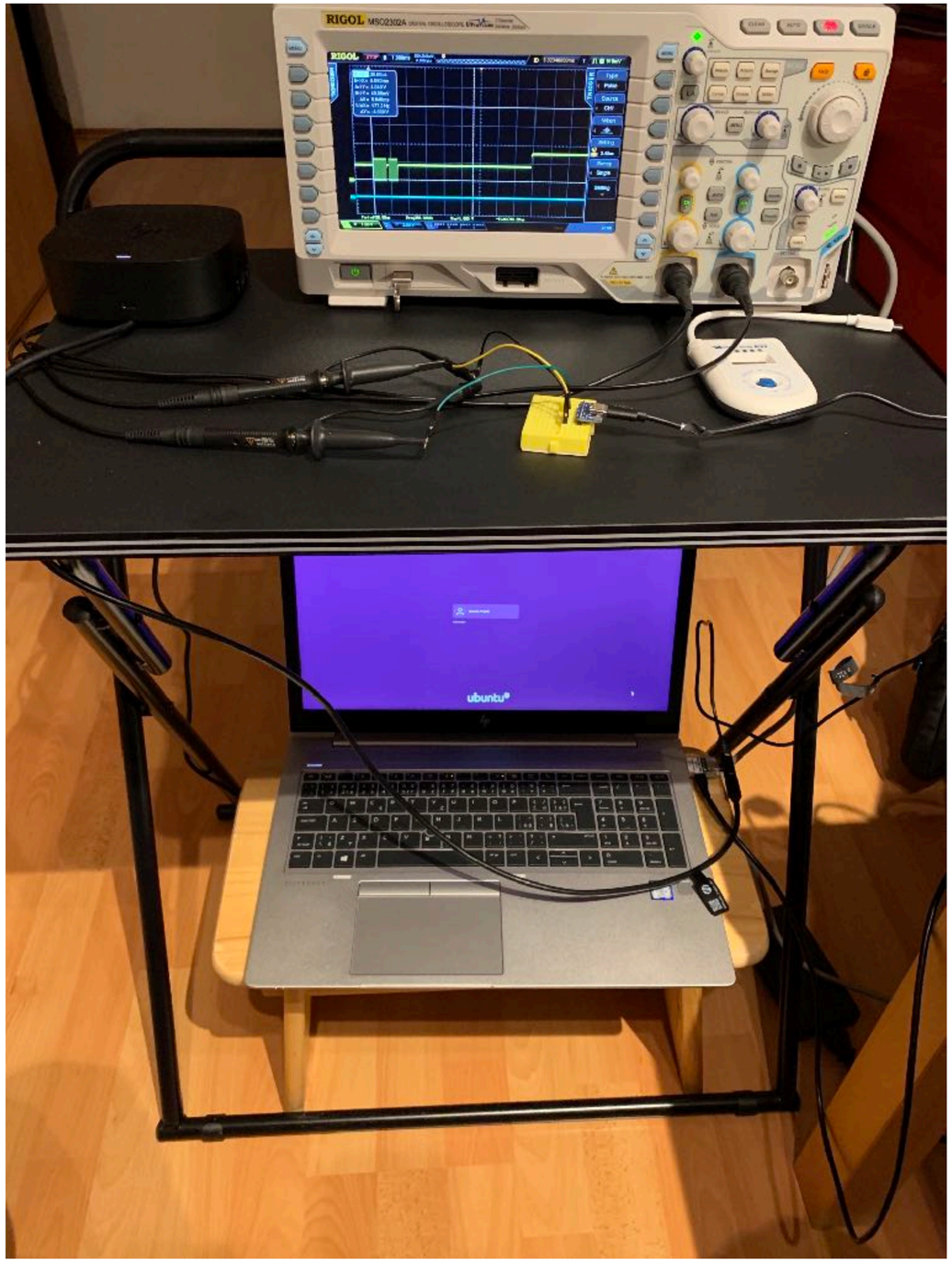
A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12
GND	TX1+	TX1−	VBUS	CC1	D+	D−	SBU1	VBUS	RX2−	RX2+	GND
GND	RX1+	RX1−	VBUS	SBU2	D−	D+	CC2	VBUS	TX2−	TX2+	GND
B12	B11	B10	B9	B8	B7	B6	B5	B4	B3	B2	B1

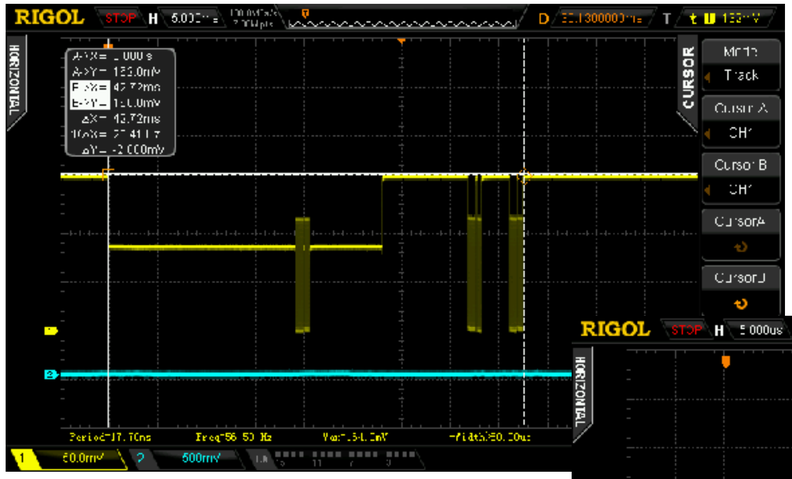
Looking into the cable or product plug:

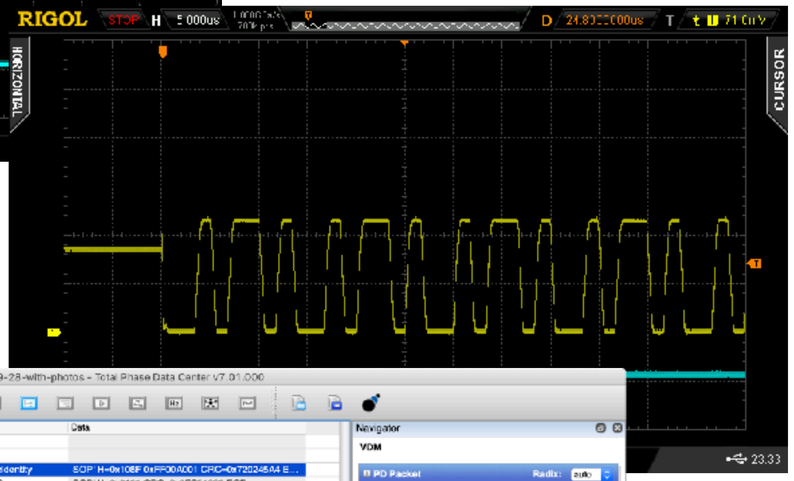
A12	A11	A10	A9	A8	A7	A6	A5	A4	A3	A2	A1
GND	RX2+	RX2−	VBUS	SBU1	D−	D+	CC	VBUS	TX1−	TX1+	GND
GND	TX2+	TX2−	VBUS	VCONN			SBU2	VBUS	RX1−	RX1+	GND
B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12

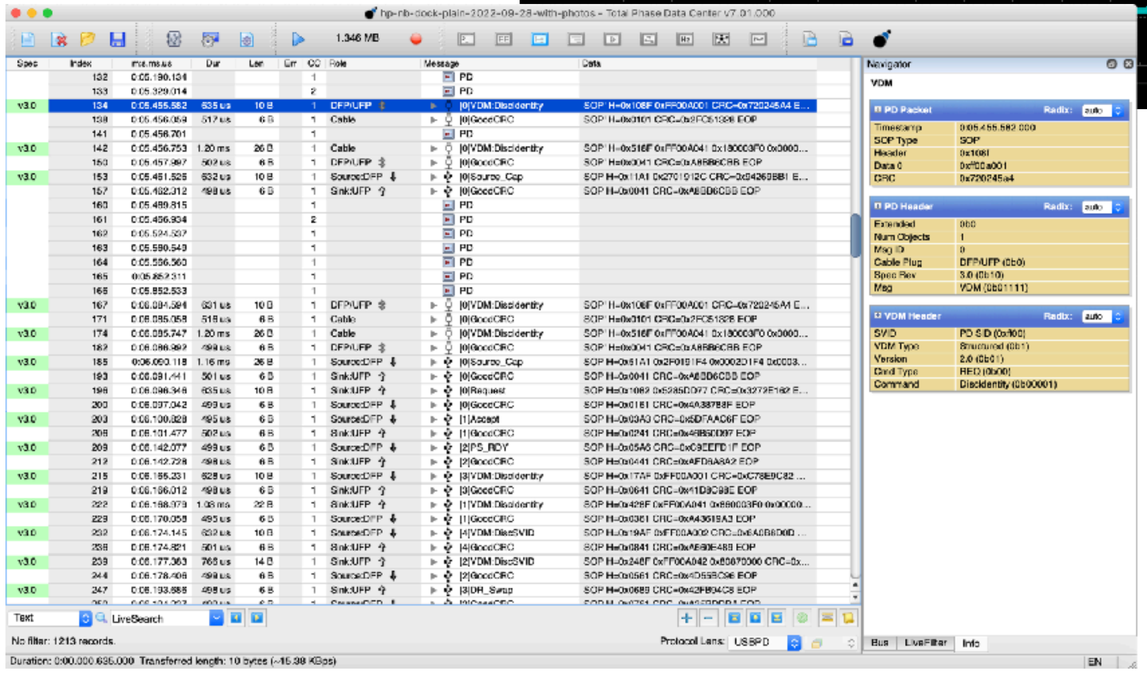
Lane 1 ***Lane 0***

Seeing Through the Mist (Total Phase Portfolio Example)


RIGOL
ubuntu


RIGOL
STOP
HORIZONTAL
CURSOR
Manual
Track
Cursor A
CH1
Cursor B
CH1
CursorA
CursorB


RIGOL
STOP
HORIZONTAL
CURSOR


hp-nb-dock-plain-2022-08-28-with-photos - Total Phase Data Center v7.01.000
Navigator
VDM
PD Packet
PD Header
VDM Header

O.MG Cables

“The O.MG Cable is a hand made USB cable with an advanced implant hidden inside. It is designed to allow your Red Team to emulate attack scenarios of sophisticated adversaries…”

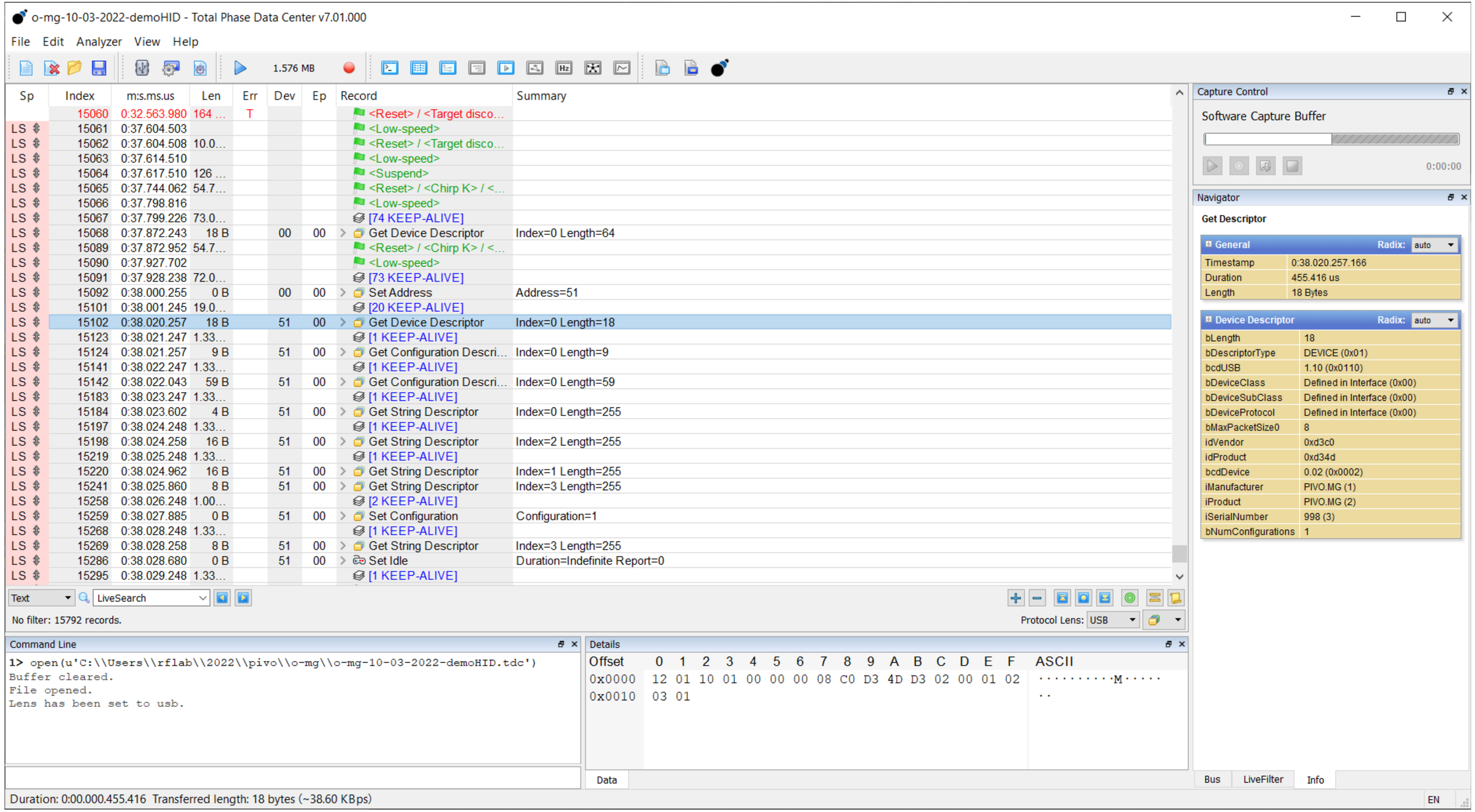
USB HID sniffing and data injection

Remote control through embedded WiFI

Low-Speed device with certain Full-Speed sniffing capability, HID typing of 125 characters per second

Debriefing Analys

1. Plausible, both attended and unattended scenarios
2. Low-speed bus profile is quite slow for today, however, HID is a rich terrain for exploitations; especially for a combined sniffer/injector
3. Detectable heuristically; there is an original forensic detector available (discerns active vs. passive cables); can stay totally quiet and show up for very a precise amount of time
4. Besides detection, there is no robust prevention on the USB data layer, needs to be solved by a system security policy that will limit HID devices impact fundamentally


o-mg-10-03-2022-demoHID - Total Phase Data Center v7.01.000
File Edit Analyzer View Help
1.576 MB
Sp Index m:s.ms.us Len Err Dev Ep Record Summary
15060 0:32.563.980 164 ... T <Reset> / <Target disco...
LS 15061 0:37.604.503 <Low-speed>
LS 15062 0:37.604.508 10.0... <Reset> / <Target disco...
LS 15063 0:37.614.510 <Low-speed>
LS 15064 0:37.617.510 126 ... <Suspend>
LS 15065 0:37.744.062 54.7... <Reset> / <Chirp K> / <...
LS 15066 0:37.798.816 <Low-speed>
LS 15067 0:37.799.226 73.0... [74 KEEP-ALIVE]
LS 15068 0:37.872.243 18 B 00 00 Get Device Descriptor Index=0 Length=64
LS 15089 0:37.872.952 54.7... <Reset> / <Chirp K> / <...
LS 15090 0:37.927.702 <Low-speed>
LS 15091 0:37.928.238 72.0... [73 KEEP-ALIVE]
LS 15092 0:38.000.255 0 B 00 00 Set Address Address=51
LS 15101 0:38.001.245 19.0... [20 KEEP-ALIVE]
LS 15102 0:38.020.257 18 B 51 00 Get Device Descriptor Index=0 Length=18
LS 15123 0:38.021.247 1.33... [1 KEEP-ALIVE]
LS 15124 0:38.021.257 9 B 51 00 Get Configuration Descri... Index=0 Length=9
LS 15141 0:38.022.247 1.33... [1 KEEP-ALIVE]
LS 15142 0:38.022.043 59 B 51 00 Get Configuration Descri... Index=0 Length=59
LS 15183 0:38.023.247 1.33... [1 KEEP-ALIVE]
LS 15184 0:38.023.602 4 B 51 00 Get String Descriptor Index=0 Length=255
LS 15197 0:38.024.248 1.33... [1 KEEP-ALIVE]
LS 15198 0:38.024.258 16 B 51 00 Get String Descriptor Index=2 Length=255
LS 15219 0:38.025.248 1.33... [1 KEEP-ALIVE]
LS 15220 0:38.024.962 16 B 51 00 Get String Descriptor Index=1 Length=255
LS 15241 0:38.025.860 8 B 51 00 Get String Descriptor Index=3 Length=255
LS 15258 0:38.026.248 1.00... [2 KEEP-ALIVE]
LS 15259 0:38.027.885 0 B 51 00 Set Configuration Configuration=1
LS 15268 0:38.028.248 1.33... [1 KEEP-ALIVE]
LS 15269 0:38.028.258 8 B 51 00 Get String Descriptor Index=3 Length=255
LS 15286 0:38.028.680 0 B 51 00 Set Idle Duration=Indefinite Report=0
LS 15295 0:38.029.248 1.33... [1 KEEP-ALIVE]
Text LiveSearch
No filter: 15792 records.
Protocol Lens: USB
Capture Control
Software Capture Buffer
0:00:00
Navigator
Get Descriptor
General Radix: auto
Timestamp 0:38.020.257.166
Duration 455.416 us
Length 18 Bytes
Device Descriptor Radix: auto
bLength 18
bDescriptorType DEVICE (0x01)
bcdUSB 1.10 (0x0110)
bDeviceClass Defined in Interface (0x00)
bDeviceSubClass Defined in Interface (0x00)
bDeviceProtocol Defined in Interface (0x00)
bMaxPacketSize0 8
idVendor 0xd3c0
idProduct 0xd34d
bcdDevice 0.02 (0x0002)
iManufacturer PIVO.MG (1)
iProduct PIVO.MG (2)
iSerialNumber 998 (3)
bNumConfigurations 1
Command Line
1> open(u'C:\\Users\\rflab\\2022\\pivo\\o-mg\\o-mg-10-03-2022-demoHID.tdc')
Buffer cleared.
File opened.
Lens has been set to usb.
Details
Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F ASCII
0x0000 12 01 10 01 00 00 00 08 C0 D3 4D D3 02 00 01 02 ....M.....
0x0010 03 01 ..
Data
Bus LiveFilter Info
Duration: 0:00.000.455.416 Transferred length: 18 bytes (~38.60 KBps)
EN

O.MG Cable Detector

"…The Malicious Cable Detector by O.MG allows you to detect malicious cables and also block data while charging. … plug just the cable into the detector, then the detector into your computer's USB port. LED activity indicates signs of life!"

Designed to discern active vs. passive cables based on power analysis on USB 2.0 power supply lines

Uses allowlists not to alarm on original active cables by Apple, etc.

Debriefing Analys

1. Plausible, worked well with several different cables and devices
2. Its focus on power analysis is both the main strength and weakness; it can detect chips in dormant mode that would be unseen through data lines; on the other hand, it is just for cables - it cannot go deeper to e.g. distinguish malicious vs. original keyboard or mouse
3. Challenging to do similar thing for USB-C, power management/noise injections hardens this task, and yet there are those allowlists
4. From the malicious device designer viewpoint: move to USB-C, try to use a clever power management, or try to mimic those predefined original accessories templates to suppress alarms

Bash Bunny

“By emulating combinations of trusted USB devices — like gigabit Ethernet, serial, … and keyboards — the Bash Bunny tricks computers into divulging data, exfiltrating documents, installing backdoors and many more exploits.”

Payloads and exfiltration results stored locally on SD card

Remote connection possible via network tethering

High-Speed quad-core multi device, HID typing 570 chars/second

Debriefing Analys

1. Plausible, both attended and unattended scenarios
2. USB 2.0 is old, but its exploitations are new and still evolving; big potential due to the **multiple profiles coherently acting together**
3. Detectable heuristically on a device layer due to its somewhat exotic nature; O.MG cable detector does not apply - it can only tell this is an active device, but this is obvious; can stay totally quiet and show up for a very precise amount of time
4. Besides (theoretical) detection, there is no robust prevention on the USB device layer, needs to be coped with at upper levels - USB function layer and higher

bb-10-03-2022-demoHID - Total Phase Data Center v7.01.000

File Edit Analyzer View Help

2.069 MB

Sp	Index	m:s.ms.us	Len	Err	Dev	Ep	Record	Summary
HS	19214	0:55.937.475	875 us				[8 SOF]	[Frames: 567.1 - 568.0]
HS	19215	0:55.938.362	8 B		46	03	Input Report	Keys=[LShift u]
HS	19220	0:55.938.475	875 us				[8 SOF]	[Frames: 568.1 - 569.0]
HS	19221	0:55.939.362	8 B		46	03	Input Report	
HS	19226	0:55.939.475	875 us				[8 SOF]	[Frames: 569.1 - 570.0]
HS	19227	0:55.940.362	8 B		46	03	Input Report	Keys=[LShift s]
HS	19232	0:55.940.475	875 us				[8 SOF]	[Frames: 570.1 - 571.0]
HS	19233	0:55.941.362	8 B		46	03	Input Report	
HS	19238	0:55.941.475	875 us				[8 SOF]	[Frames: 571.1 - 572.0]
HS	19239	0:55.942.362	8 B		46	03	Input Report	Keys=[LShift b]
HS	19244	0:55.942.475	875 us				[8 SOF]	[Frames: 572.1 - 573.0]
HS	19245	0:55.943.362	8 B		46	03	Input Report	
HS	19250	0:55.943.476	875 us				[8 SOF]	[Frames: 573.1 - 574.0]
HS	19251	0:55.944.362	8 B		46	03	Input Report	Keys=[Space]
HS	19256	0:55.944.476	875 us				[8 SOF]	[Frames: 574.1 - 575.0]
HS	19257	0:55.945.362	8 B		46	03	Input Report	
HS	19262	0:55.945.476	875 us				[8 SOF]	[Frames: 575.1 - 576.0]
HS	19263	0:55.946.362	8 B		46	03	Input Report	Keys=[o]
HS	19268	0:55.946.476	875 us				[8 SOF]	[Frames: 576.1 - 577.0]
HS	19269	0:55.947.363	8 B		46	03	Input Report	
HS	19274	0:55.947.476	875 us				[8 SOF]	[Frames: 577.1 - 578.0]
HS	19275	0:55.948.363	8 B		46	03	Input Report	Keys=[f]
HS	19280	0:55.948.476	875 us				[8 SOF]	[Frames: 578.1 - 579.0]
HS	19281	0:55.949.363	8 B		46	03	Input Report	
HS	19286	0:55.949.476	875 us				[8 SOF]	[Frames: 579.1 - 580.0]
HS	19287	0:55.950.363	8 B		46	03	Input Report	Keys=[f]
HS	19292	0:55.950.476	875 us				[8 SOF]	[Frames: 580.1 - 581.0]
HS	19293	0:55.951.363	8 B		46	03	Input Report	
HS	19298	0:55.951.476	875 us				[8 SOF]	[Frames: 581.1 - 582.0]
HS	19299	0:55.952.363	8 B		46	03	Input Report	Keys=[Return]
HS	19304	0:55.952.476	875 us				[8 SOF]	[Frames: 582.1 - 583.0]
HS	19305	0:55.953.363	8 B		46	03	Input Report	

Text LiveSearch

No filter: 19315 records.

Protocol Lens: USB

Capture Control

Software Capture Buffer

0:00:00

Navigator

HID Report

General	Radix: auto
Timestamp	0:55.938.362.100
Duration	1.000 us
Length	8 Bytes

Input Report	Radix: auto
Keyboard LeftControl	0b0
Keyboard LeftShift	0b1
Keyboard LeftAlt	0b0
Keyboard Left GUI	0b0
Keyboard RightControl	0b0
Keyboard RightShift	0b0
Keyboard RightAlt	0b0
Keyboard Right GUI	0b0
Keyboard/Keypad Array	Keyboard u and U (24)
Keyboard/Keypad Array	Reserved (no event indicated) (0)
Keyboard/Keypad Array	Reserved (no event indicated) (0)
Keyboard/Keypad Array	Reserved (no event indicated) (0)
Keyboard/Keypad Array	Reserved (no event indicated) (0)
Keyboard/Keypad Array	Reserved (no event indicated) (0)

Command Line

```
1> open(u'C:\\Users\\rflab\\2022\\pivo\\bash-bunny\\bb-10-03-2022-demoHID.tdc')
Buffer cleared.
File opened.
Lens has been set to usb.
```

Details

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ASCII
0x0000	02	00	18	00	00	00	00	00									....

Data

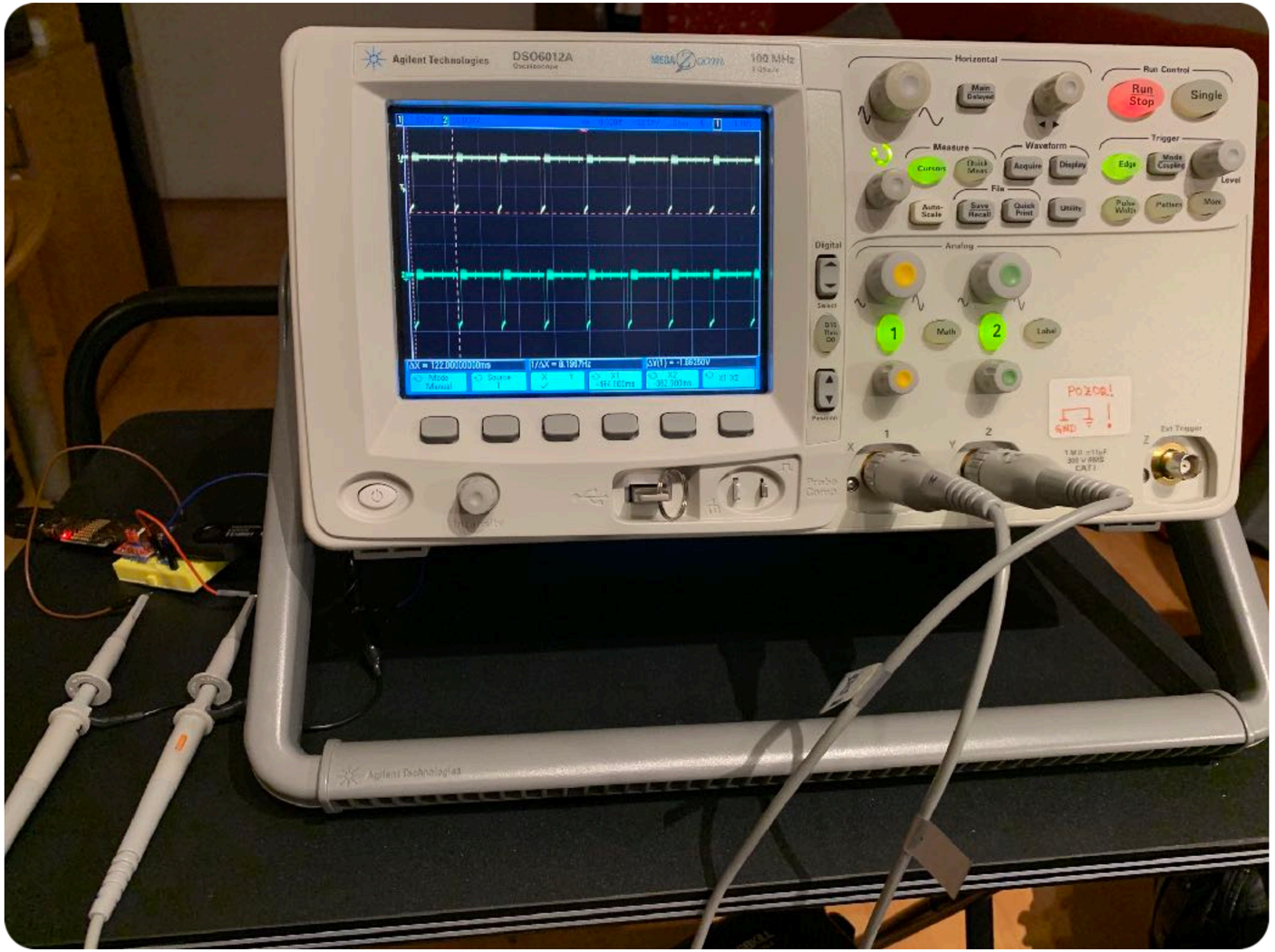
Bus LiveFilter Info

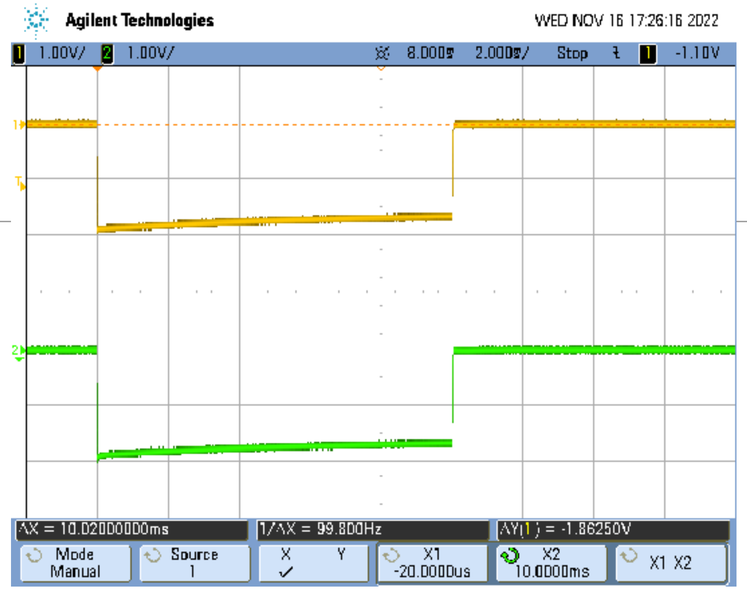
Duration: 0:00.000.001.000 Transferred length: 8 bytes (~7.629 MBps)

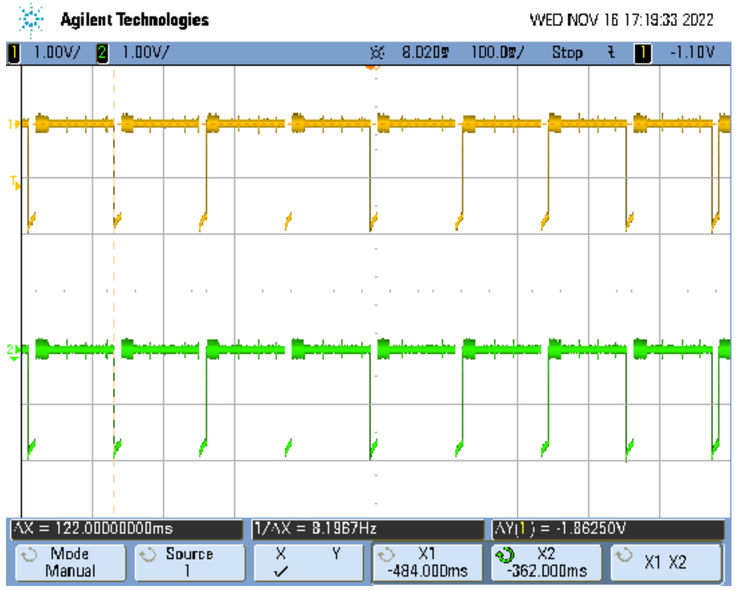
EN

Should everything else fail - USBKill

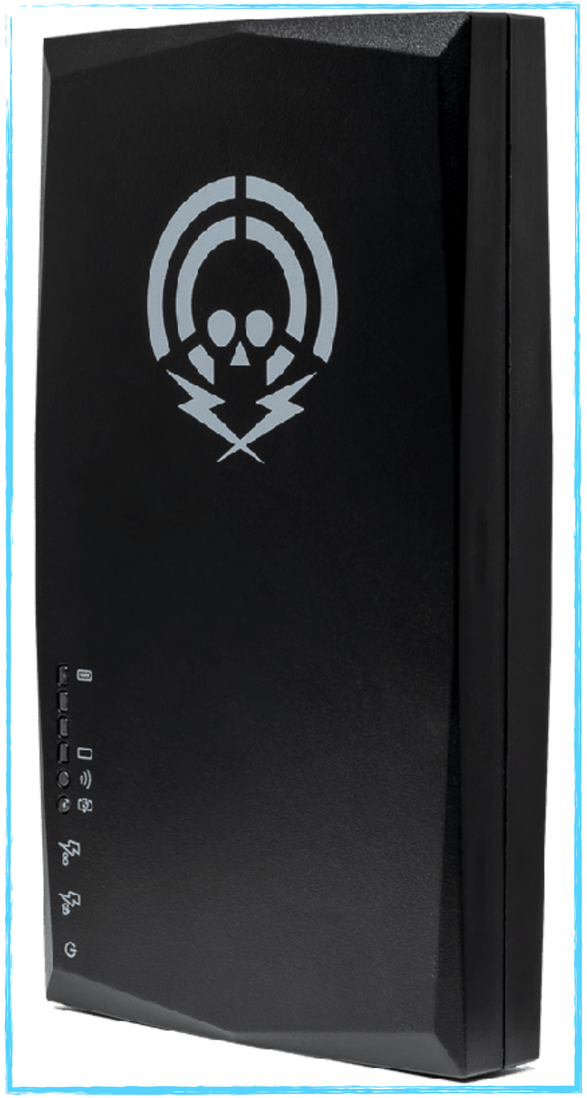
USB D+ and D-, vertical scale 101 V/div



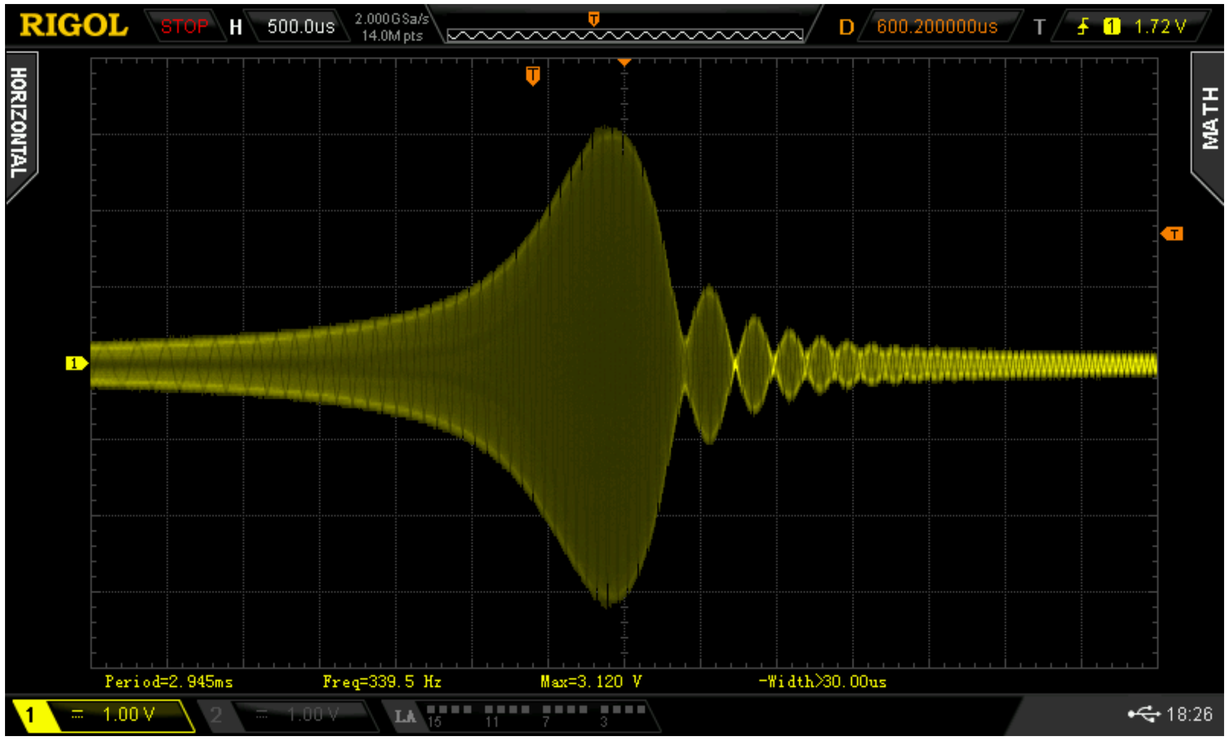




Contactless Micro-EMP Variant (NFCKill)

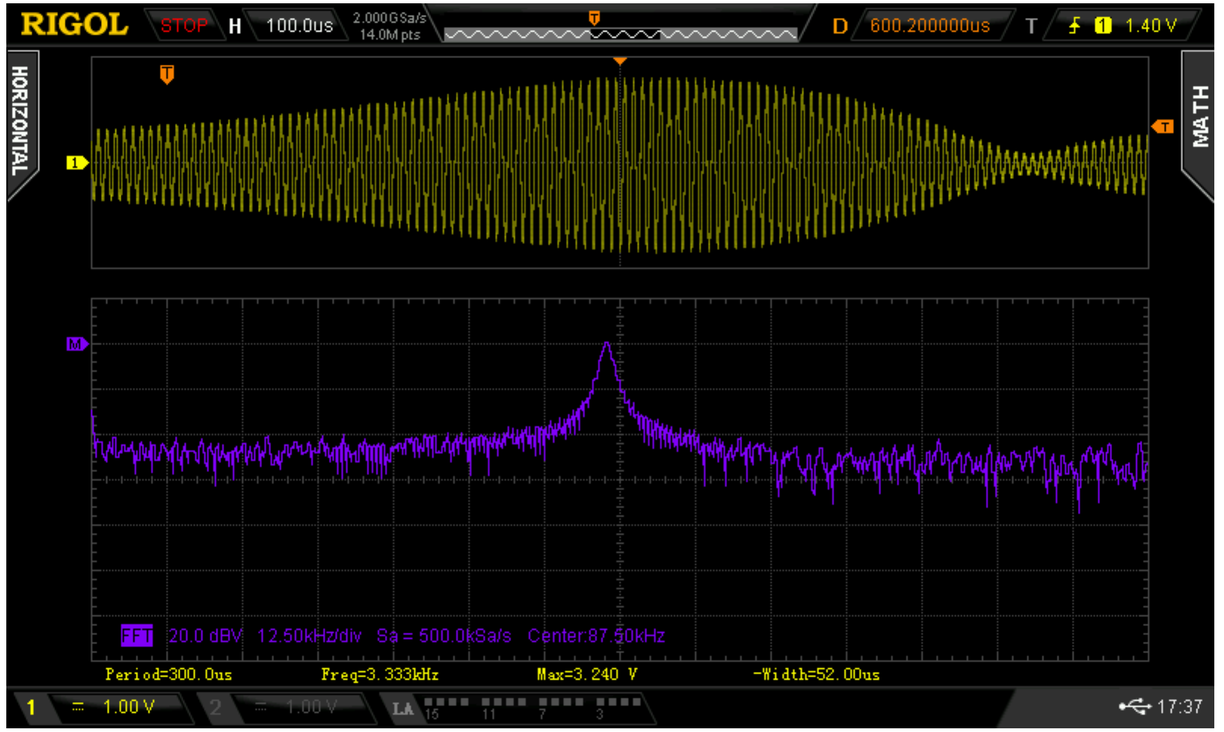


NFCKill Near-Field Magnetic Pulse (35 mm axial distance)

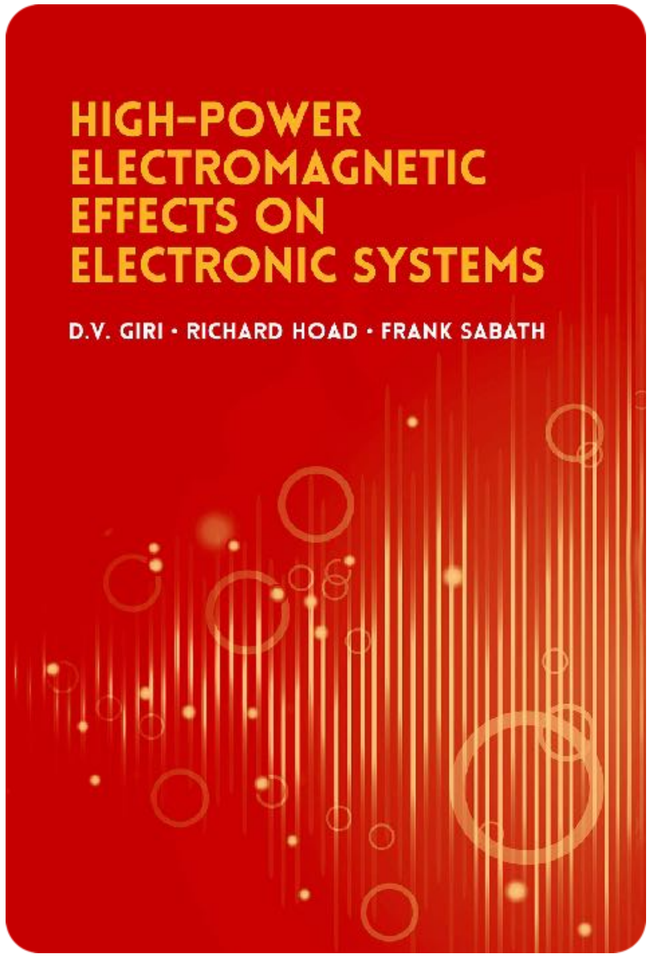


- Roughly 30-times higher peak value than for a regular NFC terminal (ACR122) in the same setup
- Will further raise sharply when approaching a closer distance
- Static discharge-like sensing observed at < 1 cm distance, their cause and effect remains unknown

- Probably, there is a high-voltage generator discharged instantly into a primary coil, producing typical high-energy transients



Electromagnetic Environments



- **HPEM** ~ High-Power Electromagnetic, general attribute defined in IEC 61000
- **HEMP** ~ High-altitude EM Pulse, i.e. a nuclear variant of the general HPEM attack
- **EMP** ~ EM Pulse, popular term mainly for HEMP, **NNEMP** then denotes non-nuclear EMP
- **HPRF DE** ~ High-Power RF Directed Energy, also known as **HPM** (High-Power Microwave)
- **IEMI** ~ Intentional EM Interference, an academic term, also covers jamming

In 2017, EMP (as Nuclear-sourced HPEM) “Exploded” in Newsrooms

[https://www.youtube.com/watch?v=fpQ8tj0aVRc]

Plasma dipole antenna

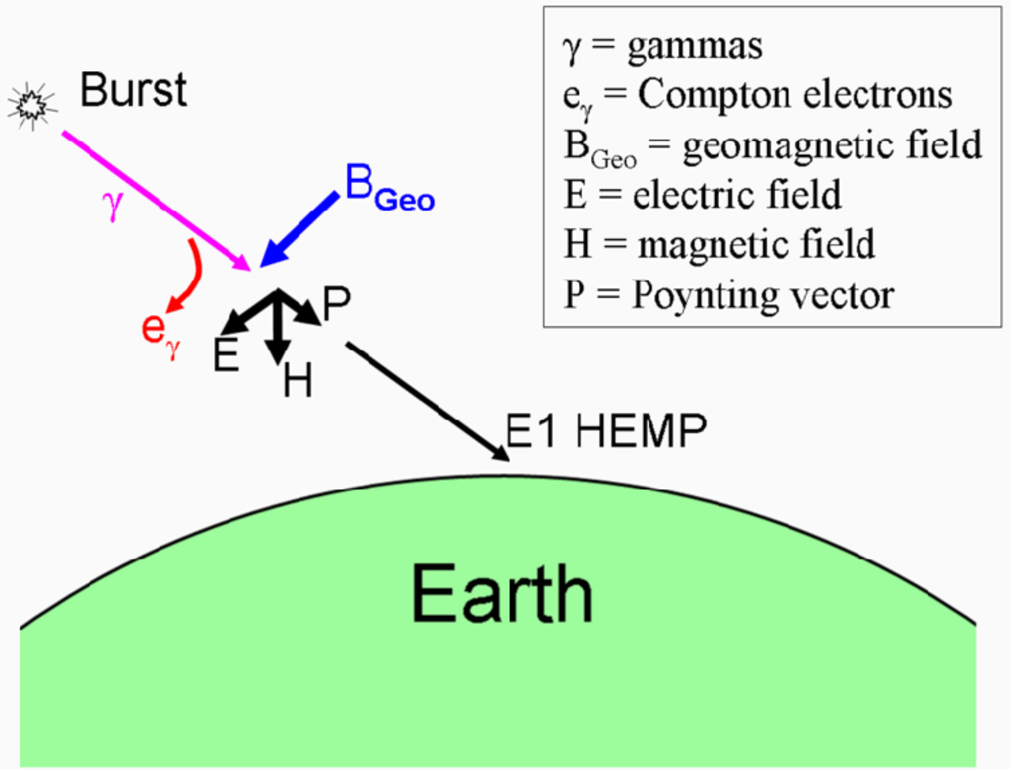
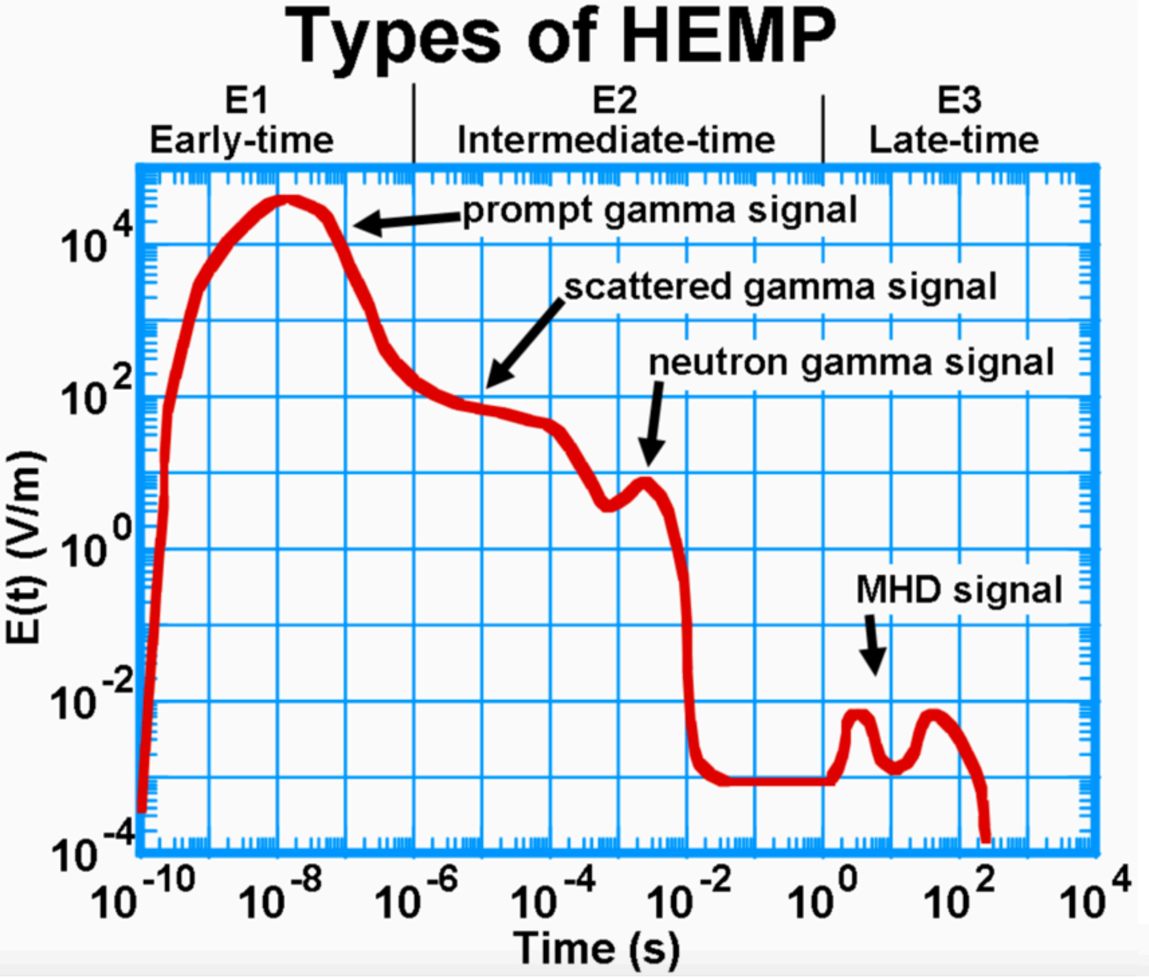


Figure 2-2. General basis of the E1 HEMP generation process. Gammas from the nuclear burst interact with the upper atmosphere – generating Compton electrons, which are turned in the Earth's geomagnetic field, and produce a transverse current that radiates an EM pulse towards the Earth.



Research papers are rare, especially those from the Soviet region

Response of Long Lines to Nuclear High-Altitude Electromagnetic Pulse (HEMP)

Vasily N. Greetsai, Andrey H. Kozlovsky, Vadim M. Kuvshinnikov, Vladimir M. Loborev, Yuri V. Parfenov, Oleg A. Tarasov, and Leonid N. Zdoukhov

Abstract— **During high-altitude nuclear testing in 1962 over Kazakhstan, several system effects were noted due to the high-altitude electromagnetic pulse (HEMP). In particular a 500-km-long aerial communications line experienced a failure due to the damage of its protective devices. In this paper, this failure is examined in detail beginning with the calculation of the incident HEMP environments, including those from the early- and late-time portions of the HEMP. In addition, the currents and voltages induced on the line are computed and the measured electrical characteristics of the protection devices are presented. With this information it is possible to determine which portions of the HEMP environment were responsible for particular protection failures. The paper concludes with recommendations for further work required to understand the best ways to protect power lines from HEMP in the future.**

early-time HEMP. MHD EMP forms due to the interaction between the disturbed region of the burst and the geomagnetic field. The electrical current systems arising during the motion of the ionized medium lead to an entire or partial pushing of the geomagnetic field out of the boundaries of the burst-perturbed region. The range of this geomagnetic effect and, hence, the intensity of the MHD EMP generation are defined by the extent of the gas-dynamic and ionized perturbation of the atmosphere following the nuclear burst.

In this paper, an example case of an aerial communication line is provided to consider the currents and voltages induced due to the different HEMP components for the specific phys-

Vasily N. Greetsai was born in Melitopol, Ukraine, on July 29, 1961. He received the Dipl. of nuclear physics from Kharkov State University, Kharkov, Ukraine, in 1984, and the Ph.D. degree from the Central Institute of Physics and Technology (CIPT), Serfiev Posad, Russia, in 1995.

In 1987, he joined the CIPT where he conducts research in pulsed electromagnetic fields.

Andrey H. Kozlovsky was born in Vologda, Russia, on May 11, 1960. He received the Dipl. of Engineer in aerodynamics and thermodynamics from Moscow Institute of Physics and Technology, Moscow, Russia, in 1983, and Ph.D. degree from the Central Institute of Physics and Technology (CIPT), Serfiev Posad, Russia, in 1992.

In 1983, he joined the CIPT where he is currently engaged in research on man-made electromagnetic pulses.

Vadim M. Kuvshinnikov was born on April 11, 1943, in Ufa, Russia. He received the Dipl. of Engineer-Physicist from the Moscow Physical Engineering Institute, Russia, in 1966, and the Ph.D. degree from the Central Institute of Physics and Technology (CIPT), Serfiev Posad, Russia, in 1987.

From 1969 to 1972, he was a Postgraduate and worked on improving his skills in theoretical physics. In 1987 he became a Professor at CIPT, where he is currently a Leading Scientist. He is the author of more than 200 scientific papers devoted to quantitative descriptions of neutron–media interaction processes, investigations of the physics of the EMP evolution from surface and magnetospheric nuclear explosions, and mathematical simulations of EMP effects on various objects.

Vladimir M. Loborev was born on November 23, 1937 in Novosibirsk, Russia. He received the Dipl. of Engineer-Chemist from the High Military Naval College, St. Petersburg, Russia, in 1960, and the Ph.D. degree from the Central Institute of Physics and Technology (CIPT), Serfiev Posad, Russia, in 1971.

He has worked at CIPT since 1962 and in 1983 he became a Professor there. Currently, he is the Director of CIPT. He is the author of more than 400 scientific papers devoted to investigations of the physics processes of nuclear weapon effects simulation, theoretical and experimental investigations of nuclear weapon effects parameters including EMP and the physics base of these effects, and substantiation of the development and application of the experimental base of simulation facilities to investigate nuclear weapon effects.

Dr. Loborev is a member of the Russian Academy of Natural Sciences and the International Academy of Information.

Oleg A. Tarasov was born in Kostroma, Russia, on April 12, 1944. He received the Dipl. of Engineer-Physicist from the Moscow Physical-Engineer Institute, Russia, in 1967, and the Ph.D. degree the Central Institute of Physics and Technology (CIPT), Serfiev Posad, Russia in 1993.

In 1987, he joined CIPT. His research interests include the effects caused by natural and man-made electromagnetic pulses on antenna-feeder facilities and communication and power systems.

Yuri V. Parfenov was born on February 16, 1947, in Dnipro, Russia. He received the Dipl. of Engineer-Physicist from the Moscow Physical Engineering Institute, Moscow, Russia, in 1971, the Ph.D. degree from the Central Institute of Physics and Technology (CIPT), Serfiev Posad, Russia, in 1982.

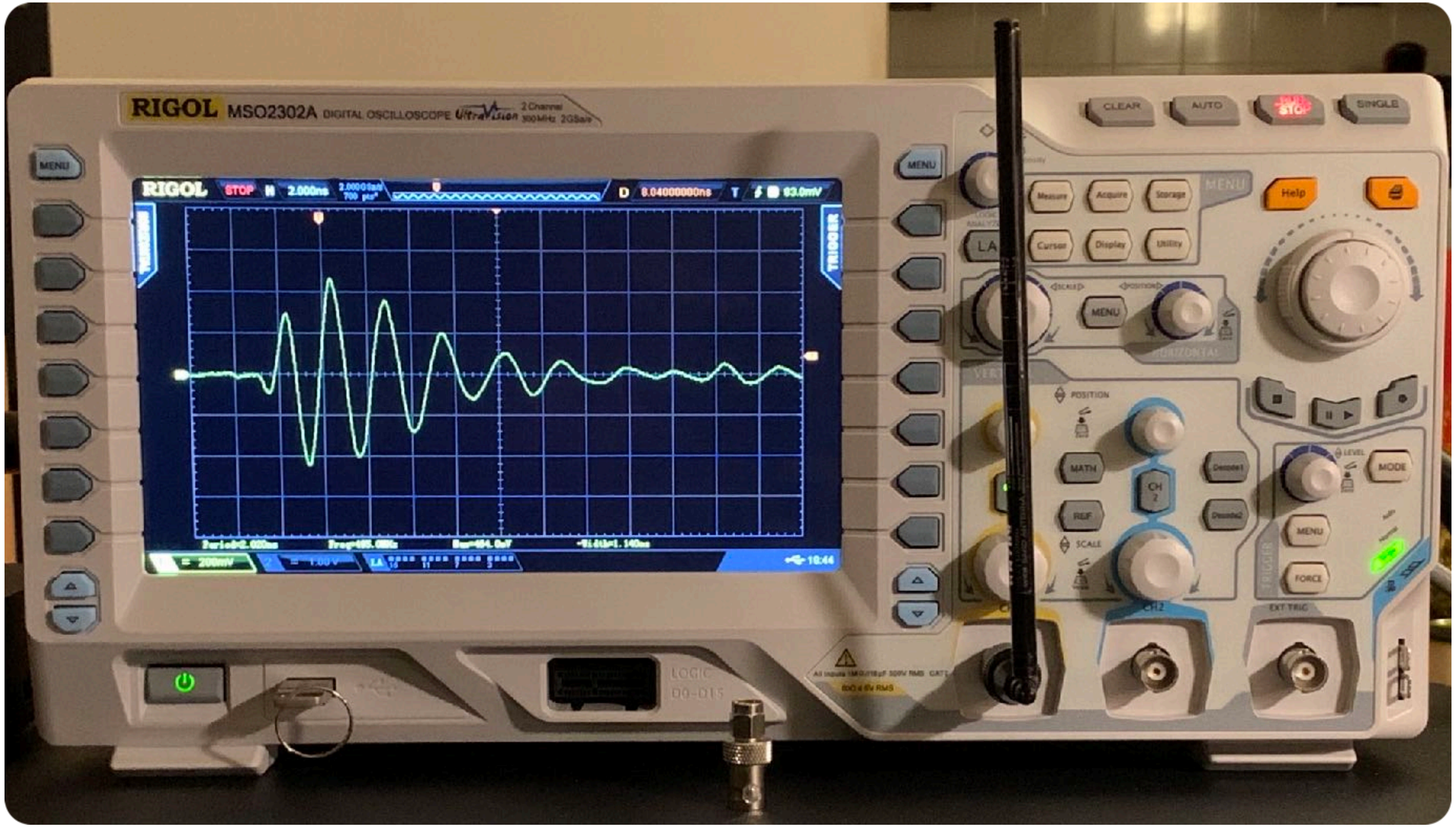
He has worked at CIPT since 1975. He became a Professor there in 1992. He is now the Deputy Director of CIPT. He is the author of more than 200 scientific papers on calculation methods to investigate EMP effects on cables and methods and simulators to reproduce these effects, calculation methods of SGEMP and experimental methods to study SGEMP effects, simulators for reproducing combined effects of SREMP and ionizing radiation, and applications of EMP simulators for nonmilitary (conversion) purposes.

Leonid N. Zdoukhov was born on January 15, 1949, in Tallinn, Estonia. He received Dipl. of radiophysics from the Leningrad State University, St. Petersburg, Russia, in 1972, and the Ph.D. degree from the Central Institute of Physics and Technology (CIPT), Serfiev Posad, Russia, in 1982.

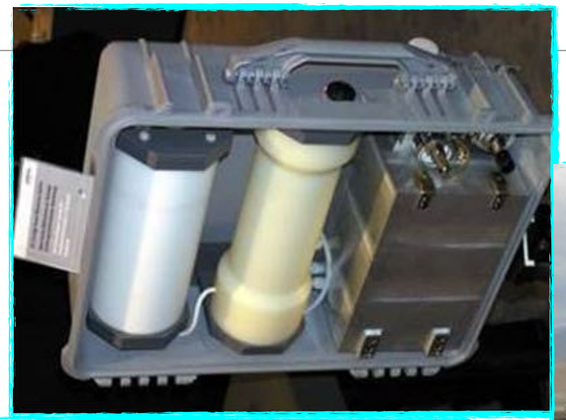
Since 1972 he has worked at CIPT of the Russian Federation Ministry of Defense, became a Professor there in 1996, and is currently a Department Head. He is the author of more than 100 scientific papers devoted to EMP coupling to aerial and underground cables, source region electromagnetic pulse (SREMP) coupling to antennas and flying vehicles, EMP simulators and applications thereof for testing system response to nuclear burst EMP effects, and computational and experimental methods to evaluate joint EMP and ionizing radiation effects on semiconductor equipment. His interests include the problems of reproducing EMP effects and system testing.

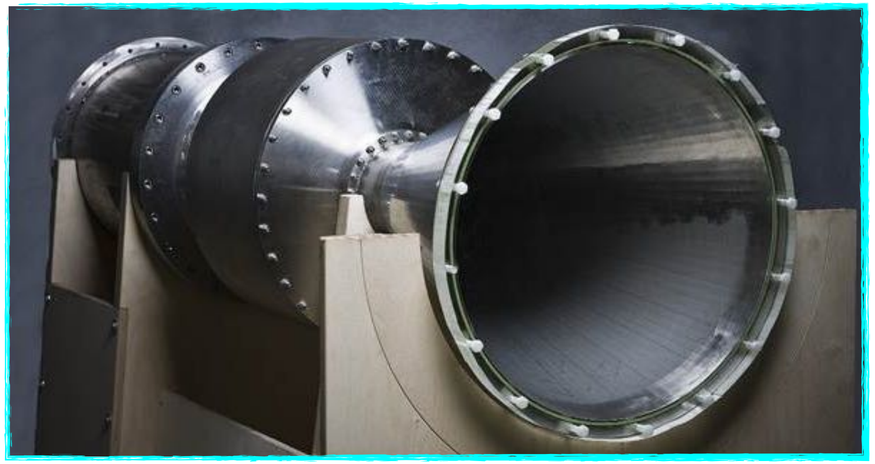

International boundary
Oblast' boundary
Main road
Secondary road
Railroad
KAPUSTIN YAR
RUSSIAN FEDERATION
Chelyabinsk
Kurgan
Petropavl
Omsk
Karasuk
NORTH KAZAKHSTAN
Qostanay
Rudnyy
Kokshetau
Kzyltu
Kachiry
Pavlodar
PAVLODAR
Lebyazh'ye
QOSTANAY
Zhailma
Astana
AQMOLA
Kurchatov
Semey
Oskemen
Oral
Furmanovo
Dzhambeyty
WEST KAZAKHSTAN
Aqtöbe
Khromtau
Kalmykovo
Arqalyk
Qaraghandy
Georgiyevka
Bestamak
Qarabulaq
Torghay
Oyyl
Embi
EAST KAZAKHSTAN
Ayaguz
Zaysan
ATYRAU
Atyrau
AQTÖBE
Yrghyz
UPLANDS
Urdzhar
Shalqar
QARAGHANDY
Zhezqazghan
Balqash
Ganyushkino
Aklumsyk
Dzhambul
Beskol
Saryshagan
Ostrova Tyuleniy
Poluostrov Buzachi
Beyneu
Baikonur Cosmodrome
BETPAQ DALA
Taldyqorghan
Fort Shevchenko
MANGGHYSTAU
Akbakay
ALMATY
Aqtau
Zhetybay
Ustyurt Plateau
Ostrova Vozrozhdeniya
ARAL SEA
Qyzylorda
Akshiy
Furmanovka
ZHAMBYL
QYZYLORDA
Shu
Almaty
CHINA
Aksu
Zhanatas
Zhambyl
SOUTH KAZAKHSTAN
Bishkek
Yiyk-Kol
Shymkent
KYRGYZSTAN
Baku (Baki)
TURKMENISTAN
UZBEKISTAN
Tashkent
Samarqand
TAJIKISTAN
CASPIAN SEA
0 100 200 300 400 500 km
0 100 200 300 mi

Just a… cigarette lighter, 1 m line of sight distance
200 mV/div vertical, 2 ns/div horizontal, untuned wire antenna



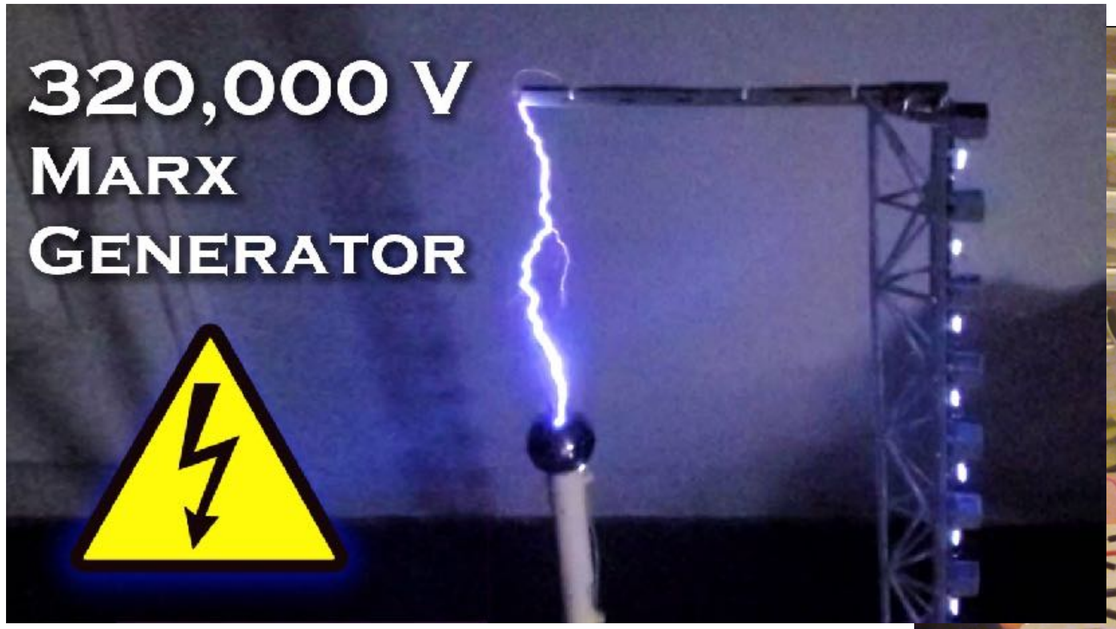
Tactical NNEMP Generators

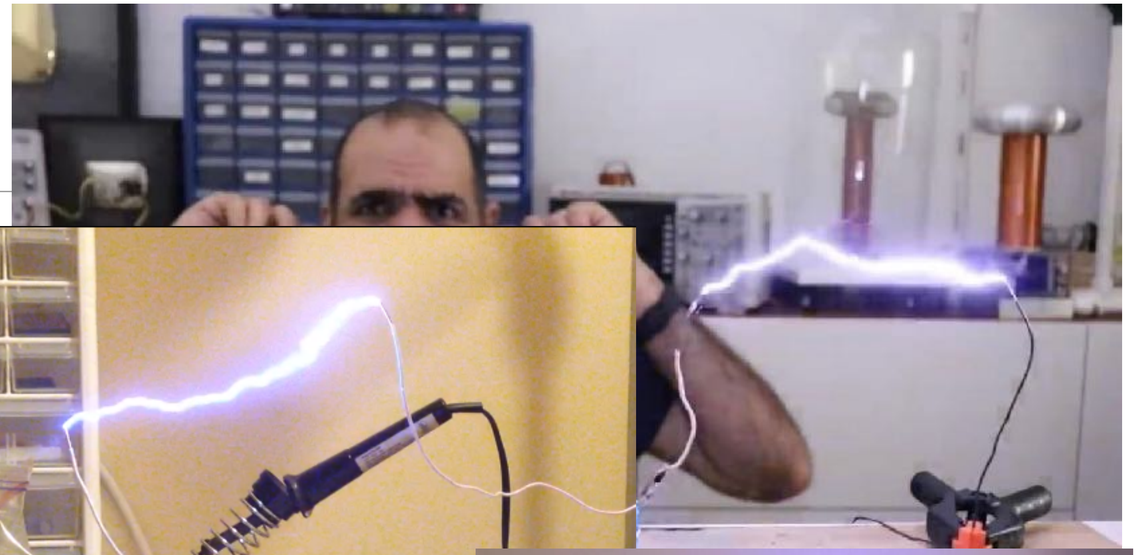


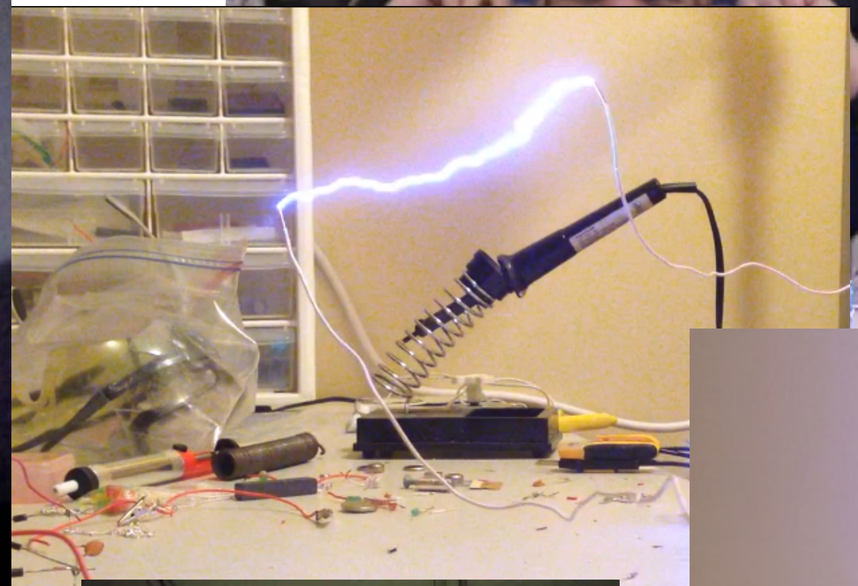


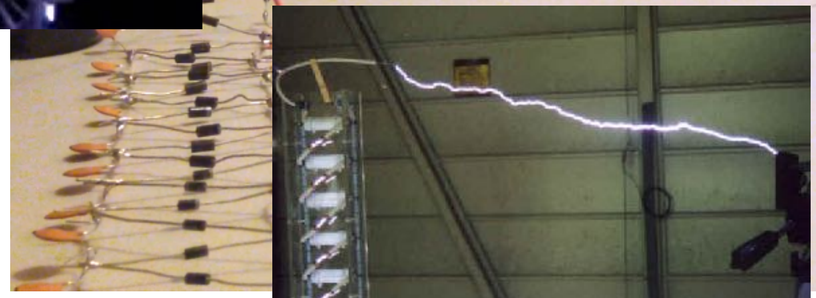
[https://vojenskerozhledy.cz/kategorie/zbrane-se-smerovou-energii]

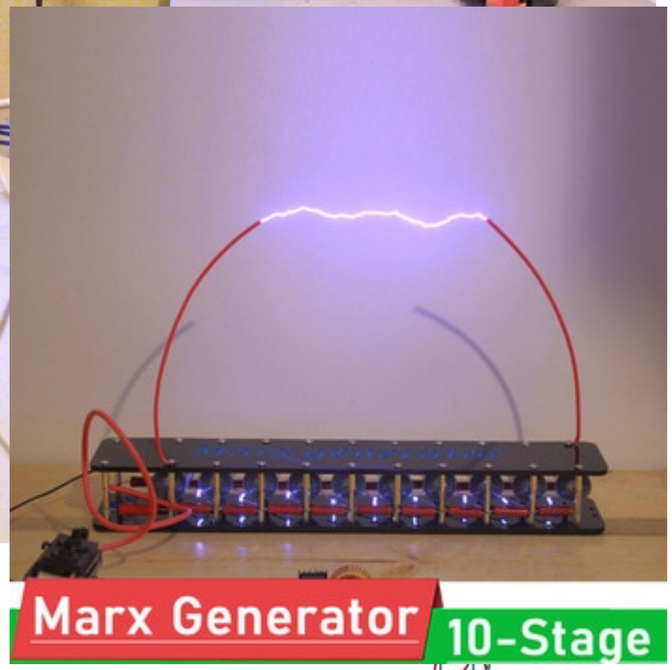
Do not underestimate electronic geeks with internet gadgets

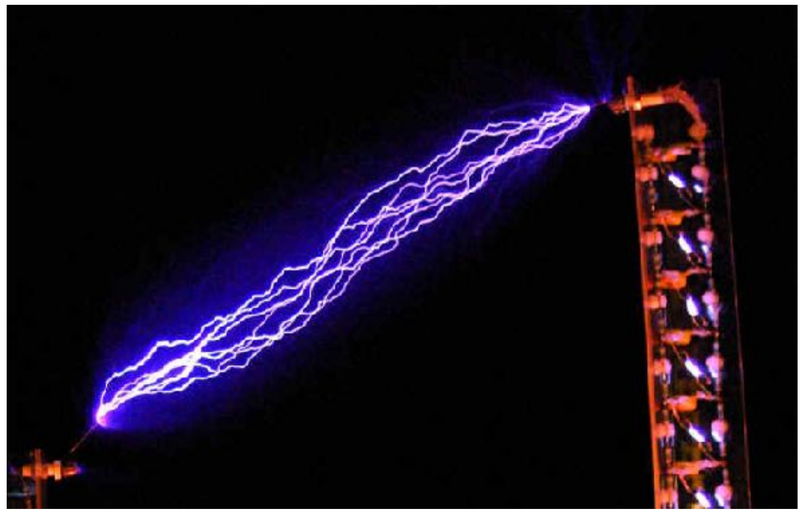












History (year-month-day format)

- 2023-03-27, created as a PIVO briefings merge