Understanding the nature of the threat and what is at stake.

An Emerging Data Breach Threat - Can a Power Line Exploitation Happen in the Data Center?

Introduction- What does this guy think he knows?

- Michael Januszewski, Product Manager for Bantam Clean Power and Digilant, LLC – one of the Lodestone Group of companies.
- Designed and managed small and medium-sized Data Centers as an IT Director
- CTO for Software Development companies
- Patent-holder with 20+ years of experience developing superior-strength surge suppressor and power filtration products utilizing the Bantam Technology
- Developed solutions for government agencies (NSA/USJFCOM/USAAF/USMC) for secure power environments (Red Power/Black Power) and their applications (SIPRnet).
- Products have been serving multiple verticals for over 16 years.

Bantam Technology

How Can a Power Line Exploitation Happen in the Data Center?

Journey

- Situation Overview
- Unpack the information and capturing of the data (How does this happen?)
- What is a PLE (power line exploitation)?
- Review the physics, keeping it simple and high level
- Uncover the source of the emissions
- In particular, what part does the grounding safety path play?
  - How the ground path helps ODINI Malware and PowerHammer exploits
- Closing thoughts and discussion

Bantam Technology

Situation Overview (Some of the ingredients)

- It is possible to extract meaningful data from IT equipment (ITE) by capturing data emitted onto the power lines
- This is an air-gapped attack, which means no physical contact with anything is necessary to obtain the data
- How is data analysis possible? High-speed and highly accurate power measuring equipment readily available
- Published papers have shown the way
- Malware is not necessary to acquire data, but it is helpful
- Net result = Billions of computer devices are exposed today.
- WikiLeaks

Bantam Technology

How Does the Exploit Happen in a Nutshell?

- This exploit involves capturing and interpreting magnetic impulses that are
  - Very low in power
  - Very high in frequency
  - Emitted onto the power supply wires
  - Blended with other electrical impulse ”noise”
  - Blended with the impulses from other electrical devices
  - Able to be acquired without touching anything
  - Generated by malware or not
- Cell phones and other devices can be easily obtained and used to capture and interpret the data.

Bantam Technology

Help me – I don’t get electricity!

Don’t worry, I have a quick and easy tutorial.

We will cover the basic electrical concepts that will allow you to understand what is going on.

Bantam Technology

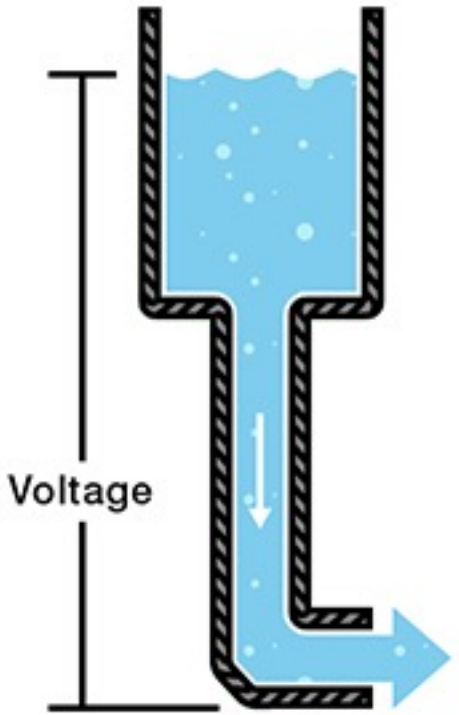
Part 1 – basic electrical values

- What is being measured and translated into data?
- Answer: Current in the form of amperage frequency and strength

Bantam Technology

Voltage (not as important for the exploit)

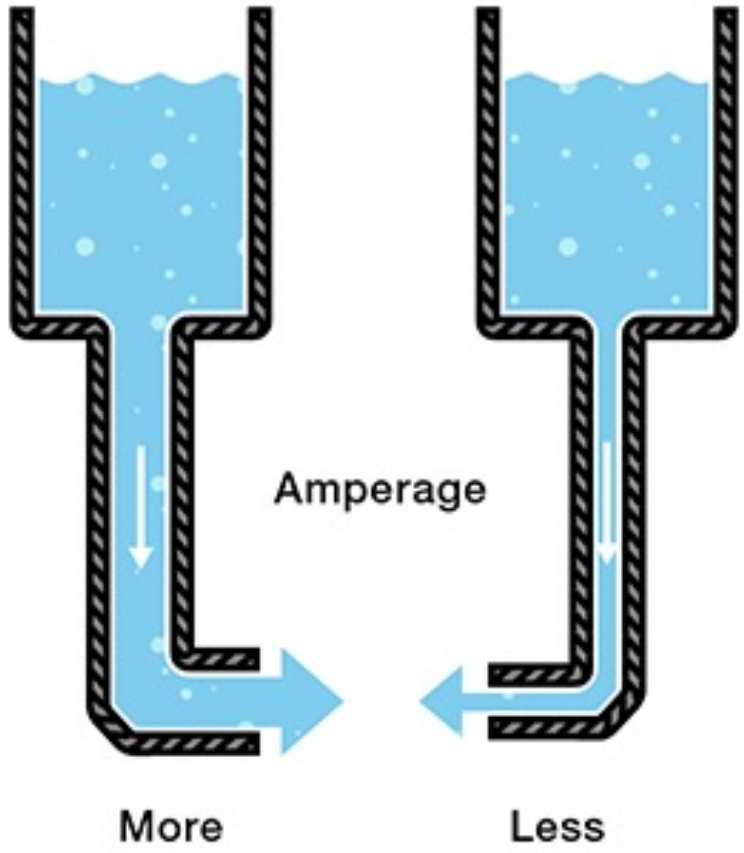
- = potential or pressure
- In this image, potential exists because of the force of gravity being present and equal on both containers.
- Because one container has more water and therefore more mass, there is a potential (voltage) between the two containers
- Therefore, water will flow until both containers have the same amount of water in them.



Bantam Technology

Amperage (part of the exploit equation)

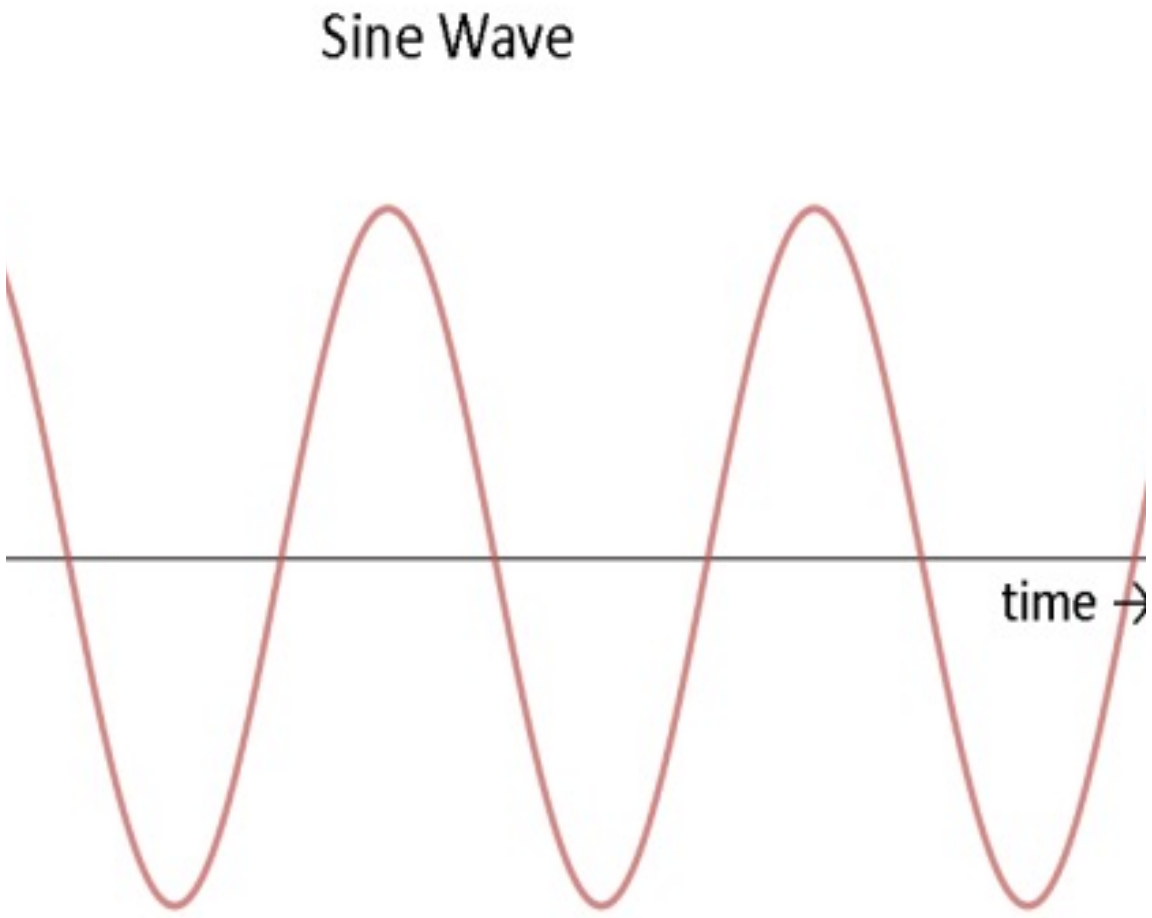
- Unit of measure for the Number of Electrons (a.k.a current) that flow past a given point
- Current cannot flow without an existing potential or voltage
- When the potential decreases, the Amperage also decreases because the pipes do not change in size
- In this example, a bigger pipe equals more current.



Bantam Technology

Why Do I Need to Understand Voltage, Amperage and Time?

- The high-speed devices used to capture the power line emissions used for the exploit are at least measuring and recording the Amperage values over time.
- Time = frequency



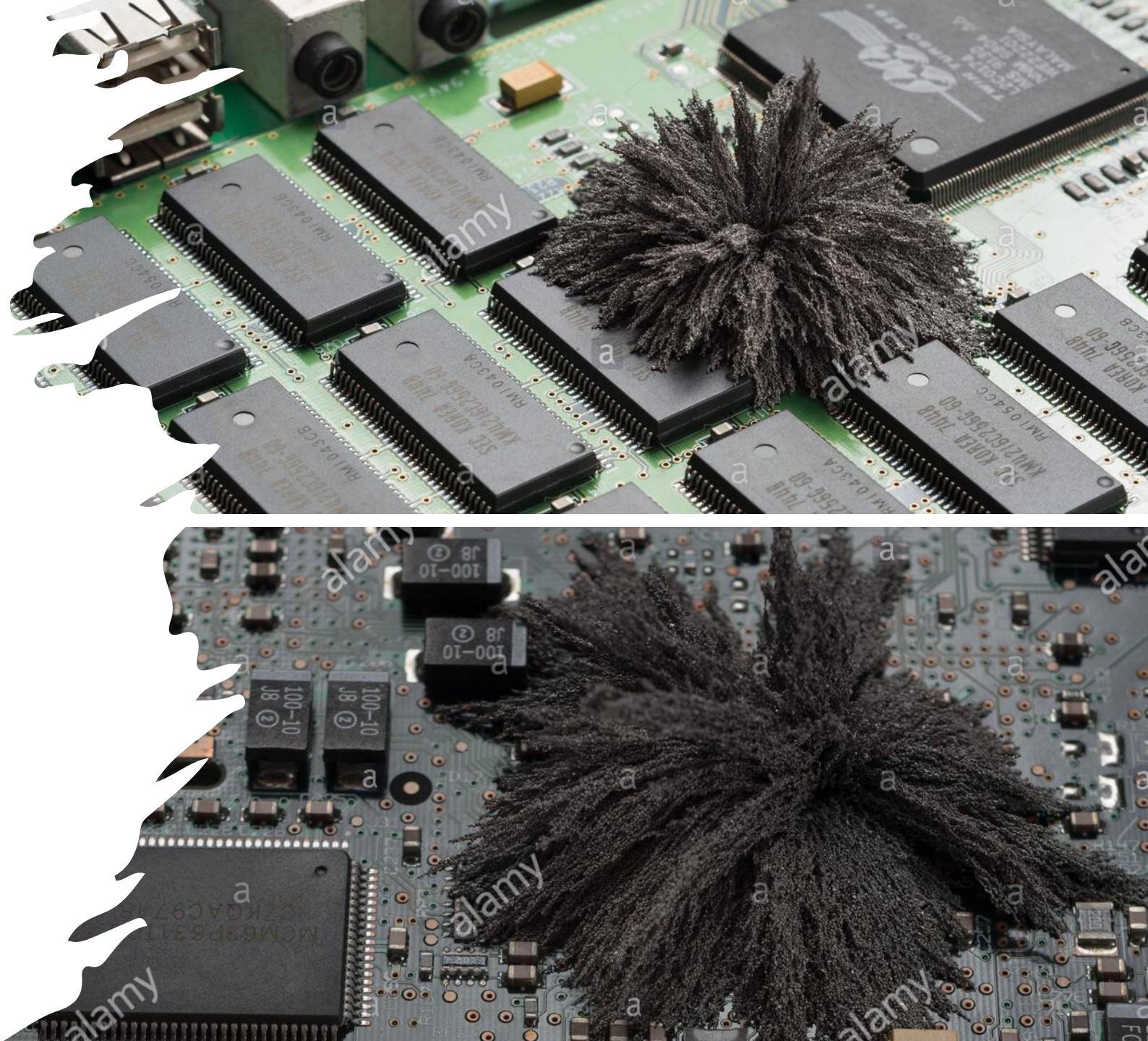
Bantam Technology

Part 2 – data propagation

- How does the data become a series of amperages?
- How does it move along the wires?
- Answer: Four phenomena come together to move data onto the power wires.

Bantam Technology

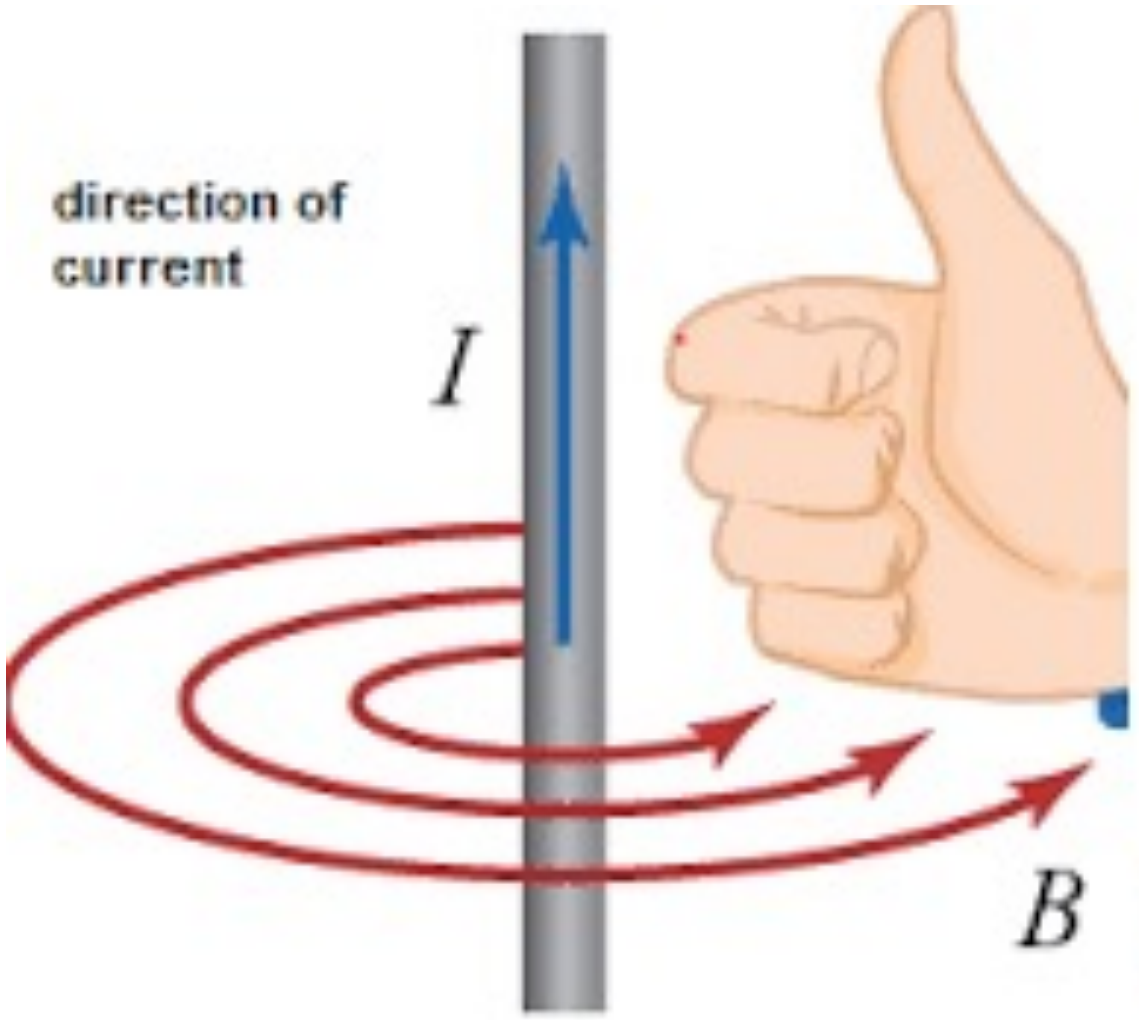
1. Magnetic fields are generated by the high-powered CPUs



Bantam Technology

2. Magnetic Right-Hand Rule of thumb

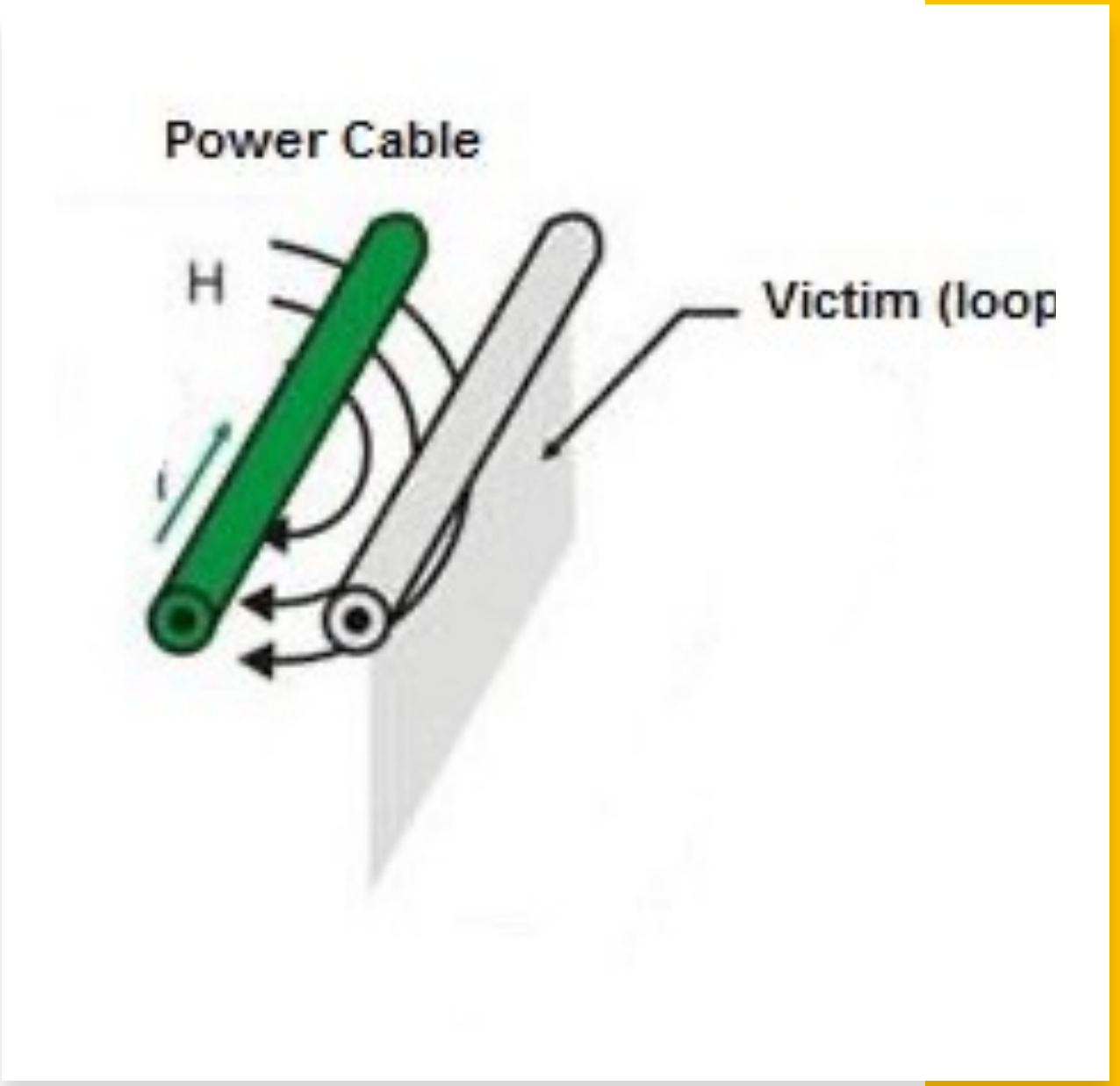
- Current flowing on a wire in the direction of your thumb has a magnetic field rotating around it in a counter-clockwise direction
- The magnetic fields are data, with varying degrees of strength and frequency
- This is the “emission” part of the equation



Bantam Technology

3. Inductive coupling (radio transmission)

- Occurs when the rotating magnetic field of one wire passes through a nearby wire
  - There are three bundled wires in (almost) every ITE power cord
- This is how data in the form of magnetic frequencies (emission) moves from wire to wire.



Bantam Technology

4. ITE has three wires in a power cord*

- Two of the wires have a voltage between them and carry current by design
- and one carries current only if there is a fault, again, by design (a.k.a. the ground wire)

*Some IT devices have a power brick or two-prong AC cord. They still transmit a signal – see Wuhan University paper

Recap - How is data being released electrically inside a computer?

The billions of transistors present in modern CPUs create enough switching energy to generate strong pulses picked up by the electrical power wires inside the computer. Those pulses move from the computer to the outside via the power cord.

Bantam Technology

How does a hacker use these pulses?

- Looks for tell-tale info to determine the make and model of the power supply
- Removes that information from the captured signal and filters for data signals

Bantam Technology

What is unique about the data gathered from this attack?

- It all depends on what the attacker gathers and how it is then used.
  - An inventory of devices on premise can be gathered
  - The movement of devices can be tracked; the absence or insertion of devices can also be tracked
  - Based on power supply signatures, certain wavelengths from devices of interest can be targeted for data exploitation.
- Coupled with malware installed on targeted devices, a compromised computer can be much more easily detected, and data gathered, without any trouble from network security devices like firewalls.

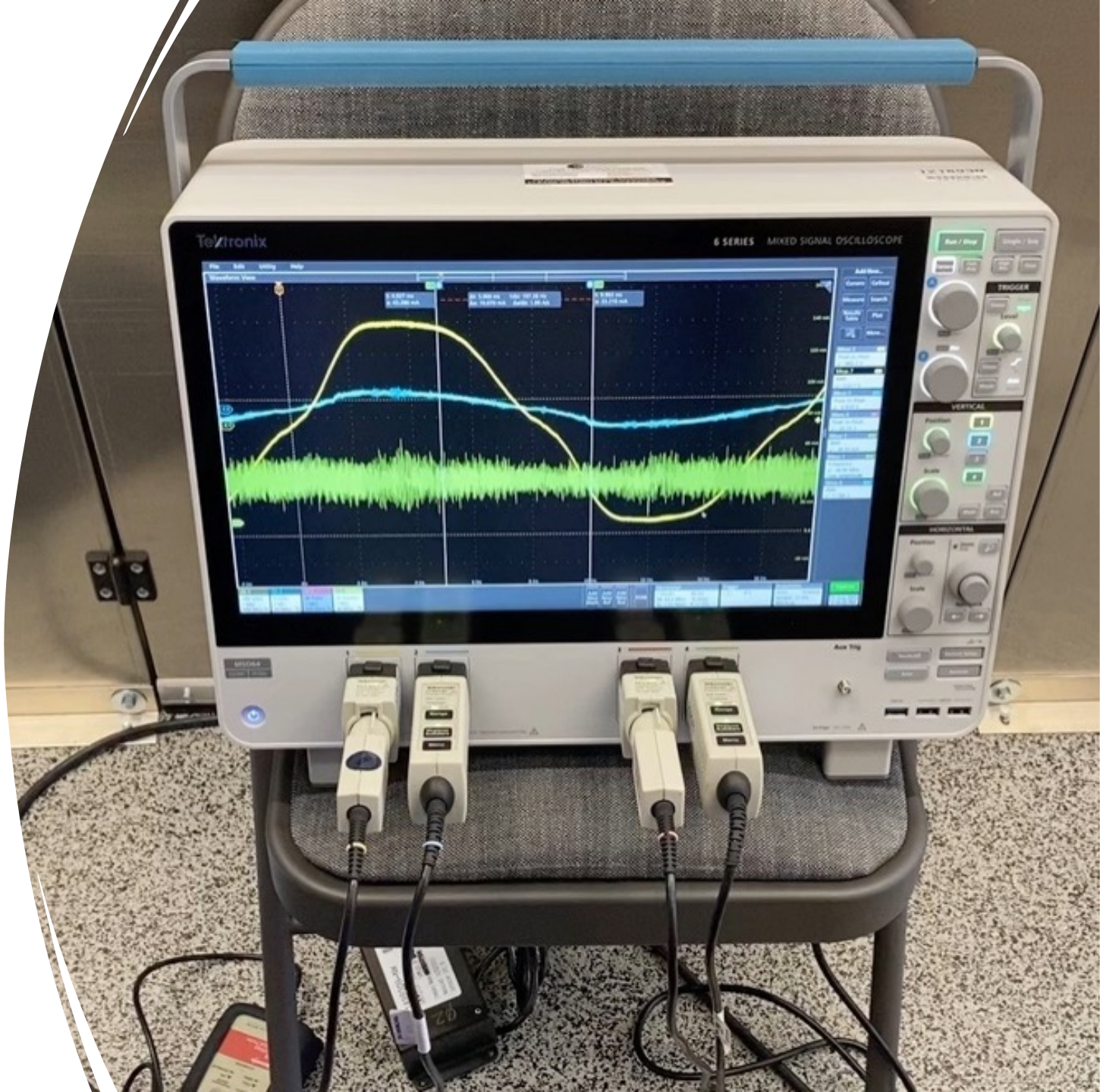
Bantam Technology

Show me how you find power line emissions.

- Voltage and Current signals are captured in their various frequencies using an oscilloscope, which is a device that plots data points over time and produces lines that sometimes look like waves, which is why the pictures it creates are called “waveforms.”
- **To get amperage or current data, the probe clamp needs to only surround a wire, or be physically near it. This is why the attack is considered air-gapped.**
- A hacker can use these big scopes or have a laptop or cell phone equipped to capture with the same accuracy.

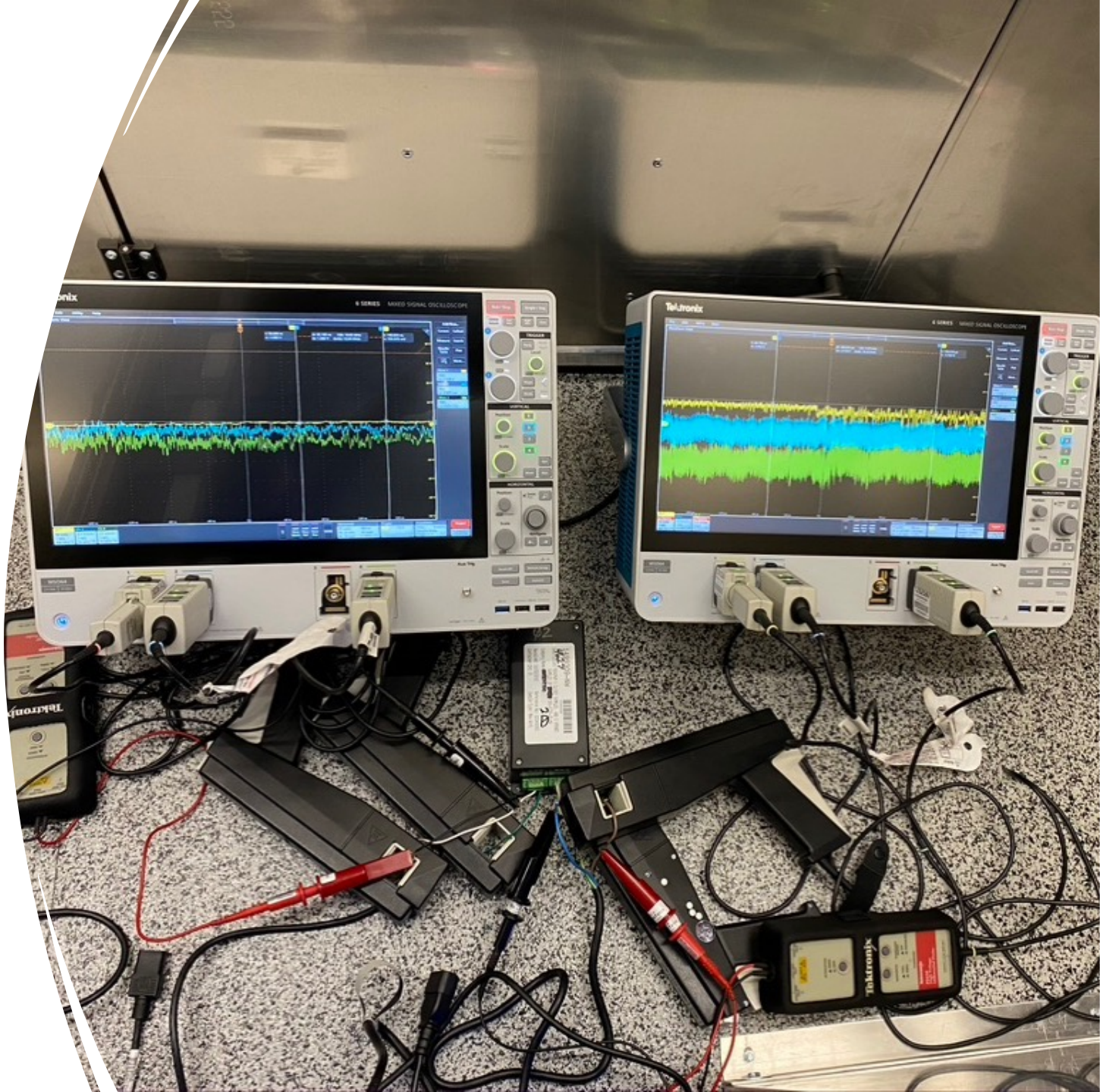
Bantam Technology

State-of-the-art high-speed oscilloscope

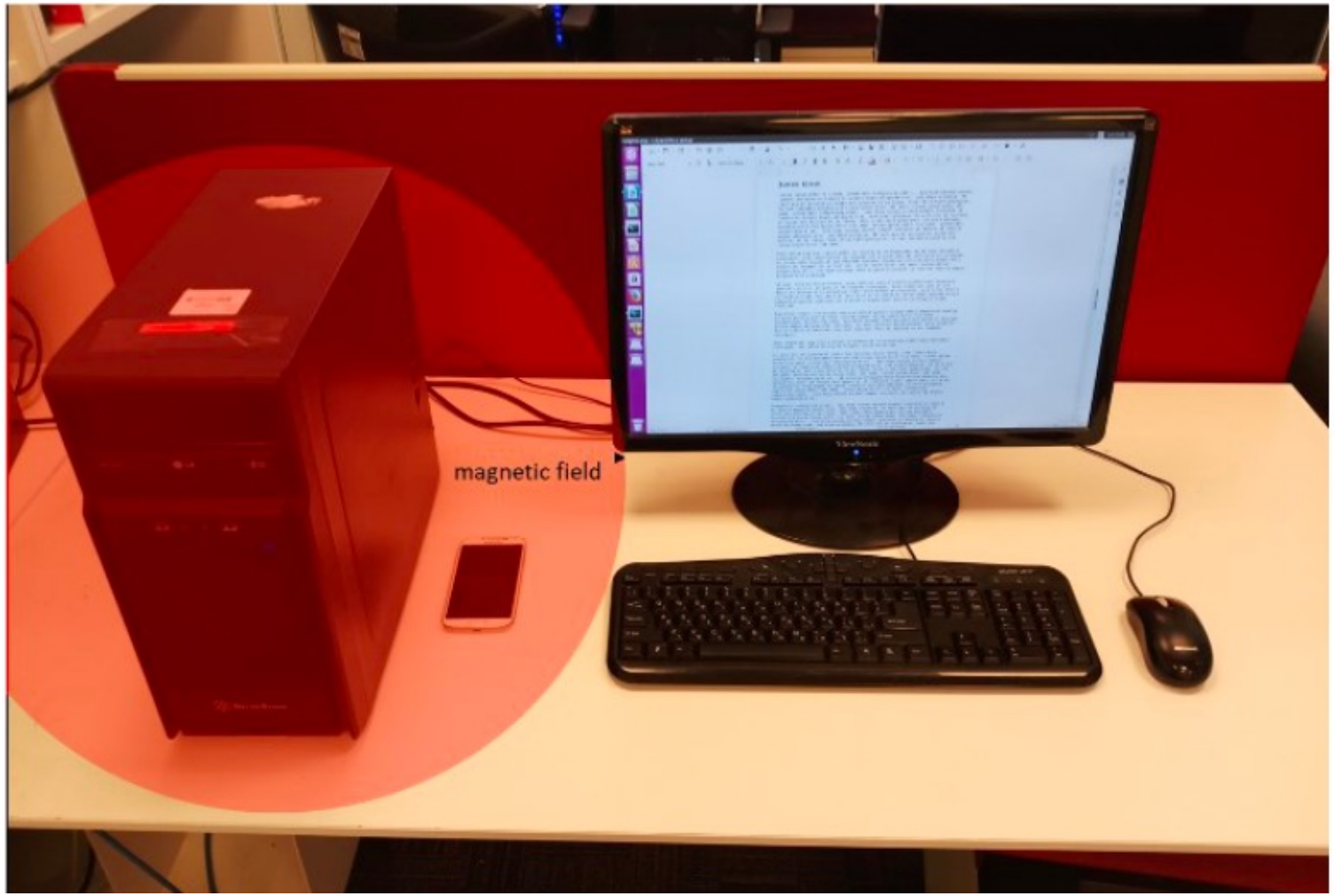


Bantam Technology

Voltage and Current probes attached to the power cord



Bantam Technology



Another Data Capture Scenario with a Cell Phone and NFC antenna

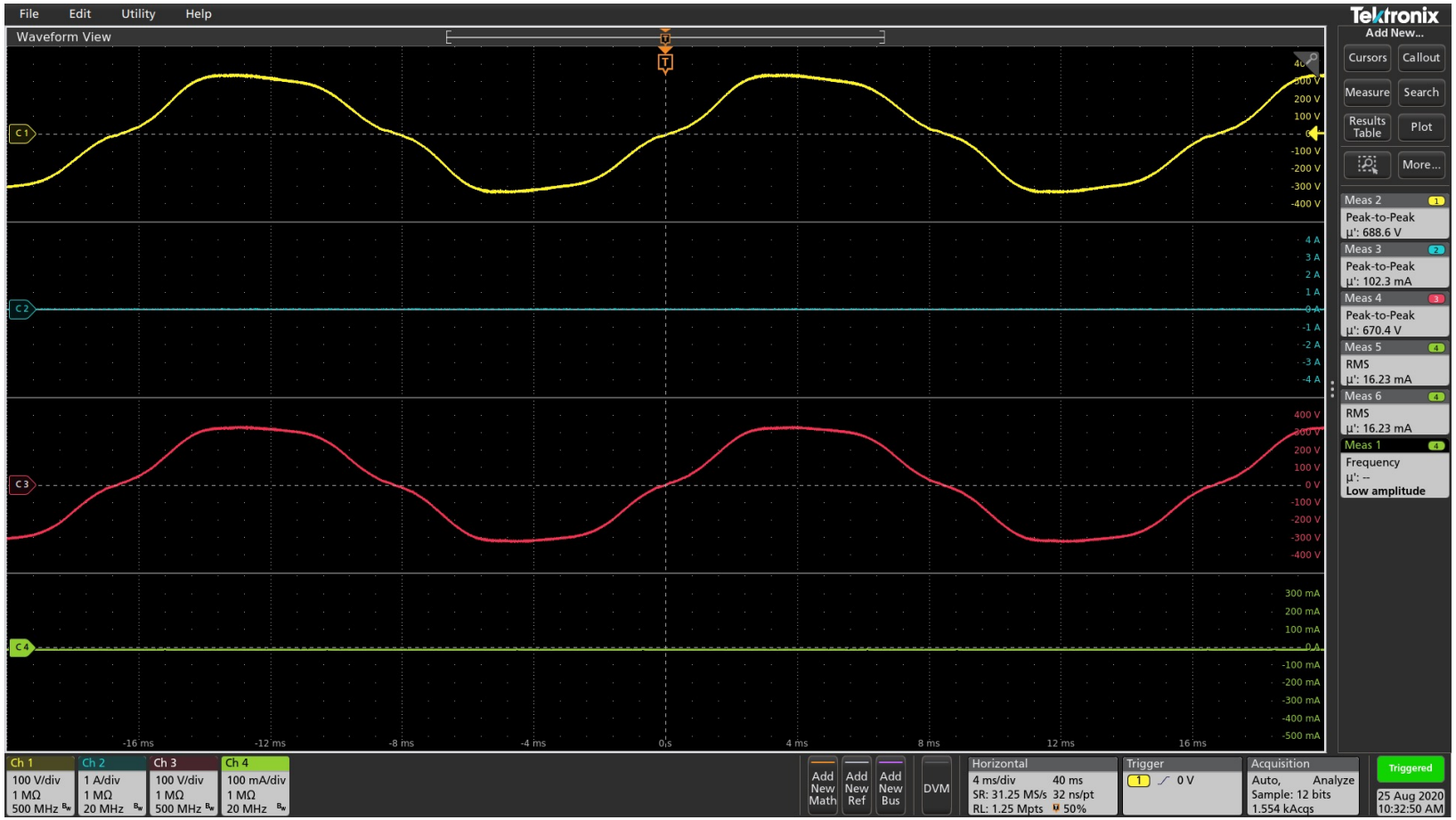
Data Capture Devices

- We are using o-scopes to more thoroughly discover and record the data signals, but this is not the only way to acquire the data, once you know what you wish to capture:
  - Near Field Antenna
  - Current transformer and data logger
  - Radio
- Much of this knowledge is more widely known now because of tactics revealed by WikiLeaks

Bantam Technology

How do I read an o-scope?

Smoother and flatter = clean; squiggly = a signal



This image is of an ideal state, with no load or current being drawn and the voltage supply distorted by other larger loads, which is typical.

Legend

- Yellow = AC Mains Voltage
- Blue = AC Mains Current
- Red = Line/Ground Voltage
- Green = Ground Current

Bantam Technology

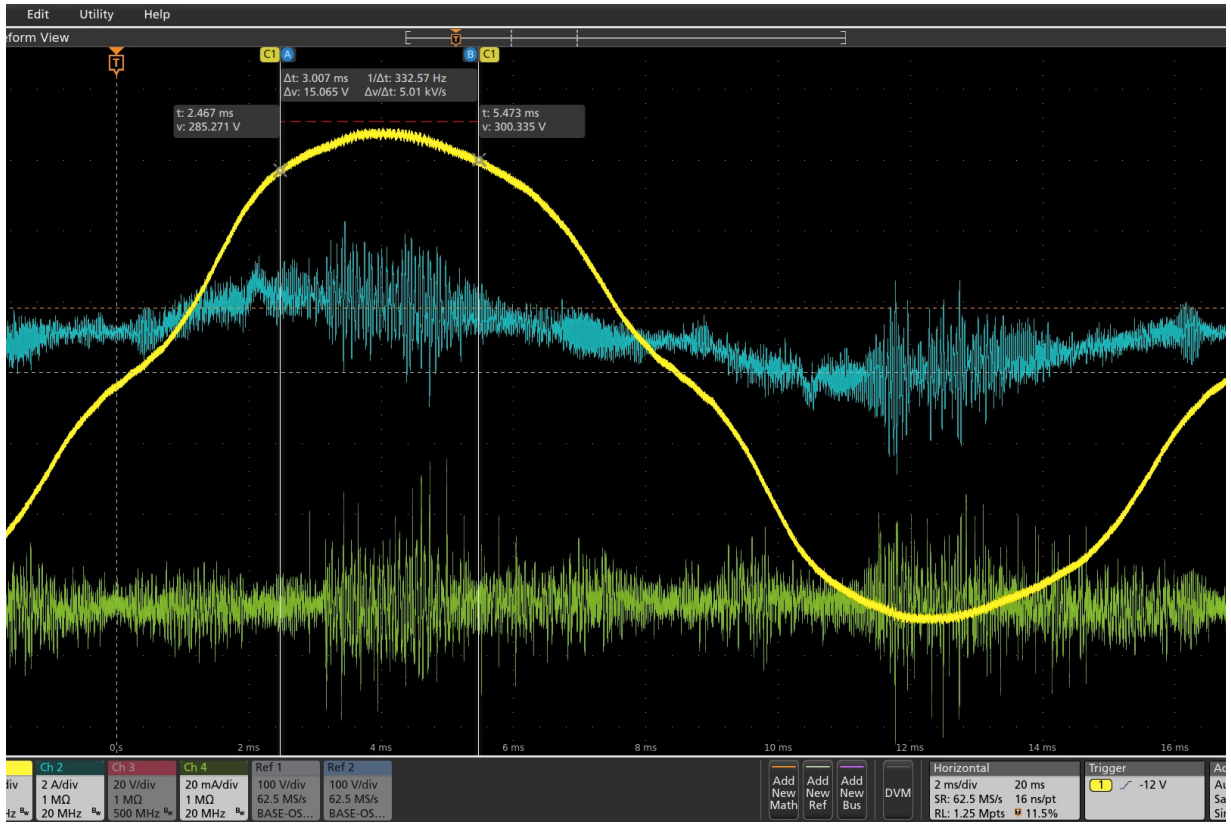
Electrical signature uniqueness examples

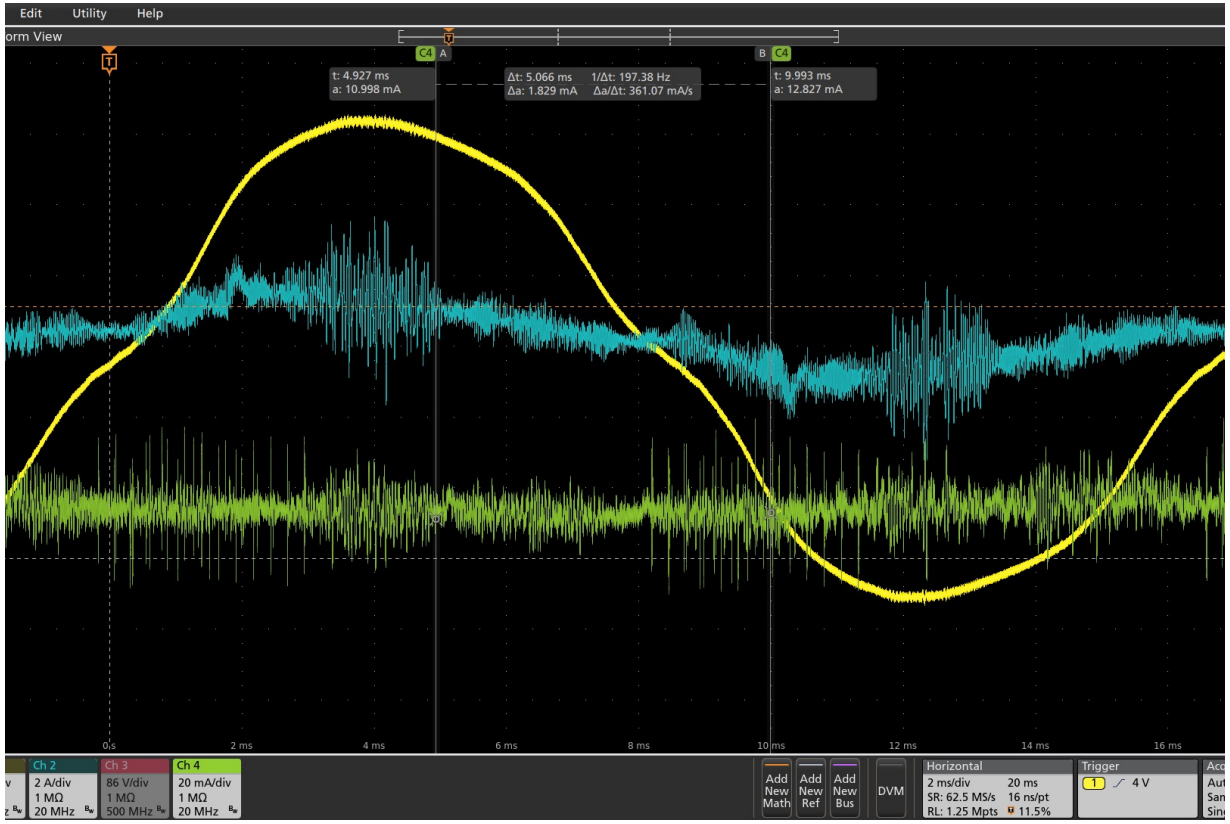
- Same Make/Model of Networking Firewall/Edge device
- Same Make/Model Server with 112 processing cores

- We will look at screen captures from an o-scope of two identical pieces equipment located in two different cabinets.

Bantam Technology

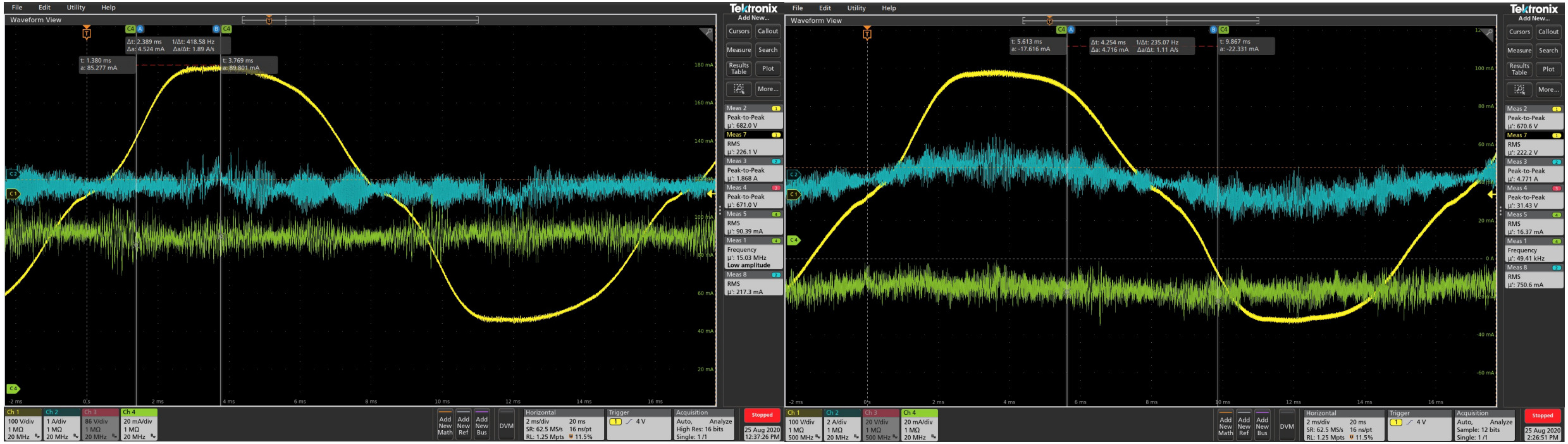
Two of the Same Make/Model of Networking Firewall/Edge device





Bantam Technology

Two of the Same Make/Model of Server with 112 processing cores each

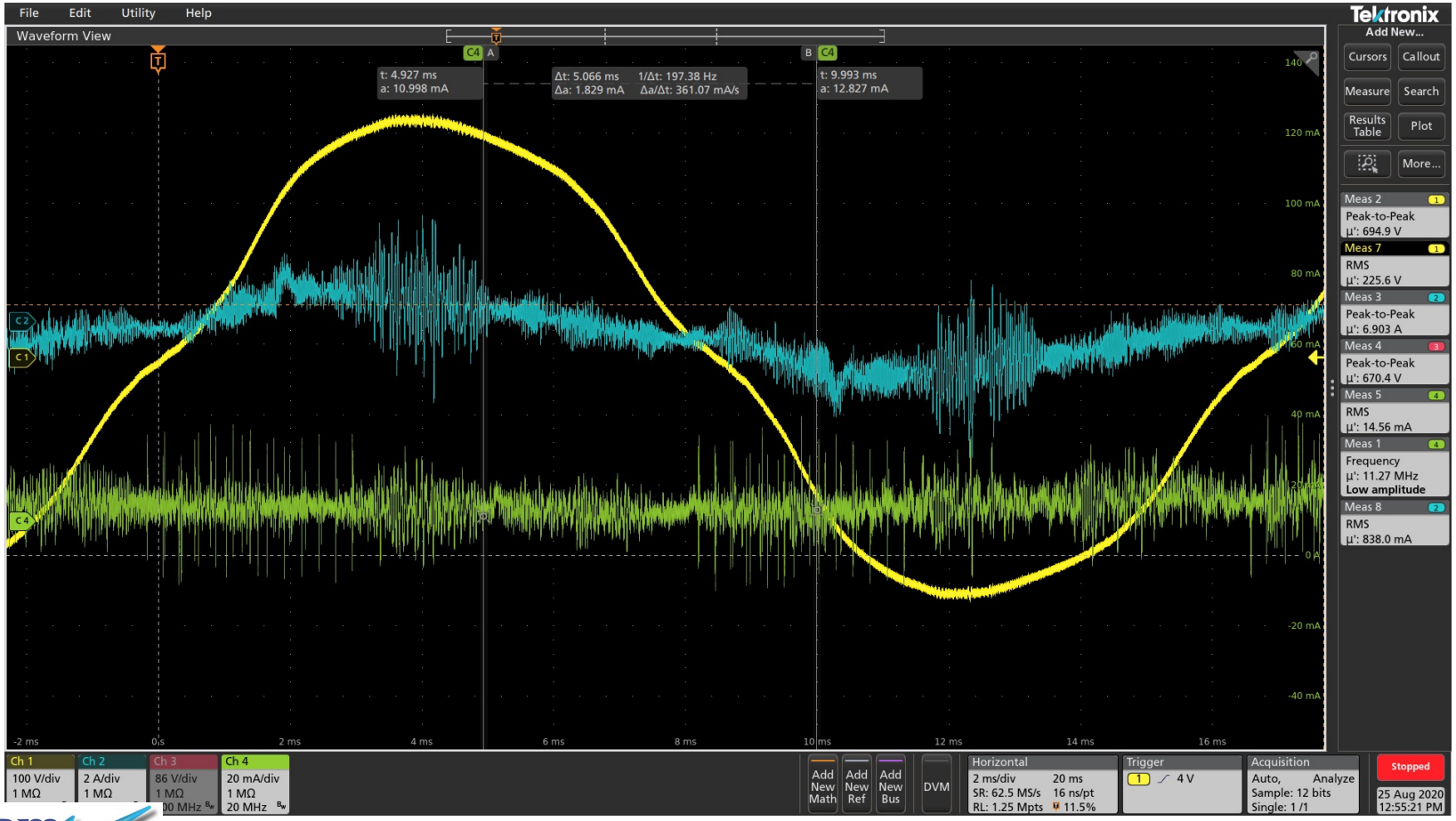


Bantam Technology

Following the Power Line Emission Upstream

- Let’s follow an emission from
  - The back of the power supply
  - To the main circuit breaker panel
  - To the outside of the building

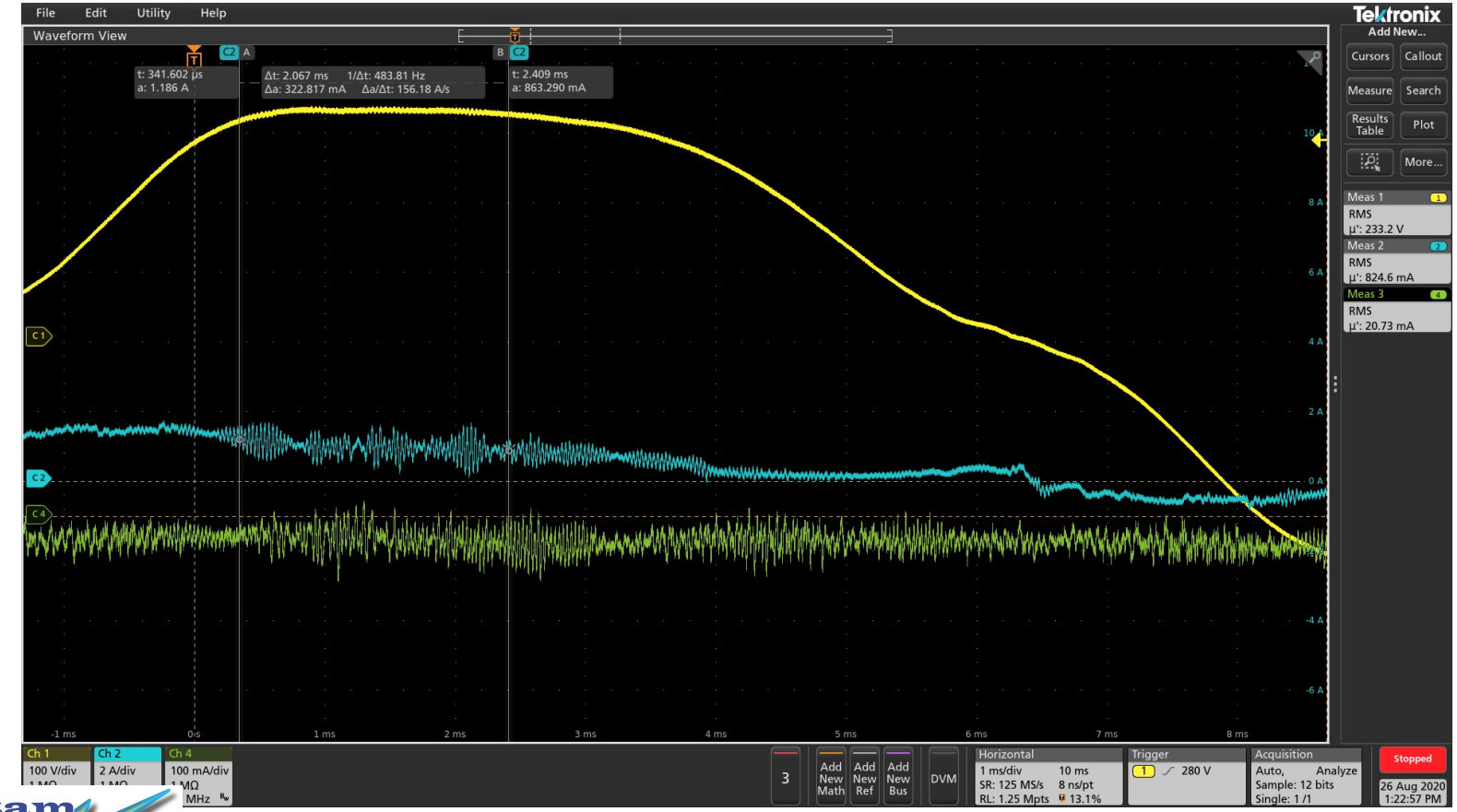
Sample ITE: network firewall device Measurement taken on power cord



We are tracking a set of signals from 20kHz through 3 GHz on the blue and green lines

Bantam Technology

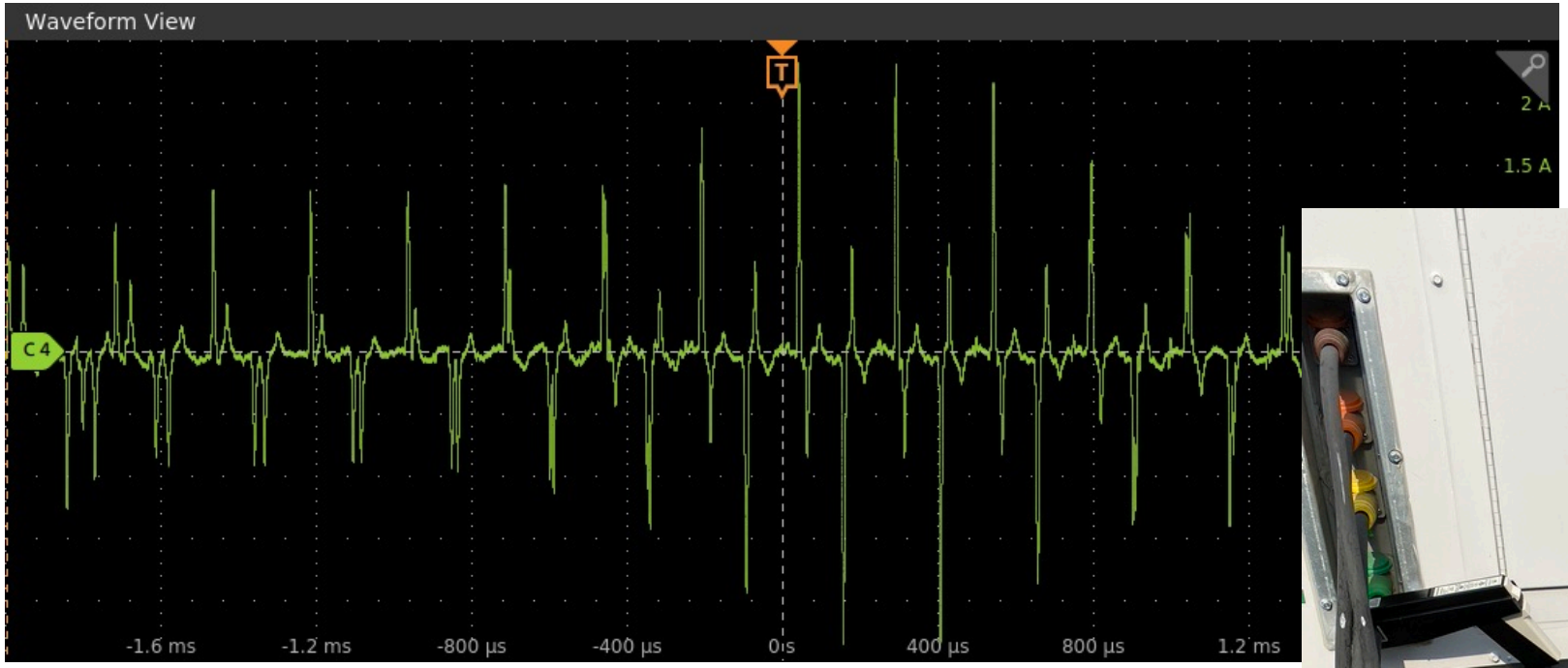
Sample ITE: network firewall device
Measurement taken on grounding path in circuit breaker panel



We are tracking a set of signals from 1kHz through 1 GHz on the blue and green lines

Bantam Technology

Sample ITE: network firewall device External Grounding Wire, outside



Bantam Technology

Published Exploits

- IEEE ODINI Malware – even Faraday shielding is insufficient
- PowerHammer – high bit-rates below the FCC filtering standard
- Magneto – CPU workload pulsing puts info on the power lines

How can I remove the powerline signals that could enable a PLE?

The solution needs to address the two main ingredients:

- Prevent the ITE's switched mode power supply imprint and the CPU transistor signals from moving upstream past the ITE's power supply
- Prevent any signals from also be induced onto ground

The ideal place to do this is inside the power supply of the ITE

The next ideal space is right next to the Point of Use, or immediately at the power input of the ITE

Bantam Technology

PLE 115 ITE Electrical Firewall

- Vertiv/Geist and Bantam Clean Power launch the very first power filter designed and tested to be an effective Power Line Exploit firewall.
  - Using patented technology, the PLE 115 permanently alters electrical impulses from all three wires , effectively removing any discernable electrical signals emitted by the ITE
  - The PLE 115 firewall plugs in between the power source and the ITE power supply.
  - One PLE115 is needed per power supply (e.g. if ITE has two redundant power supplies, two PLE115 needed)
  - Supports 110 or 230 Volts with male and female IEC320 C10 inlet and C13 outlet.

Bantam Technology

Vertiv/Geist PLE 115 featuring Bantam Technology

More info can be found at
https://www.bantamcleanpower.com/ple

Bantam Technology

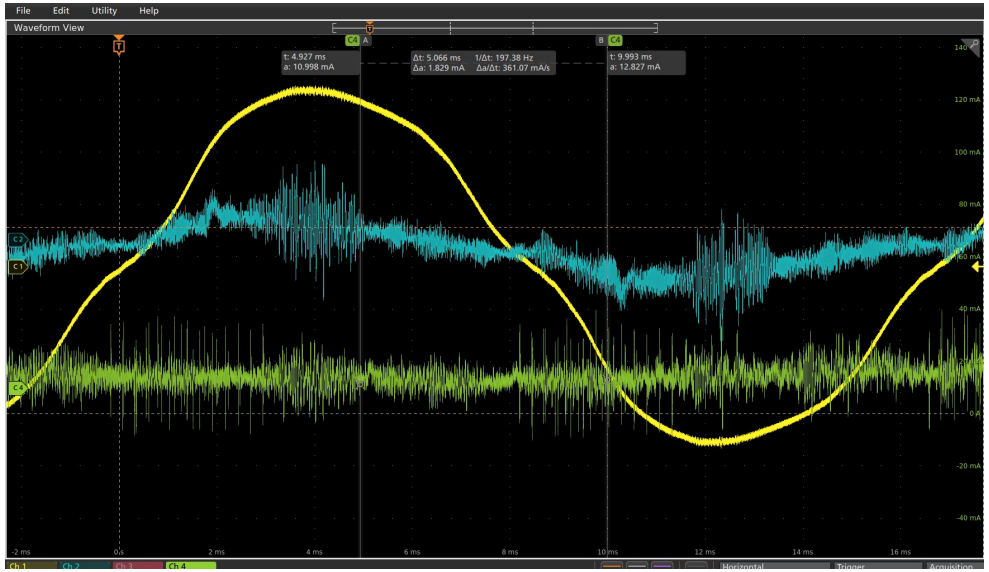
Bantam Clean Power SA3600A PLE Component

- The SA3600A PLE remediation module is a UL-Recognized under 62368-1. System designers and engineers can now obtain this technology in a ready-to-integrate sub-assembly for full PLE firewall protection inside a UPS, Server, or other Information Technology Device.
- **Protected by U.S. Patents and patents pending.**

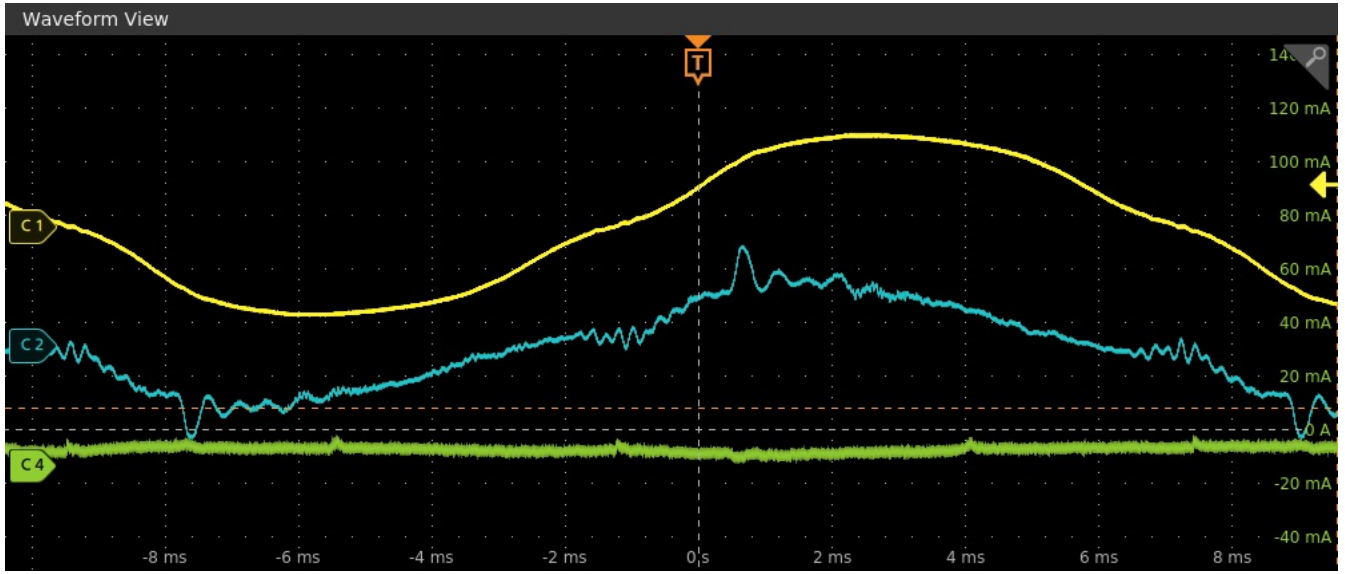
Bantam Technology

PLE Remediation Results

Network Edge Device Without Bantam Tech



Same Device With Bantam Tech firewall



Bantam Technology

Resources for further Information

- https://www.bantamcleanpower.com/ple has a complete list of the published documents of the exploits we discussed today.
- Mike Januszewski MichaelJ@lodestonepacific.com
- (630) 929-3050

7X24 Exchange
The end-to-end reliability forum.
Northwest Chapter

Thank you for attending!

Bantam Technology