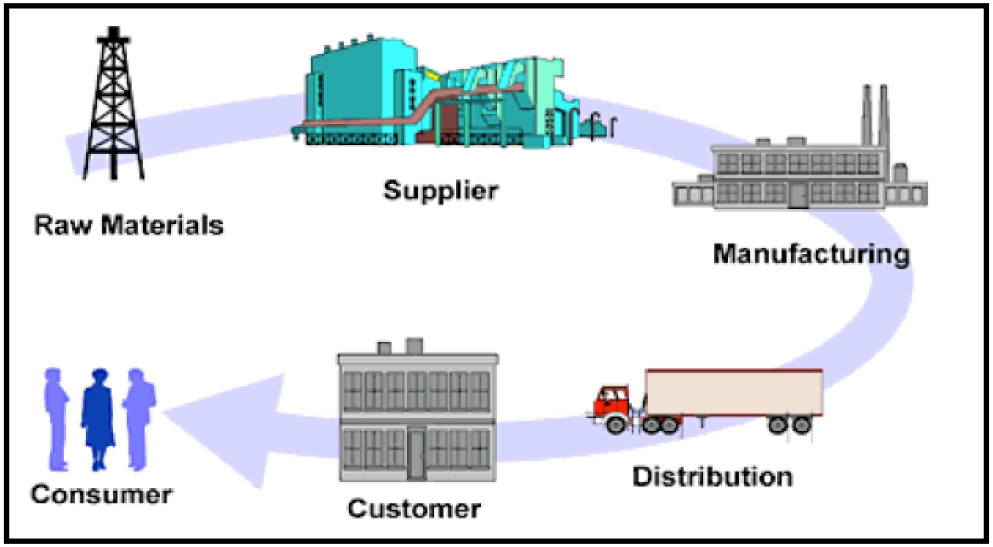
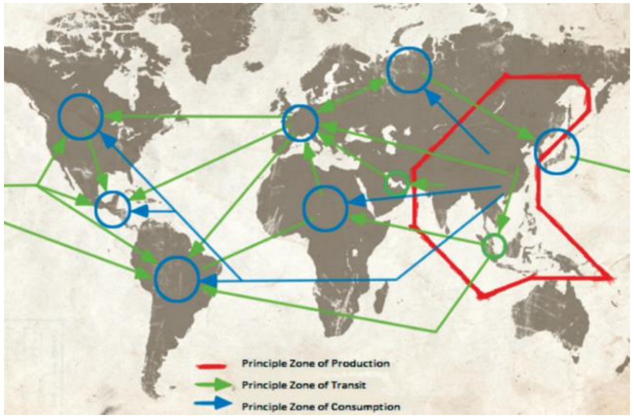
PHysical Inspection and attacKs on electronicS (PHIKS)

Navid Asadi

Supply Chain Complexity

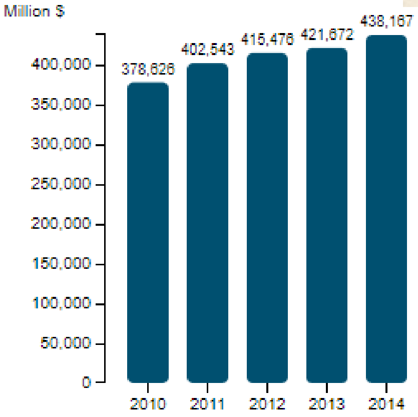


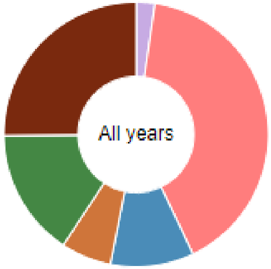
Advancements and cost reduction of transportation and rise of e-commerce are easing the globalization


Principle Zone of Production
Principle Zone of Transit
Principle Zone of Consumption

Source of complexity: Increasing number of suppliers, manufacturers, wholesales, retailers

Increases the risk of product counterfeiting





All years

Country	Value	Share
Canada	47,000	2%
China	835,690	41%
European Union	210,025	10%
Japan	126,599	6%
Mexico	320,202	16%
Sub-Saharan Africa	517	0%
All others	516,451	25%
Total	2,056,484	100%

Economic Impact

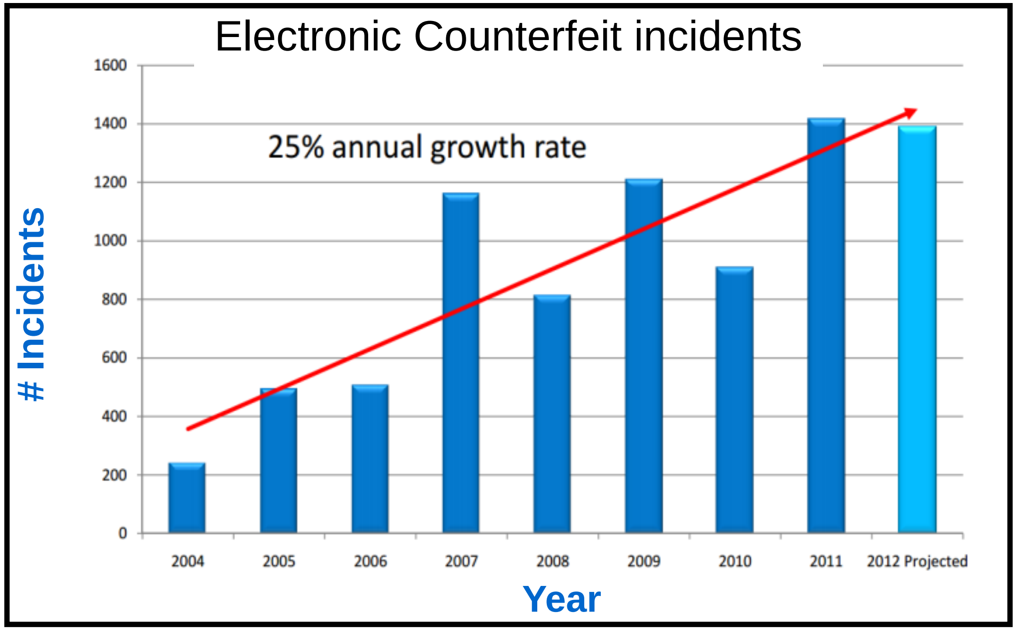
ICC

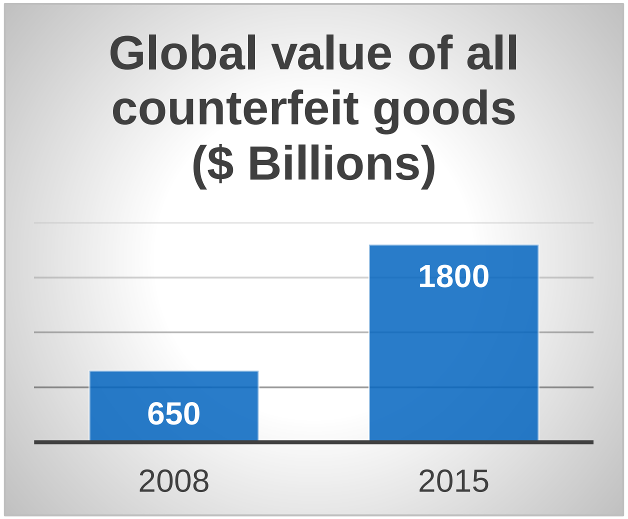
unicri
United Nations
Interregional Crime and Justice
Research Institute

OECD
BETTER POLICIES FOR BETTER LIVES

EUROPOL

Havocscope
Global Black Market Information


Electronic Counterfeit incidents


Global value of all counterfeit goods ($ Billions)

United States

- Trade secret theft is estimated to be **1-3 % of U.S. GDP**
- **NSA** and **FBI** estimated the loss to be hundreds of billion dollars annually
- **750** thousand jobs at risk

Worldwide

- **5-7** % of world trades
- **2.5** million jobs at risk every year

Electronics

Represent a hazard if incorporated in critical systems:
Transportation, Energy, Communication, health, etc.

1% of semiconductor revenue comes from military

Raytheon, Honeywell, Lockheed Martin delivered systems containing counterfeit parts

Cost of Counterfeit Incidents in Military
$4 million in 7 cases in military 2011
$165 million in Russian Mars spacecraft crashed in 2012

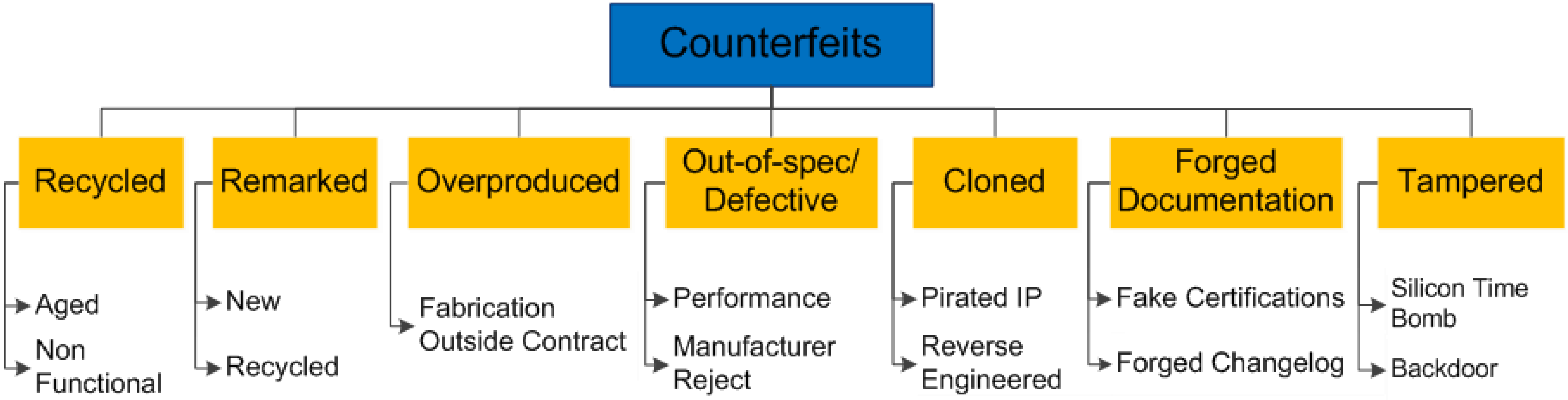
Fake electronics becoming military danger

Military Systems Affected
Aircrafts and helicopter
Weapons systems, Missile defense system

Counterfeit Chinese Parts Slipping Into U.S. Military Aircraft: Report

By LEE FERRAN · May 22, 2012

Taxonomy of Counterfeits



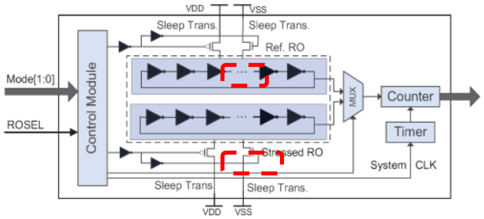
Counterfeits

- Recycled
  - Aged
  - Non Functional
- Remarked
  - New
  - Recycled
- Overproduced
  - Fabrication Outside Contract
- Out-of-spec/ Defective
  - Performance
  - Manufacturer Reject
- Cloned
  - Pirated IP
  - Reverse Engineered
- Forged Documentation
  - Fake Certifications
  - Forged Changelog
- Tampered
  - Silicon Time Bomb
  - Backdoor

Counterfeit Detection and Avoidance

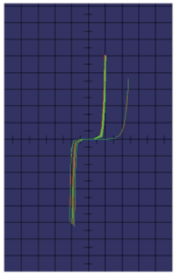
Design-for-Anti-Counterfeit (DfAC)

- On-chip (PUF, active hardware metering, SST, CDIR, etc.): only applicable to <u>new</u> parts
- On-package (DNA and nanorods): expensive and not widely accepted by industry



Electrical Testing: <u>Nontrivial</u> to cover all scenarios

- Require knowledge of each IC
- Different test setups

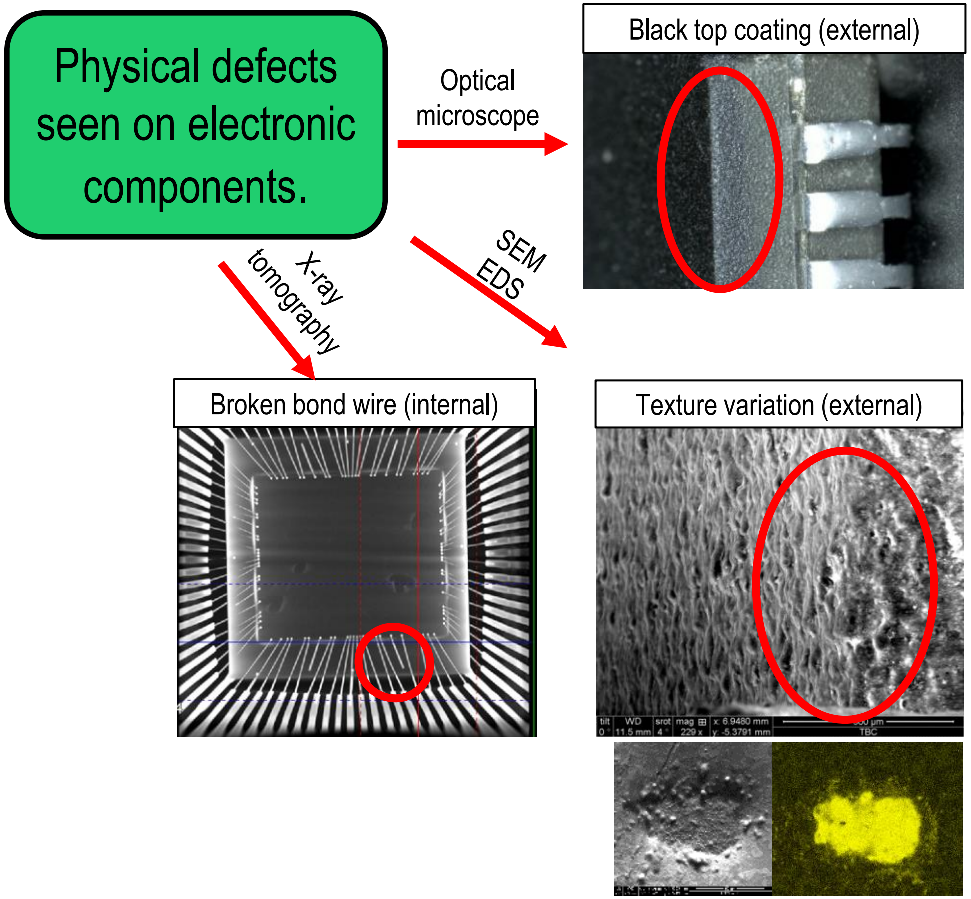


Physical Inspection: Scrutinize external, internal defects, and material composition (<u>closest</u> to all-in-one)

- Covers all part types, all states of existence, and most counterfeit types

Defect Detection

- Different imaging modalities are used for detecting defects
- Counterfeit electronics are divided into 7 different classes.



Physical defects seen on electronic components.

Optical microscope

X-ray tomography

SEM EDS

Black top coating (external)

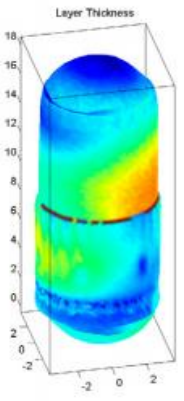
Broken bond wire (internal)

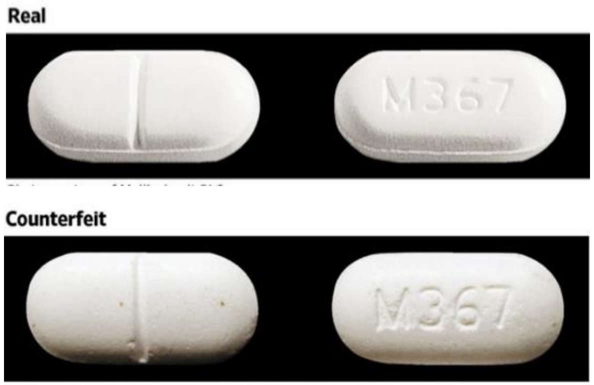
Texture variation (external)

Pharmaceutical

Ingredients found in counterfeit medicines

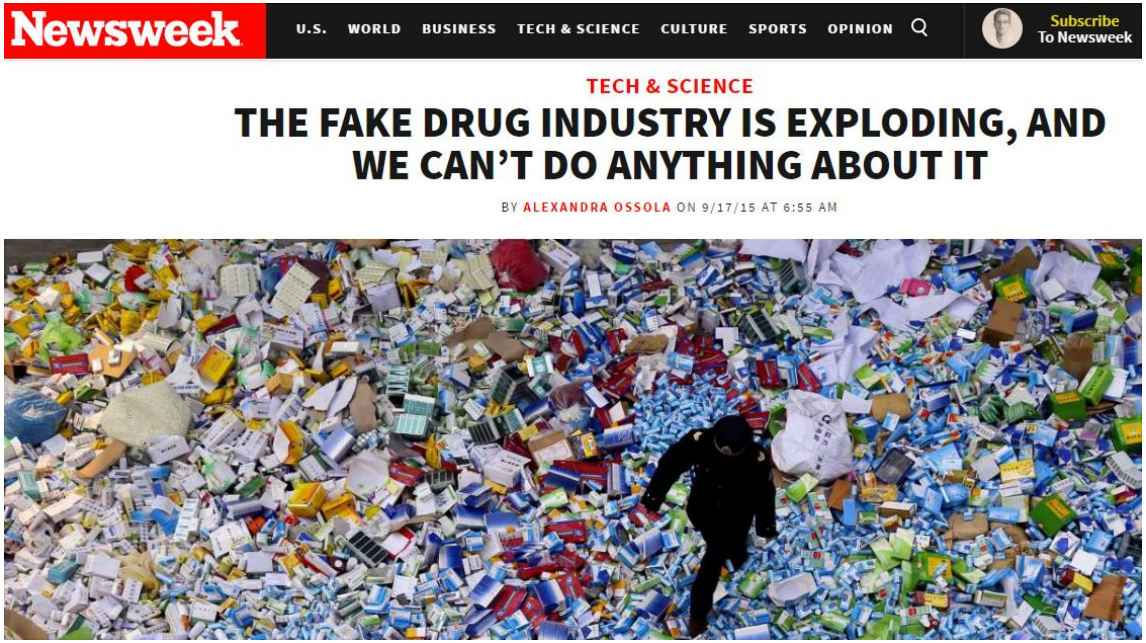
Heavy metals: Mercury, lead
Actual poison: rat poison, antifreeze
Contaminants: road paint, floor wax





Up to **1 million people die** annually from counterfeit pharmaceuticals

700 fentanyl-related **death** reports in U.S. between 2013 - 2014
65% increase of Fentanyl from 2014 to 2015



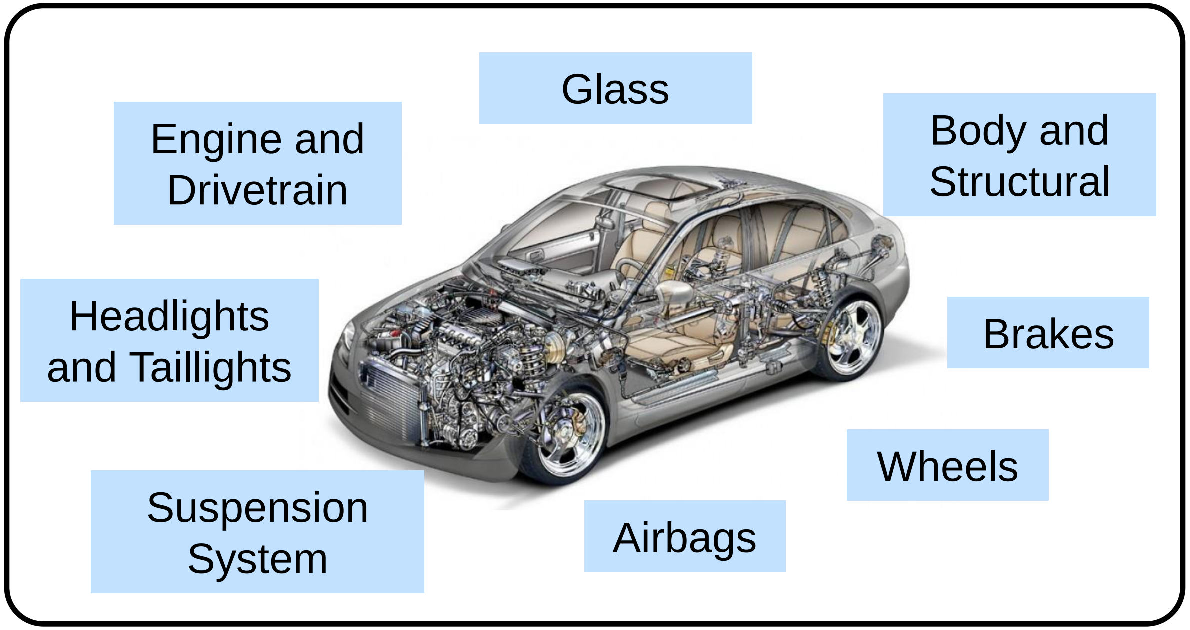
TECH & SCIENCE

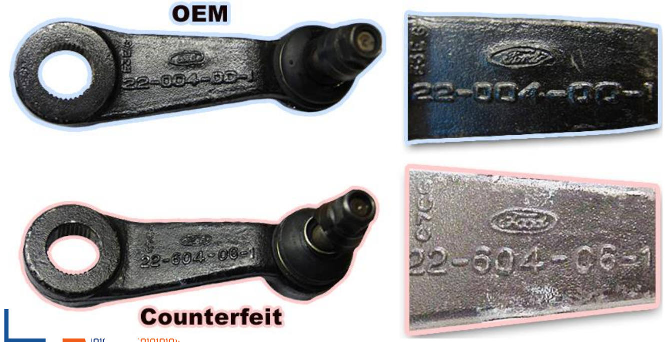
THE FAKE DRUG INDUSTRY IS EXPLODING, AND WE CAN'T DO ANYTHING ABOUT IT

BY ALEXANDRA OSSOLA ON 9/17/15 AT 6:55 AM

Automotive Parts

NHTSA Test, Video of Counterfeit Air Bags





Economical impact

In 2015, MEMA estimated automotive counterfeiting impacted **$300-$500 billion** and is growing 10% every year

Fatalities

90 **deaths** reported in Dubai roads in first half of 2010 because of counterfeits

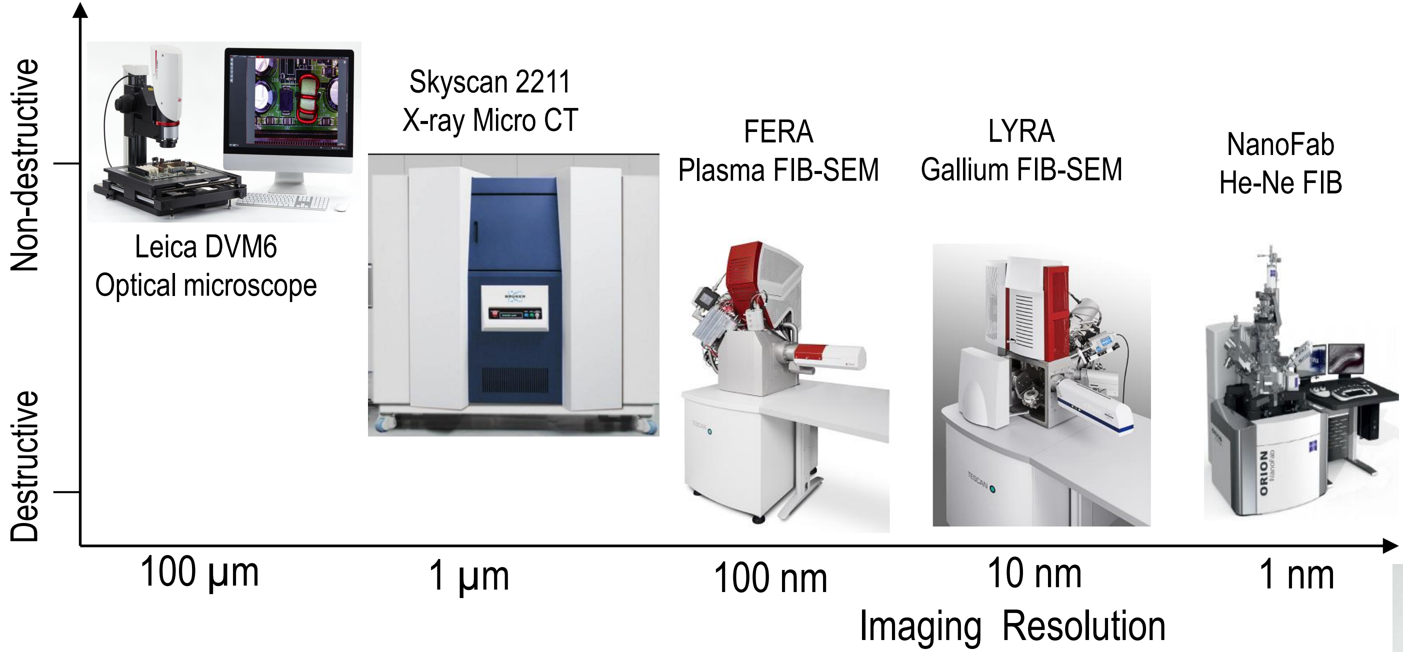
Other Products and Impacts

Ranking of Counterfeit Goods by Losses	
Pharmaceuticals	$200B
Electronics	$169B
Software Piracy	$63B
Foods	$49B
Auto Parts	$45B
Toys	$34B

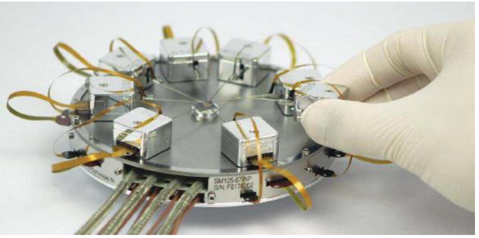
Counterfeit Socioeconomic Impacts of All Counterfeits

Consumers	Businesses	Governments
Loss of life, safety and reliability issues, theft of private information, Low quality products	Lost sales, decreased profit, loss of brand trust	Decreased tax revenue, increased spending on CBP, welfare, and health services, etc.

Microscopy and FA Tools



Phemos
Photonic Emission Microscopy



Micro/Nano probing

- Imaging and debugging tools are developed for fault analysis.
- Fast advancement in FIB/SEM imaging
- Advancement in photonic emission microscopy, LVS, IR analysis
- Development in micro and nano probing, EBIC, EBAC

Failure Analysis Market

- Failure Analysis Market by equipment (SEM, TEM, FIB, Dual), Technology (SIMS, EDX, CMP, FIB, BIM, RIE), Application (Material Science, Bio Science, Industrial & Electronics) worth $10B by 2020 with CAGR 7.5%.
- Highly competitive with a few leading players, namely, Carl Zeiss SMT GmbH (Germany), FEI Company (U.S.), JEOL Ltd. (Japan), Hitachi High-Technologies (Japan) and Tescan (U.S.), etc.

JEOL Solutions for Innovation

RAITH NANOFABRICATION

ThermoFisher SCIENTIFIC

ZEISS

TESCAN PERFORMANCE IN NANOSPACE

HITACHI Inspire the Next

HAMAMATSU PHOTON IS OUR BUSINESS

OXFORD INSTRUMENTS The Business of Science®

GATAN

BRUKER

MSA Microscopy Society of America

MAS Microanalysis Society

M&M 2018 MICROSCOPY & MICROANALYSIS August 5-9, 2018 • Baltimore, MD

ASM INTERNATIONAL

EDFAS Electronic Device Failure Analysis Society

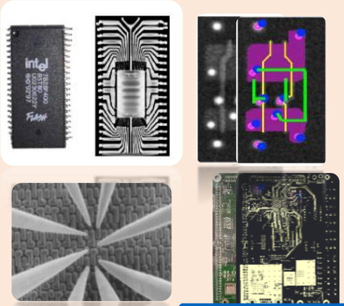
ISTFA/2018

PAINE Workshop

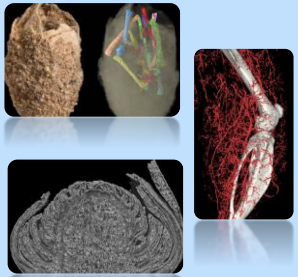
Microscopy and Imaging Applications

Electrical and Computer Engineering

Counterfeit ICs
IC RE
PCB RE
Physical Attacks



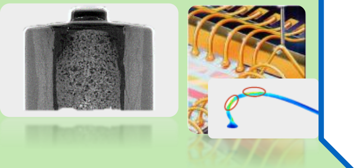
Other Applications



Medicine
Botanology
Fossils

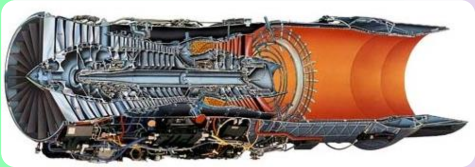
Multi scale imaging
Image processing
Reverse engineering
Failure analysis

Batteries
IC Integrity and Reliability



Dentistry
Geology

Porosity analysis
Crack growth
Failure analysis



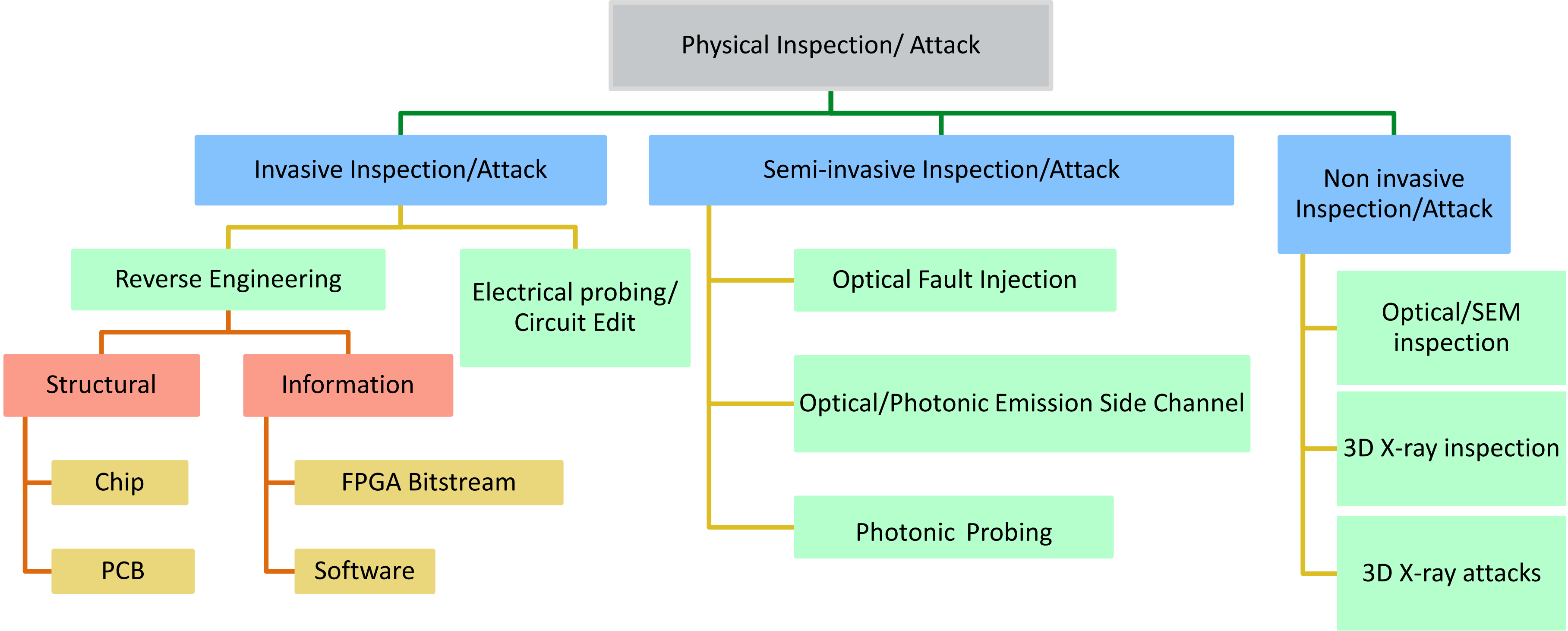
Thermal barrier coatings

Mechanical Engineering

Material diffusion
Polymer mixes
Carbon fiber composites

Material Engineering

Course Overview

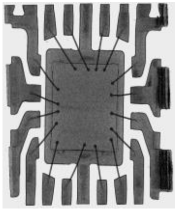

Physical Inspection/ Attack
Invasive Inspection/Attack
Semi-invasive Inspection/Attack
Non invasive Inspection/Attack
Reverse Engineering
Electrical probing/ Circuit Edit
Structural
Information
Chip
PCB
FPGA Bitstream
Software
Optical Fault Injection
Optical/Photonic Emission Side Channel
Photonic Probing
Optical/SEM inspection
3D X-ray inspection
3D X-ray attacks

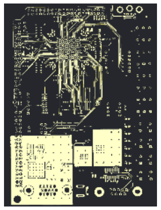
- Physical access to the chip is required
  - ➢ Non-Invasive Attack: Observe and manipulating device without any physical harm
  - ➢ Invasive Attack: Complete deprocessing of the chip to extract information
  - ➢ Semi-invasive Attack: Removing package keeping the chip structure intact

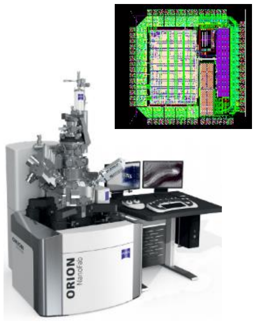
Course Overview

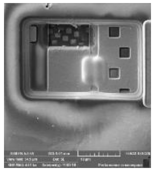
- Microscopy methods to detect defects on electronics
- Common defects and the tools to detect them automatically
- Ionization effect on ICs from X-rays during inspection
- Non-destructive testing for integrity analysis
- PCB reverse engineering (RE)
- Non-destructive PCB RE
- Image filtering and segmentation methods for netlist extraction
- IC reverse engineering methods; Sample prep, delayering, etc.
- Advanced tools for fast accurate RE, Rapid Trojan detection, etc.
- Introduce attack modules for data extraction
- reading non-volatile memory data

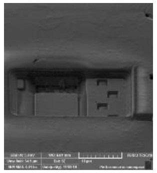
- Extract keys
- Fault injection using laser.
- Attacks on microprocessors, etc.
- Probing attacks
- Extract design for obfuscated gates
- Anti-probing techniques

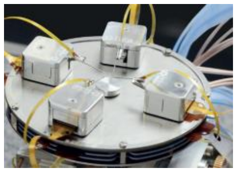




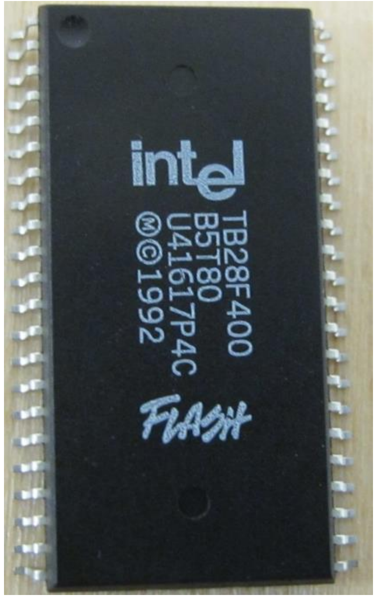




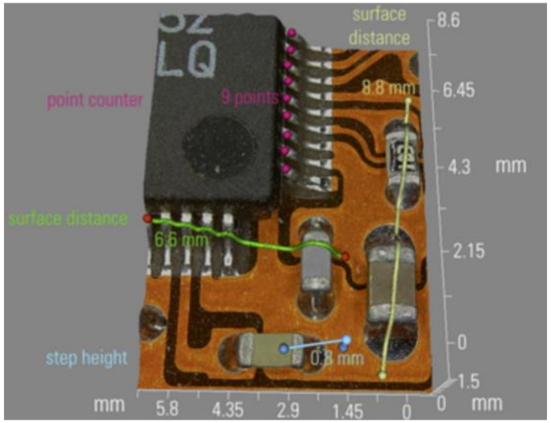


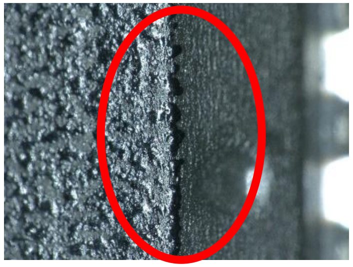


Optical Microscopy

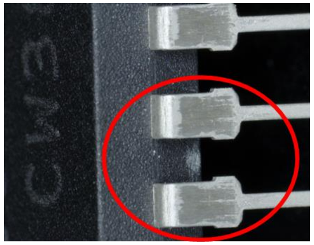


- Resolution: few um to mm
- Colorful images
- 2D and 3D **surface** images
- No sample prep required
- Fast and cheap
- Non-destructive



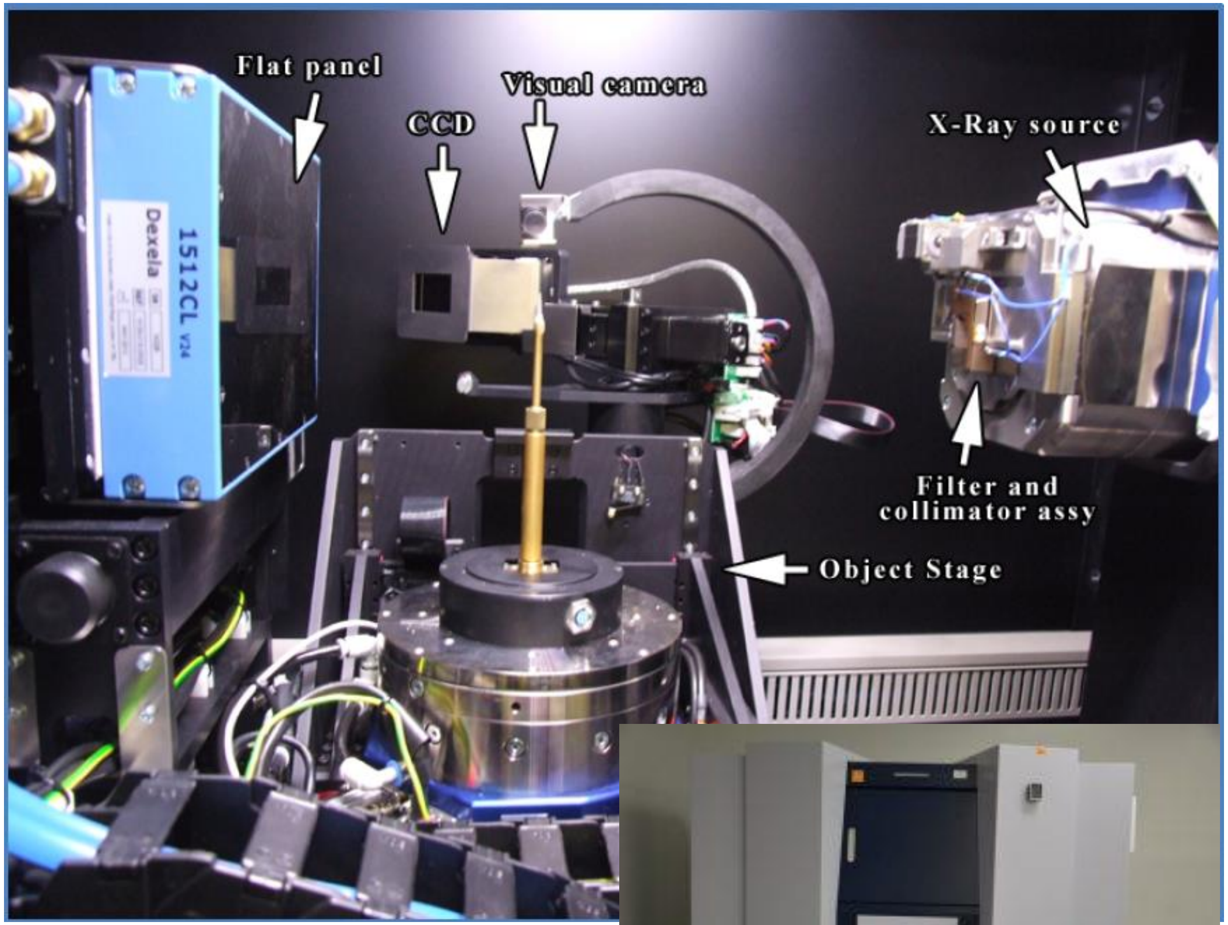


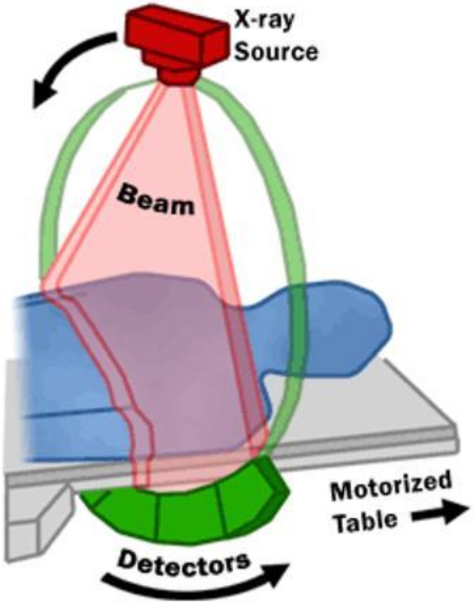
Black top



Retinning/color variations

X-ray Tomography





- Resolution: 1-50 um
- 3D images of internal structure
- Basic sample prep required
- More expensive and not slow
- Non-destructive

SEM and FIB

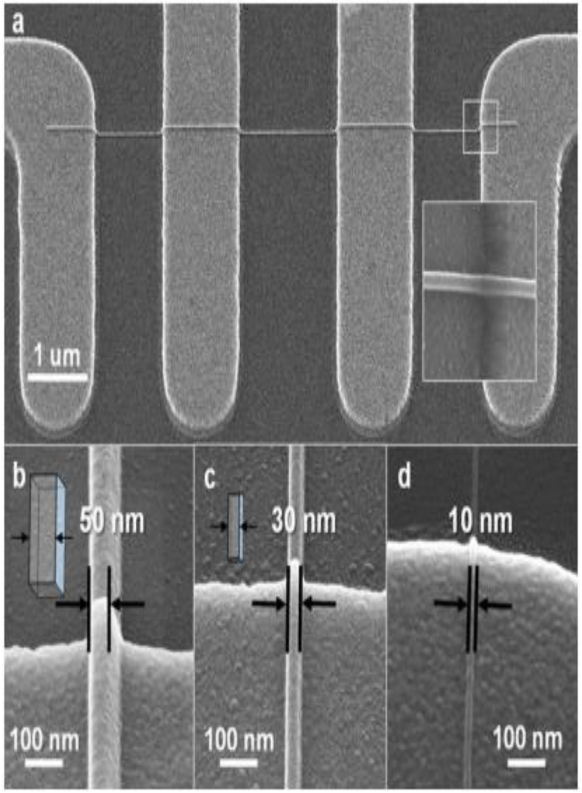
- Resolution: 5nm – few um
- 2D and 3D **surface** images
- **Advanced** sample prep required
- More expensive and comparatively slow
- Destructive/Non-destructive

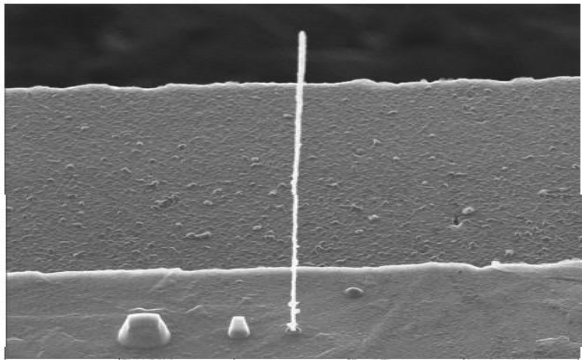
Dual beam-Plasma FIB
Probe current: 20 pA to 2 μA
Material removal rate: 2000 μm^3/s
Maximum field of view: 17 mm

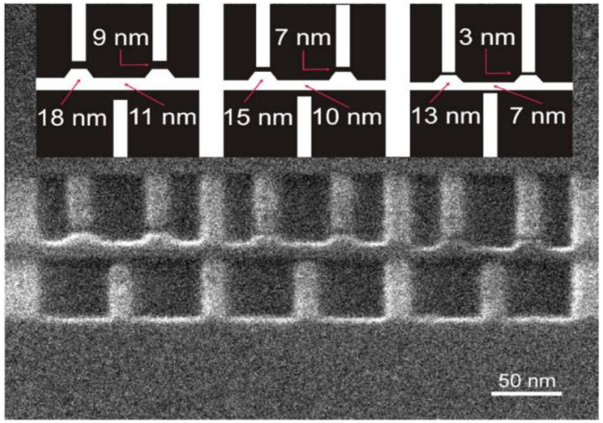
Dual beam-Ga FIB
Probe current: 1 pA to 40 nA
Material removal rate: 150 μm^3/s
Maximum field of view: 17 mm

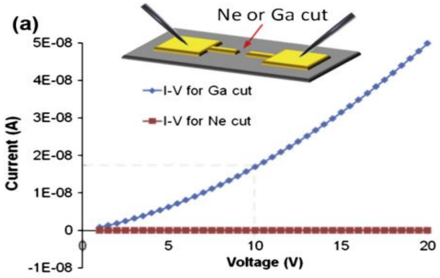
He and Ne ion Micorscopy

Comparison between He/Ne and Ga FIB parameters							
Focused Ion Beam	Maximum deposited metal resistivity	Proximal defects	Milled features aspect ratio	Probe size	Imaging resolution	Material removal speed	End point detection option
He/Ne	High	Very low	High	0.5/1.9 nm	0.2 nm	Medium	Available
Ga	Low	High	Low	Over 5nm	Sub 10 nm	High	Not available

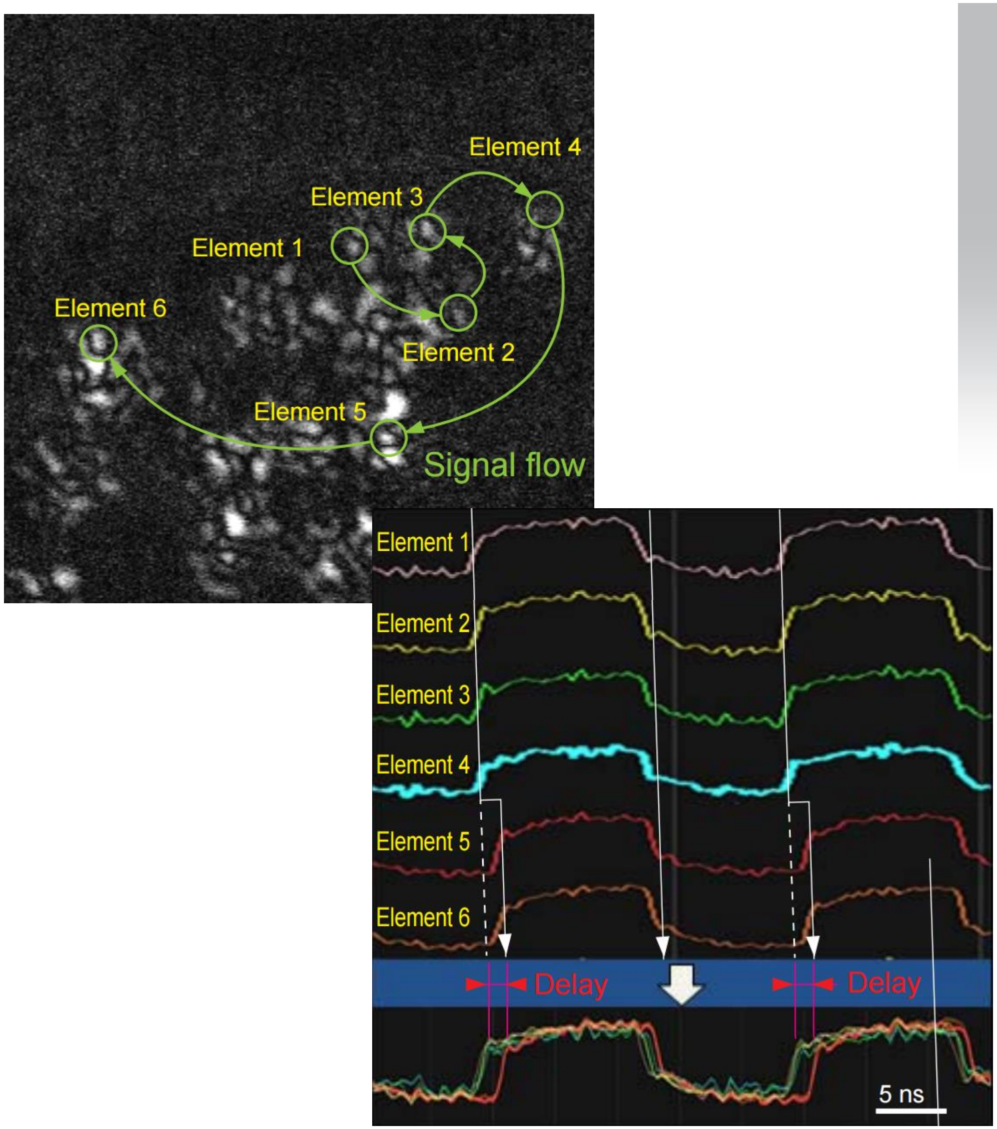


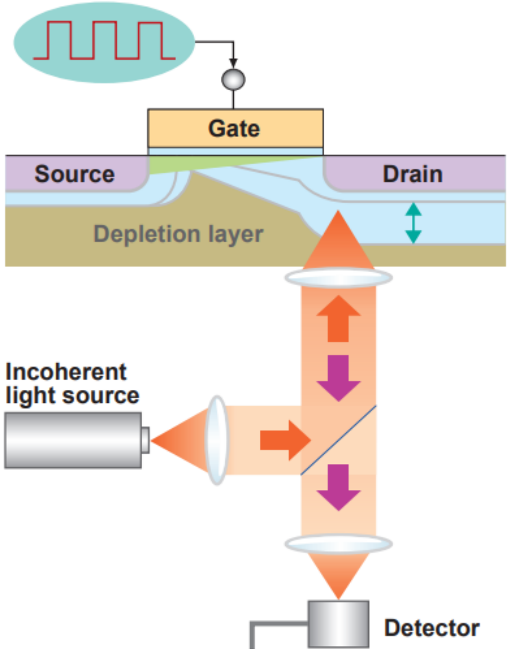






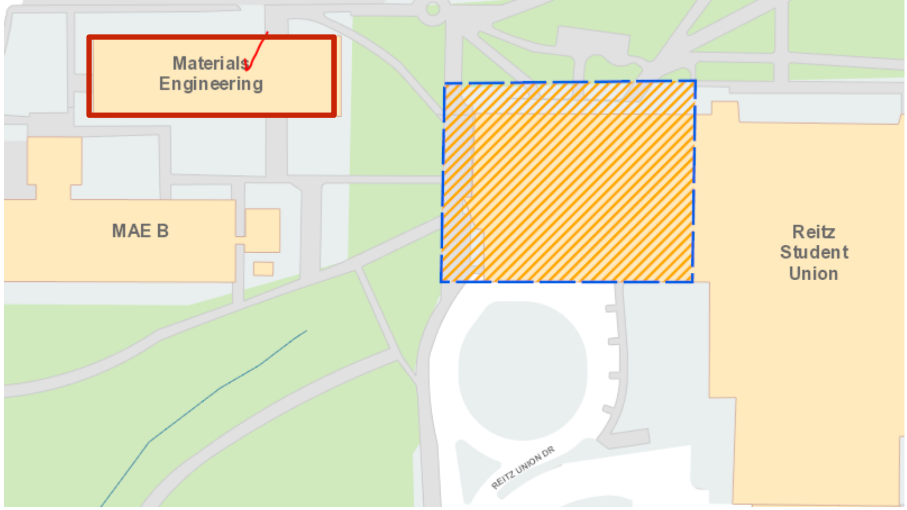
Photon Emission Microscopy





PHIKS

- **Meeting Time**
  - Tuesday 3:00 – 4:55pm
  - Thursday 4:05 – 4:55p
- **Meeting Place**
  - MAE 126 FICS conference room
  - MAE 122 SCAN lab
- **Office hours**
  - Mondays 4:00 – 5:00 pm
- **Grading**
  - Assignments: 20%
  - Exam: 20%
  - Student Presentation: 30%
  - Term Report: 30%



- **PHIKS team**
  - Tanjid Rahman (TA)
  - Nitin Varshney (lab engineer)

Reading

- Book chapter: Counterfeit Integrated Circuits: Detection, Avoidance, and the Challenges Ahead