2017 Pathways Student Showcase

Confidentiality
Integrity
Information Security
Availability

Theodore Fout

Mentor/Supervisor: Henry Yu

IT-B Security

On Board Date : 9 Jan 17

BACKGROUND

Retired from the United States Air Force (2015)

Position held while in the Air Force

- Weapons load crew (F-15) – two man
- Weapons load crew (F-16) – one man
- Unit Deployment Manager
- Squadron Training Manager
- Noncommissioned Officer Unit Weapons Safety, Ground Safety, Flight Safety
- Noncommissioned Officer in Charge Commanders Support Staff

EDUCATION

Associates in Applied Science (2011) – Community College of the Air Force

Bachelors' of Science in Cybersecurity (2015) – University of Manyland University College

Masters of Science in Cybersecurity (December 2017) - University of Manyland University College

Strategic Plans NASA

NASA intends to execute its strategic plan by achieving the following strategic goals:

1. Expand the frontiers of knowledge, capability, and opportunity in space.

By empowering the NASA community to:
- expand human presence into the solar system
- conduct research on the ISS
- enable and utilize commercial capabilities
- better understand the Sun and its effects of the solar system
- understand the solar system better
- discover how the universe works
- utilize space technologies to advance the Nation's capabilities

2. Advance understanding of Earth and develop technologies to improve the quality of life on our home planet.

By engaging the workforce and partners to:
- advance aeronautics research
- advance knowledge of Earth to improve life on it.
- optimize agency technology for national benefit
- advance STEM education and collaborate regarding the mission

3. Serve the American public and accomplish our Mission by effectively managing our people, technical capabilities, and infrastructure.

By working together to:
- conduct NASA's mission in an innovative work environment with a diverse and highly skilled work force
- ensure that strategic, technical and programmatic capabilities are available and advanced
- provide information technologies which are secure, effective, and affordable
- ensure effective management of programs and operations while performing safely and successfully.

Strategic Plans KSC

KSC intends to execute its strategic plan by achieving the following strategic goals:

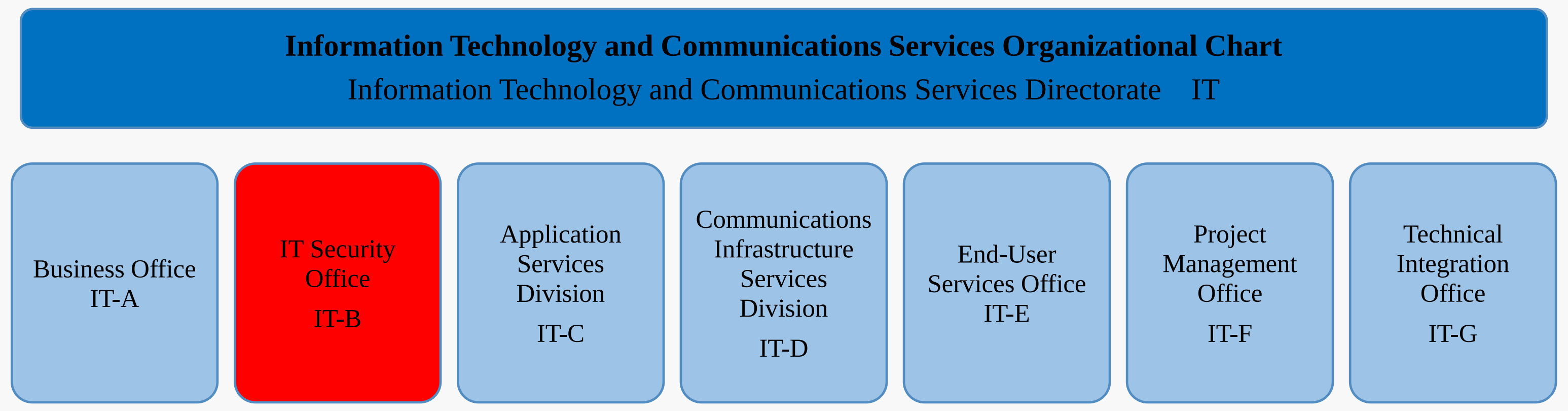
Strategic Goal 1: Kennedy Space Center manages the Commercial Crew Program (CCP) that facilitates development of U.S. commercial crew space transportation to and from low Earth orbit and the ISS. This lets NASA continue crew rotations and execute science on the ISS, including some KSC plant research and biology experiments. KSC is developing ground systems and plans for Orion and SLS assembly and integrated test for the 2014 Orion test flight, the SLS missions, and beyond. KSC is also developing or maturing crosscutting and innovative technologies, including RESOLVE, Ka- BOOM, and IGODU.

Strategic Goal 2: KSC optimizes Agency technology investments by leading ISRU technology development for multiple destinations, advancing research and technology through integrated testing in relevant environments, developing external payload carriers, and fostering innovative partnerships. KSC advances aeronautics research by developing innovative metal alloys to improve safety of spacecraft and aircraft. KSC collaborates with partners to advance STEM learning. Partners include K-12 schools, universities, the Florida Department of Energy, and youth and service organizations.

Strategic Goal 3: KSC's major transformation from a single customer to multi-customer launch complex is vital to the success of both NASA and commercial space industry. To support NASA and our partners' success, KSC ensures and provides launch services and access to space for NASA missions. KSC continually evaluates and aligns its highly valued people, and programmatic and institutional capabilities. KSC implements rigorous and innovative safety, IT, and communication services to ensure quality and reliability of products.

Strategic Plans Information Technology and Communications Services (IT)

- Vision:
  - To be *the* IT services and solutions provider for the world's preeminent launch complex
- Mission:
  - The IT Directorate provides responsive, innovative, secure, and cost-effective IT services to enable Mission and Institutional customer and partner success.
- Strategic Goals:
  - Govern all KSC IT products and services
  - Maintain leading role as the KSC IT service provider
  - Ensure a responsive, customer-focused end-to-end IT user experience for all stakeholders
  - Proactively provide innovative and cost-effective solutions
  - Enhance and strengthen information security
  - Consolidate and enhance infrastructure and services in an effective and efficient manner
  - Develop Enterprise Architecture practices in support of the Agency Information Resources Management Strategic Plan
- IT Objectives:
  - Respond to 95% of actions prior to due date
  - Meet with stakeholders quarterly to convey latest IT initiatives and seek customer feedback
  - Resolve KSC Center I3P (operational/integration) issues with appropriate Service Office Provider and/or Service Integration Manager in a timely manner
  - Adhere to Agency IT policies, guidelines, and procedures


Information Technology and Communications Services Organizational Chart
Information Technology and Communications Services Directorate IT

Business Office IT-A
IT Security Office IT-B
Application Services Division IT-C
Communications Infrastructure Services Division IT-D
End-User Services Office IT-E
Project Management Office IT-F
Technical Integration Office IT-G

IT-B INFORMATION TECHNOLOGY SECURITY OFFICE

IT-B Mission:

The IT Security Office is dedicated to providing superior information security services to the KSC/NASA customers and partners to ensure the confidentiality, integrity, and availability of KSC and NASA information and IT resources

IT-B Vision:

To become a model IT Security organization for the federal government in providing world-class IT security solutions to the KSC employees, customers, and partners.

Goals and Objectives:

1.Ensure and support a robust security architecture that meets NASA's and KSC's business needs.
2.Educate all employees to recognize and prevent cyber security threats.
3.Fully integrate information security considerations into the system development life cycle (SDLC).
4.Provide innovative and cost-effective solutions to ensure a secured IT environment for customers and partners.
5.Continue to support and develop Agency IT security solutions that satisfy the federal continuous monitoring requirements.

The IT Security Office is responsible for IT Security planning, policy development and implementation, architecture, governance, and audit support. The Office has responsibility for ensuring Federal Information Security Management Act (FISMA) compliance including Center-wide IT Security reviews, assessments and vulnerability scans, Internet content monitoring, IT Security incident response and investigations, intrusion detection services, operation system configuration management, IT Security technical expertise, and contractor compliance insight. The Office manages the Network Security Perimeter (NSP) for the Center and the Agency Security Update System (ASUS), Enterprise Reporting, and NASA Security Assessment and Authorization Repository (NSAAR) services for the Agency. The Office also provides support to Center Relationship Managers (RM) and IT Security support personnel. The Chief Information Security Officer (CISO), Center Privacy Manager (CPM), and Assessment & Authorization Official are on staff, as well as the Agency ASUS Project Manager and (NSAAR) Project Manager.

Duties

SharePoint POC
- Manages the SharePoint sites used by IT-B and Center personnel. Take input from individuals to update the content in order to provide useful information in a centralized location.

Data At Rest (DAR) Waivers POC
- As the primary point of contact for DAR waivers, tracked current waivers to ensure none expire. Work with the customer to correctly fill in requests and then route the completed forms to the required individuals.

Incident Response Team member
- Participated in table top exercise. Increased understanding of KSCs incident response posture.
- As a breach response team member, gained knowledge concerning KSCs handling of incidents.

- My work in the IT-B office aids in ensuring Federal Information Security Management Act (FISMA) compliance. Which ties back to NASA's goal of providing information technologies which are secure, effective, and affordable.

Internal Network Monitoring Project

-Working with fellow team members to evaluate hardware and software

-Evaluation is taking place in a lab environment

-Hardware being evaluated is the Interface Masters switch.
-- Used for network data aggregation

-Software being evaluated is the Security Onion Suite.
-- Security Onion consists of the following components:

Snort/Suricata – rule-based intrusion detection
Bro - analysis-driven intrusion detection
Netsniff-ng – for packet capture
Sguil – used to view alerts
Squert – used to view Sguil data
ELSA – used to query logs

-Additional software used:
-- Wireshark – protocol analyzer

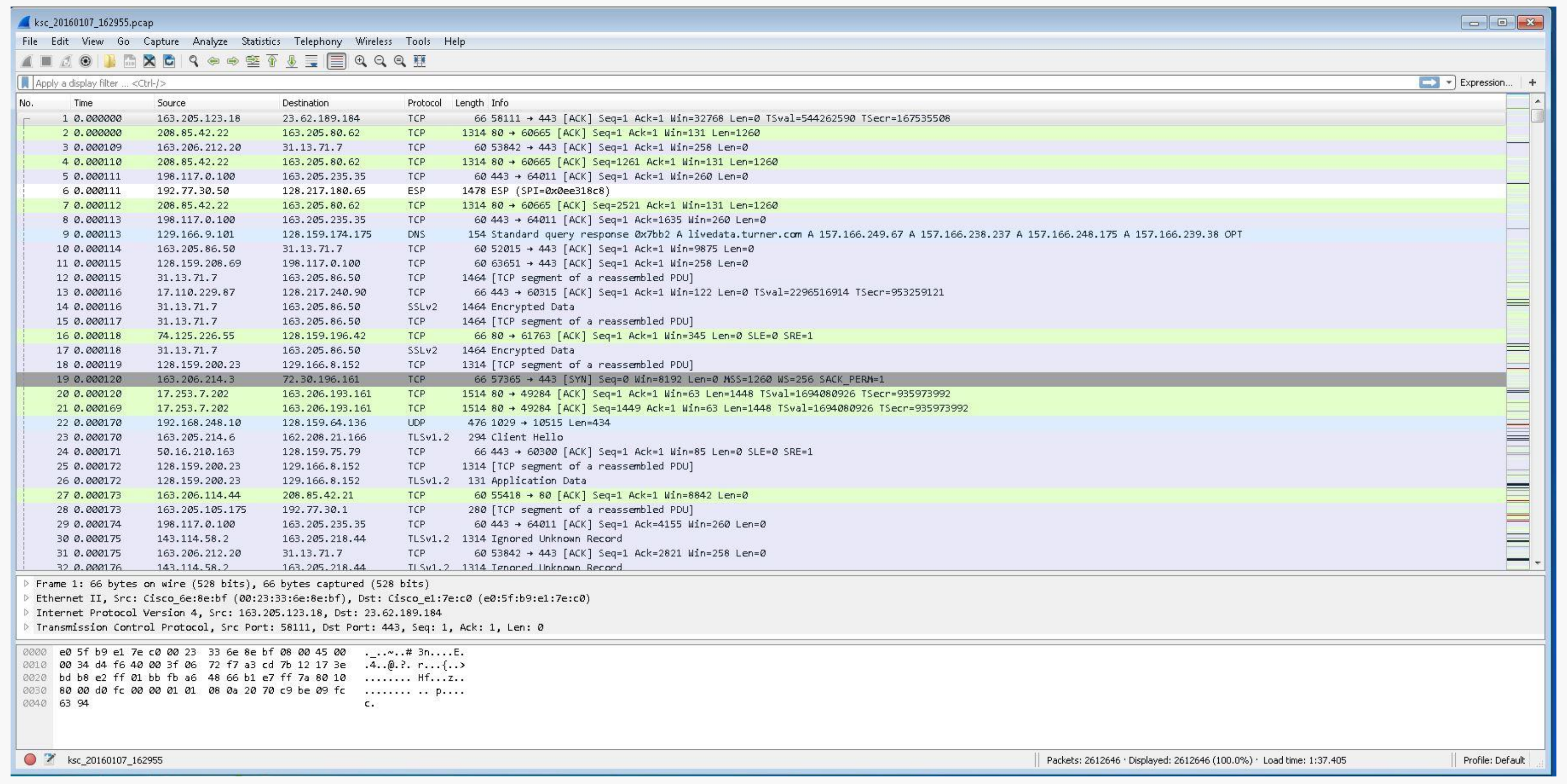
-Working on internal network monitoring falls in line with current classes in intrusion detection and prevention as well as allows the use of principles and skills learned from previous degree.

- Currently team members involved with the evaluation of hardware and software for internal monitoring are updating software and gaining familiarity with both the hardware and software.

- Next step will be running simulated network traffic through the test system to ensure it will provide the necessary functionality.

- After all tests have been completed the system will be deployed on the actual KSC network.

- The system will then be adjusted to reduce false positives and false negatives.


ksc_20160107_162955.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

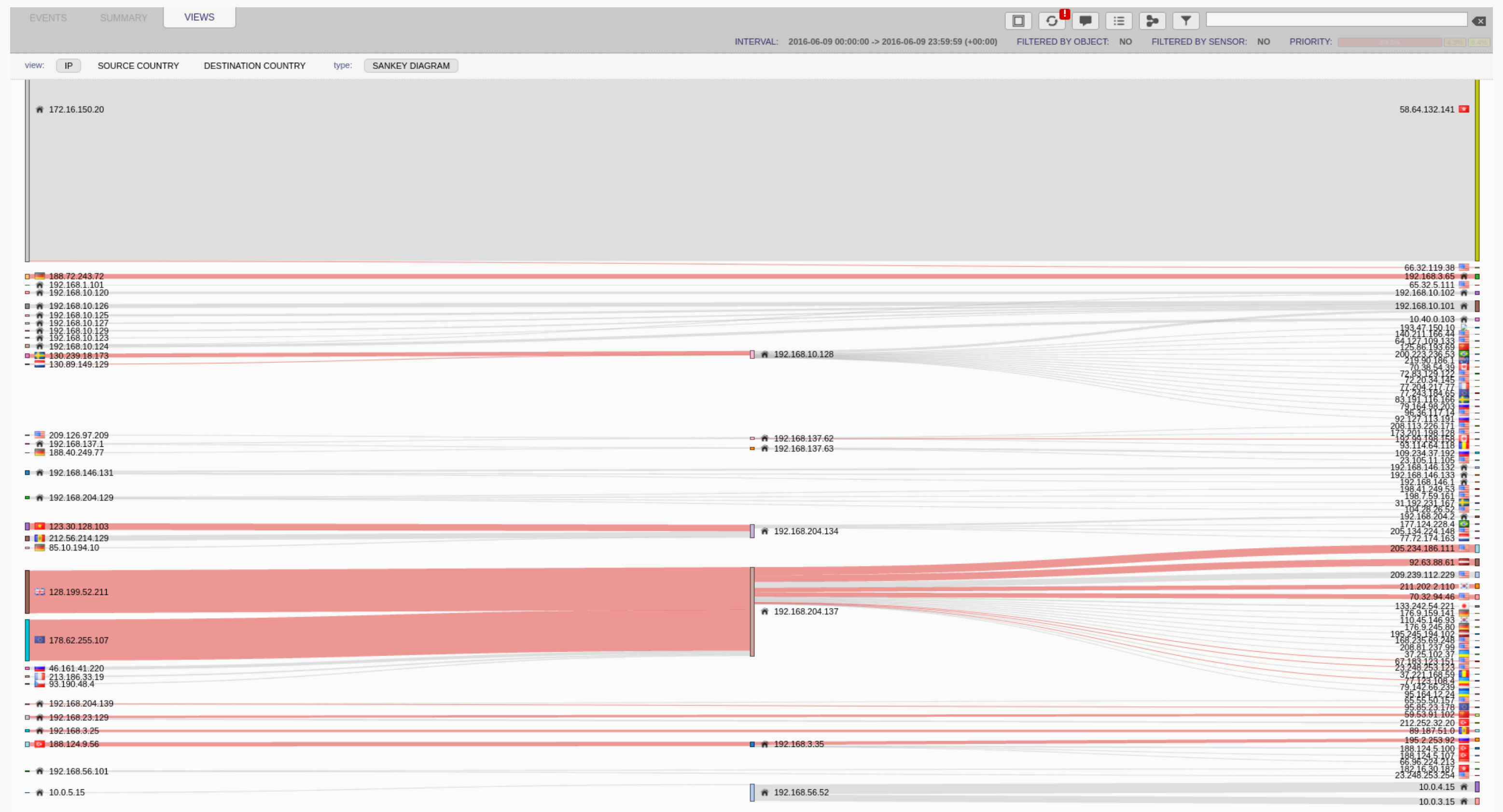
```
No.  Time      Source           Destination      Protocol Length Info
  1 0.000000  163.205.123.18   23.62.189.184    TCP        66 58111 → 443 [ACK] Seq=1 Ack=1 Win=32768 Len=0 TSval=544262590 TSecr=167535508
  2 0.000000  208.85.42.22     163.205.80.62    TCP      1314 80 → 60665 [ACK] Seq=1 Ack=1 Win=131 Len=1260
  3 0.000109  163.206.212.20   31.13.71.7       TCP        60 53842 → 443 [ACK] Seq=1 Ack=1 Win=258 Len=0
  4 0.000110  208.85.42.22     163.205.80.62    TCP      1314 80 → 60665 [ACK] Seq=1261 Ack=1 Win=131 Len=1260
  5 0.000111  198.117.0.100    163.205.235.35   TCP        60 443 → 64011 [ACK] Seq=1 Ack=1 Win=260 Len=0
  6 0.000111  192.77.30.50     128.217.180.65   ESP      1478 ESP (SPI=0x0ee318c8)
  7 0.000112  208.85.42.22     163.205.80.62    TCP      1314 80 → 60665 [ACK] Seq=2521 Ack=1 Win=131 Len=1260
  8 0.000113  198.117.0.100    163.205.235.35   TCP        60 443 → 64011 [ACK] Seq=1 Ack=1635 Win=260 Len=0
  9 0.000113  129.166.9.101    128.159.174.175  DNS       154 Standard query response 0x7bb2 A livedata.turner.com A 157.166.249.67 A 157.166.238.237 A 157.166.248.175 A 157.166.239.38 OPT
 10 0.000114  163.205.86.50    31.13.71.7       TCP        60 52015 → 443 [ACK] Seq=1 Ack=1 Win=9875 Len=0
 11 0.000115  128.159.208.69   198.117.0.100    TCP        60 63651 → 443 [ACK] Seq=1 Ack=1 Win=258 Len=0
 12 0.000115  31.13.71.7       163.205.86.50    TCP      1464 [TCP segment of a reassembled PDU]
 13 0.000116  17.110.229.87    128.217.240.90   TCP        66 443 → 60315 [ACK] Seq=1 Ack=1 Win=122 Len=0 TSval=2296516914 TSecr=953259121
 14 0.000116  31.13.71.7       163.205.86.50    SSLv2    1464 Encrypted Data
 15 0.000117  31.13.71.7       163.205.86.50    TCP      1464 [TCP segment of a reassembled PDU]
 16 0.000118  74.125.226.55    128.159.196.42   TCP        66 80 → 61763 [ACK] Seq=1 Ack=1 Win=345 Len=0 SLE=0 SRE=1
 17 0.000118  31.13.71.7       163.205.86.50    SSLv2    1464 Encrypted Data
 18 0.000119  128.159.200.23   129.166.8.152    TCP      1314 [TCP segment of a reassembled PDU]
 19 0.000120  163.206.214.3    72.30.196.161    TCP        66 57365 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1260 WS=256 SACK_PERM=1
 20 0.000120  17.253.7.202     163.206.193.161  TCP      1514 80 → 49284 [ACK] Seq=1 Ack=1 Win=63 Len=1448 TSval=1694080926 TSecr=935973992
 21 0.000169  17.253.7.202     163.206.193.161  TCP      1514 80 → 49284 [ACK] Seq=1449 Ack=1 Win=63 Len=1448 TSval=1694080926 TSecr=935973992
 22 0.000170  192.168.248.10   128.159.64.136   UDP       476 1029 → 10515 Len=434
 23 0.000170  163.205.214.6    162.208.21.166   TLSv1.2   294 Client Hello
 24 0.000171  50.16.210.163    128.159.75.79    TCP        66 443 → 60300 [ACK] Seq=1 Ack=1 Win=85 Len=0 SLE=0 SRE=1
 25 0.000172  128.159.200.23   129.166.8.152    TCP      1314 [TCP segment of a reassembled PDU]
 26 0.000172  128.159.200.23   129.166.8.152    TLSv1.2   131 Application Data
 27 0.000173  163.206.114.44   208.85.42.21     TCP        60 55418 → 80 [ACK] Seq=1 Ack=1 Win=8842 Len=0
 28 0.000173  163.205.105.175  192.77.30.1      TCP       280 [TCP segment of a reassembled PDU]
 29 0.000174  198.117.0.100    163.205.235.35   TCP        60 443 → 64011 [ACK] Seq=1 Ack=4155 Win=260 Len=0
 30 0.000175  143.114.58.2     163.205.218.44   TLSv1.2  1314 Ignored Unknown Record
 31 0.000175  163.206.212.20   31.13.71.7       TCP        60 53842 → 443 [ACK] Seq=1 Ack=2821 Win=258 Len=0
 32 0.000176  143.114.58.2     163.205.218.44   TLSv1.2  1314 Ignored Unknown Record

▷ Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
▷ Ethernet II, Src: Cisco_6e:8e:bf (00:23:33:6e:8e:bf), Dst: Cisco_e1:7e:c0 (e0:5f:b9:e1:7e:c0)
▷ Internet Protocol Version 4, Src: 163.205.123.18, Dst: 23.62.189.184
▷ Transmission Control Protocol, Src Port: 58111, Dst Port: 443, Seq: 1, Ack: 1, Len: 0

0000  e0 5f b9 e1 7e c0 00 23  33 6e 8e bf 08 00 45 00   ._..~..# 3n....E.
0010  00 34 d4 f6 40 00 3f 06  72 f7 a3 cd 7b 12 17 3e   .4..@.?. r...{..>
0020  bd b8 e2 ff 01 bb fb a6  48 66 b1 e7 ff 7a 80 10   ........ Hf...z..
0030  80 00 d0 fc 00 00 01 01  08 0a 20 70 c9 be 09 fc   ........ .. p....
0040  63 94                                              c.

ksc_20160107_162955          Packets: 2612646 · Displayed: 2612646 (100.0%) · Load time: 1:37.405          Profile: Default
```

Using a program called Wireshark network activity can be captured. Shown is a capture of the internal network activity.



Shown is the Squert program, which can be used to view event data.