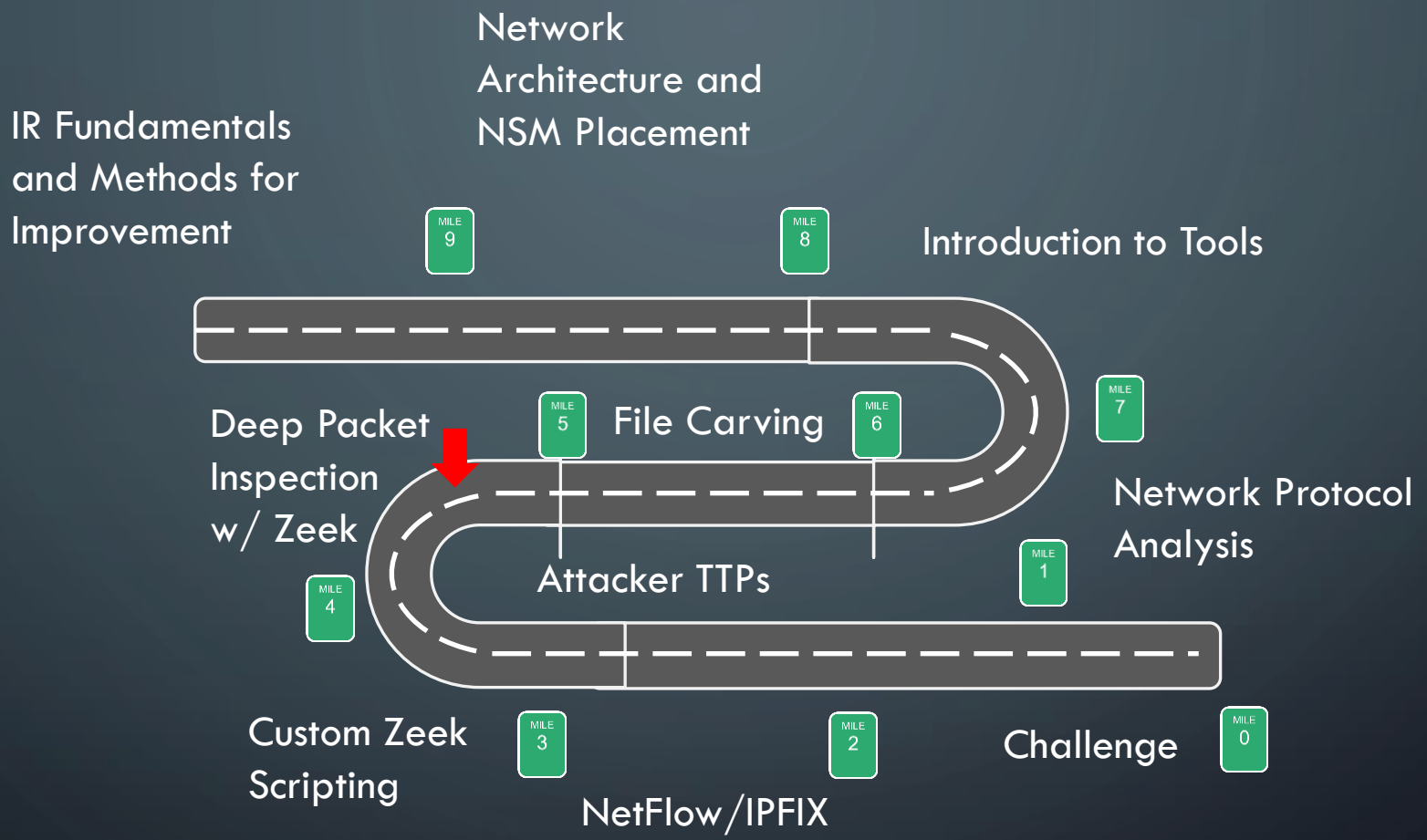
DAY 3

Roadmap



Deep Packet Inspection

Introducing Zeek

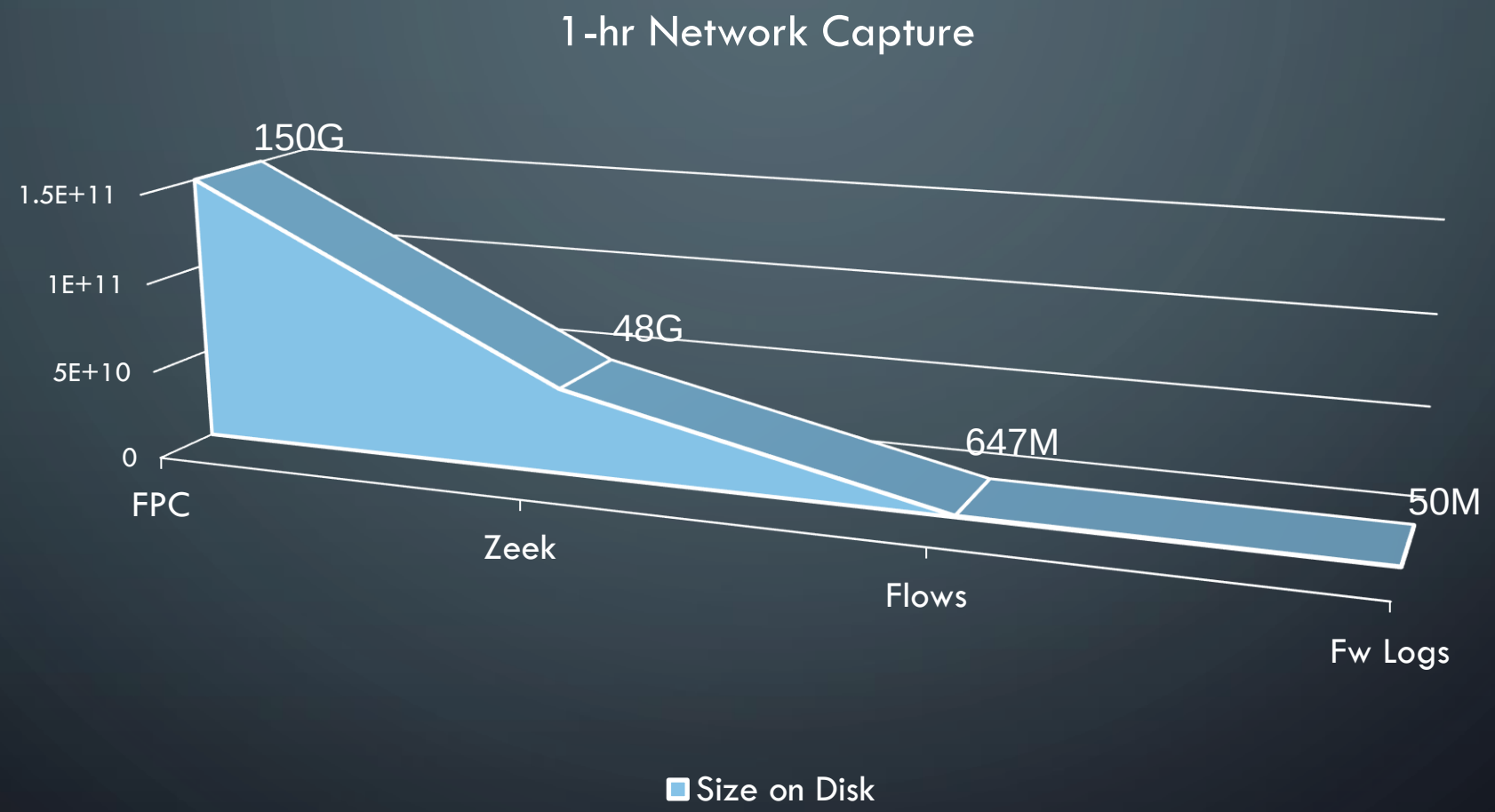
- About Zeek IDS
  - Developed by Vern Paxson
  - 25+ years old
  - IDS but more…

> *"Bro is not strictly an intrusion detection system that generates alerts, like Snort. Rather, Bro generates a range of NSM data, including session data, transaction data, extracted content data, statistical data, and even alerts -- if you want them."*
>
> - Richard Bejtlich, TaoSecurity

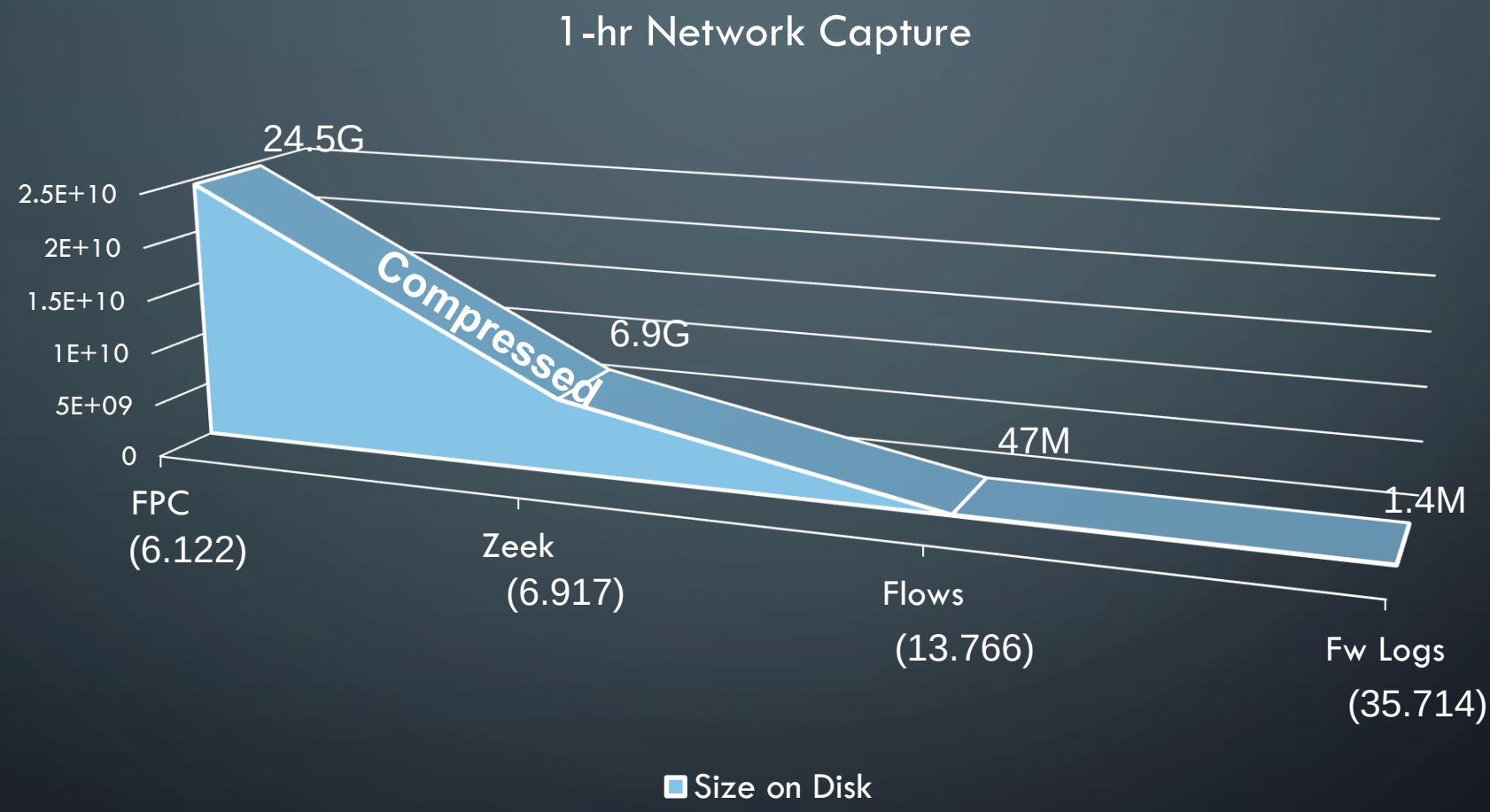
http://taosecurity.blogspot.com/2015/01/try-critical-stack-intel-client.html

- Meta-data all the things
- Built on frameworks to digest various areas of network categorization
- Rule logic constructed by hooking into "events"

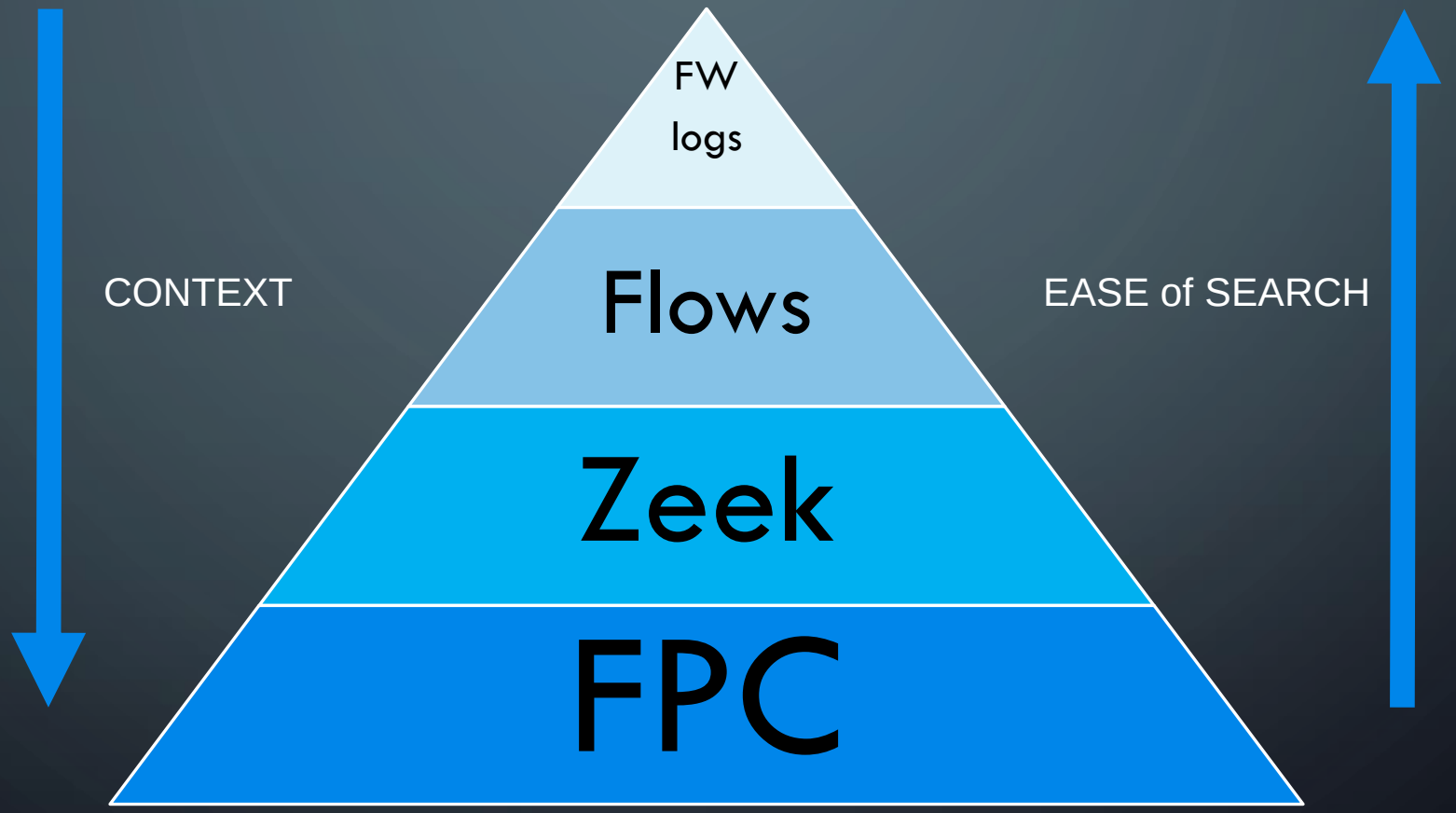
What's on Your Drive



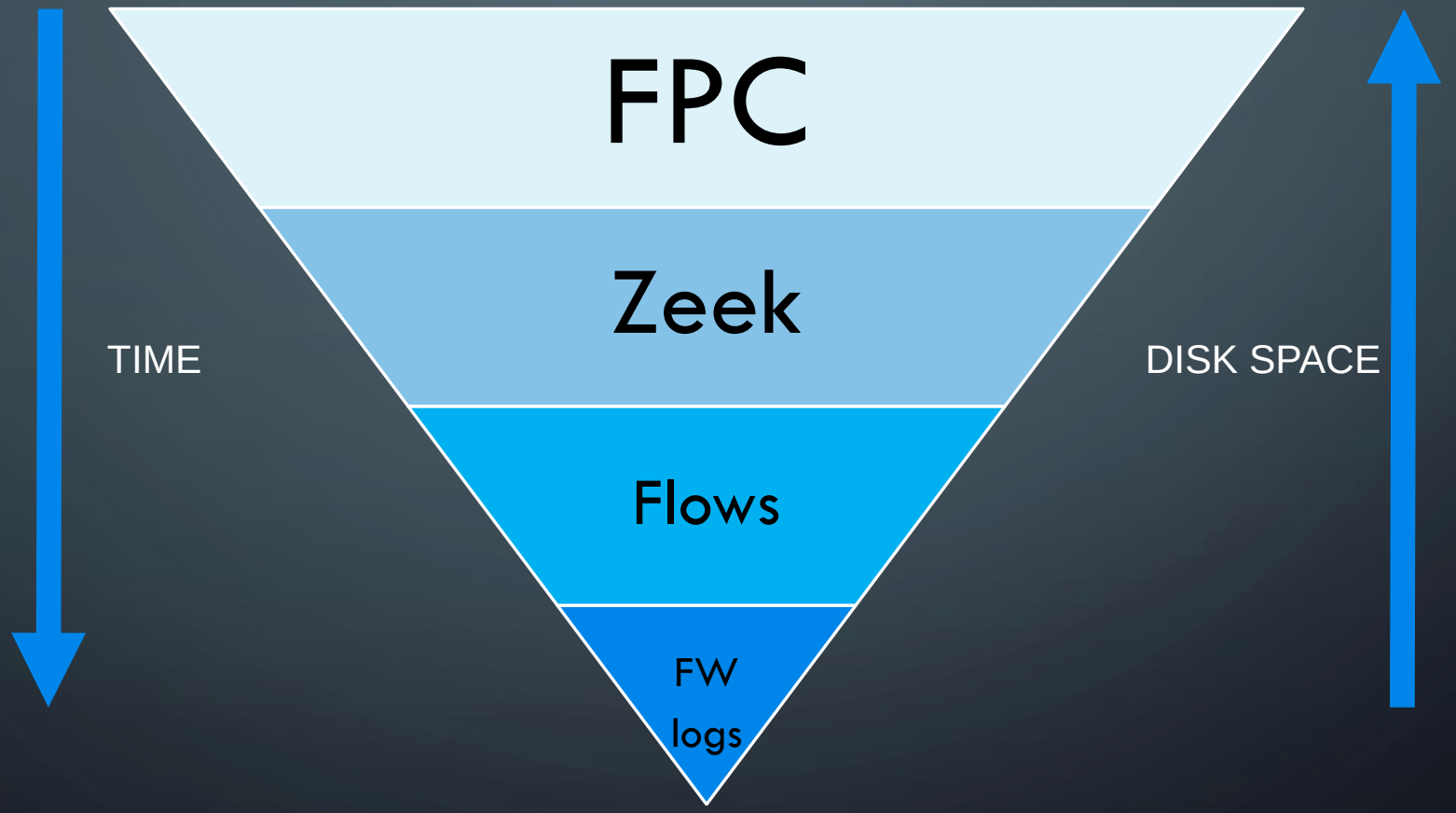
What's on Your Drive



Searching over Time



Retention over Time



Zeek Frameworks

- Logging Framework
- Notice Framework
- Input Framework
- Configuration Framework
- Intelligence Framework
- Cluster Framework
- Broker Communication Framework
- Supervisor Framework
- GeoLocation
- File Analysis
- Signature Framework
- Summary Statistics
- NetControl Framework
- Packet Analysis

https://docs.zeek.org/en/master/frameworks/index.html

Zeek – Tips, Tricks and Automobiles

- less –S
  - Tells less not to wrap the line and allows scrolling across the screen
  - Essential to viewing Zeek logs (TSV) at the command line
- date –d @*epoch-time*
  - Translate between epoch time and human-readable
- &Redef's
  - Command line too?
- Can run against saved pcaps (-r option)

Working with Zeek Logs

- Originator/Responder != Request/Response
- Logging condenses/collapses the stream (sort of)
- Nearly all logs contain a Cuid Field which can be used to correlate events observed by Zeek

Zeek Application Logs

- Application specific logs
- Connections, dns, http, smtp, oh my…
- Wait, ssl?
- Did you know…
  - IRC
  - Modbus
  - SOCKS Proxy
  - Other tunnels

Zeek – conn.log

```
#path   conn
#open   2021-09-22-12-34-04
#fields ts      uid     id.orig_h       id.orig_p       id.resp_h       id.resp_p       proto   service duratio
#types  time    string  addr    port    addr    port    enum    string  interval        count   count   string
1599856299.478688       CRqLU82lLgM0wMg944      10.9.11.101     49797   172.217.0.227   443     tcp     ssl
1599856299.403359       CU5L8l2o853oCPldl6      10.9.11.101     62666   10.9.11.1       53      udp     dns
1599856299.099262       C0XAG54vi1R4mfOXI6      10.9.11.101     49366   10.9.11.1       53      udp     dns
1599856309.849256       C5Kn4p47MkVCafWaPh      10.9.11.101     60470   10.9.11.1       53      udp     dns
1599856316.631675       ChjMmK3eqdOu8Y8fK1      10.9.11.101     49799   52.167.249.196  443     tcp     ssl
1599856317.127206       CCZ1An2E3d02gDMaH5      10.9.11.101     49804   13.74.179.117   443     tcp     ssl
1599856317.555699       CC94IL2edS5CTzbXwf      10.9.11.101     49805   13.107.246.10   443     tcp     ssl
1599856317.783951       CFmte84fDIfRMpvPE2      10.9.11.101     49806   52.167.249.196  443     tcp     ssl
1599856318.519995       CFHLDJ1NwHLikMsPyh      10.9.11.101     49807   52.114.128.69   443     tcp     ssl
1599856318.533041       C0NuiY1ZSQFfnbf6Pi      10.9.11.101     49808   52.167.249.196  443     tcp     ssl
1599856316.421025       Ct6Z6L1i0ZSQTd4Lha      10.9.11.101     63165   10.9.11.1       53      udp     dns
1599856316.720258       CydV4uDGSTxy8u148       10.9.11.101     51919   10.9.11.1       53      udp     dns
1599856316.795735       Cy5LXu3Evb1WsYsBh4      10.9.11.101     55080   10.9.11.1       53      udp     dns
1599856316.864111       CSduJ7C0Fapki66Vh       10.9.11.101     56241   10.9.11.1       53      udp     dns
1599856321.780000       CXtOekBaORMCYkTt        10.9.11.101     49810   52.114.128.69   443     tcp     ssl
1599856317.457680       CtRzNQ3k4jXIVMkVod      10.9.11.101     52454   10.9.11.1       53      udp     dns
1599856318.919963       CYUu814ApjgAPI5oqg      10.9.11.101     49809   65.52.108.90    443     tcp     ssl
```

Zeek – dns.log

- cat dns.log |/usr/local/zeek/bin/zeek-cut **id.orig_h proto query qtype_name answers TTLs**

```
10.9.11.101     udp     update.googleapis.com   A       172.217.0.227   5.000000
10.9.11.101     udp     nexusrules.officeapps.live.com  A       prod.nexusrules.live.com.akadns.net,52.109.88.36
10.9.11.101     udp     settings-win.data.microsoft.com A       settingsfd-geo.trafficmanager.net,52.167.249.196
10.9.11.101     udp     login.live.com  A       login.msa.msidentity.com,www.tm.lg.prod.aadmsa.trafficmanager.net
10.9.11.101     udp     ecn.dev.virtualearth.net        A       ssl2.tiles.virtualearth.net.edgekey.net,e4113.dsc
10.9.11.101     udp     slscr.update.microsoft.com      A       slscr.update.microsoft.com.akadns.net,sls.update.
10.9.11.101     udp     pti.store.microsoft.com A       sfd-production.azurefd.net,t-0001.t-msedge.net,edge-prod-
10.9.11.101     udp     v10.events.data.microsoft.com   A       global.asimov.events.data.trafficmanager.net,skype
10.9.11.101     udp     fe3cr.delivery.mp.microsoft.com A       fe3.delivery.mp.microsoft.com,fe3.delivery.dsp.mp
10.9.11.101     udp     wpad.localdomain        A       -       -
10.9.11.101     udp     wpad.localdomain        A       -       -
10.9.11.101     udp     wpad.localdomain        A       -       -
10.9.11.101     udp     v10.events.data.microsoft.com   A       global.asimov.events.data.trafficmanager.net,skype
10.9.11.101     udp     mrodevicemgr.officeapps.live.com        A       prod.mrodevicemgr.live.com.akadns.net,52.
10.9.11.101     udp     msedge.api.cdp.microsoft.com    A       api.cdp.microsoft.com,api.cdp.dsp.mp.microsoft.com
10.9.11.101     udp     geover.prod.do.dsp.mp.microsoft.com     A       geover.prod.dodsp.mp.microsoft.com.nsatc.
10.9.11.101     udp     cp601.prod.do.dsp.mp.microsoft.com      A       cp601.prod.dodsp.mp.microsoft.com.nsatc.n
10.9.11.101     udp     wpad.localdomain        A       -       -
```

Zeek – http.log

cat http.log |/usr/local/zeek/bin/zeek-cut method host uri referrer status_code

```
GET     205.185.113.20  /PRTKfN -       302
GET     205.185.113.20  /files/911.dll  -       200
POST    softwareserviceupdater5.com     /web/post.php   -       200
POST    softwareserviceupdater5.com     /web/post.php   -       200
POST    softwareserviceupdater5.com     /web/post.php   -       200
POST    softwareserviceupdater5.com     /web/post.php   -       200
POST    softwareserviceupdater5.com     /web/post.php   -       200
POST    softwareserviceupdater5.com     /web/post.php   -       200
POST    softwareserviceupdater5.com     /web/post.php   -       200
POST    softwareserviceupdater5.com     /web/post.php   -       200
POST    softwareserviceupdater5.com     /web/post.php   -       200
POST    softwareserviceupdater5.com     /web/post.php   -       200
POST    softwareserviceupdater5.com     /web/post.php   -       200
POST    softwareserviceupdater5.com     /web/post.php   -       200
POST    softwareserviceupdater5.com     /web/post.php   -       200
POST    softwareserviceupdater5.com     /web/post.php   -       200
POST    softwareserviceupdater5.com     /web/post.php   -       200
POST    softwareserviceupdater5.com     /web/post.php   -       200
```

Lab 0101 – Parsing Zeek Logs

Lab 0110 –Zeek Package Manager

https://packages.zeek.org/

CHECKPOINT

Zeek Scripting

- Zeek has its own scripting language that allows analysts to write custom logging and alerting scripts
- Common networking data points are types in Zeek:
  - addr (IP address: v4, v6)
  - port (layer-4 port: 22/tcp, 53/udp)
  - subnet (CIDR subnet mask: 10.0.0.0/8)
- Zeek's "Built-In Functions" are commonly referred to as BIFs

Zeek Scripting

- &priority<x> (for event hooking)
- REDEF (redefing variables on the fly)
- If the -b is not used at run time, zeek will load all scripts/plugins from: /usr/local/zeek/share/zeek/base/
- dump-events.bro
  - <zeek>/share/bro/policy/misc/dump-events.bro
  - Essential for writing custom scripts and knowing exactly what Bro knows/sees

```
##! This script dumps the events that Zeek raises out to standard output in a
##! readable form. This is for debugging only and allows to understand events and
##! their parameters as Zeek processes input. Note that it will show only events
##! for which a handler is defined.
```

Tale of Two Zeek Scripts

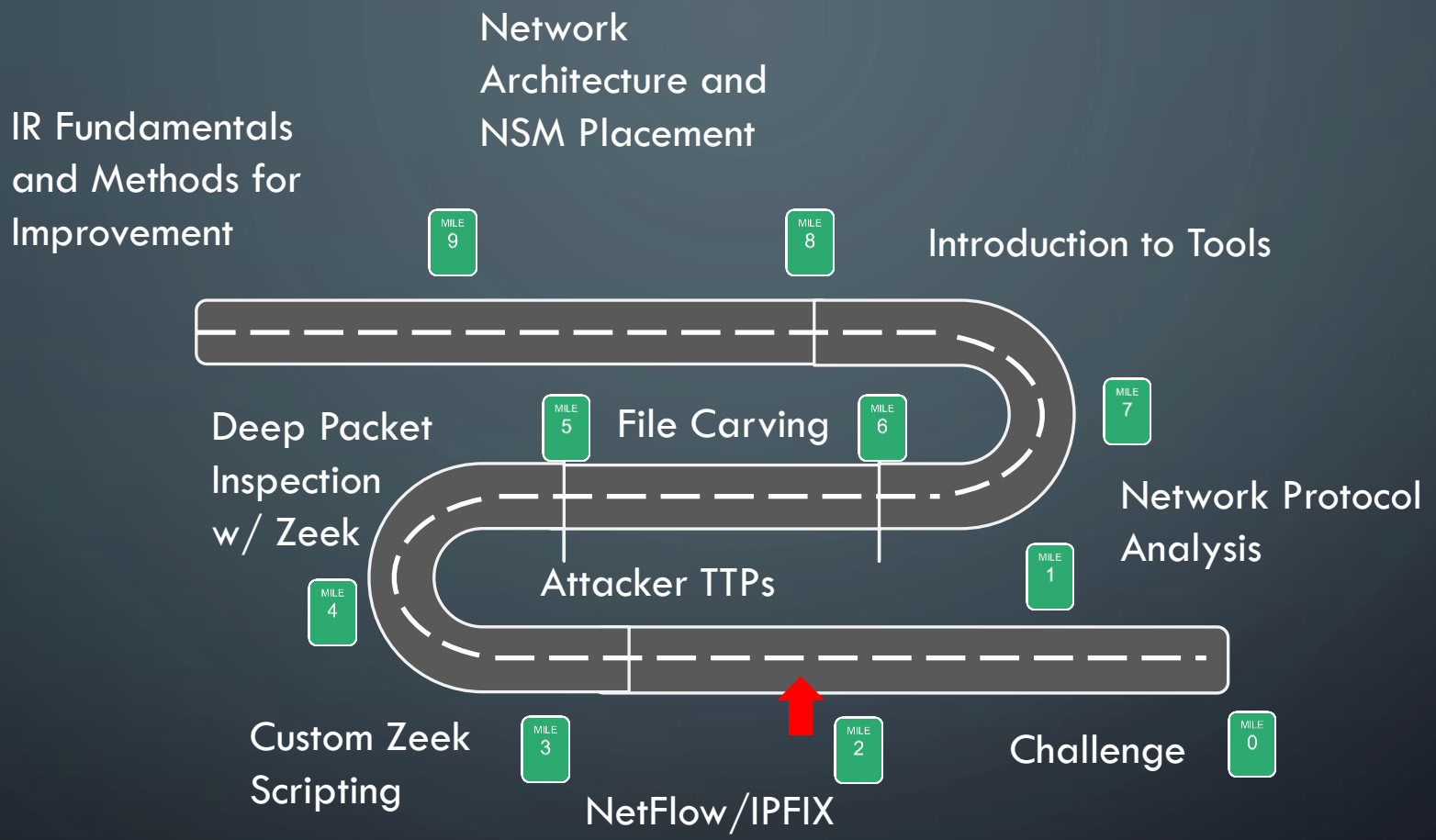
- Live
- Against saved pcaps

Lab 0111 – cAse mATteRs

Lab 1000 – Going Postal

CHECKPOINT

Roadmap



End Day 3

END OF DAY 3