Case Title

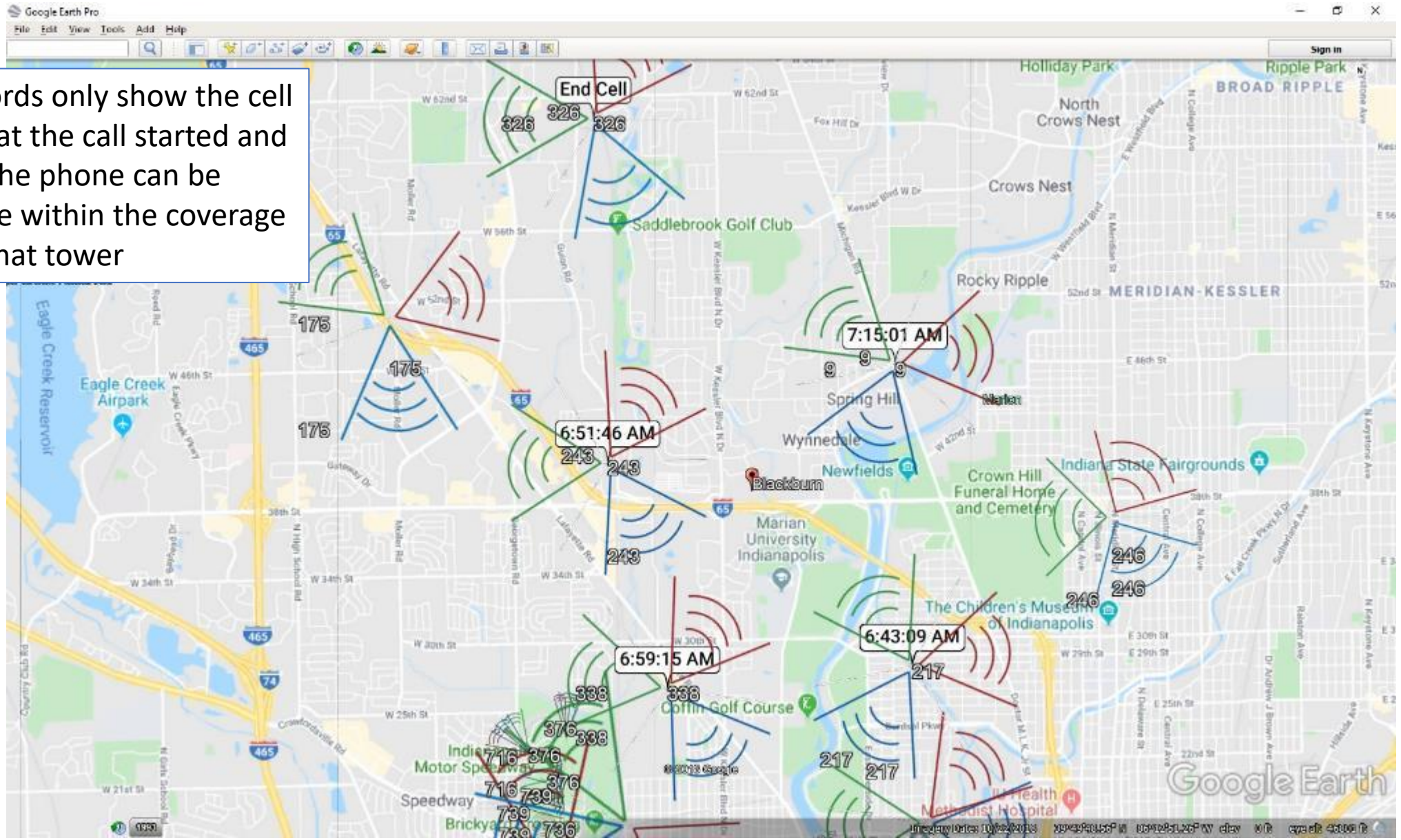
Richard Miletic – Forensic Analyst

Verizon Records

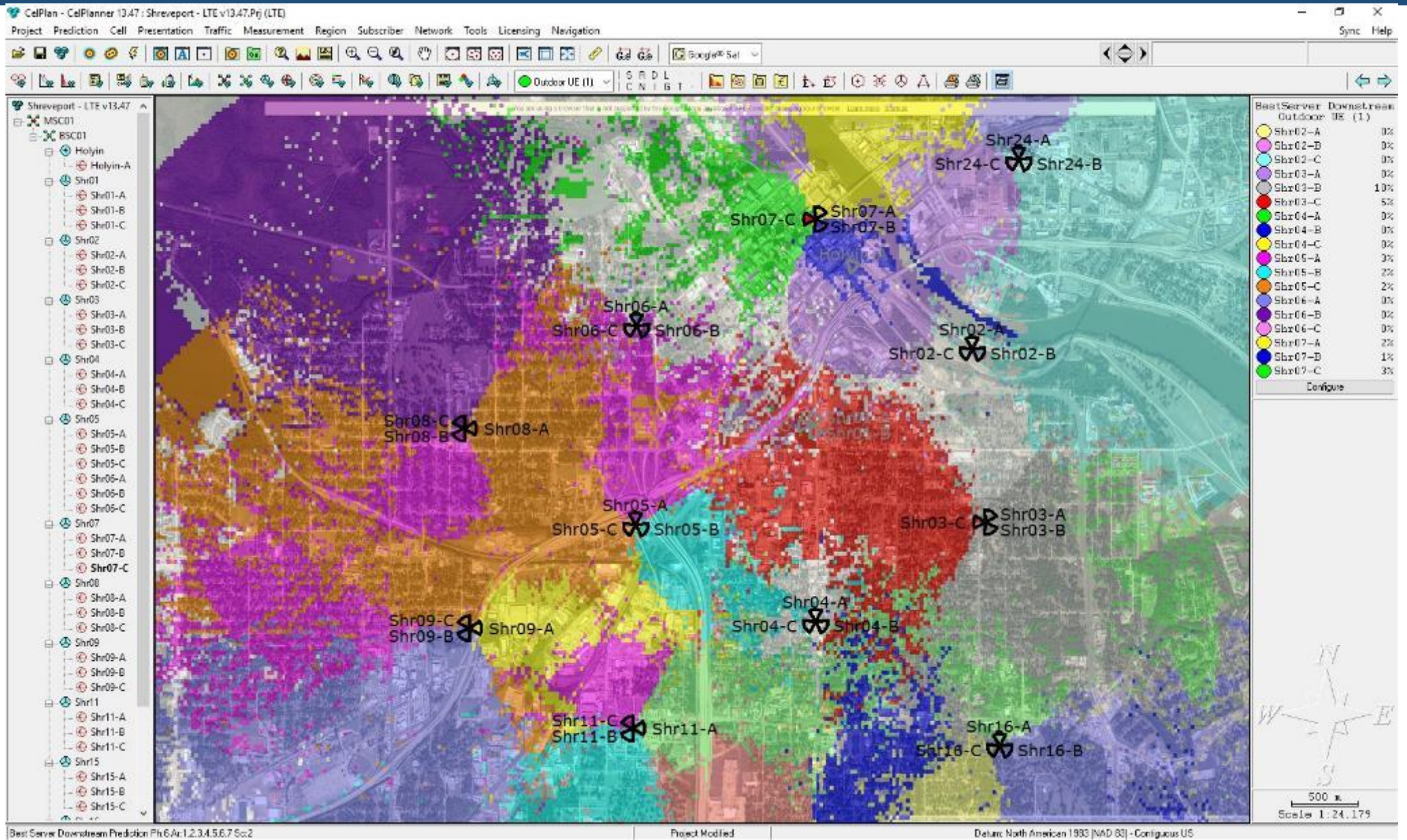
- Call Detail Record (CDR)
  - Each record indicates a phone call, SMS or Data Session
  - Includes cell site location of first and last cell site handling the call
- Range To Tower (RTT)
  - Estimates location of cell phone within a stated confidence (L, M, H)
  - Phone number, connection date and time, call length, etc.
- Cell Tower Data
  - Location of tower in latitude/longitude coordinates and address
  - Azimuth (direction) cell site antenna is pointing and beam width (angle at which the antenna transmits signal)
  - Maximum antenna range (max distance the cell site transmits signal)

CDR – All calls 5:30am to 7:30am

CDR records only show the cell tower that the call started and ended. The phone can be anywhere within the coverage area of that tower



Typical Cell Tower Coverage Map



Factors affecting Tower coverage

- *To assume every cell tower has a circular or triangular range of a stated number of miles is not reality and indicates a lack of knowledge on how a cellular system operates*

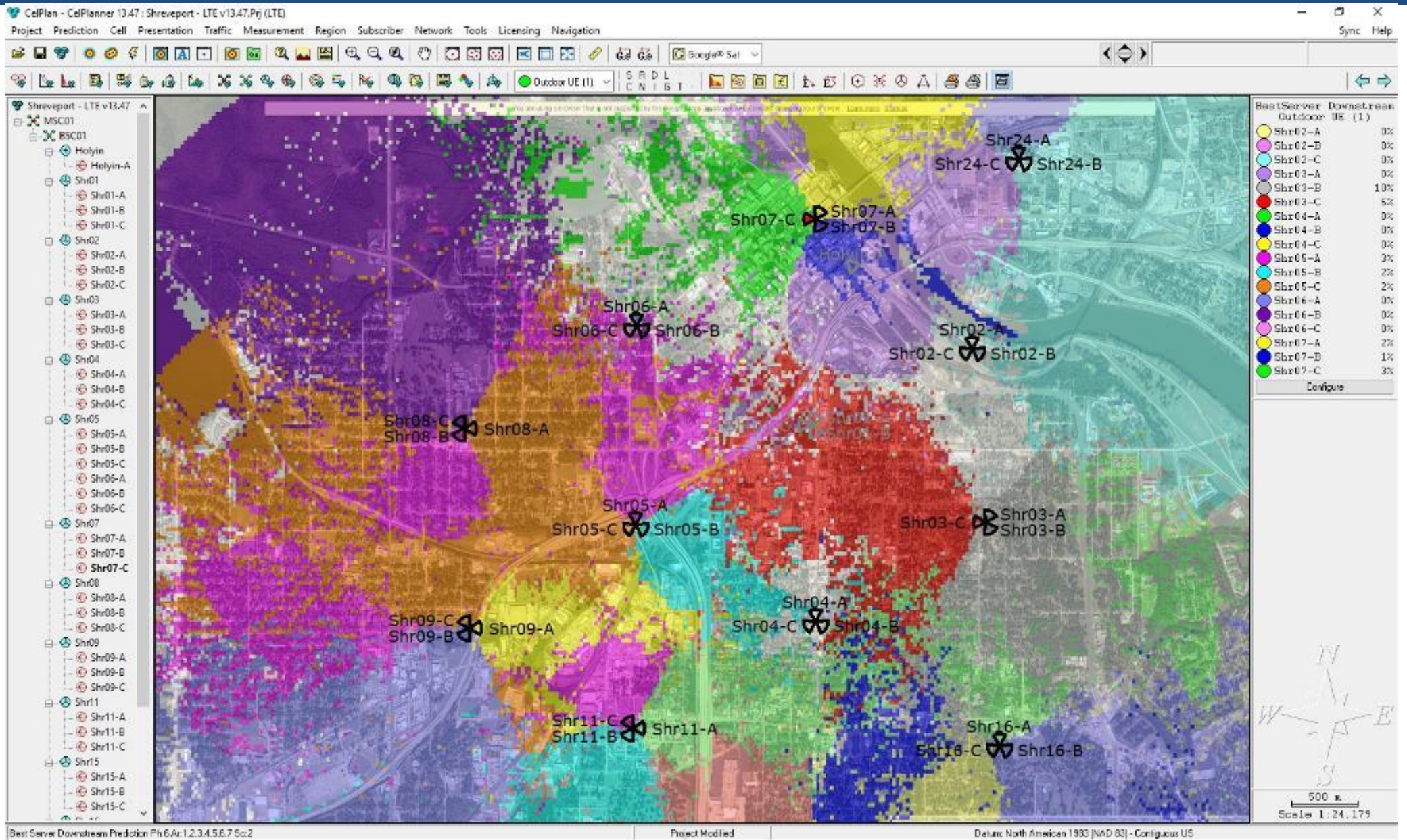
Factors affecting Tower coverage

- Antenna/Tower height
  - Higher the antenna, further the signal, larger the cell coverage
- Transmit power (output power at the antenna)
  - Higher power , further the signal, larger the cell coverage
- Antenna down tilt (angle of antenna pointing down from horizontal)
  - Greater the downward angle , smaller the cell coverage
- Terrain (hills, mountains, valleys, etc.)
  - Terrain obstructs and guides the signal along various paths
- Clutter (trees, grasses, foliage, buildings, etc.)
  - Clutter obstructs and guides the signal along various paths

Factors affecting Tower coverage

- Traffic patterns (busy times usually decrease the coverage)
  - During peak usage times such as rush hour or emergency events the cell site becomes full or close to full capacity
  - Additional phones attempting to use the closest cell may get redirected to an alternate cell
- Interference (signals from other cell sites, external transmissions or generated from poor cell site cable connections)
  - Interfering signals affect cell coverage by adding noise thus reducing the coverag area for establishing a good quality call
- Multipath interference (signals bouncing off of buildings, trees, people, vehicles, etc.)
  - Radio waves transmit in a wide pattern and bounce off objects in the environment affecting cell coverage

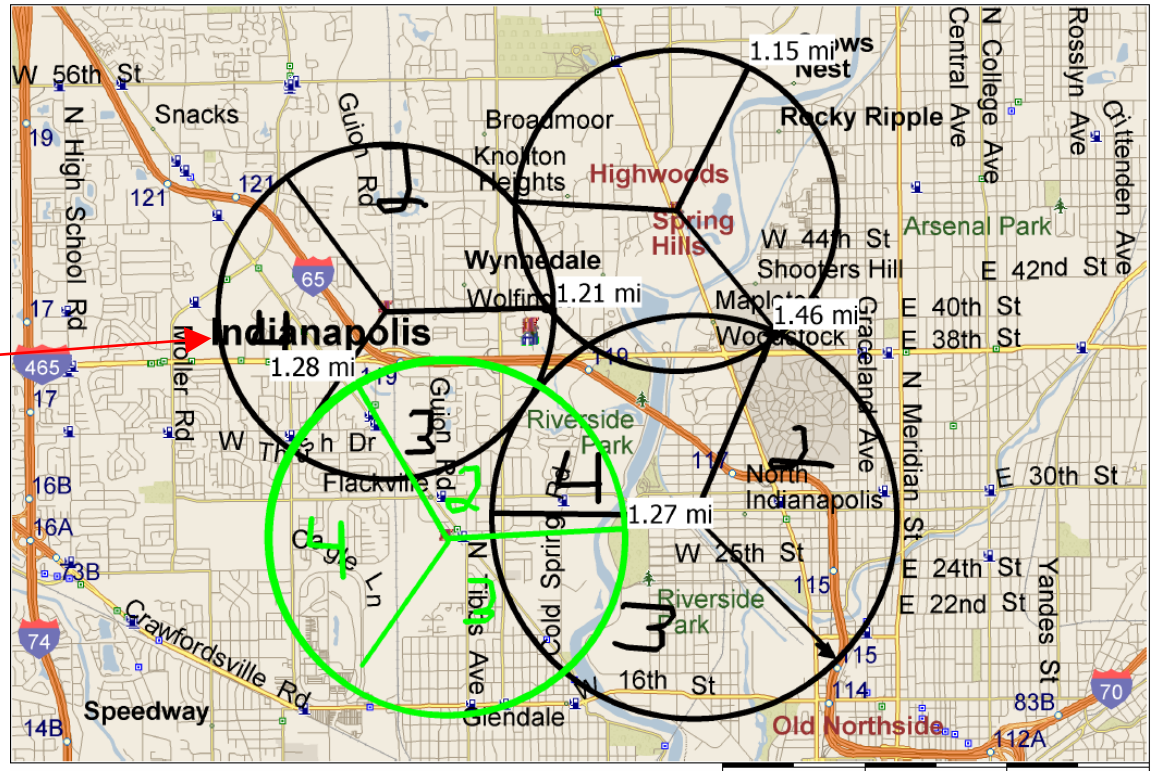
Typical Cell Tower Coverage Map



Factors affecting Tower coverage

- The factors affecting coverage are not provided in CDR, RTT or Tower records therefore it is impossible to determine the coverage area of the tower
- One can not simply guess at the coverage area and draw arbitrary circles to show cell tower coverage

Incorrect to draw arbitrary circle for coverage



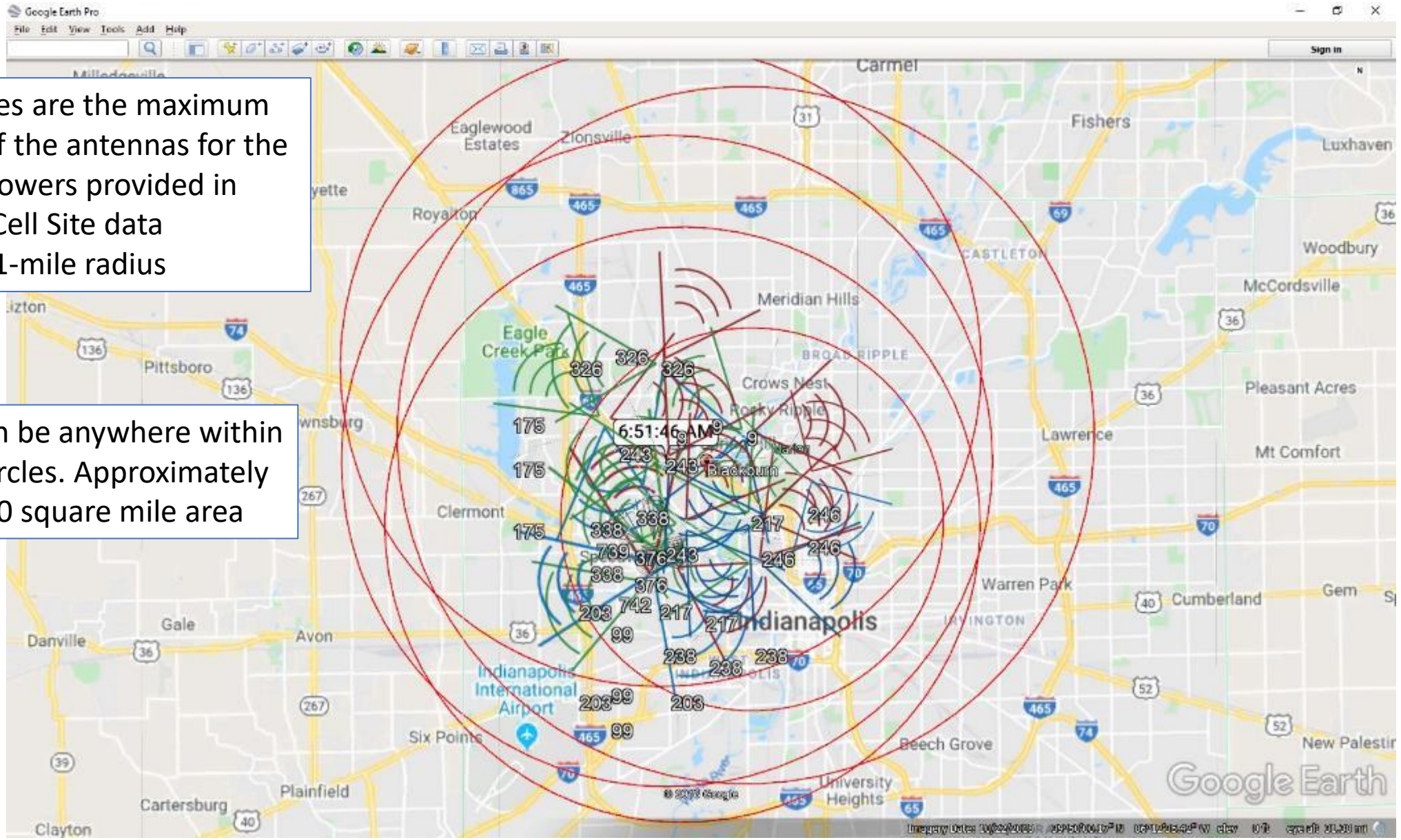
United States vs Evans Case No. 10 CR 747-3

- Court struck down “granulization theory” to determine cell site coverage. The theory assumes the phone is served by the nearest tower and estimates coverage of the tower based on “training and experience”.
- This is not the case as the nearest tower may not have the best signal or may be unable to serve the phone due to capacity constraints (i.e. can’t handle any more calls)
- Therefore without additional technical information about the network at the time of the event it is impossible to determine the actual coverage of the tower.
- Training and experience was not allowed by the court to solely determine coverage
- Coverage must be determined by scientific calculations
- Prosecution determination of cell site coverage or “granulization theory” denied

Verizon Tower Records – Max Antenna Ranges per Tower

Red circles are the maximum ranges of the antennas for the serving towers provided in Verizon Cell Site data
7.8 to 9.1-mile radius

Phone can be anywhere within the red circles. Approximately 190 to 260 square mile area



Additional Resources on Cell Coverage

- See Aaron Blank, The Limitations and Admissibility of Using Historical Cellular Site Data to Track the Location of a Cellular Phone, 18 RICH. J. L. & TECH. 3, at *7 (Fall 2011) (identifying factors that affect a tower's signal strength to include the technical characteristics of the tower, antennas and phone, environmental and geographical features and indoor or outdoor usage) Download Paper
- Matthew Tart et al., Historic cell site analysis – Overview of principles and survey methodologies, 8 DIGITAL INVESTIGATION 1, 186 (2012) ("In a perfectly flat world with equally spaced and identical masts, a mobile phone user would generally connect to the closest mast. In the real world, however, this is not necessarily the case."). Download Paper
- Richard Miletic, Determining RF Coverage in Criminal Defense Cases, published in National Association of Defense Lawyers (NACDL) publication *The Champion,* Iowa State Bar publication *The Iowa Lawyer* and the North Dakota Bar publication *The Gavel* Download Article

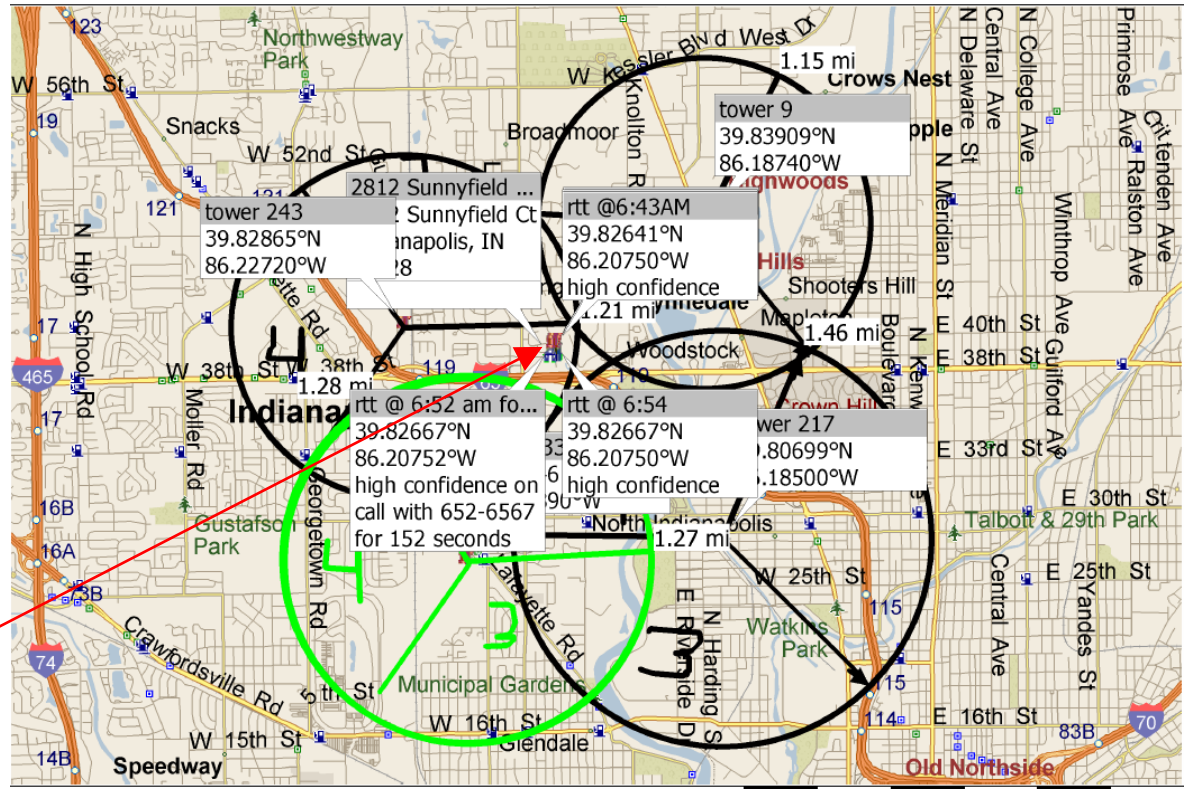
Verizon RTT Record disclaimer

"The latitude and longitude measurements on the [RTT] report are derived solely from the Round-Trip Delay measurement. They are best estimates and are not related to any GPS measurement. Measurements with a high confidence factor may be more accurate than measurements with a low confidence factor, but all measurements contained on this report are the best estimates available rather than precise location."

- No scientific formula is provided for the measurement.
- Confidence factors provided are H, M and L. There are no statistical percentage intervals provided. (e.g. Does H mean 90% confident or 50% confident?)
- There is no way to verify or test the accuracy of the location estimate
- We are supposed to accept Verizon's claim without any additional data to confirm the methodology

Range to Tower Display of Location

- Prosecution incorrectly interprets and displays the Verizon RTT data
- No link between the underlying data and the expert's display of the data
- No values for "Confidence rating" of the location estimate therefore the location could be anywhere within the cell tower coverage area



Incorrect to display location as a single point
Verizon RTT data provides a location along with a confidence rating and a disclaimer stating
"…best estimates available rather than precise location."

Range to tower calculation

- Verizon does not provide algorithm
- We can try to assume the RTT calculation of distance traveled of a radio wave based on time by the accepted formula below

$D=(T*c)/2$

D=distance traveled

T=Time radio signal travels

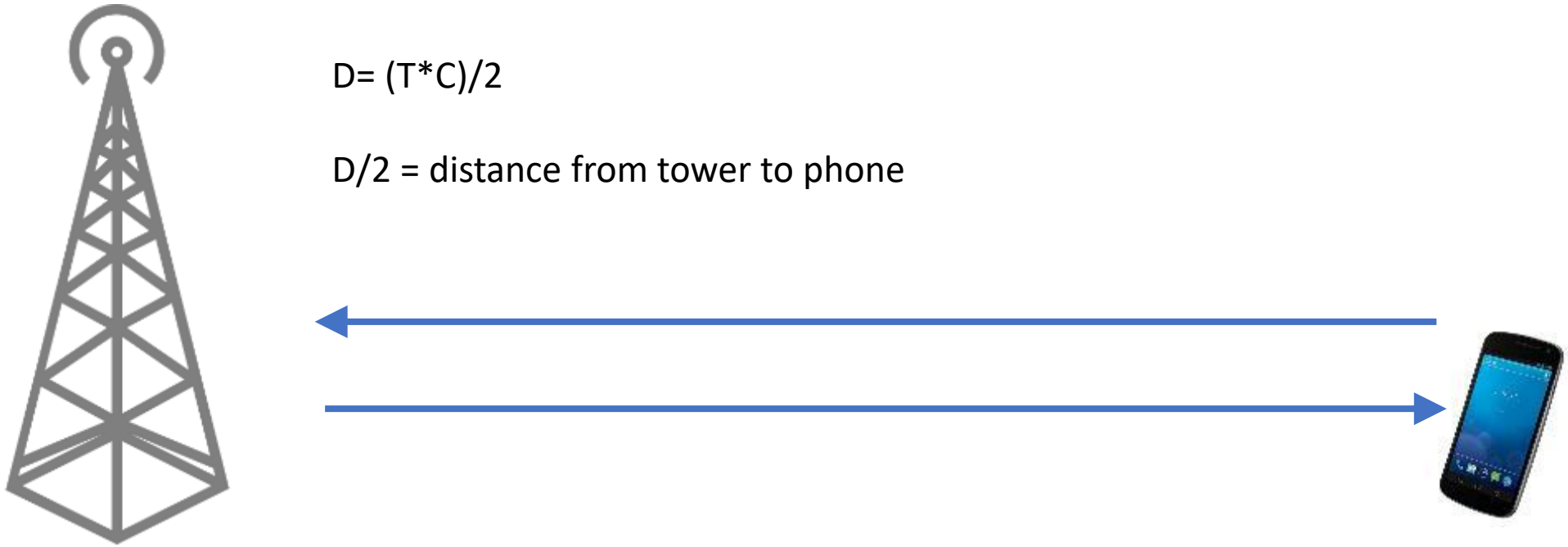
c=speed of light

Range to tower (RTT) calculation theory

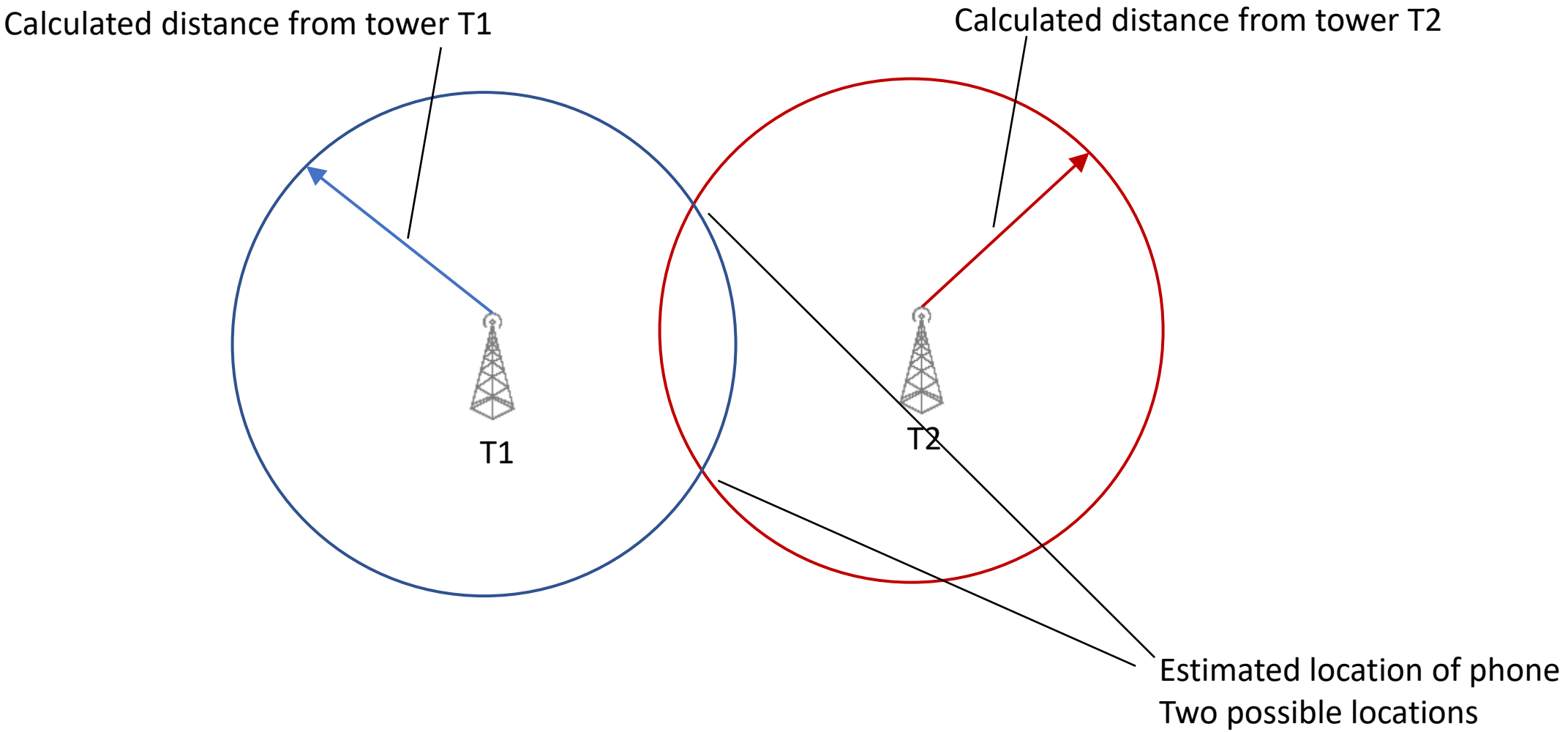
T=time from tower to phone and back to tower
D=distance from tower to phone and back to tower
C=speed of light

D= (T*C)/2

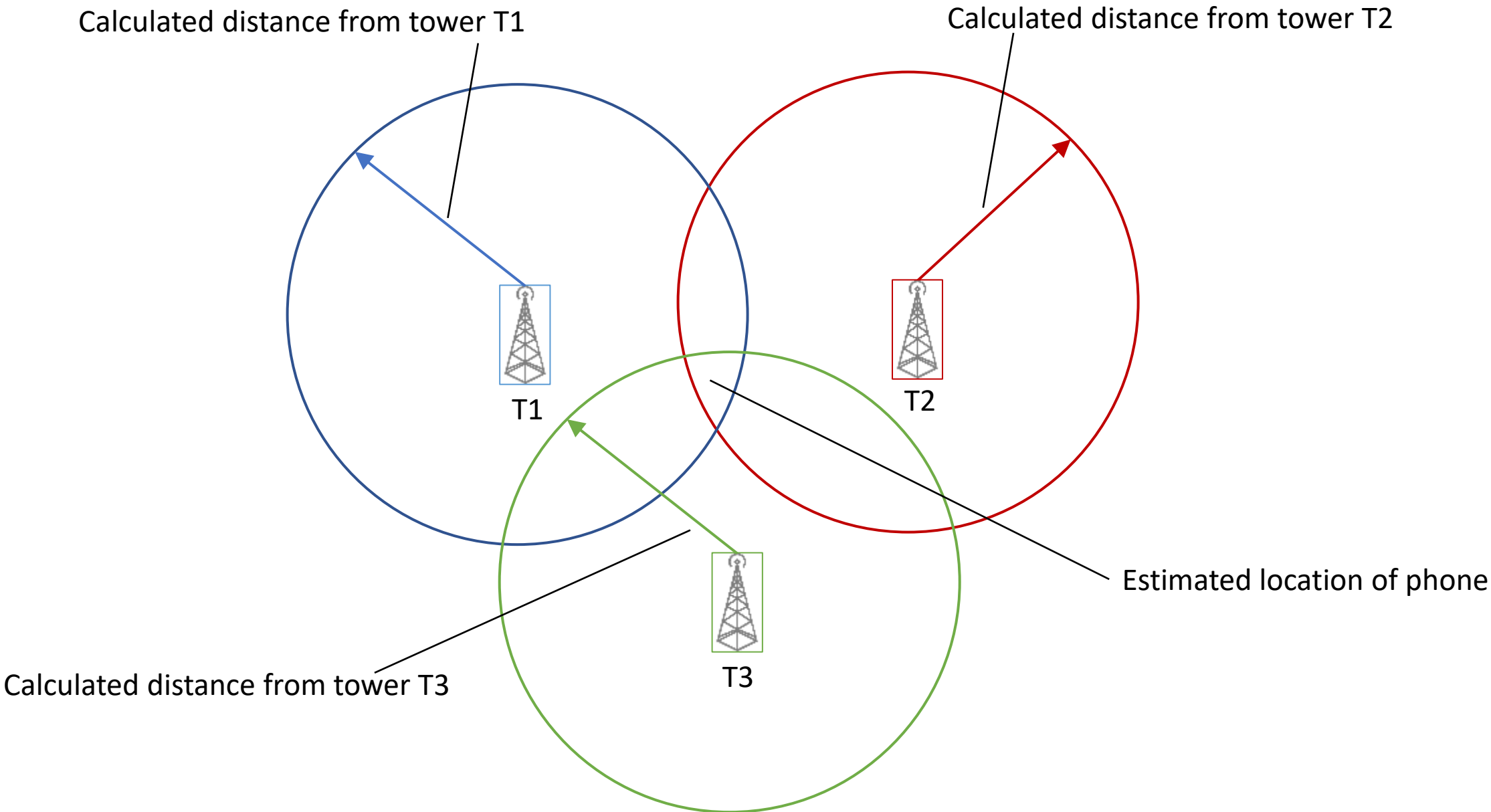
D/2 = distance from tower to phone



Range to tower (RTT) calculation theory



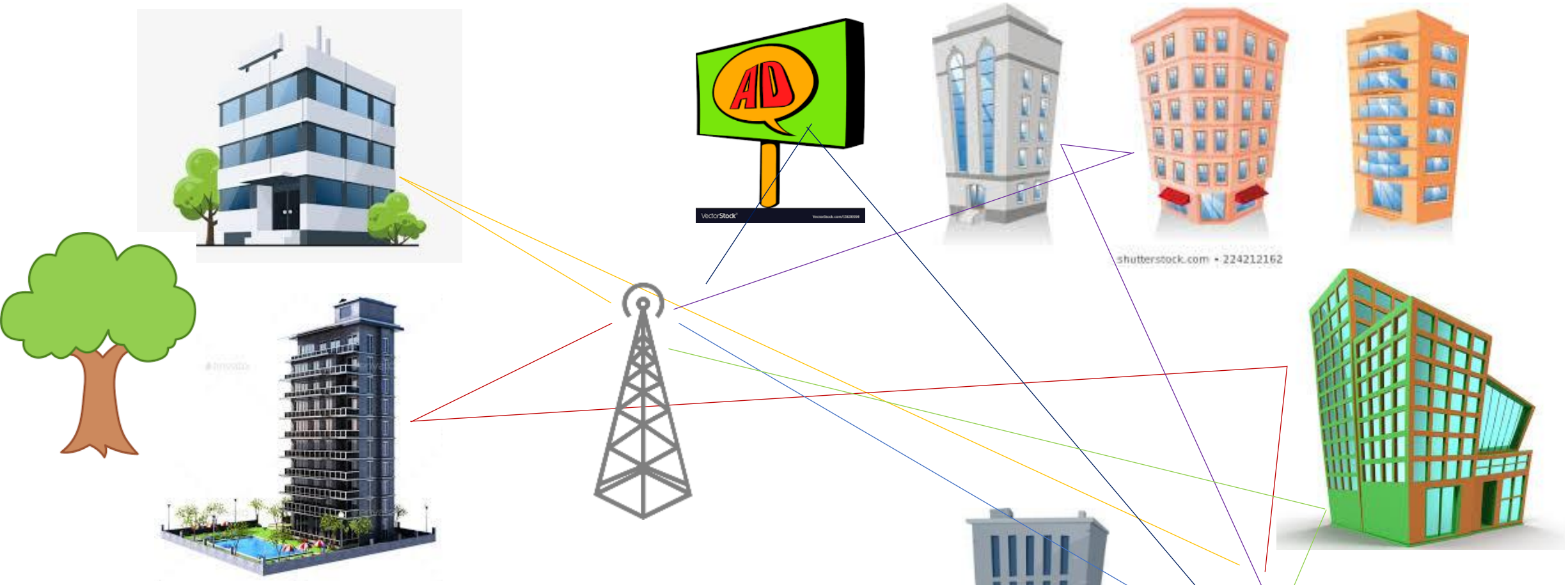
Range to tower (RTT) calculation theory



Range to tower (RTT) calculation theory

- Problem comes in the real-world application
  - Radio waves travel in multiple directions from a single point (Multipath)
  - Radio waves bounce off objects
  - Each path of the radio wave takes a different length of time to get to and from the phone

Range to tower (RTT) calculation Problem



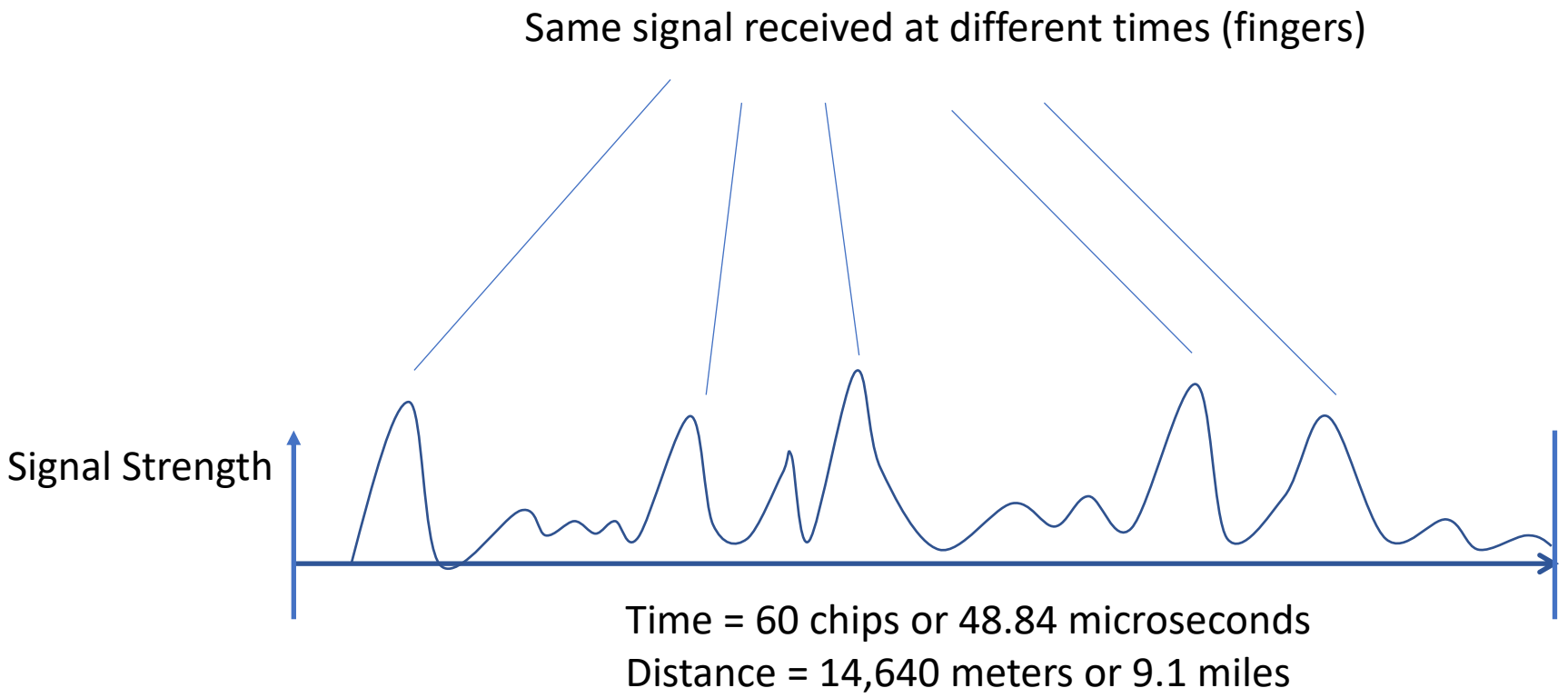
Radio waves takes infinite number of paths
Each taking a different amount of time to reach the phone

Which path do you pick to calculate the distance?

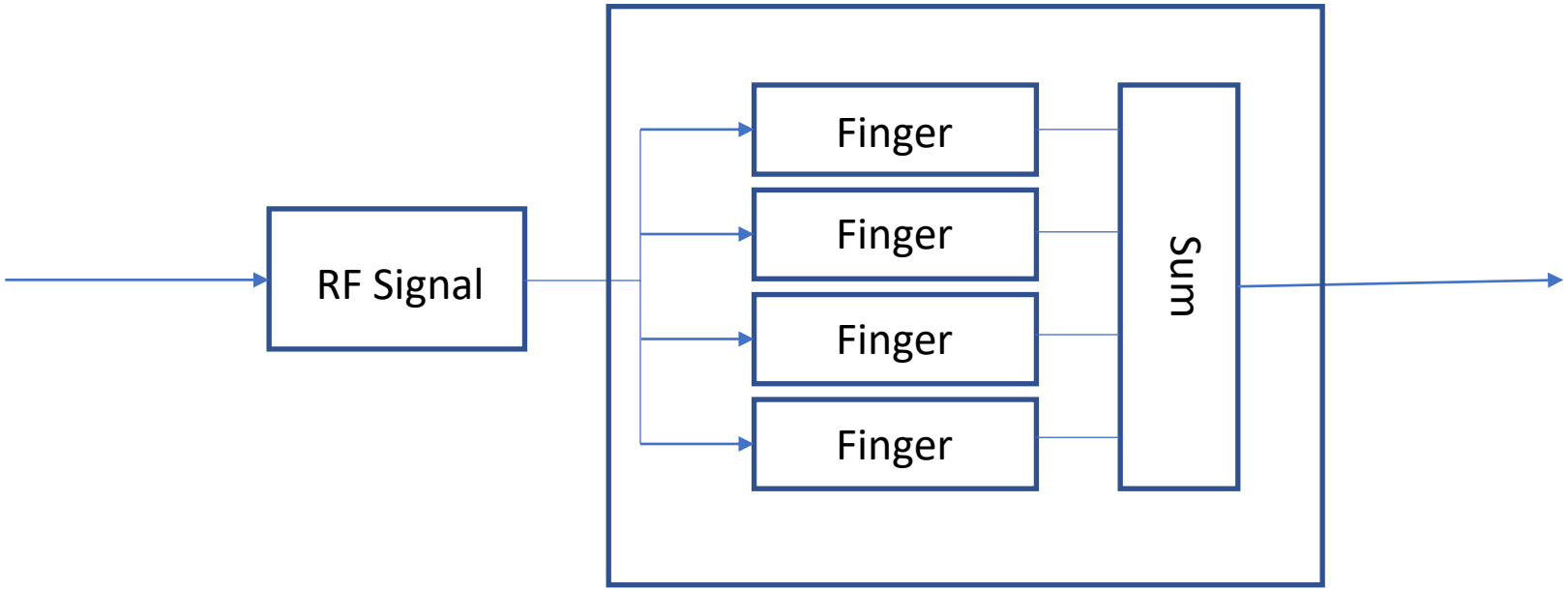
Range to tower (RTT) calculation problem

- Radio waves bounce off objects
- Each path of the radio wave takes a different length of time to get to and from the phone
- Indirect path takes longer time to reach the phone thus the distance estimate is further away than actual
- The direct path provides the best estimate of distance
- What if there is no direct path? Then the distance estimate will be incorrect
- There is no way to determine if the paths of the radio waves used by Verizon were the direct paths or indirect paths thus there is no way to determine the location of the phone

Incoming Multipath Signals



Multipath signals combined by Rake Receiver



CDMA Chip Time – Search Window

- Time of one CDMA chip is 814 ns. Multiply by the speed of light to obtain distance one chip travels equals 244 meters
- Rake receiver in CDMA combines multipath signals over many chips. This is called the search window.
- The search window size is set by the cellular engineer. Typical size for urban environment is 60 chips or 9.1 miles. The rake receiver can combine signals up to 9.1 miles apart.

Time of Arrival (TOA) Accuracy Error Factors

- Search window size – 60 chip window = 9.1 miles
- Multipath – Time delays in receiving of signals
- Interference – Low signal to noise or Ec/Io values
- GPS Time Jitter – Slight differences in GPS timing due to electrical or environmental noise
- Island Cell – Loss of GPS time by a cell
- Cell phone – Loss of GPS signal by the phone

Bottom Line

- There are well documented errors associated with estimating distance to cell using TOA
- Errors are based on several factors
- While we know Verizon uses TOA technology, we do not know the details of how it is implemented and the underlying algorithms
- We can not test the accuracy of Verizon TOA
- It is misleading to draw a point or a line for location or distance

RTT Data Record Challenge: Does not pass Rule 702

- A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if:
  - (a) the expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;
  - (b) the testimony is based on sufficient facts or data;
  - (c) the testimony is the product of reliable principles and methods; and
  - (d) the expert has reliably applied the principles and methods to the facts of the case.

Does not pass Rule 702

- (a) the expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;
  - Prosecution expert is not a cellular network engineer or Radio Engineer. His training is with respect to general cellular principles and interpreting cell phone records. Therefore he should not display RTT data since he has no understanding of how this data was generated. At a minimum he should not display the location information since these data are calculated from unknown and untested algorithms with unknown error or confidence factors.

- (b) the testimony is based on sufficient facts or data;
  - This is not true for RTT data. Verizon uses proprietary algorithms to determine location coordinates. These algorithms can not be tested. The confidence factor H, M and L are not associated with any numerical number. For example, H could mean 90% confidence or 75% or some other number.

Does not pass Rule 702

- (c) the testimony is the product of reliable principles and methods;
  - Reliability of RTT data has not been empirically tested. RTT data does not rely on GPS and is not a replacement for GPS. RTT data is not intended for the purpose of location, it is intended for the purpose of improving network quality. Verizon issues a disclaimer saying RTT measurements are “best estimates”. It is misleading to a jury as they may believe RTT location and GPS location are the same when in fact they are vastly different.

- (d) the expert has reliably applied the principles and methods to the facts of the case.
  - Since the algorithm to determine the location is unknown and untested and the confidence factor is arbitrary, presenting the location data as a single point is misleading and not representative of the underlying science. This is unfairly prejudicial to the defendant.

U.S. v. Mamah, 332 F.3d 475 (7th Cir. 2003)

It is critical under Rule 702 that there be a link between the facts or data the expert has worked with and the conclusion the expert's testimony is intended to support. *See Gen. Elec.*, 522 U.S. at 146, 118 S.Ct. 512 ("A court may conclude that there is simply too great an analytical gap between the data and the opinion proffered."). The court is not obligated to admit testimony just because it is given by an expert.

- In our case the prosecution expert concludes that the location provided by the Verizon RTT data was in fact the actual location of the phone without knowing how the location was calculated.
- There is no data provided by Verizon that shows their calculations for determining the location provided in the RTT record.
- Further, Verizon provides a single point location estimate with an arbitrary confidence rating which indicates the phone may not have been at that location, yet the expert represents the phone as being at that exact location
- The RTT data should not be admitted as there is no link between the underlying data and the expert’s presentation of the data

iPhone Extraction – Location Points

- Five points extracted from the iPhone that were located in Lake XXX all have the exact same latitude longitude value. The first point was at 4:23pm and the next one was at 11:27. It would be highly unlikely he would go back to the exact same spot within 1.11 meters so we can assume these points are in error. The interesting part is that the Lake XXX points had a 70 for the confidence factor which is the same as most of the other points he refers to as coming from the iPhone apps. Based on this we have a valid argument to exclude the locations determined from the iPhone as invalid.
- Further, the last point in Lake XXX was at 11:40:40 PM and one of the RTT files has him back on shore one mile west of there at 11:41:31 PM less than one minute later. That would be physically impossible.
- Based on this evidence at a minimum all the points from the iPhone extraction that have a confidence factor of 70 or above should be excluded.

iPhone Extraction – Location Points

- Page XX the prosecution expert says the iPhone obtains its location from GPS, WiFi or triangulation.
  - This is not technically correct. The phone determines its location either through GPS, or if it cannot obtain a GPS fix, it drops down to a coarse estimate based on the cell to which it is connected. Visually it typically looks like a large shaded circle on the mapping program on the cell phone. Wi-Fi hotspots are used to enhance location. The phone scans nearby hotspots and connects to a database to see if there is a match. The database may have the location of that hotspot which it sends to the phone so the phone knows it is within some general area of that hotspot.
  - The phone does not do any triangulation. This can only be done from the network side as triangulation requires at least the separate points from which to measure the time signal from the phone.
  - Since the apps on the phone do not provide how the location was determined then it is possible the phone did not have a GPS fix and had to use the crude method of location meaning somewhere within the coverage area of the connected cell tower.
  - Representing the iPhone location points as exact locations is misleading and not representative of the actual data. The error factors provided in the extraction report do not indicate a percentage, they just state a number like 0, 70 or 90. There is no indication these have any meaning whatsoever.

Prosecution Expert Testimony – Miscellaneous notes

- Page XX – Draws a one-mile radius for cell coverage because it's "easier to read"
- Page XX – Says RTT data is "accurate to within half a mile". How does he know this?
- Pages XX – Prosecution expert says it is impossible for the caller to be at Xth and XX or Yth and YY because it is in the opposite direction the antenna is pointing. However, in reality, it is quite possible as the signal can reflect off buildings and other objects. Antennas also have a "back lobe" which means there is some signal that gets transmitted in the opposite direction of the main lobe of the antenna.
- I could not find points on exhibits x, y, and z in any of the data files. It may not matter if we are able to exclude the data all together, but we may question this at some point.

Conclusion

- According to United States vs Evans Case No. 10 CR 747-3 coverage of a cell can not be determined by “experience and training” No scientific data was provided to determine cell coverage. Maps of cell coverage should be excluded.
- Verizon RTT data does not provide any scientific data or calculations to determine location of the phone. They do not provide any detailed data on the meaning of H, M and L confidence ratings. Since no scientific methodology is presented then this does not pass the Daubert test and thus RTT data should be excluded.
- According to *U.S. v. Mamah*, 332 F.3d 475 (7th Cir. 2003) there needs to “be a link between the facts or data the expert has worked with and the conclusion the expert's testimony is intended to support.” ("A court may conclude that there is simply too great an analytical gap between the data and the opinion proffered."). There is no underlying data provided that shows how the location was determined therefore there is no link between the data and the expert’s conclusion Further. The expert shows a point location of the phone but Verizon indicates this is an estimate with some arbitrary confidence factor. Since there is no link between the data and the expert’s conclusion the RTT data and the expert’s maps of the data should be excluded
- iPhone location data is not accurate as shown by the Lake XX example. It does not identify how the location was determined. It shows only a number for a confidence with no units of measure and thus no meaning. These measurements were presented as points on the map which were misleading and prejudicial.